1-amaliy ish

Mavzu: Tashkilot uchun axborot xavfsizligi siyosatining foydalanishlarni boshqarish bandini ishlab chiqish.

Ishdan maqsad: Axborot xavfsizligi siyosati tushunchasiga ega bo‘lish, korxona-tashkilotda axborot xavfsizligi siyosatini foydalanishlarni boshqarish modellari orqali tahlil etishni o‘rganish.

Nazariy qism

Axborotni muhofaza qilish axborotni ixtiyoriy ko‘rinishda yo‘qotishda ko‘riladigan zararning oldini olishni ta’minlashi lozim. Axborotni muhofaza qilish choralari axborot xavfsizligiga oid amaldagi qonun va me’yoriy hujjatlar asosida va axborotdan foydalanuvchilarning manfaatlariga ko‘ra tashkil etilishi zarur. Yuqori darajada axborotni mufofaza qilishni kafolatlash uchun muntazam ravishda murakkab ilmiy – texnik vazifalarni hal etish va himoya vositalarini takomillashtirish talab etiladi. Axborot xavfsizligi siyosati maxfiylikni to‘plash, yig'ish va oshirishga qaratilgan texnik vositalardan tizimli foydalanishni nazarda tutadi.

Xavfsizlik siyosati bu- tashkilotning himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yoqori sathli hujjat yoki hujjatlar to‘plami.

Xavfsizlik siyosati konfidentsiallikni foydalanuvchanlikni, yaxlitlikni va aktiv qiymatini saqlaydi.

Xavfsizlik siyosatisiz, tashkilotni bo’lishi mumkin jinoiy ish, foydaning yo’qolishi va yomon oshkorlik kabi holatlarni oldini olish imkonsiz. Biroq, u xavfsizlik siyosati asos xavfsizlik hujumlarini nazarda tutmaydi.

Xavfsizlik siyosatlarining afzalliklari:

- kuchaytirilgan ma’lumot va tarmoq xavfsizligi;
- risklarni kamaytirish;
- qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlanishi;
- tarmoqni yuqori unumdorligi;
- muammolarga tezkor javob berish va harakatsiz vaqtning kamligi;
- boshqaruvdagi stress darajasini kamayishi;
- xarajatlarni kamayishi;
- xavfsizlikni ta'minlashning asosiy bosqichlari quyidagilardan iborat;
- korxonaning axborot va texnologik aktivlarining ahamiyatini aniqlash;
- har bir aktiv uchun xavfsizlik darajasini aniqlash, shuningdek, har bir aktiv uchun iqtisodiy jihatdan samarali bo‘lgan xavfsizlik choralari Aktivlarga tahdid qilish xavfini aniqlash;
- xavfsizlik siyosatini ta'minlash uchun zarur moliyaviy resurslarni jalb qilish, shuningdek, zarur xavfsizlik vositalarini sotib olish va sozlash;

- xavfsizlik rejasining bosqichma -bosqich bajarilishini qat'iy nazorat qilish, hozirgi kechirimlilikni aniqlash, shuningdek, tashqi omillarning o‘zgarishini hisobga olish, zarur xavfsizlik usullarini yanada o‘zgartirish;
- xodimlar va boshqa mas'ul xodimlar uchun tushuntirish ishlarini o‘tkazish.

Xavfsizlik siyosatining xususiyatlari:

- qisqa va aniq;
- foydalanuvchan bo‘lishi;
- tushunarli bo‘lishi;
- amaliy bo‘lishi;
- barqaror bo‘lishi;
- mulojavaiy bardoshli bo‘lishi;
- iqtisodif asoslangan bo‘lishi;
- kiber va yuridik qonunlarga, standartlarga, qoidalarga va instruksiyalarga mos bo‘lishi kerak.

Siyosatni ishlab chiqishning asosiy bosqichlari:

- siyosat tuzish uchun etarli jamoani yaratish;
- ishlab chiqish jarayonida paydo bo‘ladigan xususiyatlar haqidagi savollarni hal qilish;
- siyosatning ko‘lami va maqsadi haqidagi savollarni hal qilish;
- ushbu hujjatni yaratish va amalga oshirish uchun mas'ul shaxslar haqidagi savollarni hal qilish.

Xavfsizlik siyosatini ishlab chiqish - bu tashkilot qoidalari ta'sir qiladigan barcha tashkilotning birgalikdagi yoki jamoaviy operatsiyasi. Umuman olganda, xavfsizlik siyosati IT -guruh tomonidan ishlab chiqilmasligi kerak, chunki xavfsizlik siyosatida ishtirok etadigan har bir kishi uni ishlab chiqarishda ishtirok etishi kerak.

