2026-yil “13” noyabr **№ 0003**

TASDIQLAYMAN
Boshqaruv raisi v.b.
F.X. Samadov

A X B O R O T X A V F S I Z L I G I S I Y O S A T I

“Navoiyazot” aksiyadorlik jamiyati

(ko‘chirma)

KELISHILGAN:
“O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi” — xulosa № 29-8/9456, sana 15.10.2026

KELISHILGAN:
“Kiberxavfsizlik markazi” DM — xulosa № 05-29-03/6269, sana 21.10.2026

Mazkur nashr Siyosatning ommaviy e’lon qilish uchun mo‘ljallangan ko‘chirmasi hisoblanadi. Himoya obyektlari, axborot xavfsizligi tahdidlari va risklari, buzg‘unchi modeli (8–10-bo‘limlar), shuningdek axborot-kommunikatsiya infratuzilmasi, qo‘riqlash tartibi va qo‘llaniladigan himoya vositalari tavsiflangan band va ilovalar e’lon qilinmaydi. Bo‘lim, band va ilovalar raqamlanishi Siyosat asl matniga muvofiq saqlangan; band ichida chiqarib tashlangan qismlar “[…]” belgisi bilan ko‘rsatilgan, ayrim bandlar umumlashtirilgan tahrirda keltirilgan.

1. Kirish

“Navoiyazot” aksiyadorlik jamiyati (keyingi o‘rinlarda – korxona) ishlab chiqarish korxonasi hisoblanadi.

Korxona xalqaro hamkor maqomiga ega bo‘lgan, dinamik rivojlanayotgan ko‘p tarmoqli sanoat-ishlab chiqarish majmuasi hisoblanadi. U mineral o‘g‘itlar, kimyoviy reaktivlar va boshqa kichik tonnajli kimyoviy mahsulotlar ishlab chiqarish faoliyatini amalga oshiradi.

O‘z faoliyatini amalga oshirayotganda O‘zbekiston Respublikasi Iqtisodiyot va moliya vazirligiga bo‘ysunadi va u yagona aksiyador hisoblanadi.

Korxona hisoblanadi:

- Qonunchilikka muvofiq himoya qilinishi kerak bo‘lgan ma’lumotni qayta ishlash uchun mo‘ljallangan axborotlashtirish obyektlariga ega ishlab chiqarish korxonasi;
- Konfidensial ma’lumotlarni qayta ishlash va davlat axborot tizimlari bilan integratsiya qilinuvchi korxona axborotlashtirish obyektlarining egasi;
- Muhim axborot infratuzilmasi subyekti (keyingi o‘rinlarda – MAI).

O‘z faoliyatini amalga oshirish uchun korxonada raqamli texnologiyalar asosida axborot-kommunikatsiya infratuzilmasi shakllantiriladi va rivojlantiriladi.

Korxona axborot xavfsizligini ta’minlash masalalarini hal etishda, korxonaning axborot-kommunikatsiya infratuzilmasining ishonchli va uzluksiz ishlashini hamda qonunchilikka muvofiq himoya qilinishi kerak bo‘lgan ma’lumotlar xavfsizligini ta’minlash uchun zarurdir.

Axborot xavfsizligi siyosati korxonada axborot xavfsizligini boshqarish tizimini (keyingi o‘rinlarda – AXBT) shakllantirish uchun asos bo‘lib xizmat qiladi. Ushbu Siyosat korxona o‘z faoliyatida amal qiladigan axborot xavfsizligini ta’minlash sohasidagi hujjatlashtirilgan yo‘naltiruvchi prinsiplar, qoidalar, tartib-taomillar va amaliy usullar majmuasini ifodalaydi.

2. Me’yoriy hujjatlarga havolalar

1. Ushbu Siyosatda quyidagi hujjatlarga havolalar ishlatilgan:

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

2) O‘zbekiston Respublikasining 2004 yil 29 apreldagi “Elektron hujjat aylanishi to‘g‘risida”gi 611-II - sonli Qonuni;

3) O‘zbekiston Respublikasining 2014 yil 11 sentyabrdagi “Tijorat siri to‘g‘risida”gi 374-sonli Qonuni;

4) O‘zbekiston Respublikasining 2019 yil 2 iyuldagi “Shaxsga doir ma’lumotlar to‘g‘risida”gi 547-sonli Qonuni;

5) O‘zbekiston Respublikasining 2022 yil 15 apreldagi “Kiberxavfsizlik to‘g‘risida”gi 764-sonli Qonuni;

6) O‘zbekiston Respublikasining 2022-yil 29-sentabrdagi “Elektron tijorat to‘g‘risida”gi 792-sonli Qonuni;

7) O‘zbekiston Respublikasining 2022-yil 12-oktyabrdagi “Elektron raqamli imzo to‘g‘risida”gi 793-sonli Qonuni;

8) 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;

9) 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;

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

11) 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;

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

13) 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;

14) O‘zbekiston Respublikasi Prezidentining 2022-yil 22-avgustdagi “2022-2023-yillarda axborot-kommunikatsiya texnologiyalari sohasini yangi bosqichga ko‘tarish chora-tadbirlari to‘g‘risida”gi PQ-357-son Qarori;

15) 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;

16) O‘zbekiston Respublikasi Prezidentining 27.01.2025 yildagi “O‘zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi “O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida”gi PQ-614-son qaroriga o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi PQ-30-son qarori;

17) 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 VMQ-137-sonli Qarori;

18) O‘zbekiston Respublikasi Vazirlar Mahkamasining 2005 yil 22 noyabrdagi “Axborotlashtirish sohasidagi normativ-huquqiy bazani takomillashtirish to‘g‘risida”gi 256-son qarori;

19) 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 VMQ-126-sonli Qarori;

20) 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 VMQ-296-sonli Qarori;

21) 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 VMQ-295-sonli Qarori;

22) 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 VMQ-365-sonli Qarori;

23) 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” VMQ-930-sonli Qarori;

24) O‘zbekiston Respublikasi Vazirlar Mahkamasining 2021 yil 15 iyundagi “Raqamli iqtisodiyot va elektron hukumatning rivojlanish holatini reyting baholash tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida” VMQ-373-sonli Qarori;

25) O‘zbekiston Respublikasi Vazirlar Mahkamasining 2020 yil 8 fevraldagi “Shaxsga doir ma’lumotlar bazalarining davlat reyestrini yuritish bo‘yicha davlat xizmatini ko‘rsatishning ma’muriy reglamentini tasdiqlash to‘g‘risida”gi VMQ-71-sonli Qarori;

26) 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 VMQ-570-sonli Qarori;

27) O‘zbekiston Respublikasi Vazirlar Mahkamasining 2024 yil 24 oktyabrdagi “Davlat organlari va korxonalari xodimlari tomonidan “Lochin” kommunikatsiya platformasidan foydalanish tartibi to‘g‘risidagi nizomni tasdiqlash haqida”gi VMQ-699-son Qarori;

28) O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025 yil 4 dekabrdagi “Xizmat doirasida foydalanish uchun grifli hujjatlar bilan ishlash tartibini takomillashtirish to‘g‘risida”gi VMQ-766-son Qarori;

29) 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”gi 91-son Buyrug‘i;

30) 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;

31) 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;

32) O‘zbekiston Respublikasi Adliya vazirligida 2024-yil 14-noyabrda 3573-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati raisining 2024-yil 15-oktabrdagi “Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish tartibi to‘g‘risidagi nizomni tasdiqlash haqida”gi 113-son Buyrug‘i;

33) O‘zbekiston Respublikasi Adliya vazirligida 2024-yil 14-noyabrdagi 3574-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati Raisining 2024-yil 15-oktyabrdagi “Axborot tizimlari va resurslarining kiberxavfsizligini ta’minlash uchun qo‘llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirish tartibi to‘g‘risidagi nizomni tasdiqlash haqida”gi 114-son Buyrug‘i;

