"Tenge Bank" ATB AXBOROT XAVFSIZLIGI SIYOSATI

1-bob. Kirish

1. Ushbu "Tenge Bank" ATBning axborot xavfsizligi siyosati (bundan keyin Siyosat deb yuritiladi) axborot xavfsizligini ta’minlashning maqsad va tamoyillarini belgilaydi, axborotni himoya qilishning asosiy yo‘nalishlari va talablarini bayon etadi, axborot xavfsizligi rejimini ta’minlash uchun asos bo‘lib xizmat qiladi hamda "Tenge Bank" ATB (bundan keyin Bank deb yuritiladi)ning tegishli ichki hujjatlarini ishlab chiqishda qo‘llanma vazifasini bajaradi.
2. Siyosatning normativ-huquqiy asosini O‘zbekiston Respublikasining axborot tizimlaridan foydalanish va axborot xavfsizligi masalalariga oid qonun hujjatlari, shuningdek, axborot xavfsizligini boshqarishning xalqaro standartlari talablari tashkil etadi.
3. Siyosat qoidalariga Bankning barcha xodimlari rioya qilishlari shart, shuningdek, ular Bankning axborot tizimlari va hujjatlariga kirish huquqiga ega bo‘lgan mijozlar va boshqa uchinchi shaxslarga, Bank va ularning faoliyati bilan bevosita bog‘liq qismida ma’lum qilinishi lozim.
4. Siyosat Bank egasi va foydalanuvchisi bo‘lgan barcha axborot tizimlari va hujjatlarini qamrab oladi. Bank axborot xavfsizligini ta’minlash jarayonini boshqarish uchun mo‘ljallangan umumiy boshqaruv tizimining bir qismi sifatida axborot xavfsizligini boshqarish tizimining yaratilishi va ishlashini ta’minlaydi. Axborot xavfsizligini ta’minlash Bankning tijorat faoliyatini muvaffaqiyatli amalga oshirish shartlaridan biridir. Bankda aylanayotgan axborot bankning eng muhim aktivlaridan biri hisoblanadi.
5. Bankning axborot xavfsizligi (keyingi o‘rinlarda - AX) - elektron axborot resurslari, axborot tizimlari va axborot-kommunikatsiya infratuzilmasining Bank, uning aksiyadorlari, xodimlari yoki mijozlariga moddiy zarar yetkazishi, obro‘siga putur yetkazishi yoki boshqa zarar yetkazishi mumkin bo‘lgan tashqi va ichki tahdidlardan himoyalanganlik holatidir.
6. AX Bank rahbariyatining umumiy siyosatining bir qismi sifatida biznes talablariga asoslanadi, Bankdagi xatarlarni boshqarishning umumiy qoidalariga muvofiq ishlab chiqiladi va amalga oshiriladi. Bu sohadagi qoidabuzarliklar jiddiy oqibatlarga, jumladan, mijozlar ishonchini yo‘qotish va raqobatbardoshlikning pasayishiga olib kelishi mumkin.
7. Axborot xavfsizligini ta’minlash barcha mavjud vositalarni qo‘llashni o‘z ichiga oladi va Bank xodimlarining vakolatlari doirasida axborot va uni qo‘llab-quvvatlovchi infratuzilmani himoya qilishga qaratilgan vositalarni qamrab oladi.

8. Axborot xavfsizligini tashkil etishning ajralmas qismi ko‘rilayotgan chora-tadbirlar samaradorligini uzluksiz nazorat qilish hisoblanadi, xodimlar uchun yo‘l qo‘yilmaydigan harakatlar (harakatsizlik) ro‘yxatini, ularning mumkin bo‘lgan oqibatlari va javobgarligini belgilash.Ushbu Siyosat O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi bilan kelishilgan (2021-yil 1-fevraldagi 01-19-01/191-son xat)

2-bob. Normativ havolalar

Axborot xavfsizligi siyosati va tizimi umuman quyidagi me’yoriy-huquqiy hujjatlar va xalqaro standartlarga asoslanadi (ushbu bo‘limda Bankning axborot xavfsizligi tizimini yaratish jarayoniga bevosita ta’sir ko‘rsatadigan asosiy me’yoriy hujjatlar ko‘rsatilgan. Shu bilan birga, davlat darajasida axborot xavfsizligini rivojlantirishning strategik jihatlarini tavsiflovchi yoki faoliyatning alohida yo‘nalishlarini axborot jihatidan himoya qilish qoidalarini tartibga soluvchi bir qator hujjatlar ham mavjud):

- O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-sonli Qonuni "Axborotlashtirish to‘g‘risida";
- O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi 562-II-sonli Qonuni "Elektron raqamli imzo to‘g‘risida";
- O‘zbekiston Respublikasining 2004-yil 29-apreldagi 611-II-sonli Qonuni "Elektron hujjat aylanishi to‘g‘risida";
- O‘zbekiston Respublikasining 2003-yil 30-avgustdagi 530-II-sonli Qonuni "Bank siri to‘g‘risida";
- O‘zbekiston Respublikasining 2006-yil 4-apreldagi O‘RQ-30-sonli Qonuni "Avtomatlashtirilgan bank tizimida axborotni himoya qilish to‘g‘risida"gi
- O‘zbekiston Respublikasining 2014-yil 11-sentyabrdagi 374-sonli Qonuni; "Tijorat siri to‘g‘risida"gi Qonun;
- O‘zbekiston Respublikasining 2019-yil 2-iyuldagi "Shaxsga doir ma’lumotlar to‘g‘risida"gi O‘RQ-547-sonli
- Qonuni; O‘zbekiston Respublikasi Prezidentining 2007-yil 3-apreldagi PQ-614-sonli Qarori; "O‘zbekiston Respublikasida axborotni kriptografik himoya qilishni tashkil etish chora-tadbirlari to‘g‘risida"gi
- O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi PQ-1572-sonli Qarori; "Milliy axborot resurslarini himoya qilish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida"gi Qaror;
- O‘zbekiston Respublikasi Vazirlar Mahkamasining Qarori; "Axborotlashtirish sohasidagi normativ-huquqiy bazani takomillashtirish to‘g‘risida"gi 2005-yil 22-noyabrdagi 256-sonli Qaror;
- O‘zbekiston Respublikasi Vazirlar Mahkamasining 2011-yil 4-maydagi 126-sonli "Vazirlar Mahkamasining ijro etuvchi apparati, davlat va xo‘jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlarida yagona himoyalangan elektron pochta va elektron hujjat aylanish tizimini joriy etish hamda ulardan foydalanish chora-tadbirlari to‘g‘risida"gi Qarori;