Xavfsizlik siyosati ma'lumotli, tartibga soluvchi va maslahatchi bo‘lishi mumkin, umuman olganda quyidagi toifalarga bo‘linadi:

- Jismoniy xavfsizlik: Bu xodimlarni ham, rahbariyatni ham jismoniy aktivlarni himoya qilish uchun qanday himoya vositalarini qo‘llashni taqozo etadi, eshiklar, kirish joyi, kuzatuv, signalizatsiya va boshqalarni o‘z ichiga oladi.
- Xodimlarni boshqarish: ular o‘z xodimlariga har kungi ish faoliyatini xavfsiz tarzda qanday olib borish yoki boshqarishni aytib berishlari kerak, masalan, parolni boshqarish, maxfiy axborot xavfsizligi va boshqalar.
- Uskuna va dasturiy ta'minot: U administratorga qanday texnologiya turidan foydalanishni, tarmoqni boshqarish nima va qanday sozlanishi kerakligini ko‘rsatib beradi va tizim va tarmoq ma'murlariga qo‘llaniladi.

Amaliy qism

Quyida tashkilot uchun axborot xavfsizligi siyosatining foydalanishlarni boshqarishda kredit markazi namuna sifatida keltirib o‘tilgan.

KREDIT MARKAZI
AXBOROT XAVFSIZLIGI SIYOSATI

1.1-jadval.
Shartnoma varaqasi

№	Lavozimi	Ism va familyasi	imzo
1	Yuridik bo‘lim boshlig’i	Музыка А.Ч.	
2	Avtomatlashtirish bo‘limi boshlig'i	Авилкин И.А.	
3	Tarmoq va axborot xavfsizligi boshqarmasi boshlig‘i	Шапцов В.Э.	
4	Ichki nazorat xizmati rahbari vazifasini bajaruvchi	Стриганина О.С.	

MUNDARIJA

Umumiy tushunchalar

1.1. “Kredit markazi” berish korxonasida axborot xavfsizligi siyosati Rossiya Federatsiyasi qonunchiligiga va axborot xavfsizligi qonun normalariga, Rossiya Federatsiyasi Markaziy bankining me'yoriy hujjatlari talablariga, xavfsizlik sohasidagi vakolatli federal ijro etuvchi organga, texnik razvedka va axborotni texnik muhofaza qilishga qarshi kurashish sohasidagi vakolatli federal ijro etuvchi organga muvofiq ishlab chiqilgan. Umumiy qoidalar va Rossiya banki standartlashtirish sohasidagi tavsiyalar Rossiya Federatsiyasi bank tizimi tashkilotlarining axborot xavfsizligini ta'minlash. 100 IBBS-1.0 talablariga muvofiq axborot xavfsizligini ta'minlash bo‘yicha hujjatlar bo‘yicha uslubiy tavsiyalar (RF IBBS-2.0-2007).

1.2. Siyosat bankning umumiy maqsadlari va maqsadlarini, shu jumladan, siyosat talablarini amalga oshirishni nazorat qilish usullarini belgilovchi yuqori darajadagi hujjatdir. Siyosat bankning axborot xavfsizligini ta'minlash faoliyatining mazmuni, maqsadi va talablarini belgilaydi.

1.3. Siyosat bank xodimlari va mijozlari uchun qulay hujjat bo‘lib, bank rahbariyati tomonidan bankning axborot xavfsizligini ta'minlash, axborot xavfsizligini qurish muammolariga nisbatan rasman qabul qilingan pozitsiyani ifodalaydi. Siyosat barcha xodimlar va bank rahbariyati, shuningdek, bank axborot resurslaridan foydalanuvchilar tomonidan qo‘llanilishi shart.

1.4. Bank boshqaruvi bank faoliyatini tartibga solish qonunchiligi va normalarini rivojlantirish, shuningdek, amalga oshirilayotgan bank texnologiyalari va bank mijozlari va boshqa manfaatdor tomonlarning istiqbollarini rivojlantirish nuqtai nazaridan axborot xavfsizligini ta'minlash choralari va vositalarini takomillashtirish muhimligini tushunadi. Axborot xavfsizligi talablariga rioya qilish bankka raqobatbardosh afzalliklarni yaratish, uning moliyaviy barqarorligini, huquqiy, tartibga soluvchi va shartnoma talablariga muvofiqligini ta'minlash imkonini beradi.