34) O‘zbekiston Respublikasi Adliya vazirligida 2024-yil 11-noyabrdagi 3570-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati Raisining 2024-yil 24-oktyabrdagi “O‘zbekiston Respublikasi muhim axborot infratuzilmasi obyektlarining toifalash va ularning yagona reestrini shakllantirish tatibi to’g’risida”gi 118-son Buyrug‘i;

35) O‘zbekiston Respublikasi Bosh vaziri o‘rinbosari — davlat sirlarini muhofaza qilish masalalari bo‘yicha idoralararo komissiya raisi tomonidan 2006 yil 5 dekabrda tasdiqlangan “Maxfiy bo‘lmagan, tarqatilishi cheklangan ma’lumotlarga ega hujjatlar, fayllar va nashrlarni ro‘yxatga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnoma”;

36) O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi hamda davlat va xo‘jalik boshqaruvi organlari o‘rtasida axborot xavfsizligi hodisalariga javob berish, ularni tekshirish va oldini olish bo‘yicha hamkorlik reglamenti (O‘zbekiston Respublikasi axborot-kommunikatsiya xavfsizligi masalalari bo‘yicha Texnik kengashining 2017 yil 17 noyabrdagi 7-sonli bayonnomasiga 1-ilova);

37) O‘zMSt 841:2026 Axborot texnologiyasi. Kiberxavfsizlik. Amaliy dasturiy ta’minot. Talablar;

38) O‘zMSt 840:2026 Axborot texnologiyalari. Kiberxavfsizlik. Axborotni muhofaza qilish vositalari. Tasniflash va umumiy texnik talablar;

39) O‘zMSt 839:2026 Axborot texnologiyasi. Kiberxavfsizlik. Zararli dasturlardan muhofaza qilish dasturiy vositalari. Talablar;

40) O‘zMSt 838:2026 Axborot texnologiyasi. Kiberxavfsizlik. Bostirib kirishlarni aniqlash va oldini olish tizimlarining dasturiy ta’minoti. Talablar;

41) O‘zMSt 816:2025 Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni himoya qilish. Axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha qo‘llanma;

42) O‘zMSt 810:2025 Axborot texnologiyasi. Kiberxavfsizlik. Axborotlarni chiqib ketishining oldini olish tizimining dasturiy ta’minoti. Talablar;

43) O‘zMSt 605:2025 Axborot texnologiyasi. Atamalar va ta’riflar;

44) O‘zMSt 522:2025 Axborot texnologiyasi. Axborotni kriptografik himoyalash Atamalar va ta’riflar;

45) O‘zMSt 286:2024 “Axborot texnologiyalari. Axborotni kriptografik himoya qilish. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari”;

46) O‘zMSt 285:2024 Axborot texnologiyalari. Axborotni kriptografik himoya qilish. Xesh funksiyasi;

47) O‘zMSt 270:2024 Axborot texnologiyasi. Axborotni kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi;

48) O‘zMSt 149:2024 Axborot texnologiyasi. Elektron davlat xizmatlari. Axborot xavfsizligini ta’minlashga qo‘yiladigan umumiy talablar;

49) O‘z DSt 1204:2009 Axborot texnologiyasi. Axborotni kriptografik muhofazasi. Kriptografik modullarga xavfsizlik talablari;

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

51) O‘z DSt 2814:2014 Axborot texnologiyasi. Avtomatlashtirilgan tizimlar. Axborotdan ruxsatsiz foydalana olishdan himoyalanganlik darajalari bo‘yicha tasniflash;

52) O‘z DSt 2815:2014 Axborot texnologiyasi. Tarmoqlararo ekranlar. Axborotdan ruxsatsiz foydalana olishdan himoyalanganlik darajalari bo‘yicha tasniflash;

53) 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;

54) O‘z DSt 2817:2014 Axborot texnologiyasi. Hisoblash texnikasi vositalari. Axborotdan ruxsatsiz foydalana olishdan himoyalanganlik darajalari bo‘yicha tasniflash;

55) O‘z DSt 2875:2014 Datamarkazlar uchun talablar. Infratuzilma va axborot xavfsizligini ta’minlash standartidagi telekommunikatsiya obyektlari infratuzilmasining tayyorligi va xavfsizligini ta’minlash;

56) O‘z DSt 2927:2015 Axborot texnologiyalari. Axborot xavfsizligi. Atamalar va ta’riflar

57) O‘z DSt 3078:2016 Telekommunikatsiyalar tarmoqlari. Virtual xususiy tarmoqlar (VPN). Umumiy talablar;

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

59) O‘z DSt 3361:2019 Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Hodisalarni tekshirish usulining yaroqliligi va yetarliligini ta’minlash bo‘yicha qo‘llanma;

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

61) 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-qism.

Insidentlarga ta’sir etishni rejalashtirish va unga tayyorlanish bo‘yicha rahbariy ko‘rsatmalar;

62) O‘z DSt ISO/IEC 27000:2025 (ISO/IEC 27000:2018, IDT) Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Sharh va lug‘at;

63) O‘zMSt ISO/IEC 27001:2024 (ISO/IEC 27001:2022, IDT) Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni himoya qilish. Axborot xavfsizlik boshqarish tizimlari. Talablar;

64) O‘zMSt ISO/IEC 27002:2024 (ISO/IEC 27002:2022, IDT) Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni himoya qilish. Axborot xavfsizligini boshqarish vositalari;

65) O‘zMSt ISO/IEC 27005:2024 (ISO/IEC 27005:2022, IDT) Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni himoya qilish. Axborot xavfsizligi risklarini boshqarish bo’yicha qo’llanma;

66) O‘z DSt ISO/IEC 27007:2025 (ISO/IEC 27007:2020, IDT) Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni muhofaza qilish. Axborot xavfsizligini boshqarish tizimlarini audit qilish bo‘yicha rahbariy ko‘rsatmalar;

67) O‘z DSt ISO/IEC 27011:2025 (ISO/IEC 27011:2024, IDT) Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni himoya qilish. ISO/IEC 27002 standarti asosida telekommunikatsiya korxonalari uchun axborot xavfsizligini boshqarish vositalari;

68) O‘z MSt ISO/IEC 27014:2024 (ISO/IEC 27014:2020, IDT) Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni muhofaza qilish. Axborot xavfsizligini boshqarish;

69) O‘zMSt ISO/IEC 27042:2025 (ISO/IEC 27042:2015, IDT) Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Raqamli dalillarni tahlil qilish va talqin etish bo‘yicha yo‘riqnomalar;

70) O‘zMSt ISO/IEC 27043:2025 (ISO/IEC 27043:2015, IDT) Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Insidentlarni tekshiruv o‘tkazish tamoyillari va jarayonlari;

71) O‘z DSt ISO/IEC 9594-8:2018 Axborot texnologiyalari. Ochiq tizimlar o‘zaro bog‘liqligi. 8-qismi. Ochiq kalit sertifikati va atributlar tuzilmasi;

72) O‘z DSt ISO/IEC 11770-1:2017 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Kalitlarni boshqarish. 1-qism. Asosiy qoidalar;

73) O‘z DSt ISO/IEC 27003:2022 (ISO/IEC 27003:2017, IDT) Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimini joriy etish bo‘yicha qo‘llanma;

74) O‘z DSt ISO/IEC 27004:2022 (ISO/IEC 27004:2016, IDT) Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish. Monitoring, o‘lchash, tahlil qilish va baholash;

75) O‘z DSt ISO/IEC 27006:2013 Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlarini audit va sertifikatlash organlariga qo‘yiladigan talablar;

76) O‘z DSt ISO/IEC 27008:2022 (ISO/IEC TS 27008:2019, IDT) Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish bo‘yicha auditorlar uchun qo‘llanma;

