ID-6270 (V-1)

O‘ZBEKISTON RESPUBLIKASI MARKAZIY BANKI BOSHQARUVI QARORI

Elektron faktoring platformalarining axborot tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda ularni IT-auditidan o‘tkazish bo‘yicha minimal talablar to‘g‘risidagi nizomni tasdiqlash haqida

O‘zbekiston Respublikasining “O‘zbekiston Respublikasining Markaziy banki to‘g‘risida”gi Qonuni hamda O‘zbekiston Respublikasi Prezidentining 2024-yil 12-avgustdagi PQ–109-sonli “Faktoring xizmatlari bozorini jadal rivojlantirish chora-tadbirlari to‘g‘risida”gi Farmoniga muvofiq Markaziy bank boshqaruvi **qaror qiladi:**

1. Elektron faktoring platformalarining axborot tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda ularni IT-auditidan o‘tkazish bo‘yicha minimal talablar to‘g‘risidagi nizom ilovaga muvofiq tasdiqlansin.

2. Mazkur qaror O‘zbekiston Respublikasi Davlat xavfsizlik xizmati, Raqamli texnologiyalar vazirligi va O‘zbekiston Savdo-sanoat palatasi bilan kelishilgan.

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

O‘zbekiston Respublikasi
Markaziy banki boshqaruvining
2025-yil - _____dagi
–/– - sonli qaroriga
ILOVA

Elektron faktoring platformalarining axborot tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda ularni IT-auditidan o‘tkazish bo‘yicha minimal talablar to‘g‘risidagi nizom

Mazkur Nizom kredit tashkiloti bo‘lmagan shaxslar (bundan buyon matnda Tashkilot deb yuritiladi) tomonidan tashkil etiladigan elektron faktoring platformalarida (bundan buyon matnda Platforma deb yuritiladi) axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda ularni IT-auditidan o‘tkazish tartibini belgilaydi.

1-BOB. UMUMIY QOIDALAR

1. Mazkur Nizomda quyidagi asosiy tushunchalardan foydalaniladi:

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

faktoring elektron platformasi – Internet tarmog‘ida joylashtirilgan, Faktoring (pul talabnomasidan boshqa shaxs foydasiga voz kechish evaziga moliyalash) bozori ishtirokchilari (moliya agentlari, yetkazib beruvchilar va debitorlar) o‘rtasida yuridik ahamiyatga ega bo‘lgan elektron tarzdagi munosabat hamda elektron hujjat almashinuvini tashkil etishga qaratilgan axborot tizimi;

identifikatsiya – platformalarga identifikator tayinlash va/yoki belgilangan identifikatorlar ro‘yxati bilan identifikatorlarni taqqoslash;

axborot tizimlari – idoralararo va idoraviy axborot tizimlari va axborot resurslari hamda boshqa dasturiy mahsulotlar;

axborot xavfsizligi – axborot munosabatlarining subyektlariga nomaqbul ziyonlarni keltirishi mumkin bo‘lgan tabiiy yoki sun’iy xususiyatli

tasodifiy yoki qasddan qilingan ta’sirlardan axborot va ta’minlab turadigan infratuzilmaning muhofaza qilinganligi;

kiberxavfsizlik – kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati;

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

2-BOB. AXBOROT XAVFSIZLIGI VA KIBERXAVFSIZLIKNI TA’MINLASH BO‘YICHA AMALGA OSHIRILADIGAN TASHKILIY CHORALAR

2. Tashkilot o‘zining axborot tizimlari va resurslarining xususiyatlaridan kelib chiqib, quyidagilarni bajaradi:

a) axborot xavfsizligi siyosatini ishlab chiqadi va tasdiqlaydi. Bunda:

axborot tizimlari va resurslarda axborot xavfsizligi va kiberxavfsizlikni ta'minlash bo‘yicha talablar belgilanishi;

belgilangan talablar Tashkilotning har bir xodimiga tanishtirilishi hamda ushbu talablarga xodimlarning qat’iy rioya qilishi ta’minlanishi lozim.

b) axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha mas’ul xodimni tayinlaydi. Mas’ul xodim o‘z faoliyatida:

axborot tizimlari va resurslarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash choralarini ko‘rish uchun talablarni belgilashi hamda ushbu talablar Tashkilot bo‘linmalari va xodimlar tomonidan bajarilishini nazorat qilishi;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimini tashkil qilishi;

ish jarayonida xodimlarga konfidensial, bank sirini tashkil etuvchi va shaxsga doir ma’lumotlarni sir saqlash majburiyati, javobgarliklari to‘g‘risida tushuntirish ishlarini olib borishi va ushbu ma’lumotlar saqlanishini nazorat qilishi;

axborot tizimlariga o‘zgartirishlar kiritilishini nazorat qilishi;

foydalanuvchilarning axborot resurslarida ishlash huquqlari va chegaralarini belgilashi;

axborot tizimlariga kirishni nazorat qilishi;

axborot tizimlari va axborot resurslaridan ruxsatsiz foydalanishni cheklashi;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash yuzasidan ichki me’yoriy hujjatlarni ishlab chiqishi;

axborot xavfsizligi va kiberxavfsizlikni ta'minlash masalalarida rahbariyatga takliflar berishi;

axborotning saqlanishi ustidan umumiy nazoratni tashkil etishni ta’minlaydi.

v) konfidensial, bank sirini tashkil etuvchi va shaxsga doir ma’lumotlarning yaxlitligi va daxlsizligini ta’minlaydi hamda ulardan foydalanish tartibini ishlab chiqadi. Bunda:

ichki hujjatlar bilan tartibga solinadigan himoyalanadigan ma’lumotlar bilan ishlashda xavfsizlik va konfidensiallikni ta’minlash talab va qoidalarini ishlab chiqish;

axborot tizimlariga kirishda

xodimlar bilan konfidensial, bank sirini tashkil etuvchi va shaxsga doir ma’lumotlar oshkor etilishining oldini olish bo‘yicha majburiyatnomalar (shartnomalar) tuzish va ushbu ma’lumotlardan foydalanish huquqlarini xodimlarning lavozim majburiyatlaridan kelib chiqib belgilash;

konfidensial ma’lumotlar ro‘yxatini shakllantirish va tasdiqlash;

konfidensial ma’lumotlar bilan ishlashga ruxsat berilgan xodimlar ro‘yxatini shakllantirish va tasdiqlash;

tashqi saqlovchi qurilmalar va texnik vositalarni binodan tashqariga olib chiqilishi hamda o‘g‘irlanishini oldini olish choralari nazarda tutilishi lozim.

g) axborot tizimlarida yuzaga keladigan risklarni baholash hamda boshqarish bo‘yicha talablarni belgilaydi.

d) axborot tizimlarida yuzaga kelgan to‘xtalishlar, uzilishlar va kiberxavfsizlik hodisalarini aniqlash, oldini olish, bartaraf etish va ular to‘g‘risidagi ma’lumotlarni saqlash hamda ro‘yxatini yuritish tartibini ishlab chiqadi.

3. Tashkilotlar tizimli ravishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash sohasiga ixtisoslashgan o‘quv kurslarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha mas’ul xodimlarini o‘qitish ishlarini tashkil etilishi lozim.

3-BOB. AXBOROT XAVFSIZLIGI VA KIBERXAVFSIZLIKNI TA’MINLASHGA DOIR MINIMAL TALABLAR

4. Tashkilotlar o‘z faoliyatining barqarorligini ta’minlashlari hamda axborot tizimlari va resurslarida yuzaga kelishi mumkin bo‘lgan axborot xavfsizligi va kiberxavfsizlik hodisalarini aniqlash, oldini olish va bartaraf etish choralarini ko‘rishlari lozim.

5. Foydalanuvchilarining Platformaga kirishi himoyalangan protokollardan foydalangan holda Internet orqali amalga oshiriladi.

6. Platforma foydalanuvchilari o‘rtasida almashinadigan ma’lumotlar va hujjatlarning haqqoniyligini tasdiqlash elektron raqamli imzo kalitlari orqali amalga oshiriladi.

7. Platforma O‘zbekiston Respublikasida joylashgan TIER talablariga javob beruvchi ma’lumotlarni qayta ishlash markazlarida joylashtiriladi.

8. Tashkilotlarning shaxsga doir ma’lumotlar bazasi Shaxsga doir ma’lumotlar bazalarining davlat reestridan ro‘yxatdan o‘tkazilishi lozim.