1.5. Bank hujjatlar, axborot tizimlari, texnologiyalari va ularni ta'minlash vositalarining egasi bo‘lib, uning mablag'lari hisobidan ishlab chiqariladi, qonuniy ravishda sotib olinadi, sovg'a, meros yoki boshqa qonuniy yo‘l bilan olinadi.

1.6. Bank, axborot resurslari, axborot tizimlari, texnologiyalari va ularni ta'minlash vositalarining egasi sifatida ushbu ob'ektlarga egalik qilish, ulardan foydalanish, ularni tasarruf etish vakolatlarini to‘liq amalga oshiradi va ushbu mahsulotlardan foydalanish shartlarini belgilaydi.

1.7. Bank, bankning tijorat sirini tashkil etuvchi axborot egasi sifatida, ushbu bitim bankning majburiyatlariga zid kelmasa, huquqlarni buzmasa va bankka, uning xodimlariga, mijozlariga yoki muxbirlariga zarar etkazmasa, uni boshqa yuridik va jismoniy shaxslarga tovar sifatida sotish va sotish huquqiga ega.

1.8. Bank faoliyati davomida bankning mulki bo‘lgan axborotni ruxsatsiz olish va undan foydalanish xavfi mavjud bo‘lib, buning natijasida bankka, uning

mijozlariga va muxbirlariga moddiy, ma'naviy yoki boshqa zarar yetkazilishi mumkin.

1.9. Tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish uchun hujjatlashtirilgan axborot, axborot tizimlari, texnologiyalar va ularni ta'minlash vositalari himoya qilinadi.

1.10. Ushbu siyosatning axborot xavfsizligining turli sohalariga taalluqli qoidalarini batafsil bayon etuvchi xususiy siyosatchilar bankning alohida ichki normativ hujjatlari shaklida rasmiylashtiriladi.

I. Atama va ta’riflar

Avtomatlashtirilgan bank tizimi-bank funktsiyalarini bajarish texnologiyasini amalga oshiruvchi avtomatlashtirilgan tizim.

Aktiv-bu bank uchun ahamiyatga ega bo‘lgan va uning ixtiyorida bo‘lgan hamma narsa.

Bank axborot xavfsizligi auditi-bank tomonidan axborot xavfsizligini ta'minlash bo‘yicha belgilangan talablarni bajarish darajasini aniqlash maqsadida auditorlik guvohnomalarini olish va ularni xolisona baholash uchun davriy, mustaqil va hujjatlashtirilgan jarayon.

Bank texnologik jarayoni-bank faoliyatini amalga oshirishda foydalaniladigan yoki bank xizmatlarini amalga oshirish uchun zarur bo‘lgan aktivlarning holatini o‘zgartirish va (yoki) aniqlash bo‘yicha operatsiyalarni amalga oshiruvchi texnologik jarayon.

Bank axborot texnologik jarayoni-bank faoliyati uchun zarur bo‘lgan va to‘lov axboroti bo‘lmagan axborot aktivlarining holatini o‘zgartirish va (yoki) aniqlash bo‘yicha operatsiyalarni amalga oshiruvchi bank texnologik jarayonining bir qismi.

Bank to‘lov jarayoni – bank jarayonining bir qismi, bankning axborot aktivlari bo‘yicha bank operatsiyalarini amalga oshirish, pul mablag'larini bir hisobdan ikkinchisiga o‘tkazish va (yoki) ushbu operatsiyalarni nazorat qilish bilan bog'liq.

Axborot - xabarlar, ma'lumotlarlarni taqdim etish shaklidan qat'i nazar.

Axborot aktivi-uni aniqlash imkonini beruvchi rekvizitlar bilan ma'lumot; bank uchun ahamiyatga ega.

Shaxsiy ma'lumotlarning axborot tizimi-ma'lumotlar bazasida mavjud bo‘lgan shaxsiy ma'lumotlar to‘plami, shuningdek, bunday shaxsiy ma'lumotlarni avtomatlashtirish vositalaridan foydalangan holda yoki bunday vositalardan foydalanmasdan qayta ishlashga imkon beruvchi axborot tizimi.

Bankning axborot xavfsizligi-axborot sohasidagi tahdidlar sharoitida bank manfaatlarini (maqsadlarini) himoya qilish holati.

Axborot xavfsizligi hodisasi-bu ib tahdidining amalga oshirilishi, amalga oshirilishi yoki amalga oshirilishi mumkinligini ko‘rsatuvchi voqea.