77) O‘z DSt ISO/IEC 27010:2015 Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Sohalararo va korxonalararo kommunikatsiyalarda axborot xavfsizligini boshqarish bo‘yicha qo‘llanma;

78) 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;

79) O‘z DSt ISO/IEC 27032:2017 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Kiberxavfsizlik bo‘yicha rahbariy ko‘rsatmalar;

80) O‘z DSt ISO/IEC 27033-1:2016 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 1-qism;

81) 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;

82) O‘z DSt ISO/IEC 27033-3:2016 Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 3-qism. Standart tarmoq senariylari. Tahdidlar, loyihalashtirish usullari va boshqaruv masalalari;

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

84) 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;

85) O‘z DSt ISO/IEC 27033-6:2018 Axborot texnologiyalari. Xavfsizlik usullari. Tarmoq xavfsizligi. 6-qism: Simsiz IP tarmog‘iga xavfsiz kirish;

86) O‘z DSt ISO/IES 27037:2017 Axborot texnologiyalari. Xavfsizlik usullari. Raqamli dalillarni aniqlash, to‘plash, olish va saqlash bo‘yicha ko‘rsatmalar;

87) O‘z DSt ISO/IEC 27039:2017 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Bostirib kirishlarni aniqlash va oldini olish tizimlarini tanlash, qo‘llash va operatsiyalari;

88) O‘z DSt ISO/IEC 27040:2018 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Ma‘lumotlami saqlash xavfsizligi.

3. Atamalar va ta’riflar

2. Ushbu hujjatda quyidagi davlat standartlariga muvofiq atamalar qo‘llanilgan: O‘z DSt 2927:2015 “Axborot xavfsizligi. Atamalar va ta’riflar”, O‘zMSt 605:2025 “Axborot texnologiyasi. Atamalar va ta’riflar” hamda O‘zMSt 522:2025 “Axborot texnologiyasi. Axborotni kriptografik himoyalash. Atamalar va ta’riflar”. Shuningdek, hujjat matnida quyidagi tegishli ta’riflarga ega bo‘lgan atamalar ham uchraydi:

1) risklar tahlili: ma’lumotlarni qayta ishlash tizimi resurslarini, ushbu resurslarga tahdidlarni va tizimning bu tahdidlarga nisbatan zaifliklarini aniqlash bo‘yicha tartibga solingan protseduralarni tizimli ravishda bajarish;

2) ma’lumotlar bazasi: ma’lumotlarni saqlash, tavsiflash va ularni dasturiy vositalardan mustaqil ravishda boshqarishning umumiy tamoyillarini nazarda tutgan holda belgilangan qoidalarga binoan tashkil etilgan ma’lumotlar majmuasi;

3) buzuvchi (yovuz niyatli shaxs): axborot tizimi va uning resurslariga ruxsatsiz kirishni qo‘lga kiritishga qiziqqan va bunga erishish yoki axborotni o‘zgartirish maqsadida ataylab harakat qilgan shaxs yoki korxona;

4) axborot resursi: alohida hujjatlar, hujjatlar majmuasi, axborot tizimidagi hujjatlar va hujjatlar majmualari (kutubxonalar, arxivlar, fondlar, ma’lumotlar bazalari va boshqalar);

5) axborot tizimi: axborotni yig‘ish, saqlash, qidirish, qayta ishlash va undan foydalanishni ta’minlovchi axborot resurslari, axborot texnologiyalari va aloqa vositalarining tashkiliy ravishda tartibga solingan majmuasi;

6) axborot xavfsizligi insidenti: himoyalanayotgan axborotning oshkor bo‘lish xavfi yoki axborot xavfsizligiga tahdid yuzaga kelishi ehtimolini keltirib chiqaruvchi yagona yoki bir qator istalmagan yoki kutilmagan axborot xavfsizligi voqealari;

7) tijorat siri: uchinchi shaxslarga noma’lumligi bois ilmiy-texnik, texnologik, ishlab chiqarish, moliyaviy-iqtisodiy va boshqa sohalarda tijorat qiymatiga ega bo‘lgan, qonuniy asosda erkin foydalanish imkoniyati bo‘lmagan va egasi uning konfidensialligini ta’minlash choralarini ko‘radigan axborot;

8) nazorat qilinadigan zona: doimiy yoki bir martalik ruxsati bo‘lmagan shaxslar va transport vositalarining nazoratsiz kirishi istisno qilingan makon (hudud, bino, binoning bir qismi).

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

- korxonaning nazorat qilinadigan hududining perimetri;

- agar binoning o‘zi nazorat qilinmaydigan hududda joylashgan bo‘lsa, himoyalanadigan bino yoki binoning himoyalanadigan qismidagi to‘sqinlik konstruktsiyalari;

9) konfidensial ma’lumot: davlat sirlarini tashkil etuvchi ma’lumotlarni o‘z ichiga olmagan, foydalanishi qonun hujjatlariga muvofiq cheklangan hujjatlashtirilgan ma’lumotlar;

10) ruxsatsiz kirish: subyektning obyektga yoki ma’lumotga tizimda o‘rnatilgan kirishni cheklash qoidalariga zid ravishda kirishi;

11) axborotlashtirish obyekti: turli daraja va tayyorgarlikdagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotni qayta ishlash texnik vositalari, ushbu vositalar o‘rnatilgan va ishlatiladigan joylar hamda shu jumladan, konfidensial bo‘lgan muzokaralar olib borish uchun mo‘ljallangan alohida xonalar;

12) muhim axborot infratuzilmasi obyektlari: davlat boshqaruvi va davlat xizmatlari ko‘rsatish, mudofaa, davlat xavfsizligini, huquq-tartibotni ta’minlash, yoqilg‘i-energetika majmui (atom energetikasi), kimyo, neft-kimyo tarmoqlari, metallurgiya, suvdan foydalanish va suv ta’minoti, qishloq xo‘jaligi, sog‘liqni saqlash, uy-joy kommunal xizmatlar ko‘rsatish, bank-moliya tizimi, transport, axborot-kommunikatsiya texnologiyalari, ekologiya va atrof-muhitni muhofaza qilish, strategik ahamiyatiga ega bo‘lgan foydali qazilmalarni qazib olish va qayta ishlash sohasida, ishlab chiqarish sohasida, shuningdek iqtisodiyotning boshqa tarmoqlarida va ijtimoiy sohada qo‘llaniladigan axborotlashtirish tizimlari;

13) risklarni baholash: hisoblangan risk va risk mezonlarini taqqoslash jarayoni, uning qiymatini aniqlash maqsadida bajariladi;

14) shaxsga doir ma’lumotlar: fuqaroning shaxsini aniqlash imkonini beruvchi hayoti haqidagi faktlar, voqealar va holatlar haqidagi ma’lumotlar;

15) dasturiy ta’minot: axborotni qayta ishlash tizimining dasturlari va ushbu dasturlarni ishlatish uchun zarur bo‘lgan dasturiy hujjatlar majmui;

16) risk: axborotni qayta ishlash tizimining ma’lum bir zaifligini ma’lum bir tahdidni amalga oshirish uchun ishlatish imkoniyati;

17) Domen nazorati serveri: foydalanuvchilarni markazlashtirilgan autentifikatsiya va avtorizatsiyasini hamda domen tarmog‘i resurslarini boshqarishni ta’minlaydigan server.

18) axborot xavfsizligini boshqarish tizimi: biznes-risklarni baholash usullaridan foydalanishga asoslangan umumiy boshqaruv tizimining qismi bo‘lib, axborot xavfsizligini ishlab chiqish, joriy etish, ishlash, monitoring qilish, tahlil qilish, xizmat ko‘rsatish va takomillashtirish uchun mo‘ljallangan;

19) axborotni himoya vositalari: axborotni himoya qilish uchun mo‘ljallangan texnik, kriptografik va boshqa vositalar, shu jumladan axborotni himoya samaradorligini nazorat qilish vositalari;

20) tahdid: kompyuter xavfsizligining buzilishi uchun potensial imkoniyat;

21) zaiflik: axborotni qayta ishlash tizimidagi kamchilik, undan foydalanish tizimning yaxlitligini buzish va noto‘g‘ri ishlashiga olib kelishi mumkin.