- O‘zbekiston Respublikasi Vazirlar Mahkamasining Qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2013-yil 14-iyundagi 170-sonli "O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi PQ-1572-son "Milliy axborot resurslarini himoya qilish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida"gi Qarorini amalga oshirishga doir qo‘shimcha chora-tadbirlar to‘g‘risida"gi Qarori;

- O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktyabrdagi

O‘zbekiston Respublikasi axborotlashtirish obyektlarida maxfiy axborotning xavfsizligini tashkil etish va ta’minlash tartibi to‘g‘risidagi nizomni tasdiqlash haqida 295-son;

- O‘zbekiston Respublikasi Markaziy banki Boshqaruvining 2020-yil 25-yanvardagi 2/4-sonli qarori "O‘zbekiston Respublikasi tijorat banklarining avtomatlashtirilgan bank tizimlarida axborotni himoya qilish to‘g‘risidagi nizomni tasdiqlash haqida";
- O‘z DSt ISO/IEC 13335-1:2009 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot-kommunikatsiya texnologiyalari xavfsizligini boshqarish. (1-qism). Axborot-kommunikatsiya texnologiyalari xavfsizligini boshqarish tushunchalari va modellari;
- O‘z DSt ISO/IEC 15408-1:2016 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot texnologiyalari xavfsizligini baholash mezonlari. 1-qism. Kirish va umumiy model;
- O‘z DSt ISO/IEC 15408-2:2016 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot texnologiyalari xavfsizligini baholash mezonlari. 2-qism. Xavfsizlikning funksional komponentlari;
- O‘z DSt ISO/IEC 15408-3:2016 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot texnologiyalari xavfsizligini baholash mezonlari. 3-qism. Xavfsizlikka ishonch komponentlari;
- O‘z DSt ISO/IEC 27000:2014 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Sharh va lug‘at";
- O‘z DSt ISO/IEC 27001:2016 "Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Talablar";
- O‘z DSt ISO/IEC 27002:2016 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarishning amaliy qoidalari";
- O‘z DSt ISO/IEC 27003:2014 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimini joriy etish bo‘yicha qo‘llanma";
- O‘z DSt ISO/IEC 27005:2013 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi xatarlarini boshqarish";
- O‘z DSt 3388:2019 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlarining auditi va sertifikatsiyasini amalga oshiruvchi organlarga qo‘yiladigan talablar;

- O‘z DSt ISO/IEC 27007:2015 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlarini audit qilish bo‘yicha yo‘riqnoma;
- O‘z DSt ISO/IEC 27010:2015 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Sohalar va tashkilotlar o‘rtasidagi muloqotda axborot xavfsizligini boshqarish bo‘yicha qo‘llanma;
- O‘z DSt ISO/IEC 27011:2014 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Telekommunikatsiya tashkilotlarida axborot xavfsizligini boshqarish bo‘yicha yo‘riqnoma";
- O‘z DSt 3386:2019 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi hodisalarini boshqarish. 1-qism. Hodisalarni boshqarish tamoyillari;
- O‘z DSt 3387:2019 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi hodisalarini boshqarish. 2-qism. Hodisalarga javob berishni rejalashtirish va tayyorlash bo‘yicha yo‘riqnoma;
- O‘z DSt 2814:2014 "Axborot texnologiyasi. Avtomatlashtirilgan tizimlar. Axborotdan ruxsatsiz foydalanishdan himoyalanganlik darajasi bo‘yicha tasniflash";
- O‘z DSt 2815:2014 "Axborot texnologiyasi. Tarmoqlararo to‘siqlar. Axborotdan ruxsatsiz foydalanishdan himoyalanganlik darajasi bo‘yicha tasniflash";
- O‘z DSt 2816:2014 "Axborot texnologiyasi. Axborotni muhofaza qilish vositalarining dasturiy ta’minotini e’lon qilinmagan imkoniyatlar mavjud emasligini nazorat qilish darajasi bo‘yicha tasniflash";
- O‘z DSt 2817:2014 "Axborot texnologiyasi. Hisoblash texnikasi vositalari. Axborotdan ruxsatsiz foydalanishdan himoyalanganlik darajasi bo‘yicha tasniflash";
- O‘z DSt 2927:2015 "Axborot texnologiyasi. Axborot xavfsizligi. Atamalar va ta’riflar";
- O‘z DSt 1047:2018 "Axborot texnologiyasi. Atamalar va ta’riflar";
- O‘zbekiston Respublikasi hududida axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha uslubiy qo‘llanmalar (O‘zbekiston Respublikasi Milliy axborot-kommunikatsiya tizimini rivojlantirishning 2013-2020-yillarga mo‘ljallangan kompleks dasturini amalga oshirishni muvofiqlashtirish bo‘yicha Respublika komissiyasining 2016-yil 23-fevraldagi 7-sonli bayonnomasiga 10-ilova);
- "O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi hamda davlat va xo‘jalik boshqaruvi organlari o‘rtasida axborot xavfsizligi hodisalariga munosabat bildirish, ularni tekshirish va oldini olish bo‘yicha o‘zaro hamkorlik reglamenti" (O‘zbekiston Respublikasi Axborot-kommunikatsiya xavfsizligi masalalari bo‘yicha texnik kengashining 2017-yil 17-noyabrdagi 7-sonli bayonnomasiga 1 va 2-ilovalar);
- "Davlat va xo‘jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlarining axborot xavfsizligini ta’minlashga doir talablar" (O‘zbekiston Respublikasining 2013-2020-yillarga mo‘ljallangan Milliy axborot-kommunikatsiya tizimini rivojlantirish kompleks dasturini amalga oshirishni muvofiqlashtirish bo‘yicha Respublika komissiyasining 2017-yil 11-noyabrdagi 7-sonli bayonnomasiga 2-ilova)