Axborot aktivlarini tasniflash-bankning mavjud axborot aktivlarini turlari bo‘yicha taqsimlash, ularning muhim xususiyatlarini yo‘qotishdan kelib chiqadigan oqibatlarning jiddiyligi darajasiga muvofiq amalga oshiriladi.

Bankning axborot xavfsizligini monitoring qilish (BAX monitoringi) – BAX monitoringi voqealarini doimiy kuzatish, kuzatuv natijalarini yig'ish, tahlil qilish va umumlashtirish.

Axborot xavfsizligi siyosati-bankning yuqori darajadagi maqsadlari, mazmuni va asosiy yo‘nalishlarini belgilovchi hujjatlar.

Shaxsiy ma'lumotlar-bevosita yoki bilvosita aniqlangan yoki aniqlangan shaxsga (shaxsiy ma'lumotlar sub'ektiga) tegishli har qanday ma'lumot.

Xavf-bu tahdidni amalga oshirish ehtimoli va ushbu tahdidni amalga oshirishdan zarar (zarar) miqdorini hisobga olgan holda o‘lchovdir.

Axborot xavfsizligini buzish xavfi – ib buzilishi xavfi) - ib tahdidi bilan bog'liq xavf.

Bankning axborot xavfsizligini o‘z-o‘zini baholash-bank faoliyatida axborot xavfsizligini ta'minlash bo‘yicha o‘z-o‘zini baholash guvohnomalarini olish va bankdagi axborot xavfsizligini o‘z-o‘zini baholash mezonlarini bajarish darajasini aniqlashning tizimli va hujjatlashtirilgan jarayonidir.

Axborot xavfsizligi tizimi-himoya choralari, himoya vositalari va ulardan foydalanish jarayonlari, jumladan, resurs va ma'muriy (tashkiliy) ta'minot.

Axborot xavfsizligini boshqarish tizimi-ibni ta'minlash tizimini yaratish, amalga oshirish, ulardan foydalanish, monitoring qilish, tahlil qilish, qo‘llab-quvvatlash va takomillashtirish uchun mo‘ljallangan bank boshqaruvining bir qismi.

Axborot xavfsizligini ta'minlash tizimi-CIB va SMIB jamiyati Bank.

Zarar-aktivlarning yo‘qolishi, aktivlar va (yoki) infratuzilmaning zararlanishi.

Bank yoki bankning aktivlariga va (yoki) infratuzilmasiga boshqa zarar, axborot xavfsizligi zaifliklari orqali ib tahdidlarini amalga oshirish natijasida yuzaga keldi.

Tahdid-bu yo‘qotish (zarar) ehtimoli bo‘lgan xavf.

Axborot xavfsizligi tahdidi – axborot xavfsizligi xususiyatlarini buzish xavfi
bankning axborot aktivlarining mavjudligi, yaxlitligi yoki maxfiyligi.

II. Belgilar va qisqartmalar

ABT-avtomatlashtirilgan bank tizimi.
AX-axborot xavfsizligi.
ShMAT-shaxsiy ma'lumotlar axborot tizimi.
RK-ruxsatsiz kirish.
BVDBH-berilgan vakolatlar doirasida belgilangan harakatlar.
ShM-shaxsiy ma’lumotlar.
RF-Rossiya Federatsiya.
AXBT-axborot xavfsizligini boshqarish tizimi.
AXT-axborot xavfsizligi tizimi.
AXTT-axborot xavfsizligini ta'minlash tizimi.
FXX-Federal xavfsizlik xizmati.

TENBFX-texnik va eksport nazorati bo‘yicha federal xizmat.
EXM-elektron hisoblash mashinasi.

III. Bankning axborot xavfsizligini ta'minlashning dastlabki kontseptual sxemasi

4.1 Bank axborot xavfsizligining kontseptual sxemasi uning axborot aktivlarini tajovuzkorlarning noqonuniy xatti-harakatlaridan kelib chiqadigan tahdidlardan himoya qilishga, xavfni kamaytirishga va baxtsiz hodisalardan, xodimlarning noto‘g'ri xatti-harakatlaridan, texnik kamchiliklardan, noto‘g'ri texnologik va tashkiliy echimlardan axborotni qayta ishlash, uzatish va saqlash jarayonlarida potentsial zararni kamaytirishga va texnologik jarayonlarning normal ishlashini ta'minlashga qaratilgan.