4. Belgilar va qisqartmalar

3. Mazkur Siyosatda quyidagi belgilar va qisqartmalar qo‘llanilgan:

CRM (Customer Relationship Management) – Mijozlar bilan o‘zaro munosabatlarni boshqarish tizimi;

DMZ (Demilitarized Zone) – Demilitarizatsiya qilingan zona;

EDR (Endpoint Detection and Response) – Oxirgi qurilmalarda tahdidlarni aniqlash, tahlil qilish, javob berish va bartaraf etish tizimi;

HIPS (Host-based Intrusion Prevention System) – Bostirib kirishni oldini olish tizimi.

IDPS (Intrusion Detection & Prevention System) – bostirib kirishni aniqlash va oldini olish vositalari (tizimi);

DLP (Data Leak Prevention) – Ma’lumotlarni ruxsatsiz chiqib ketishini oldini olish tizimi;

NVR (Network Video Recorder) – tarmoq videoregistratori;

PAM (Privileged Account Management) – Imtiyozli foydalanuvchilarni boshqarish tizimi

SIEM (Security Information and Event Management) – axborot xavfsizligi insidentlarini monitoring qilish va boshqarish tizimi;

VLAN (Virtual Local Area Network) – virtual lokal kompyuter tarmog‘i;

VMS (Video Management System) – videoni boshqarish tizimi;

VPN (Virtual Private Network) – virtual shaxsiy tarmoq;

WAF – veb-ilovalarda tarmoqlararo ekran;

IChBAT– ishlab chiqarishni boshqarish avtomatlashtirilgan tizimi;

TJBAT – texnologik jarayonlarni boshqarish avtomatlashtirilgan tizimi;

OTAL – optik tolali aloqa liniyasi;

MAI – muhim axborot infratuzilma;

IIP – idoralararo integratsiyalashuv platformasi;

IMUT – idoralararo ma’lumot uzatish tarmog‘i;

AKHV – ma’lumotlarni kriptografik himoya vositasi;

KBNT – kirishni boshqarish va nazorat qilish tizimi;

AXBT – axborot xavfsizligini boshqarish tizimi;

MBBT – ma’lumotlar bazasini boshqarish tizimi;

EHAT – elektron hujjat aylanish tizimi;

MQIM – ma’lumotlarni qayta ishlash markazi;

MBP – markaziy boshqaruv pulti;

ERI – elektron raqamli imzo;

5. Amal qilish sohasi

4. Ushbu Siyosat talablarining amal qilinishi korxonaning barcha himoyalanadigan ma’lumotiga hamda ushbu ma’lumotni yaratish, qayta ishlash, saqlash, uzatish, himoya qilish va yo‘q qilish vositalariga taalluqlidir, davlat siri hisoblanadigan ma’lumotlar bundan mustasno. Davlat siri hisoblanadigan ma’lumotlarning himoyasi qonunchilikka muvofiq ta’minlanadi.

5. Ushbu Siyosatning amal qilinishi korxona tarkibiy tuzilmasiga kiruvchi quyidagi obyektlarga taalluqlidir:

1) Korxona barcha boshqaruv ijro organiga;

2) Korxona tashkiliy tuzilmasining barcha ishlab chiqarish, sexlar, boshqarmalar, bo‘limlar va bo‘linmalari.

6. Ushbu Siyosatning talablaridan quyidagilarga majburiy tarzda amal qiladi:

- Korxonaning barcha axborot tizimlari va resurslari, shuningdek boshqa axborortlashtirish obyektlari, jumladan korxona tasarrufidagi korxonaning MAI obyekti;

- Korxonaning barcha xodimlari (shtatda, vaqtinchalik, shartnoma asosida ishlovchi va boshqalar);

- uchinchi shaxslar, korxona bilan o‘zaro aloqada bo‘lgan (ta’minotchilar, pudratchilar, mijozlar, auditorlar, tashrif buyuruvchilar, xizmat ko‘rsatuvchi xodimlar va hokazo) shu va boshqa turli sabablar bilan korxonaning binolari va himoya obyektlariga axborot resurslari va tizimlariga qonuniy kirish huquqiga ega bo‘lgan shaxslar.

7. Korxonaning tuzilmaviy bo‘linma rahbarlari, shuningdek korxonaning Axborot xavfsizligi bo‘yicha mutaxassislari mazkur Siyosat talablarining bajarilishini muntazam nazorat qilinishini ta’minlashlari shart.

6. Maqsad va vazifalar

8. Korxonaning axborot xavfsizligi sohasidagi maqsadlari:

1) Korxonaning axborot munosabatlar subyektlari yoki Korxona xizmatlaridan foydalanuvchilarni axborot xavfsizligi tahdidlarining tasodifiy yoki qasddan ta’siri orqali ularga moddiy, jismoniy, ma’naviy yoki boshqa turdagi zarar yetkazilishidan himoya qilish;

2) Korxonaning axborot resurslari va ma’lumotlarining konfidensialligi, yaxlitligi hamda foydalanish imkoniyatini saqlash;

3) axborot xavfsizligini ta’minlash bo‘yicha qonunchilik va me’yoriy hujjatlar talablariga rioya etish;

4) Axborot munosabatlari subyektlarining yoki korxona foydalanuvchilarining shaxsga doir ma’lumotlari yoki boshqa kirish huquqiga cheklangan konfidensial ma’lumotlarning oshkor etilmasligi bo‘yicha qonuniy huquqlarini himoya qilish;

5) Korxonaning axborotlashtirish obyektlarini axborot xavfsizligi tahdidlaridan himoya qilish orqali ularning barqaror va ishonchli ishlashini ta’minlanishi, korxonaning o‘z faoliyatini muvaffaqiyatli va uzluksiz amalga oshirishiga xizmat qiladi;

6) Korxonaning MAI obyektini axborot xavfsizligi tahdidlaridan himoya qilish, shu orqali korxonaning ishlab chiqarish faoliyati va texnologik jarayonlarini uzluksiz va barqaror amalga oshirilishini ta’minlash.

9. Korxonada axborot xavfsizligining maqsadlariga erishishda axborot xavfsizligi vazifalari:

1) Korxonada Axborot xavfsizligini boshqarish tizimini (AXBT) tashkil etish va rivojlantirish, korxona Nizomi (Ustav), qonunchilik, milliy standartlar hamda O‘zbekiston Respublikasining boshqa me’yoriy hujjatlar talablariga muvofiq;

2) Axborotlashtirish obyektlari va himoyalanadigan ma’lumotlarni turli tahdidlardan himoya qilish, shuningdek, axborot xavfsizligi risklarini kamaytirish maqsadida samarali boshqaruv usullari va vositalarini joriy etish;

3) Axborot xavfsizligi tahdidlarini o‘z vaqtida aniqlash va bartaraf etish maqsadida himoyalanish holatini doimiy nazorat qilishni ta’minlash;

4) Axborot xavfsizligi tahdidlariga tezkor javob berish mexanizmi va sharoitlarini yaratish;

5) Korxonada axborot xavfsizligi sohasidagi mutaxassislar malakasini oshirish, xodimlarning xabardorlik darajasini oshirish va ularni axborot xavfsizligini boshqarish jarayonlariga jalb qilish;

6) Ma’lumotlarni qayta ishlash jarayonida xodimlarning axborotni himoya qilish talablariga rioya qilishini nazorat qilish;

7) Korxonaning axborotlashtirish obyektlari va MAI obyektining himoyalanish darajasini oshirish hamda ishonchli faoliyatini ta’minlash.