O‘zbekiston Respublikasi Markaziy banki Boshqaruvining 2020-yil 10-martdagi 3224-sonli "O‘zbekiston Respublikasi tijorat banklarining avtomatlashtirilgan bank tizimida axborotni himoya qilish to‘g‘risidagi nizomni tasdiqlash haqida"gi qarori.

3-bob. Qo‘llanish doirasi

9. Axborot xavfsizligi siyosati Bankning barcha xodimlariga, shu jumladan amaliyotchilar, shartnoma asosida ishlovchilar va tashqi tashrif buyuruvchilarga (mijozlar, texnik xizmat ko‘rsatuvchi xodimlar va boshqalar) tegishli bo‘lib, ular u yoki bu sababga ko‘ra Bank axborot resurslariga, uning mijozlari va korrespondentlariga qonuniy kirish huquqiga ega. Shuningdek, u bank xodimlarining avtomatlashtirilgan ish joylari, ofis texnikasi va Bank axborot infratuzilmasining boshqa resurslariga nisbatan ham qo‘llaniladi.

10. Axborot xavfsizligi siyosati axborot davlat sirlarini o‘z ichiga olgan ma’lumotlarni uzatish, qayta ishlash va saqlash uchun mo‘ljallangan axborotlashtirish tizimlari hamda obyektlari. Davlat sirlarini o‘z ichiga olgan axborotni himoya qilish O‘zbekiston Respublikasi qonunchiligi asosida ta’minlanadi.

4-bob. Maqsad va vazifalar

11. Siyosatning barcha qoidalari yo‘naltirilgan asosiy maqsad axborot xavfsizligiga tahdid soluvchi hodisalarning oldini olish yoki ularning oqibatlarini eng kam darajaga tushirish orqali zararni minimallashtirish hisoblanadi.

12. Ishonchli axborot himoyasini yaratish jarayoni uzluksiz davom etadi. Axborot xavfsizligi tizimining yetarli darajada ishonchliligini ta’minlash uchun uning parametrlarini doimiy ravishda sozlash, tashqi va ichki muhitdan kelib chiqadigan yangi tahdidlarni bartaraf etishga moslash zarur. Zarurat tug‘ilganda standartlar, tartib-qoidalar yoki Siyosatga o‘zgartirishlar kiritishda hech qanday to‘siqlar bo‘lmasligi kerak.

Ushbu qoidaga muvofiq, axborot xavfsizligini boshqarish siklining quyidagi bosqichlari belgilanadi (PDCA modeli: Rejalashtirish-Bajarish-Tekshirish-Harakat qilish):

1) Rejalashtirish – Rejalashtirish (ishlab chiqish) – Bankning umumiy strategiyasi va maqsadlariga muvofiq natijalar olish uchun xavflarni tahlil qilish, xavflarni boshqarish va axborot xavfsizligini takomillashtirishga oid Siyosat, maqsadlar, vazifalar, jarayonlar, protseduralar, dasturiy-apparat vositalarini belgilash;

2) Bajarish – Amalga oshirish (joriy etish va foydalanish) – Siyosat, nazorat mexanizmlari, jarayonlar, protseduralar, dasturiy-apparat vositalarini joriy etish va ulardan foydalanish;

3) Tekshirish - Nazorat (monitoring va tahlil) - baholash va tegishli hollarda Siyosat, maqsadlar va amaliy tajribaga muvofiq jarayonlarning bajarilish xususiyatlarini o‘lchash, axborot resurslarining xavfsizligiga ta’sir etuvchi tashqi va ichki omillarning o‘zgarishini tahlil qilish, tahlil uchun rahbariyatga hisobotlar taqdim etish;

4) Harakat - Tuzatish (qo‘llab-quvvatlash va takomillashtirish) - axborot xavfsizligi boshqaruv tizimini uzluksiz takomillashtirishni ta’minlash maqsadida axborot xavfsizligi holatini ichki va tashqi tekshiruvlar natijalari, rahbariyat talablari va boshqa omillarga asoslangan holda tuzatuvchi va oldini oluvchi choralarni qabul qilish.