4.2 Bankka zarar yetkazishning eng katta imkoniyati o‘z xodimlariga ega. Xodimlarning xatti-harakatlari yomon niyat bilan (tajovuzkorning bank ichida va tashqarisida sheriklarga ega bo‘lishi mumkin) yoki noto‘g'ri noto‘g'ri xarakterga ega bo‘lishi mumkin. Baxtsiz hodisalar va texnik nosozliklar xavfi texnik parkning holati, energiya ta'minoti va telekommunikatsiya tizimlarining ishonchliligi, xodimlarning malakasi va g'ayritabiiy vaziyatda etarli harakat qilish qobiliyati bilan belgilanadi.

4.3 Bankdagi axborot xavfsizligi tahdidlariga qarshi kurashish uchun mavjud tajriba asosida gumon qilingan tahdidlarning bashoratli modeli va huquqbuzar modeli tuziladi. Prognoz qanchalik aniq bo‘lsa (tahdid modeli va huquqbuzar modeli tuzilgan bo‘lsa), bankdagi ibni buzish xavfi past bo‘ladi.

4.4 Axborot xavfsizligi siyosati prognozi asosida ishlab chiqilgan va unga muvofiq axborot xavfsizligini ta'minlash tizimi bank uchun ibni buzish xavfini minimallashtirishga erishishning eng to‘g'ri va samarali usuli hisoblanadi. Bank vaqti-vaqti bilan monitoring va audit ma'lumotlari asosida tahdid va huquqbuzar modellari yangilanadi.

4.5 Axborot xavfsizligi siyosatiga rioya qilish asosan korporativ axloqning elementidir, Shuning uchun bankda ham jamoa, ham jamoa, ham egasi yoki egasi o‘rtasidagi munosabatlarni boshqarish masalalariga jiddiy e'tibor qaratiladi.egasi manfaatlarini ifodalovchi bank boshqaruvi.

4.6 “Kredit markazi” KM rahbariyat va mulkdorlar tomonidan ishlab chiqilgan axborot xavfsizligi siyosatini amalga oshirish, axborot xavfsizligi boshqaruvi jarayonlarini muvofiqlashtirish, ib intsidentlarini aniqlash va oldini olish vazifasi yuklatilgan tuzilmaviy bo‘linma ib ni ta'minlash uchun javobgardir.

4.7 Bank xodimlari Rossiya Federatsiyasining amaldagi qonunchiligi va bankning axborot xavfsizligi bo‘yicha ichki hujjatlari talablariga rioya qilishadi, shuningdek, ularning bevosita rahbarlarini axborot xavfsizligi buzilishi (buzilishlarga olib kelishi mumkin) bilan bog'liq barcha voqealar haqida xabardor qilishadi. Har qanday darajadagi tarkibiy bo‘linma rahbari Rossiya Federatsiyasining amaldagi qonunchiligi va bankning ichki hujjatlari talablariga rioya qiladi, shuningdek, uning bo‘linmalari xodimlari tomonidan bunday talablarni bajarilishini nazorat qiladi.

4.8 bankdagi ibni ta'minlash strategiyasi buzg'unchilarning hujumlariga qarshi bo‘lgan axborot xavfsizligini ta'minlash bo‘yicha oldindan ishlab chiqilgan chora-tadbirlar rejasiga muvofiq samarali foydalanish va AX modellari va siyosatini muntazam qayta ko‘rib chiqish va Soibni tuzatishdan iborat.

4.9 AXTT bankini qurish uchun asos Rossiya Federatsiyasi qonunchiligining talablari, Rossiya bankining me'yoriy hujjatlari, bankning shartnoma talablari, shuningdek, bank aktivlarini aniqlash, huquqbuzar va tahdidlarning modelini yaratish asosida ifodalangan biznes shartlari.

VI. Axborot xavfsizligining maqsad va vazifalari

5.1 Axborot xavfsizligini ta'minlashning asosiy maqsadi bankning barqaror ishlashini ta'minlash va bankka, uning aktsiyadorlariga, investorlarga va mijozlarga tasodifiy (noto‘g'ri) va noqonuniy tajovuz, oshkor qilish, yo‘qotish, oqish, buzilish, modifikatsiya qilish va himoyalangan ma'lumotlarni yo‘q qilishga qaratilgan axborot aktivlarini himoya qilishdir.