7. Axborot xavfsizligini ta’minlash tamoyillari

10. Axborot xavfsizligi siyosati axborot xavfsizligini ta’minlashning quyidagi asosiy tamoyillariga asoslanadi:

1) qonuniylik – axborot xavfsizligini ta’minlashda qonunchilik va me’yoriy hujjatlar talablariga rioya qilish;

2) jalb etilganlik – rahbariyat va barcha xodimlarning axborot xavfsizligini boshqarish jarayonlarida ishtiroki;

3) vazifalarni ajratish – xodimlar o‘rtasida axborot xavfsizligini ta’minlash masalalaridagi rollar va javobgarlikni aniq taqsimlash;

4) shaxsiy javobgarlik –xodimlarning shaxsiy javobgarligini belgilash va uni mehnat shartnomalarida, lavozim yo‘riqnomalarida, shuningdek kontragentlar bilan tuziladigan shartnomalar (bitimlar)da mustahkamlash;

5) professionallik – axborot xavfsizligini ta’minlash uchun mas’ul bo‘lgan xodimlarning bilim darajasini doimiy ravishda oshirish va uni axborot xavfsizligini boshqarish jarayonlarida qo‘llash;

6) o‘zaro hamkorlik va harakatlarning muvofiqligi – axborot xavfsizligini ta’minlashga doir harakatlar manfaatdor tarkibiy bo‘linmalar o‘rtasidagi aniq o‘zaro hamkorlik asosida amalga oshirilishi va maqsadlar, vazifalar, tamoyillar, usullar va vositalar bo‘yicha o‘zaro muvofiqlashtirilgan bo‘lishi kerak;

7) iqtisodiy maqsadga muvofiqlik – axborot xavfsizligini ta’minlash choralarini amalga oshirish xarajatlari, axborot xavfsizligi tahdidlarining yuzaga kelish ehtimoli va tahdid yuzaga kelgan taqdirda mumkin bo‘lgan yo‘qotishlar hajmini inobatga olgan holda tanlash;

8) kuchaytirilgan himoya – axborot xavfsizligi tahdidlaridan samarali himoya qiluvchi axborot xavfsizligi choralarni belgilash;

9) tizimli yondashuv – AXBTni shakllantirishda axborot xavfsizligini ta’minlash muammosini tushunish va hal etish uchun muhim bo‘lgan barcha o‘zaro bog‘liq, o‘zaro ta’sir qiluvchi va vaqt o‘tishi bilan o‘zgaruvchi elementlar, shart-sharoitlar va omillar inobatga olinishi kerak;

10) komplekslik – himoya qilishning turli usul va vositalaridan foydalanilishi, ular birgalikda himoyaning yaxlit tizimini tashkil qilishi va “Navoiyazot” AJning barcha himoyalanadigan obyektlari uchun pog‘onali himoyani ta’minlashi kerak;

11) himoyaning uzluksizligi – “Navoiyazot” AJda axborot xavfsizligini boshqarish jarayonlari vaqt bo‘yicha doimiy bo‘lishi kerak;

12) ko‘p darajali himoya – axborot xavfsizligini boshqarish jarayonlari “Navoiyazot” AJning barcha darajalari va bo‘g‘inlarida amalga oshirilishi kerak;

13) harakatlar ustidan nazorat va hisob – xodimlar tomonidan axborot xavfsizligi talablariga rioya qilinishini nazorat qilish va axborot tizimlaridagi barcha harakatlarini hisobga olish.

11. Axborot xavfsizligini ta’minlash choralari

28. Korxonada kompleks axborot xavfsizligini boshqarish tizimini (AXBT) yaratish uchun barcha axborot xavfsizligini ta’minlash choralari amalga oshiriladi, ular quyidagilarga bo‘linadi:

- normativ-huquqiy choralar;
- Axloqiy-etik himoya choralari;
- tashkiliy choralar;
- muhandislik-texnik choralar;
- texnik choralar;
- dasturiy-texnik choralar;
- tashqi korxonalar va foydalanuvchilarga nisbatan xavfsizlik choralari.

11.1. Normativ-huquqiy choralar

29. Korxonada normativ hujjatlar bilan ta’minlash choralari axborot xavfsizligini boshqarishda ularga asos bo‘lib xizmat qiluvchi normativ hujjatlar bazasini shakllantirishga qaratilgan.

30. Axborot xavfsizligini boshqarish bo‘yicha normativ hujjatlar bazasi Korxonada alohida shakllantiriladi va Korxona xodimlari uchun majburiy hisoblanadi.

31. Korxonaning axborot xavfsizligini boshqarish bo‘yicha normativ hujjatlar bazasi normativ-huquqiy va normativ hujjatlar, jumladan O‘zbekiston Respublikasi milliy standartlari shuningdek, axborot xavfsizligini ta’minlash masalalarini tartibga soluvchi korxonaning ichki hujjatlarini o‘z ichiga oladi.

32. Korxonaning normativ hujjatlar bazasi korxonaning Avtomatik boshqarish tizimi tomonidan shakllantiriladi va yuritiladi.

33. Ko‘rsatilgan bo‘linmalar quyidagilarni ta’minlashi lozim:

- Ichki hujjatlarni ishlab chiqish;
- Ichki hujjatlarni normativ-huquqiy hujjatlar va normativ talablarga, amaldagi tashkiliy, texnologik va axborot infratuzilmasiga muvofiqligini yangilash, ularning talab, usul va protseduralar samaradorligini baholash;
- Ichki hujjatlarga o‘zgartirish va qo‘shimchalar kiritish;
- Ichki hujjatlarni amaliyotga joriy etish – ichki hujjat talablari bajarilishini ta’minlash choralarini ishlab chiqish va qabul qilish;
- Ichki hujjatlarning talablari bilan struktura bo‘limlari, xodimlar, tashqi foydalanuvchilar yoki qiziqish bildirgan tashqi korxonalarni tanishtirish va ularni xabardor qilish;
- Ichki hujjat talablariga rioya etilishini nazorat qilish (monitoring qilish).

34. Korxonada normativ hujjatlar bazasi elektron va qog‘oz shaklida yuritiladi.

35. Korxona tomonidan ishlab chiqiladigan axborot xavfsizligi bo‘yicha ichki hujjatlar korxonaning mas’ul rahbari bilan kelishilishi lozim.

Korxonaning axborot xavfsizligi sohasidagi ichki hujjatlari quyidagi darajadagi hujjatlardan iborat:

1) asosiy hujjat – Korxonaning Axborot xavfsizligi siyosati.

2) himoya obyektlarini belgilovchi va tasniflovchi hujjatlar (ro‘yxatlar va tasniflar).

3) vazifalar va javobgarlikni taqsimlovchi hujjatlar (tuzilmaviy bo‘linmalar nizomlari, lavozim yo‘riqnomalari.

4) axborot xavfsizligini boshqarish jarayonlari va protseduralarini tartibga soluvchi hujjatlar (nizomlar, tartiblar, qoidalar, reglamentlar, yo‘riqnomalar, metodikalar).

5) axborot xavfsizligi choralarini amalga oshirishga yo‘naltirilgan tashkiliy va taqsimlovchi hujjatlari (buyruqlar, topshiriqlar, rejalar).

6) himoya obyektlari va vositalariga qo‘yiladigan talablarni belgilovchi hujjatlar (talablar, texnik topshiriqlar, loyihalar).

7) foydalanish hujjatlari (qo‘llanmalar, foydalanish bo‘yicha yo‘riqnomalar).

8) axborot xavfsizligini ta’minlash bo‘yicha amalga oshirilgan jarayon va ishlarni qayd etish va tasdiqlash uchun ishlatiladigan hujjatlar (ish shakllari, jurnallar, hisobotlar, arizalar, bayonnomalar, aktlar).