13. Bank axborot xavfsizligi boshqaruv tizimini qurish va uning faoliyat ko‘rsatishi quyidagi asosiy tamoyillarga muvofiq amalga oshirilishi lozim:

1) qonuniylik - axborot xavfsizligini ta’minlash uchun ko‘riladigan har qanday chora amaldagi qonunchilik asosida, Bankning axborot muhofazasi obyektlariga salbiy ta’sirlarni aniqlash, oldini olish, cheklash va bartaraf etishning qonun doirasida ruxsat etilgan barcha usullarini qo‘llagan holda amalga oshiriladi;

2) biznesga yo‘naltirilganlik - axborot xavfsizligi Bankning asosiy faoliyatini qo‘llab-quvvatlash jarayoni sifatida qaraladi. Axborot xavfsizligini ta’minlash bo‘yicha har qanday chora Bank faoliyatiga jiddiy to‘sqinlik qilmasligi kerak;

3) uzluksizlik - axborotni himoya qilish tizimlarini boshqarish vositalarini qo‘llash, Bankning axborot himoyasini ta’minlash bo‘yicha har qanday chora-tadbir Bankning joriy biznes jarayonlarini uzmasdan yoki to‘xtatmasdan amalga oshirilishi lozim;

4) komplekslilik - axborot resurslarining butun hayot sikli davomida, ulardan foydalanishning barcha texnologik bosqichlarida va faoliyat rejimlarida xavfsizligini ta’minlash;

5) asoslanganlik va iqtisodiy maqsadga muvofiqlik - qo‘llaniladigan himoya imkoniyatlari va vositalari fan va texnika taraqqiyotining tegishli darajasida amalga oshirilishi, belgilangan xavfsizlik darajasi nuqtai nazaridan asosli bo‘lishi hamda qo‘yilgan talablar va me’yorlarga mos kelishi lozim. Har qanday holatda axborot xavfsizligi choralari va tizimlarining qiymati har qanday turdagi xavfdan yuzaga kelishi mumkin bo‘lgan zarar miqdoridan kam bo‘lishi shart;

6) ustuvorlik - Bankning barcha axborot resurslarini axborot xavfsizligiga nisbatan mavjud va potensial tahdidlarni baholashda muhimlik darajasi bo‘yicha toifalash (darajalash);

7) zaruriy bilim va imtiyozlarning eng past darajasi - foydalanuvchi faqat o‘z vakolatlari doirasidagi faoliyatni amalga oshirish uchun zarur bo‘lgan ma’lumotlarga kirish huquqiga va imtiyozlarning eng past darajasiga ega bo‘ladi;

8) ixtisoslashuv - texnik vositalardan foydalanish va axborot xavfsizligi chora-tadbirlarini amalga oshirish Bankning maxsus tayyorgarlikdan o‘tgan mutaxassislari tomonidan bajarilishi lozim;

9) xabardorlik va shaxsiy javobgarlik - barcha darajadagi rahbarlar va ijrochilar axborot xavfsizligining barcha talablaridan xabardor bo‘lishlari, ushbu talablarning bajarilishi hamda axborot xavfsizligining belgilangan choralariga rioya etilishi uchun shaxsan javobgar bo‘lishlari shart;

10) o‘zaro hamkorlik va muvofiqlashtirish - axborot xavfsizligi chora-tadbirlari Bankning tegishli tarkibiy bo‘linmalarining o‘zaro aloqasi asosida, qo‘yilgan maqsadlarga erishish uchun ularning sa’y-harakatlarini muvofiqlashtirish orqali, shuningdek, tashqi tashkilotlar, kasb-hunar uyushmalari va jamoalar, davlat organlari, yuridik va jismoniy shaxslar bilan zarur aloqalarni o‘rnatish yo‘li bilan amalga oshiriladi;

11) tasdiqlanish imkoniyati - muhim hujjatlar va barcha yozuvlar, ya’ni axborot xavfsizligi talablarining bajarilishini va uni tashkil etish tizimining samaradorligini tasdiqlovchi hujjatlar, tezkor kirish va tiklash imkoniyati bilan yaratilishi va saqlanishi lozim.

5-bob. Asosiy qoidalar

14. Axborot xavfsizligi uchta asosiy tarkibiy qismdan iborat:

- maxfiylik: ushbu ma’lumotlarga kirish huquqiga ega bo‘lgan subyektlar doirasini cheklash zarurligini ko‘rsatuvchi xususiyat bo‘lib, u tizimning (muhitning) ko‘rsatilgan ma’lumotlarni ularga kirish vakolatiga ega bo‘lmagan subyektlardan sir saqlash qobiliyati bilan ta’minlanadi;
- yaxlitlik: axborotning mavjud bo‘lish xususiyati buzilmagan ko‘rinishda (uning ma’lum bir belgilangan holatiga nisbatan o‘zgarishsiz);
- foydalanish imkoniyati: tegishli vakolatlarga ega bo‘lgan subyektlarning axborotdan o‘z vaqtida va to‘siqsiz foydalana olish qobiliyati bilan tavsiflanadigan xususiyat.

15. Axborot xavfsizligi siyosati axborotni himoya qilishning tashkiliy, rejimli, texnik, dasturiy va boshqa usullari hamda vositalarini qo‘llash asosida axborot xavfsizligini ta’minlashni, shuningdek, axborot xavfsizligini ta’minlash bo‘yicha amalga oshirilgan chora-tadbirlar samaradorligini har tomonlama uzluksiz nazorat qilishni nazarda tutadi.