5.2 *Bankdagi axborot xavfsizligini ta'minlashning asosiy vazifalari quyidagilardan iborat:*

- qochqinning oldini olish, o‘g'irlik, yo‘qotish, buzilish, axborotni soxtalashtirish;
- shaxsiyat xavfsizligiga tahdidlarning oldini olish, bank;
- axborotni yo‘q qilish, o‘zgartirish, buzish, nusxalash, blokirovkalash bo‘yicha ruxsatsiz harakatlarning oldini olish;
- axborot resurslari va axborot tizimlariga noqonuniy aralashuvning boshqa shakllarini oldini olish;
- hujjatlashtirilgan axborotning huquqiy rejimini mulk ob'ekti sifatida ta'minlash;
- fuqarolarning shaxsiy sirlarini va axborot tizimlarida mavjud bo‘lgan shaxsiy ma'lumotlarning maxfiyligini saqlashga bo‘lgan konstitutsiyaviy huquqlarini himoya qilish.

5.3 bankdagi axborotni himoya qilish bo‘yicha tashkiliy, texnologik va texnik chora-tadbirlar amaldagi Qonunchilik, FSTEK, FSB, Rossiya Federatsiyasi Markaziy banki (Rossiya federatsiyasi Markaziy banki) normativ-uslubiy materiallar va bankning ibni ta'minlash bo‘yicha tashkiliy-ma'muriy hujjatlari talablariga muvofiq amalga oshiriladi.

VI. Ob’ektlarni himoyalash

6.1 *Bankdagi asosiy himoya ob'ektlari quyidagilardir:*

- tijorat, bank sirini tashkil etuvchi, tasodifiy va ruxsatsiz ta'sirlarga nisbatan sezgir bo‘lgan va ularning xavfsizligini buzuvchi boshqa axborot resurslari, shu jumladan, taqdim etish shakli va turidan qat'i nazar, hujjatlar va axborot massivlari shaklida taqdim etilgan ochiq (ochiq) ma'lumotlar tashuvchi);

- axborot texnologiyalari, axborotni yig'ish, qayta ishlash, saqlash va uzatish tartib-qoidalari, bank xodimlari;
- axborotni qayta ishlash, saqlash va tahlil qilish tizimlari, uni uzatish, saqlash, qayta ishlash va namoyish etishning texnik va dasturiy vositalari, shu jumladan axborot almashinuvi va telekommunikatsiya kanallari, axborotni muhofaza qilish tizimi va vositalari kiradi.

VII. Bank axborot xavfsizligini buzuvchi tahdidlar

7.1 Bankni ta'minlash bo‘yicha chora-tadbirlarni muvaffaqiyatli amalga oshirish uchun unga mumkin bo‘lgan tahdidlarni tushunish kerak.

7.2 Tahdid va buzg'unchilarning modellari (ibning prognozi) bankning xavfsizlik tizimini joylashtirish, saqlash va takomillashtirishda hal qiluvchi ahamiyatga ega.

7.3 Bank faoliyati uning tarkibiga kiruvchi axborot infratuzilmasi tomonidan qo‘llab-quvvatlanadi, bu bank texnologiyalarini joriy etishni ta'minlaydi va quyidagi asosiy darajalarning ierarxiyasi sifatida taqdim etilishi mumkin:

- jismoniy (aloqa liniyalari, apparat va boshqalar);
- tarmoq (tarmoq apparatlari: routerlar, kalitlar, hublar va boshqalar);
- tarmoq ilovalari va xizmatlari;
- operatsion tizimlar (OS);
- ma'lumotlar bazasini boshqarish tizimlari;
- bank texnologik jarayonlari va ilovalari;
- bankning biznes jarayonlari.

7.4 Tajovuzkorning asosiy maqsadi biznes jarayonlari darajasida aktivlarni nazorat qilishdir. Tajovuzkorning boshqa maqsadlari, masalan, axborot aktivlarining mavjudligi yoki yaxlitligini buzish orqali, masalan, zararli dasturlarni tarqatish yoki kompyuter yoki ularning tarmoqlarini ishlatish qoidalarini buzish orqali bankning biznes-jarayonlari faoliyatining buzilishi bo‘lishi mumkin.