37. Korxona xodimlari uchun axborot xavfsizligi bo‘yicha ichki hujjatlarning talablariga rioya qilinishi majburiydir.

Axborot xavfsizligi bo‘yicha ichki normativ hujjatlarning alohida turlari mazkur Siyosat ilovalarida keltirilgan.

11.2. Axloqiy-etik himoya choralari

38. Axloqiy-etik himoya choralar quyidagi maqsadlarni ko‘zlaydi:

- xodimlar tomonidan axborot xavfsizligi masalalariga mas’uliyatli va vijdonan yondashishni rag‘batlantirish va ularga amal qilishni ta’minlash;
- inson omili bilan bog‘liq salbiy harakatlar va axborot xavfsizligini buzish ehtimolini kamaytirish;
- ma’lumotlarni himoya qilish tartibini buzishda shaxsiy psixologik omillarning ta’sirini istisno qilish.

39. Axloqiy-etik himoya choralariga quyidagilar kiradi:

- axborot xavfsizligi sohasida xodimlarning axloqiy-etik, xulq-atvor qoidalarini belgilash;

- xodimlarning xulq-atvori bo‘yicha tushuntirish ishlarini olib borish;

- jamoada psixologik tendensiyalar, qonuniyatlar yoki o‘zgarishlarni aniqlash, shuningdek axborot xavfsizligini ta’minlash normalari va qoidalariga rioya qilmaslikning psixologik sabablarini baholash maqsadida psixologik monitoring o‘tkazish.

Mazkur choralar axborot xavfsizligi administratorlari tomonidan amalga oshiriladi.

40. Korxona xodimlari tomonidan huquqbuzarliklarning oldini olish, ularning sodir etilishiga sabab bo‘luvchi omillar va shart-sharoitlarni bartaraf etish maqsadida Korxona rahbariyati tomonidan belgilangan xodimlarning axloqiy xulq-atvor kodeksiga rioya qilinishi lozim.

Korxona xodimlari uchun alohida normalar va qoidalar mazkur Siyosat ilovasidagi hujjatlarda belgilangan bo‘lib, xodimlarga majburiyatlar alohida nusxa (eslatma) shaklida yetkaziladi.

41. Korxonada tushuntirish ishlari maxsus mashg‘ulotlar yoki individual suhbatlar shaklida quyidagi maqsadlarda olib boriladi:

- Xodimlarda tahdidlarning korxona faoliyatiga ta’siri va ularning mumkin bo‘lgan oqibatlarini tushunishni shakllantirish;

- Xodimlarga axborot xavfsizligi bo‘yicha oddiy amallar va talablarni bajarish zarurligini anglatuvchi tushunchalar berish;

- Xodimlarning axborot xavfsizligini ta’minlash masalalarida ongli va mas’uliyatli bo‘lish darajasini oshirish;

- Xodimlarda axborot xavfsizligini ta’minlash qoidalari va talablariga rioya qilishga yordam beruvchi xulq-atvor va axloqiy normalarni shakllantirish;

- Axborot xavfsizligini ta’minlashda to‘g‘ri qarar qabul qilishida xodimlar o‘rtasida birdamlikni yaratish.

Ushbu tushuntirish ishlari xodimlarga ishga qabul qilinish vaqtida ham, ish faoliyati davomida ham amalga oshiriladi.

42. Psixologik monitoring alohida shaxsga nisbatan ham, tarkibiy bo‘linmalarga nisbatan ham, shuningdek, Korxona miqyosida ham qo‘llaniladi. Hususan, xodimlar orasida qandaydir norozilik yoki bezovtalik holatlarini aniqlash, qoidalar va me’yorlarga rioya etish masalasida mas’uliyatli hamda vijdonli xodimlarni, shuningdek, mas’uliyatsiz va loqayd xodimlarni aniqlash maqsadida amalga oshiriladi. Bunday xodimlar nazoratga olinishi yoki ularga nisbatan tegishli choralar ko‘rilishi lozim.

11.3. Tashkiliy choralar

43. Korxona tashkiliy chora-tadbirlar quyidagilarga qaratilgan:

- aktivlarni boshqarish;

- inson resurslarini boshqarish (xodimlarning xabardorligi va malakasini oshirish);

- himoya qilinishi kerak bo‘lgan obyektlarga jismoniy kirishni cheklash (jismoniy xavfsizlik);

- himoya qilinadigan ma’lumotlarni axborot xavfsizligi;

- axborotni himoya qilish tizimi va vositalarini yaratish, ularning faoliyatini ta’minlash va rivojlantirish, shuningdek axborot xavfsizligini boshqarish;

- himoyalanganlik darajasini nazorat qilish va baholash.

11.3.1. Aktivlarni boshqarish bo‘yicha tashkiliy choralar

44. Korxonada aktivlarni boshqarish bo‘yicha tashkiliy choralar aktivlarni identifikatsiya qilish va ularni himoya qilish bo‘yicha tegishli mas’uliyatni belgilash maqsadida amalga oshiriladi.

45. Aktivlarni boshqarish bo‘yicha tashkiliy chora-tadbirlarga quyidagilar kiradi:

1) aktivlar va ular bilan bog‘liq ma’lumotni qayta ishlash, saqlash hamda himoya qilish vositalarini aniqlash maqsadida inventarizatsiya qilish;

2) aktivlarni ro‘yxatdan o‘tkazish va hisobga olish – ushbu aktivlarning inventarizatsiya ro‘yxatini (reyestrini) shakllantirish hamda uni doimiy ravishda aktualligini saqlash;

3) aktivlarga egalik qilish – aktiv egalarini tayinlash, ularning aktivlarga nisbatan vazifalari va javobgarligini belgilash;

4) aktivlarni qonunchilik talablari, ularning muhimligi va Korxona uchun sezgirligiga ko‘ra tasniflash hamda ularni yetarli darajada himoya qilishni ta’minlash;

5) tasniflash tizimida qabul qilingan aktivlarni markirovkalash (jismoniy belgilar, maxsus belgilar, g‘riflar, meta-ma’lumotlar);

6) aktivlarni xavfsiz saqlash – himoyalangan xonalar va saqlash joylaridan (seyflar, qulflanadigan shkaflar) foydalanish;

7) axborot aktivlaridan maqbul foydalanish va ularni boshqarish – axborot aktivlari hamda ular bilan bog‘liq ma’lumotni qayta ishlash vositalaridan foydalanish va boshqarish qoidalarini hujjatlashtirish va joriy etish;

8) ayrim turdagi aktivlarni olib kirish yoki olib chiqishni cheklash;

9) aktivni qayta foydalanish uchun topshirish, mehnat shartnomasi bekor qilinganda aktivni qaytarish, aktiv yo‘qolishi, o‘g‘irlanishi yoki shikastlanishi, undan foydalanish siyosati talablari buzilishi, shuningdek aktivni hisobdan chiqarish va utilizatsiya (yo‘q qilish) qilish holatlari bo‘yicha qoidalar va tartib-taomillarni belgilash;

10) ma’lumotlarni kafolatli o‘chirish (yo‘q qilish) maqsadida aktivni tegishli (xavfsiz) va nazorat ostida yo‘q qilish (utilizatsiya qilish).

46. Korxonada inventarizatsiya, hisobga olish, egalik qilish, tasniflash, markirovkalash, reyestrni shakllantirish, shuningdek axborot aktivlarini boshqarish bo‘yicha boshqa tartib-taomillar mazkur Siyosatning 7-ilovasida keltirilgan Axborot aktivlarini boshqarish tartibiga muvofiq amalga oshiriladi.