16. Axborot xavfsizligi siyosatini amalga oshirish jarayonida unga o‘zgartirish va qo‘shimchalar kiritilishi mumkin.

6-bob. Himoya obyektlari

17. Bankda axborot xavfsizligini ta’minlashning asosiy obyektlari sifatida quyidagi elementlar e’tirof etiladi:

1) amaldagi qonunchilik va Bankning ichki me’yoriy hujjatlariga muvofiq bank va tijorat siri, shaxsiy ma’lumotlar, moliyaviy ma’lumotlar hamda Bankning normal faoliyatini ta’minlash uchun zarur bo‘lgan har qanday boshqa ma’lumotlarni o‘z ichiga olgan bank, uning mijozlari va korrespondentlarining axborot resurslari (bundan keyin – himoyalanadigan ma’lumotlar);

2) himoyalanadigan ma’lumotlarga ishlov berish, uzatish va saqlash amalga oshiriladigan axborotlashtirish vositalari va tizimlari (hisoblash texnikasi vositalari, axborot-hisoblash komplekslari, tarmoqlari, tizimlari);

3) Bank avtomatlashtirilgan tizimining himoyalanadigan ma’lumotlarga ishlov berishda qo‘llaniladigan dasturiy vositalari (operatsion tizimlar, ma’lumotlar bazasini boshqarish tizimlari, boshqa umumtizimli va amaliy dasturiy ta’minot);

4) Bankning axborot resurslarini boshqarish va ulardan foydalanish bilan bog‘liq jarayonlari;

5) himoyalanadigan ma’lumotlarga ishlov berish vositalari joylashgan xonalar;

6) Bank xodimlarining ish xonalari va xonalari, yopiq muzokaralar va majlislar o‘tkazish uchun mo‘ljallangan Bank binolari;

7) himoyalangan ma’lumotlarga kirish huquqiga ega bo‘lgan Bank xodimlari;

8) ochiq axborotni qayta ishlovchi, ammo himoyalanadigan axborot qayta ishlanadigan xonalarga joylashtirilgan texnik vositalar va tizimlar.

18. Bank axborot tizimlaridan foydalanuvchilar ro‘yxati, ularning axborotdan foydalanish huquqlari va ustuvorliklari kirish matritsalariga kiritilgan, dasturiy va texnik vositalarga vakolatlar Bank bo‘linmalarining kirish matritsalariga muvofiq beriladi, jarayonlar Bankning axborot resurslaridan ruxsat etilgan foydalanish qoidalari va Bankning axborot resurslariga mantiqiy kirishni boshqarish qoidalari bilan tartibga solinadi.

19. Himoyalanishi lozim bo‘lgan axborot quyidagicha bo‘lishi mumkin:

1) qog‘oz tashuvchilarga joylashtirilgan;

2) elektron shaklda mavjud (hisoblash texnikasi vositalari bilan qayta ishlanadigan, uzatiladigan va saqlanadigan, texnik vositalar yordamida yoziladigan va ko‘paytiriladigan);

3) telefon, telefaks, teleks va shunga o‘xshash vositalar orqali elektr signallari ko‘rinishida uzatiladigan;

4) yig‘ilishlar va muzokaralar paytida havo muhitida va to‘siq konstruksiyalarida akustik va tebranish signallari ko‘rinishida mavjud bo‘ladigan.

7-bob. Axborot xavfsizligiga tahdidlar xavfi va modeli

I. Axborot xavfsizligi xavflari

20. AT xavfi - bu bankka zarar yetkazish uchun muayyan tahdid orqali aktiv yoki aktivlar guruhining zaifliklaridan foydalanish ehtimoli. AT xavflarini boshqarish uchun xavflarni aniqlash va bartaraf etishning tegishli usullari zarur bo‘lib, ular xarajatlar va iqtisodiy samaradorlikni hisoblash, qonunchilik talablari, manfaatdor tomonlarning manfaatlari va boshqa tegishli ma’lumotlarni o‘z ichiga olishi mumkin.

21. Bankda qabul qilingan xavflarni aniqlash jarayoni identifikatsiyalash, xavfni qiyosiy baholash va xavfni qabul qilish mezonlari hamda Bank uchun maqsadlarning muhimligiga muvofiq ustuvorliklarni belgilashni o‘z ichiga oladi. AT xavflarini aniqlash natijalari rahbariyatga AT xavflarini boshqarish, AT xavflarini boshqarishda ustuvorliklarni belgilash va joriy etish bo‘yicha qarorlar qabul qilishga yordam beradi

ushbu xavflardan himoyalanish uchun tegishli xavfsizlik boshqaruvi vositalarini joriy etish bo‘yicha qarorlar qabul qilishga yordam beradi.

22. Xavfni baholash uchun xavflarni aniqlash jarayoni xavf miqdorini baholashning tizimli usulini (xavfni tahlil qilish) va taxmin qilinayotgan xavfni tegishli xavf mezonlari bilan taqqoslash jarayonini o‘z ichiga oladi. Xavfni aniqlash vaqti-vaqti bilan amalga oshirilishi kerak, bu AT talablarining o‘zgarishini va xavfli vaziyatlarning yuzaga kelishini, shuningdek, sodir bo‘lgan muhim o‘zgarishlarni o‘z vaqtida hisobga olish imkonini beradi. Xavfni aniqlash uchun taqqoslanadigan va takrorlanadigan natijalarni ta’minlaydigan usullardan foydalanish kerak.

23. AKni xavfini samarali aniqlash uchun uning ta’sir doirasi aniq belgilanadi. AK xavfini aniqlash faoliyatning boshqa sohalari uchun xavflarni aniqlash bilan o‘zaro bog‘liq bo‘ladi (zarur hollarda). Xavflarga ishlov berish boshlanishidan oldin xavflarni qabul qilish mezonlari o‘rnatiladi. Agar xavf darajasi past yoki uni bartaraf etish xarajatlari Bank uchun iqtisodiy jihatdan samarasiz ekanligi aniqlansa, xavf qabul qilinadi va ushbu mezonlar hujjatlashtiriladi.