7.5 Bankning asosiy tahdid manbalari sifatida ko‘rib chiqiladi:

- Axborot xavfsizligining tashqi huquqbuzarlari (bankning sobiq xodimlari, bankning texnik ta'minoti masalalari bo‘yicha o‘zaro hamkorlik qiluvchi tashkilotlar vakillari, bank mijozlari, bank binolari va binolariga tashrif buyuruvchilar, raqobatchilar, terrorchilar va jinoiy tuzilmalar, xakerlar;
- axborot xavfsizligi ichki huquqbuzarlari (bank tizimining ro‘yxatdan o‘tgan foydalanuvchilari, xizmat ko‘rsatuvchi xodimlar, ma'murlar, axborot xavfsizligi ma'murlari va boshqalar);
- birgalikda tahdid manbalari: tashqi va ichki, birgalikda va/yoki birgalikda harakat qilish birgalikda);
- dasturiy va texnik vositalarning uzilishi, rad etilishi, yo‘q qilinishi/shikastlanishi;
- yetkazib beruvchilar/provayderlar/hamkorlar/mijozlarga qaramlik;

- nazorat va tartibga solish organlari, amaldagi qonunchilik talablariga mos kelmasligi.

VIII. Bankning axborot xavfsizligi tizimi

8.1 Axborot xavfsizligi talablariga rioya qilish ibning to‘g'ri darajasini ta'minlash uchun asos bo‘lib xizmat qiladi.

8.2 Bankning axborot xavfsizligi tizimi ibning bir necha hududlari uchun tuziladi.

8.3 *Xodimlarga ishonchni ta'minlash rollarini tayinlash va tarqatishda axborot xavfsizligini ta'minlash:*

- ishga qabul qilishda shaxsning kimligi, e'lon qilingan malakasi, biografik faktlarning aniqligi va to‘liqligi, tavsiyalar mavjudligi tekshiriladi;
- bank xodimlarining malakasi bajarilayotgan vazifalarga mos keladi. Xodimlarning malakasi axborot xavfsizligi ta'lim jarayonlari, xodimlarning xabardorligi va vakolat darajasini muntazam tekshirish orqali ta'minlanadi;
- bankning barcha xodimlari maxfiylik, korporativ axloq qoidalariga rioya qilish, shu jumladan manfaatlar to‘qnashuvining oldini olish bo‘yicha talablarni bajarish bo‘yicha yozma majburiyatni taqdim etadi;
- tashqi tashkilotlar uchun axborot xavfsizligi talablari shartnomalarga (bitimlarga) kiritilgan qoidalar bilan tartibga solinadi.

IX. Bankning axborot xavfsizligini boshqarish tizimi

9.1 Axborot xavfsizligini ta'minlash AX menejment tizimini joylashtirish, ishga tushirish va takomillashtirishni o‘z ichiga oladi, bu bankning boshqaruv va boshqaruv bo‘yicha muvofiqlashtirilgan faoliyat tizimi hisoblanadi.

9.2 Axborot resurslariga axborot xavfsizligi qoidalarini qo‘llash sohasi resurslarni tasniflash asosida aniqlanadi. Shu bilan birga, axborot aktivlarining tarkibi (ro‘yxati) va ularning ahamiyati, bank faoliyati jarayonlarining uzluksizligi majburiydir.

9.3 AXTM tarqatish, amalga oshirish va ulardan foydalanish tarmoq va axborot xavfsizligi bo‘limi tomonidan amalga oshiriladi.

9.4 AXTM rejalashtirish – amalga oshirish – tekshirish – takomillashtirish - rejalashtirish:

9.5 Bankda AXTM bilan bog'liq asosiy jarayonlar amalga oshirilmoqda:

- AX talablarini bajarish jarayonlarini rejalashtirish bilan;
- himoya choralarini amalga oshirish va ulardan foydalanish;
- AX talablarini bajarish jarayonlarini tekshirish bilan;
- AX talablarini bajarish jarayonlarini takomillashtirish.

X. Axborot xavfsizligi siyosatini amalga oshirish va qayta ko‘rib chiqish tartibi

10.1 Ushbu siyosat bank boshqaruvi tomonidan tasdiqlanadi.

10.2 Siyosatni qayta ko‘rib chiqish uchun sabab bo‘lishi mumkin:

- Axborot xavfsizligi bank siyosati o‘zgarishlari;
- Rossiya Federatsiyasining amaldagi qonunchiligidagi o‘zgarishlar, shuningdek, Rossiya bankining AXni ta'minlash sohasidagi sanoat standartlari.