47. Aktivlarni inventarizatsiya qilish korxonada axborot xavfsizligi administratori tomonidan kamida yiliga bir marotaba tashkil etiladi va o‘tkaziladi. Inventarizatsiya yakunlariga ko‘ra, zarurat bo‘lsa, himoya obyektlari ro‘yxatiga, axborot aktivlari (resurslari) reyestriga va konfidensial ma’lumotlar ro‘yxatiga o‘zgartirish va qo‘shimchalar kiritiladi. Bundan tashqari, inventarizatsiya natijalariga ko‘ra xonalar ro‘yxati hamda ularga kiruvchi texnik va dasturiy vositalar majmui tarkibi belgilanadi.

48. Himoya obyektlarini toifalash va tasniflash normativ hujjatlar talablari hamda Korxonada qabul qilingan tasniflash tizimiga muvofiq amalga oshiriladi.

49. Korxonada ma’lumotni qayta ishlash, saqlash va uzatish vositalarini olib kirish yoki olib chiqish bo‘linma rahbarining moddiy ruxsati asosida, KABT boshqarmasi bilan kelishilgan holda amalga oshiriladi.

50. Korxonada mobil qurilmalarni boshqarish tartibi mazkur Siyosatning 12-ilovasida keltirilgan Mobil qurilmalar bilan ishlashda xavfsizlikni ta’minlash bo‘yicha Yo‘riqnomada belgilangan.

51. Ma’lumotlarni saqlovchi va tashuvchi (flash-xotira) qurilmalar bilan ishlash hamda boshqarish, shu jumladan ularni utilizatsiya qilish (yo‘q qilish) tartibi mazkur Siyosatning 13-ilovasida keltirilgan “Ma’lumot saqlovchi va tashuvchi (flash-xotira) qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo‘yicha yo‘riqnoma”da belgilangan.

11.3.2 Inson resurslarini boshqarish bo‘yicha tashkiliy choralar

52. Inson resurslarini boshqarish bo‘yicha tashkiliy choralarga quyidagilar kiradi:

1) Xodimlarni tanlash (ishga qabul qilishdan oldin):

- axborot xavfsizligini ta’minlash uchun mas’ul mutaxassislarning malaka talablari hamda ma’lumotni qayta ishlash va axborot xavfsizligini ta’minlash jarayonlari bilan bog‘liq ishlarni bajaruvchi xodimlarning bilim darajasini belgilash;

- ishga qabul qilishda nomzodlarning bilim va ko‘nikmalari korxonada belgilangan malaka talablariga muvofiqligini tekshirish.

2) Ishga qabul qilish jarayonida:

- xodimlar bilan tuziladigan mehnat shartnomalarida axborot xavfsizligi sohasidagi javobgarlikni belgilash;

- mazkur Siyosat bilan tanishtirish;

- axborot xavfsizligi talablari va konfidensial ma’lumotlarni oshkor etmaslik bo‘yicha dastlabki ko‘rsatmalar berish;

- lavozim yo‘riqnomalarida belgilangan axborot xavfsizligi sohasidagi vakolatlar, majburiyatlar va javobgarlik, shuningdek axborot xavfsizligi talablarini bajarmaganlik uchun korxonada qo‘llaniladigan rag‘batlantirish va intizomiy choralar bilan tanishtirish.

3) Ish faoliyati davomida:

- xabardorlikni oshirish, o‘quv mashg‘ulotlar va seminar-treninglar o‘tkazish;

- axborot xavfsizligini ta’minlash uchun mas’ul xodimlarni qayta tayyorlash va malakasini oshirish (zarur ko‘nikmalarni shakllantirish);

- xodimlarning xabardorlik va malaka darajasini tekshirish yoki baholash;

- mazkur Siyosat hamda axborot xavfsizligi sohasidagi normativ hujjatlar talablarini xodimlarga yetkazish;

- xodimlar tomonidan axborot xavfsizligi tartib-taomillari va talablariga rioya etilishini nazorat qilish;

- axborot xavfsizligi talablari buzilgan taqdirda intizomiy choralarni belgilash va qo‘llash.

4) Ish faoliyati tugatilganda yoki o‘zgartirilganda:

- ishdan bo‘shagan yoki lavozimi o‘zgargan xodim bilan mehnat shartnomasida konfidensiallikka rioya etish majburiyatini belgilash, mazkur majburiyat mehnat shartnomasi bekor qilingandan so‘ng 5 yil davomida amal qilishi lozim;

- ishdan bo‘shagan yoki lavozimi o‘zgargan xodim tomonidan mehnat faoliyati davomida foydalanilgan konfidensial ma’lumotlarni saqlovchi va tashuvchi (flash-xotira) qurilmalarini qaytarib olish;

- ishdan bo‘shagan yoki lavozimi o‘zgargan xodimlarning himoya obyektlariga bo‘lgan barcha mantiqiy va jismoniy kirish huquqlarini bekor qilish.

53. Axborot xavfsizligini boshqarish tartiblari, himoya obyektlari va axborot xavfsizligi vositalari bo‘yicha vazifalar (rol va javobgarlik) tarkibiy bo‘linmalar yoki lavozim bo‘yicha taqsimlanishi mazkur Siyosatning 14-bo‘limida keltirilgan.

54. Axborot xavfsizligini ta’minlash uchun mas’ul mutaxassislarning malaka talablari, ma’lumotni qayta ishlash jarayonlari bilan bog‘liq ishlarni bajaruvchi xodimlarning ko‘nikma darajasi hamda ularning vazifalari KABT boshqarma boshlig‘i tomonidan belgilanadi. Ishga qabul qilishda nomzodlarning malakasini baholash kadrlar bo‘limlari tomonidan KABT boshqarmasi bilan birgalikda amalga oshiriladi.

55. Mehnat shartnomalarida axborot xavfsizligi sohasidagi vazifalar va javobgarlikni belgilash hamda xodimlarni ushbu majburiyatlar bilan tanishtirish kadrlar bo‘limlarining vakolatiga kiradi.

56. Korxonaning yangi xodimlari uchun axborot xavfsizligini ta’minlash bo‘yicha dastlabki tanishtirish ishlarini amalga oshirishlari shart. Ushbu kirish tanishtirish ishlari korxonada KABT boshqarmasi, tizimosti korxonada esa KABT boshqarmasi tomonidan amalga oshiriladi.

57. Axborot xavfsizligi bo‘yicha xodimlarning xabardorligini oshirish, malakasini rivojlantirish, o‘qitish va seminar-treninglar o‘tkazish hamda xabardorlik va malaka darajasini baholash korxonada muntazam ravishda amalga oshiriladi. Ushbu jarayon KABT boshqarmasi va xodimlar bilan ishlash boshqarmasi tomonidan tashkil etiladi.

58. Axborot xavfsizligini ta’minlash uchun mas’ul xodimlarning malakasini oshirish va korxona xodimlarini axborotni himoya qilish bo‘yicha o‘qitish maqsadida xodimlar bilan ishlash boshqarmasi mutaxassislari malakasini oshirish kurslari va o‘qitish jadvalini har yili tuzadi va tasdiqlaydi. Mutaxassislarning malakasini oshirish axborot xavfsizligi sohasidagi ta’lim muassasalarida amalga oshiriladi. Korxona xodimlarini o‘qitish (seminar-treninglar) xodimlar bilan ishlash boshqarmasi tomonidan tashkil etiladi.

59. Korxona xodimlari hamda mutaxassislarining xabardorlik malaka baholash markazi tomonidan test va savolnomalar orqali tekshirilib baholanadi. Ushbu baholash natijalariga asoslanib, Korxona rahbariyatiga xodimlarning axborot xavfsizligini ta’minlash bo‘yicha bilim-ko‘nikmalari haqida hisobot tayyorlanadi va taqdim etiladi.