24. Har bir aniqlangan xavf uchun uni bartaraf etish to‘g‘risida qaror qabul qilinishi kerak. Xavflarni boshqarishning mumkin bo‘lgan variantlariga quyidagilar kiradi:

- xavflarni kamaytirish uchun tegishli boshqaruv choralarini qo‘llash;
- xavflarni ongli va xolisona qabul qilish, agar ular Bankning xavflarni qabul qilish talablari va mezonlariga to‘liq javob bersa;
- boshqa tomonlar, masalan, sug‘urta kompaniyalari yoki yetkazib beruvchilar bilan birgalikdagi xavflarni taqsimlash.

25. Xavflarni bartaraf etish to‘g‘risida qaror qabul qilingandan so‘ng, ilgari tanlangan va joriy etilgan tegishli boshqaruv choralari qo‘llaniladi. Tashqi tashkilotlar ishlab chiqarish sabablari tufayli Bankning axborot aktivlari va ma’lumotlarni qayta ishlash vositalariga kirishiga to‘g‘ri kelgan hollarda, shuningdek, tashqi tashkilotlardan tovarlar va xizmatlar olingan taqdirda, axborot xavfsizligi va boshqaruv choralariga qo‘yiladigan talablar uchun mumkin bo‘lgan oqibatlarni aniqlash maqsadida xavf-xatarlar tahlili o‘tkaziladi. Bunday chora-tadbirlar tashqi tashkilot bilan kelishilishi va shartnomada belgilanishi lozim.

26. Xavflarni aniqlash, qayta ishlash va qabul qilish, xavflar haqida axborot almashish, xavflarni nazorat qilish bo‘yicha barcha harakatlar O‘z DSt ISO/IEC 27005:2013 standartiga muvofiq amalga oshirilishi shart.

II. Axborot xavfsizligiga tahdidlar

27. Axborot xavfsizligiga tahdidlar deganda axborot xavfsizligi hodisasi yuzaga kelishiga sharoit yaratuvchi omillar va holatlar majmui tushuniladi.

28. Axborot xavfsizligi tahdidlari quyidagilarga bo‘linadi:

1) tasodifiy - tabiiy ofatlar (tabiiy xavf manbalari - zilzila, yong‘in, yog‘ingarchilik, sel va boshqalar), Bank xodimlarining bexosdan qilgan xatolari, apparat va dasturiy vositalarning nosozliklari va hokazo;

2) qasddan, ya’ni ma’lumotlarni ataylab soxtalashtirish yoki yo‘q qilish, ma’lumotlardan g‘ayriqonuniy foydalanish, kompyuter jinoyatlari va shu kabilar.

29. Axborot xavfsizligi tahdidlariga quyidagilar kiradi (ammo bular bilan cheklanmaydi):

1) Bank sirini, tijorat sirini va qonun bilan himoyalanadigan boshqa ma’lumotlarni tashkil etuvchi axborotning yo‘qolishi;

2) himoyalanadigan axborotni buzib ko‘rsatish (ruxsatsiz o‘zgartirish, qalbakilashtirish);

3) axborotning sizib chiqishi - begona shaxslarning himoyalangan ma’lumotlar bilan ruxsatsiz tanishishi (ruxsatsiz kirish, nusxa ko‘chirish, o‘g‘irlash va boshqalar);

4) axborot resurslaridan ruxsatsiz foydalanish (suiiste’mol qilish, firibgarlik va hokazo);

5) Axborotning to‘sib qo‘yilishi, uskunalar yoki dasturlarning ishlamay qolishi va nosozligi, ishchi stansiyalar operatsion tizimlari, serverlar, faol tarmoq uskunalari, ma’lumotlar bazalarini boshqarish tizimlari, taqsimlangan hisoblash tarmoqlari faoliyatining izdan chiqishi, viruslar, tabiiy ofatlar va boshqa fors-major holatlar ta’siri natijasida axborotga kirish imkoniyatining yo‘qligi, va g‘arazli harakatlar.

30. Ko‘rsatilgan tahdidlarning ta’siri natijasida Bankning axborot xavfsizligi holati va uning normal faoliyatiga ta’sir ko‘rsatadigan quyidagi salbiy oqibatlar yuzaga kelishi mumkin:

1) himoyalangan axborotning chiqib ketishi, oshkor etilishi yoki ruxsatsiz o‘zgartirilishi bilan bog‘liq moliyaviy yo‘qotishlar;

2) yo‘qotilgan ma’lumotlarni yo‘q qilish va keyinchalik tiklash bilan bog‘liq moliyaviy yo‘qotishlar;

3) Bankning axborot resurslaridagi ruxsatsiz harakatlar bilan bog‘liq moliyaviy yo‘qotishlar;

4) Bank faoliyatining izdan chiqishi natijasida yetkazilgan zarar, uning o‘z majburiyatlarini bajara olmasligi bilan bog‘liq moliyaviy va obro‘ga putur yetkazuvchi yo‘qotishlar;

5) noxolis axborot asosida boshqaruv qarorlarini qabul qilishdan ko‘rilgan zarar;

6) Bank rahbariyatida xolis ma’lumotning yo‘qligi sababli yetkazilgan zarar;

7) Bank obro‘siga yetkazilgan zarar;

8) boshqa turdagi zararlar.