9. Tashkilotlar axborotni shakllantirish, uzatish, saqlash va unga ishlov berishning barcha bosqichlarida konfidensial, bank sirini tashkil etuvchi va shaxsga doir ma’lumotlarni uzluksiz himoya qilish uchun quyidagi choralarni ko‘rishlari lozim:

identifikasiya, autentifikasiya va avtorizasiya qilish tizimini joriy etish;

tizimga ruxsatsiz kirishni oldini olish usullarini (login, parol, ko‘p faktorli autentifikasiya (MFA) va boshqa) qo‘llash;

ma'lumotlar bazasi administratorining paroli kamida 12 ta belgidan kam boʻlmasligi ta'minlashi, bunda parolning belgilari sifatida pastki va yuqori registr harflari, raqamlar va maxsus belgilarni (@,#, $, &, % va h.k.) qoʻllash;

hujjatlar va identifikasiya ma’lumotlarini qalbakilashtirish, ruxsatsiz koʻchirish, oʻzgartirish, oʻchirish hamda uchinchi shaxslarga taqdim etishdan himoyalash;

axborot tizimlaridagi dasturiy ta’minotlarning nazorati va hisobini yuritish hamda dasturiy ta’minot talqinlari, apparat-dasturiy qurilmalar va dasturiy vositalarning uzluksiz ishlashini ta’minlash;

axborot tizimlarini aktual holatda (oxirgi versiyada) boʻlishini ta’minlash, bunda dasturiy ta’minotning yangi talqinini tekshiruvdan oʻtkazgandan soʻng axborot tizimiga joriy etish;

korporativ tarmoqda ilova serverlari bilan foydalanuvchilar oʻzaro axborot almashinuvida himoyalangan protokol qoʻllanilishi lozim;

axborot tizimlarini asosiy va zaxira aloqa kanallari bilan ta’minlash;

serverlarda ish faoliyati uchun zarur boʻlmagan portlarni yopish va xizmatlarni toʻxtatish;

axborot tizimiga ruxsatsiz kirish yoki kiberxavfsizlik hodisalari sodir etilganda, ularni tahlil qilish asosida himoya tizimlarini mustahkamlab borish choralarini koʻrish;

axborot tizimiga boshqa tashkilotlarning axborot tizimlarini integratsiya qilishda yaratiladigan veb-servislar (WebAPI) metodlaridan foydalanishda ularga avtorizatsiyadan oʻtkazish jarayoni berilgan token orqali ishlashni yoʻlgan qoʻyish.

10. Platforma va AKT-infratuzilmasini masofadan turib boshqarishga asosli sabablar boʻlganda (texnik nosozliklarda, axborot tizimi va AKT-infratuzilmasida yangilash ishlar amalga oshirilganda, aniqlangan zaifliklarni bartaraf etishda) hamda tegishli koʻrinishda rasmiylashtirilgan va boshqa holatlarda axborot tizimiga masofadan ulanishni cheklaydi.

Bunda Tashkilotning axborot tizimlaridan imtiyozli foydalanish huquqiga ega foydalanuvchilarga (administratorlar) faqatgina himoyalangan IPSec tunel orqali masofadan ulanishga ruxsat beriladi.

11. Tashkilot axborot tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash uchun keyingi avlod tarmoqlararo ekranlar qurilmalarining apparat-dasturiy vositalarini joriy etishi lozim. Shuningdek, tarmoqdagi hujumlarni aniqlash, oldini olish va to‘sish uchun mo‘ljallangan tajovuslarni aniqlash va oldini olish tizimi (IDS/IPS) joriy etishi lozim.

12. Platformani boshqa tashkilotning axborot tizimiga integratsiya qilishda o‘zaro ma’lumot almashish uchun himoyalangan IPSec tunel orqali ulanish va u orqali ma’lumot almashinuvini yo‘lga qo‘yish lozim.

13. Tashkilot axborot tizimlarida faqat litsenziyalangan antivirus dasturidan foydalanish, ularning rusumlari va bazalari aktualligi hamda yangilanib borilishini ta’minlash uchun quyidagi choralarni amalga oshirish:

antivirus dasturlarining avtomatik tarzda ishlashini ta’minlash;

internet va korporativ tarmoqlar orqali kelgan axborotlarni antivirus dasturi orqali tekshirish.