10.3 Ushbu siyosat kamida uch yilda bir marta qayta ko‘rib chiqilishi kerak.

XI. Mas’ullar

11.1 Bank xavfsizligini ta'minlash bo‘yicha mahalliy qoidalarga rioya qilmaslik bilan bog'liq qonunbuzarliklar xavfi darajasiga qarab ikki guruhga bo‘linadi:

- bank uchun keraksiz oqibatlarning boshlanishiga olib kelgan buzilishlar (axborot oqimi yoki yo‘q qilinishi);
- bank uchun keraksiz oqibatlarga olib kelishi mumkin bo‘lgan (axborotni yo‘q qilish yoki yo‘qotish tahdidi).

11.2 Bankni ta'minlash bo‘yicha bankning mahalliy normativ hujjatlari talablarini buzish favqulodda hodisa bo‘lib, Rossiya Federatsiyasining amaldagi qonunchiligida, mahalliy normativ hujjatlarda, bank va xodimlar o‘rtasida tuzilgan shartnomalar va bank va kontragentlar o‘rtasida tuzilgan shartnomalarda ko‘zda tutilgan oqibatlarga olib keladi.

11.3 AX sohasidagi mahalliy normativ hujjatlar talablarini buzganlik uchun javobgarlik darajasi bankka yetkazilgan zarar miqdoridan kelib chiqqan holda belgilanadi.

11.4 Ushbu siyosatning amal qilishi barcha kontragentlar, ishchilar va bank amaldorlariga nisbatan qo‘llaniladi.

11.5 Barcha darajadagi rahbarlar ushbu siyosatning qoidalariga rioya qilish va uning nazorati ostidagi bo‘linmalarda iblar darajasini saqlab qolish uchun shaxsan javobgardir.

11.6 Tarkibiy bo‘linmalar rahbariyati, shuningdek, tijorat sirini tashkil etuvchi va uning oqishiga yo‘l qo‘ygan ma'lumotlarga ega bo‘lgan bankning har bir xodimi maxfiy ma'lumotlarni oshkor qilish uchun javobgardir.

11.7 Maxfiy ma'lumotlarni oshkor qilish, bunday ma'lumotlarni o‘z ichiga olgan tashuvchilarni yo‘qotish, shuningdek maxfiy axborot bilan ishlashda boshqa huquqbuzarliklar uchun jinoyatchilar ishdan bo‘shatilgunga qadar javobgarlikka tortiladi.

11.8 Cheklangan axborotni boshqarish bo‘yicha ayrim federal qonunlarda nazarda tutilgan javobgarlik turlari:

- fuqarolik javobgarligi;
- intizomiy javobgarlik;
- ma'muriy javobgarlik;
- jinoiy javobgarlik.

11.9 Bank sirini tashkil etuvchi ma'lumotlarni oshkor qilish uchun xodimlar Rossiya Federatsiyasining amaldagi qonunchiligiga muvofiq jinoiy javobgarlikka tortilishi mumkin (Rossiya Federatsiyasi Jinoyat kodeksining 183 moddasi.

Topshiriq

Quyidagi jadval asosida muassa nomlari keltirib o‘tilgan bo‘lib, talaba o‘z tartib raqami bilan berilgan variant asosida axborot xavfsizlik siyosatini ishlab chiqish.

Variantlar	Muassasalar
1	Tijorat bankining filiali
2	Poliklinika
3	Kollej
4	Sug’urta idorasi
5	Ishga yo‘llash agentligi
6	Onlayn magazin
7	Davlat xizmatlar agentligi
8	Ichki ishlar
9	Auditorlik kompaniyasi
10	Dizayn firmasi
11	Internet-provayderi
12	Advokatura
13	Ko‘chmas mulk-agentligi
14	Sayoxat- agentligi
15	Xayriya jamg’armasi
16	Nashriyot
17	Konsalting firmasi
18	Reklama agentligi

19	Soliq qo‘mitasi
20	Notarius udorasi
21	Ilmiy-dizayn korxonasi
22	FHDYO markazi
23	Gazeta tahririyati
24	Mehmonxona
25	Turistik kompaniya
26	Shahar arxivi
27	Taksi dispercherlik xizmati
28	Temir yo‘l kassasi
29	Aloqa bank filiali
30	Davlat test markazi

Nazorat savollari

1. Axborot xavfsizligi nima?
2. Axborot xavfsizligi siyosati deganda nimani tushunasiz?
3. Foydalanishlarni boshqarish deganda nimani tushunasiz?

Foydanilgan adabiyotlar ro‘yxati

1. **https://ipb.ru/doc/about/%D0%9F%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8%2022.04.2016.pdf (murojat vaqti:8.01.22).**
2. **https://www.ccb.ru/download/doc/ITSec.pdf (murojat vaqti:8.01.22).**