8-bob. Axborot xavfsizligini buzuvchi modeli

31. Axborot xavfsizligini buzuvchilar quyidagicha tasniflanadi:

1) ichki qoidabuzarlar - axborot xavfsizligi tartibini bilmagan holda yoki qasddan buzayotgan Bank xodimlari;

2) Tashqi qoidabuzarlar - Bank bilan mehnat munosabatlariga ega bo‘lmagan shaxslar (jumladan, amaliyotchilar va stajyorlar) bo‘lib, ular bezorilik yoki g‘arazli maqsadlarda Bankning axborot resurslariga zarar yetkazishi mumkin bo‘lgan harakatlarni amalga oshiradilar.

32. Qoidabuzarning xavfliligi ko‘p jihatdan u foydalanishi mumkin bo‘lgan axborot resurslarining soni va ahamiyat darajasiga bog‘liq. Shu sababli, yuqori va o‘rta bo‘g‘in rahbarlari, axborot resurslari ma’murlari hamda katta hajmdagi mijozlar va moliyaviy ma’lumotlar bilan ishlaydigan shaxslarni eng xavfli toifalar deb hisoblash lozim.

33. Ichki qoidabuzarlarning asosiy turlari:

1) "O‘qitilmagan/beparvo xodim" - bilmasdan yoki o‘z beparvoligi tufayli yomon niyatsiz qoidabuzarlikka yo‘l qo‘yadigan Bank xodimi;

2) "Raqobatchi xodim" - shaxsiy adovati yoki boshqa sabablarga ko‘ra boshqa xodimga zarar yetkazishga urinadigan Bank xodimi. Uning harakatlari natijasida nafaqat uning "nishoni", balki butun Bank ham zarar ko‘rishi mumkin;

3) "Manfaatdor qoidabuzar" - uchinchi tomonning Bankka nisbatan noqonuniy xatti-harakatlaridan yoki shaxsiy manfaatidan manfaatdor bo‘lgan Bank xodimi. Odatda, u Bank bilan mehnat munosabatlarini davom ettirishdan manfaatdor bo‘lib, uni to‘g‘ridan-to‘g‘ri obro‘sizlantiradigan harakatlarni amalga oshirmaydi. Eng ehtimoliy qoidabuzarlik - axborot sizishi (shaxsiy manfaatdan manfaatdor bo‘lgan taqdirda - moliyaviy firibgarliklar);

4) "kiritilgan buzg‘unchi" - uchinchi shaxslar manfaatlarini ko‘zlab noqonuniy xatti-harakatlar sodir etish maqsadida ishga kirgan Bank xodimi. U Bank bilan keyingi mehnat munosabatlaridan deyarli manfaatdor emas;

5) "ishdan bo‘shayotgan xodim" - Bank bilan mehnat munosabatlarini o‘zaro da’volarsiz tugatayotgan xodim. U bevosita kirish huquqiga ega bo‘lgan ma’lumotlarning sizib chiqish ehtimoli yuqori;

6) "xafa bo‘lgan xodim" - mehnat faoliyati sharoitlaridan qoniqmagan Bank xodimi yoki, boshqa tomondan, Bank rahbariyati xodimning faoliyatidan aniq norozi bo‘lgan holat. Har qanday, hatto eng mantiqsiz qoidabuzarliklar, ayniqsa mehnat munosabatlari bekor qilinayotgan paytda sodir bo‘lishi mumkin.

34. Tashqi qoidabuzarlarning asosiy turlari (ushbu bo‘limda quyidagilar ishlatiladi hozirgi vaqtda axborot xavfsizligi bo‘yicha mutaxassislar hamjamiyatida qabul qilingan atamalar):

1) "Script Kiddie" yoki "Boshlovchi" - umumiy ma’lum zaifliklarni o‘z ichiga olgan har qanday axborot resursini buzib kirishga qiziqqan shaxs.
U aynan Bankning axborot resurslarini buzib kirishni maqsad qilmagan, jiddiy himoya vositalari aniqlangan taqdirda hujumni osongina to‘xtatadi. Odatda, keng tarqalgan buzib kirish usullaridan foydalanadi, o‘z vositalarini ishlab chiqmaydi;

2) "Black hat" - "Qora xaker" - "Script Kiddie"dan farqli o‘laroq, ma’lum bir resursni buzishda qat’iyatli, himoya tizimlarini chetlab o‘tishni "or-nomus ishi" deb biladi, oddiy hujum vositalarini ishlab chiqishi mumkin. U o‘zini ko‘rsatish yoki shaxsiy foyda olish maqsadida harakat qiladi, o‘z xizmatlarini jinoiy tuzilmalarga sotishi mumkin;

3) "Elite hacker" yoki "Guru" - axborot tizimlarini buzishda yuqori malakali mutaxassis. Odatda, jinoiy tuzilmalar yoki raqobatchi tashkilotlarning buyurtmasi asosida ishlaydi. Birinchi holatda moliyaviy firibgarlikni amalga oshirishga, ikkinchisida esa - ma’lumotlarning sizib chiqishiga yoki serverlarning ishdan chiqishiga va Bankning mijozlar oldida obro‘sini tushirishga qaratilgan bo‘ladi. Uning arsenalida maxsus dasturiy ta’minotning to‘liq to‘plami mavjud
-texnik ta’minot, shuningdek, ijtimoiy muhandislik usullaridan foydalanadi;

4) "Hamkor" - Bankning axborot tizimlariga kirish huquqiga ega bo‘lgan hamkor tashkilot xodimi. Uni ichki qoidabuzarning har qanday turi sifatida belgilash mumkin, ammo u odatda kamroq nazorat qilinadi va Bankda qabul qilingan axborot xavfsizligi talablari haqida kamroq xabardor bo‘ladi;