14. Platformani amaliyotga joriy etishdan oldin ishlab chiqilgan (modernizatsiya qilingan) barcha funksiyalarini test-sinov ishlari uchun mo‘ljallangan serverlarda to‘liq tekshiruvdan o‘tkazish shart.

15. Axborot tiziminining uzluksiz va barqaror ishlashini ta’minlash maqsadida quyidagi choralar ko‘rilishi lozim:

axborot tizimi bilan bog‘liq tarmoq va boshqa qurilmalar nosoz holatga kelganda uni ish jarayoniga keltirish va uzluksiz ishlashini ta’minlash;

ma’lumotlarning zaxiraga olingan (backup) nusxalarini texnik nosozliklarda va favqulodda vaziyatlarda qayta tiklash rejasini ishlab chiqish;

operatsion tizimlar, dasturiy ta’minotlar, axborot tizimlarining dasturlari, ma’lumotlar (ma’lumotlar bazasi, sozlamalari, elektron bayonnomalar) nusxalarini zaxiraga (backup) olinishi va elektron arxivda

saqlash hamda ularni qayta tiklash tartibini (mexanizmini) ishlab chiqish, ularning hisobini yuritish va nazoratini olib borish.

16. Axborot tizimi ma’lumotlariga kirish, ishlov berish, ularni saqlash, taqdim etish jarayonini hamda AKT-infratuzilmasi, axborot tizimi administratori va foydalanuvchilarining harakatlari (IP-adres, MAC-adres) to‘g‘risidagi ma’lumotlar elektron bayonnomalarda (log-fayl) avtomatik tarzda shakllantirish hamda ushbu elektron bayonnomalarni kamida besh yil saqlanishini ta’minlash.

17. Platforma faoliyati tugatilganda unda mavjud elektron arxiv ma’lumotlari davlat arxivlariga topshiriladi.

18. Platforma faoliyati tugatilib, boshqa tashkilotga qo‘shib yuborilganda arxiv ma’lumotlar qo‘shib yuborilayotgan tashkilotning elektron arxiviga topshiriladi.

19. Platformani boshqa tashkilotlarning axborot tizimlari bilan integratsiya qilishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash talablariga muvofiq holda tashkil etilishi zarur.

20. Tashkilotlar Platforma foydalanuvchilari tomonidan firibgarlik holatlari yuzaga kelishini oldini olish bo‘yicha tashkiliy va texnik choralarini belgilashi hamda ularni nazorat qilishga majburdir.

21. Platforma va AKT-infratuzilmasini texnik qo‘llab-quvvatlash O‘zbekiston Respublikasi hududidan tashqaridagi autsorsing tashkilotlar xizmatiga berilmaydi.

22. Platforma hamda AKT-infratuzilmasida axborot xavfsizligi va kiberxavfsizlikni ta’minlash ishlari autsorsing tashkilotlar xizmatiga berilmaydi.

23. Tashkilotlar Markaziy bank bilan axborot almashinuvida axborot xavfsizligi va kiberxavfsizlikni ta’minlashi shart.

24. Tashkilotlar axborot tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlanganligi yuzasidan IT auditdan o‘tkazishi o‘tgan hisobot davri uchun keyingi yilning 1-yarim yilligiga qadar O‘zbekiston

Respublikasi hududida axborot xavfsizligi va kiberxavfsizlik boʻyicha auditdan oʻtkazish vakolatiga ega tashkilotlar tomonidan amalga oshiriladi. Audit natijalari hujjatlashtirilishi va kamida 5 yil davomida saqlanishi shart.

25. Tashkilotlar axborot tizimidagi axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bogʻliq hodisalar toʻgʻrisida Markaziy bankka zudlik bilan yozma yoki elektron shaklda xabar berishi lozim.

26. Tashkilotlar firibgarlik holatlari aniqlangan taqdirda bir kun muddatda tahlil qilingan toʻliq ma’lumotlarni tezkorlik bilan Markaziy bank “CERT-CBU” kiberxavfsizlik markaziga taqdim etishi lozim.

27. Mazkur hujjatda belgilangan talablarga rioya etilishi yuzasidan Markaziy bank tomonidan tekshiruvlar oʻtkaziladi.

4-BOB. YAKUNIY QOIDA

28. Mazkur hujjat talablarining buzilishida aybdor boʻlgan shaxslar qonunchilik hujjatlarida belgilangan tartibda javobgar boʻladi.