5) "Maslahatchi" - axborot resurslariga kirish huquqiga ega bo‘lgan xizmat ko‘rsatuvchi kompaniya xodimi. Xizmat ko‘rsatilayotgan axborot tizimi doirasida, odatda, ruxsat etilmagan faoliyatning turli ko‘rinishlari namoyon bo‘lishi mumkin;

6) "Amaliyotchi/stajyor" - odatda axborotdan foydalanish imkoniyati cheklangan va axborot tizimlariga, biroq doimiy ravishda Bank hududida bo‘ladi hamda bilvosita yoki ijtimoiy muhandislik usullari orqali ma’lumot olishi mumkin. Faqatgina ushbu amaliyotchi/stajyorga rahbarlik qiluvchi Bank xodimi o‘z majburiyatlariga e’tiborsizlik bilan yondashgan taqdirdagina jiddiy zarar yetkazishi mumkin;

7) "Mijoz" - Bankning masofaviy bank xizmatlaridan foydalanish huquqiga ega bo‘lgan mijoz. U xizmatlardan noto‘g‘ri foydalanish, identifikatsiya ma’lumotlarini yo‘qotish yoki bank axborot resurslariga cheklangan bo‘lsa-da, kirish imkoniyatiga ega bo‘lgan holda, tashqi buzg‘unchilarning dastlabki uch turi kabi harakat qilish orqali zarar yetkazishi mumkin.
bank resurslariga.

9-bob. Axborot xavfsizligi choralari

35. Bankning axborot xavfsizligini ta’minlashning asosiy chora-tadbirlari quyidagilardan iborat:

1) ma’muriy-huquqiy va tashkiliy chora-tadbirlar;

2) jismoniy xavfsizlik choralari;

3) dasturiy-texnik chora-tadbirlar.

36. Ma’muriy-huquqiy va tashkiliy chora-tadbirlar quyidagilarni o‘z ichiga oladi (ammo ular bilan cheklanmaydi):

1) O‘zbekiston Respublikasi qonunchiligi va ichki hujjatlar talablarining bajarilishini nazorat qilish;

2) Siyosatni qo‘llab-quvvatlovchi qoidalar, uslubiyotlar va yo‘riqnomalarni ishlab chiqish, joriy etish va ularning bajarilishini nazorat qilish;

3) Biznes jarayonlarining Siyosat talablariga muvofiqligini nazorat qilish;

4) Bank xodimlarini axborot resurslari bilan ishlash va axborot xavfsizligi talablari bo‘yicha xabardor qilish hamda o‘qitish;

5) hodisalarga munosabat bildirish, ularni mahalliylashtirish va oqibatlarini kamaytirish;

6) axborot xavfsizligi bo‘yicha yangi xavflarni tahlil qilish;

7) jamoada ma’naviy va ishbilarmonlik muhitini kuzatib borish va yaxshilash;

8) favqulodda vaziyatlar yuzaga kelganda zarur harakatlarni belgilash;

9) Bank xodimlarini ishga qabul qilish va ishdan bo‘shatishda profilaktik choralarni amalga oshirish;

10) belgilangan harorat va namlik ko‘rsatkichlarini saqlab turuvchi tizimni tashkil etish va ta’minlash;

11) videokuzatuv tizimi bilan ta’minlash;

12) ma’naviy-axloqiy (psixologik) choralar.

37. Jismoniy xavfsizlik choralari quyidagilarni o‘z ichiga oladi (biroq ular bilan cheklanmaydi):

1) kirish-chiqish va ichki obyekt tartibini tashkil etish;

2) himoyalanadigan obyektlar xavfsizlik chegarasini shakllantirish;

3) maxsus obyektlarni, shu jumladan texnik xavfsizlik vositalaridan foydalangan holda, kecha-kunduz qo‘riqlashni tashkil etish;

4) qo‘riqlanadigan obyektlarda yong‘in xavfsizligini ta’minlash;

5) Bank xodimlarining kirishi cheklangan xonalarga kirishini nazorat qilish.

38. Dasturiy-texnik choralar quyidagilarni o‘z ichiga oladi (biroq ular bilan cheklanmaydi):

1) litsenziyali dasturiy ta’minot va axborotni himoyalashning sertifikatlangan vositalaridan foydalanish;

2) chegara himoyasi vositalaridan foydalanish (firewall, Intrusion Prevention System (IPS) kabilar);

3) kompleks antivirus himoyasini joriy etish;

4) axborot tizimlariga o‘rnatilgan axborot xavfsizligi vositalaridan foydalanish;

5) axborot xavfsizligining maxsus majmualaridan foydalanish (ham elektron axborot resurslarini himoyalash, ham elektromagnit va akustik kanallar orqali ma’lumot chiqib ketishidan himoyalash);

6) axborotni muntazam ravishda zaxiralashni ta’minlash;

7) foydalanuvchilarning, ayniqsa imtiyozli foydalanuvchilarning huquqlari va harakatlarini nazorat qilish;

8) axborotni kriptografik himoyalash tizimlarini qo‘llash;

9) apparat vositalarining uzluksiz ishlashini ta’minlash;

10) axborot tizimining muhim elementlari holatini kuzatib borish.

"Tenge Bank" ATB Axborot xavfsizligi siyosati bilan
Tanishib chiqqaningiz uchun tashakkur!

*Ushbu hujjat o’zbek tiliga avtomashtirilgan tarjima vositalari yordamida tarjima qilingan. Tafovutlar yuzaga kelgan taqdirda, hujjatning rus tilidagi asl nusxasi ustuvor hisoblanadi.