60. Shuningdek, korxona KABT boshqarmasi xodimlarning axborot xavfsizligi talablariga rioya qilinishini doimiy ravishda monitoring qiladi. Monitoring natijalariga asoslanib, axborot xavfsizligini buzgan xodimlar haqida hisobot tayyorlanadi va Korxona rahbariyatiga taqdim etiladi, ularga nisbatan intizomiy choralar ko‘riladi.

61. Korxona xodimning axborot xavfsizligi talablarini buzganligi uchun O‘zbekiston Respublikasi Mehnat kodeksi talablariga muvofiq intizomiy choralar qo‘llaniladi. Ushbu choralar quyidagilarga qaratilgan:

- axborot xavfsizligi siyosati yoki tartib-qoidalarini buzgan xodimlarning intizomiy javobgarligini belgilash;
- xodimlarni mazkur Siyosat yoki axborot xavfsizligi tartib-qoidalarini, shuningdek boshqa axborot xavfsizligi buzilishlaridan qaytarish (yo‘l qo‘ymaslik);
- axborot xavfsizligini qasddan buzgan aybdorlarni javobgarlikka tortish;
- xodimlarni axborot xavfsizligini ta’minlash masalalariga mas’uliyat bilan yondashishga rag‘batlantirish.

11.3.3. Jismoniy xavfsizlik bo‘yicha tashkiliy choralar

62. Jismoniy xavfsizlik bo‘yicha tashkiliy chora-tadbirlar korxona himoya obyektlariga ruxsatsiz jismoniy kirish, shikastlanish va boshqa salbiy jismoniy ta’sirlarni oldini olishga qaratilgan.

63. Korxona boshqarmasi, hududiy boshqarmalar va bino hamda hududlarining jismoniy xavfsizlik perimetrlarini aniq belgilash lozim.

64. Korxonada jismoniy xavfsizlik bo‘yicha tashkiliy choralar quyidagilardan iborat:

1) Hududlar, binolar va xonalar bo‘yicha:

- korxona obyektlari hududiga va binolarga kirishda qo‘riqlash va nazoratli o‘tkazish tartibini tashkil etish;
- korxona binolari va obyektlarini xavfsizlik zonalariga ajratish;
- tashrif buyuruvchilar yoki uchinchi tomon shaxslarini faqat past xavfsizlik zonalarida qabul qilish va xizmat ko‘rsatish;
- tashrif buyuruvchilar yoki uchinchi tomon shaxslarini hudud, bino va xizmat xonalarida kuzatuvini tashkillashtirish;
- binoga, obyektlarga va himoyalanadigan xonalarga kirishga ruxsat berilgan shaxslar ro‘yxatini shakllantirish;
- obyektlarga jismoniy kirishni boshqarish – jismoniy kirish huquqiga ega vakolatli shaxslar ro‘yxatini shakllantirish, ko‘rib chiqish, o‘zgartirish, jismoniy kirish ruxsatini olish, to‘xtatish yoki bekor qilish;
- himoya obyektlariga jismoniy kirish, shu jumladan tashrif buyuruvchilar va uchinchi tomon shaxslarini ro‘yxatga olish va hisobga olish;
- binoga va korxona obyektlariga moddiy qiymatlar va mulkni olib kirish va olib chiqish uchun moddiy ruxsatnomalar berish;
- Korxona ishlab chiqarish hududida foto va videotasvirlarga olishni taqiqlash;

- Korxona ishlab chiqarish hududiga kirish-chiqishda xodimlar, tashrif buyuruvchilar va uchinchi tomon shaxslarini arkali yoki qo‘l metall detektorlaridan foydalanib ko‘zdan kechirish.

2) Ma’lumotni qayta ishlash, saqlash, uzatish va himoya qilish vositalari bo‘yicha:

- axborotlashtirish obyektlarini nazorat qilinadigan zona chegarasidan maksimal masofada joylashtirish hamda ularning ma’lumotni qayta ishlash, uzatish va himoya qilish texnik vositalarini himoyalangan server xonalariga joylashtirish;

- vositalarni qulflanadigan kommutatsiya shkaflarda o‘rnatish;

- uskuna tashqi korpusida qulflar, bir martalik plombalar, himoya yopishtiruvchi tasmalar yoki himoya va gologramali etiketalardan foydalanish.

3) Oxirgi qurilmalar bo‘yicha:

- xodimlarning ishchi stantsiyalari tashqi korpusida qulflar, bir martalik plombalar, himoya yopishtiruvchi tasmalar yoki himoya gologrammali etiketalardan foydalanish;

- Korxonada ishlatiladigan mobil qurilmalarni hisobga olish.

4) Qog‘oz shaklidagi konfidensial ma’lumot, raqamli ma’lumot tashuvchi (flash-xotira)lar va texnologik jarayonda ishlatiladigan tashuvchilar bo‘yicha:

- seyflar, qulflanadigan po‘lat shkaflar va boshqa himoyalangan saqlash joylaridan foydalanish;

- ularni jurnallarda hisobga olish.

5) Elektr ta’minoti va tarmoq kabellarini shikastlanishini oldini olish maqsadida hamda ma’lumotlarni o‘g‘irlanishi yoki ularni ochilishdan (ruxsatsiz kirish va ulashdan) himoya qilish bo‘yicha tashkiliy choralar qo‘llaniladi, ular mazkur Siyosatning 13-bo‘limida keltirilgan.

66. Korxona boshqaruv binosiga uchinchi tomon shaxslarni kiritish tashrif buyutuvchilar jurnaliga qayd etish orqali amalga oshiriladi, mazkur jurnal ruxsatnonalar berish byurosi tomonidan yuritiladi. Korxona boshqaruv binosiga kirish uchun tashrif buyuruvchilar korxonaga kirishni boshqarish va nazorat qilish tizimida (KBNT) yuz tasviri (Face ID) bo‘yicha ro‘yxatdan o‘tkazish yoxud tashrif buyuruvchilarga bir martalik ruxsatnoma berish orqali ro‘yxatdan o‘tkaziladi.

Korxonaning ishlab chiqarish hududiga uchinchi tomon shaxslarni kiritish faqat bir martalik ruxsatnoma asosida, kuzatuv nazorati va tahlil bo‘limdan ruxsat olingan holda va tashrif buyuruvchilarni maxsus jurnalga qayd etish orqali amalga oshiriladi. Mazkur jurnal kuzatuv nazorati va tahlil bo‘limi tomonidan yuritiladi.

Korxona barcha obyektlarida tashrif buyuruvchilar xodimlar tomonidan kuzatib boriladi.

67. Korxona xodimlarining hamda tashrif buyuruvchilarning kelib-ketishi kirishni boshqarish va nazorat qilish tizimi (KBNT) orqali ro‘yxatga olinadi.

68. Korxona boshqaruvi xizmat xonalari ish vaqtidan tashqari paytda qulflanadi va qo‘riqlash xizmatiga topshiriladi. Korxonaning ma’muriy xizmat xonalari ish vaqtidan tashqari paytda qulflanadi va jurnalga imzo qo‘ydirgan holda tizimosti qo‘riqlash xizmatiga topshiriladi. Korxonaning ayrim xonalari plombalanadi hamda plombalar kalitlar bilan birga tubusda (penalda) ish kuni yakunida tizimosti qo‘riqlash xizmatiga topshiriladi.

69. Korxonaning himoyalanadigan xonalarga kirish kuzatuv nazorati va tahlil bo‘limi tomonidan KBNT orqali boshqariladi.

Korxonaning server xonasiga kirish faqat KABT boshqarmasi xodimlariga ruxsat etiladi. KABT boshqarmasi xodimlarining server xonasiga kirishi-chiqishi jurnalga qayd etiladi.

70. Korxona binosi va obyektlarida moddiy boyliklar hamda mulkni olib kirish va olib chiqish tartibi “Ruxsatnomalar byurosi tomonidan, ruxsatnomalar hamda tovar-moddiy boyliklarni korxona hududiga olib kirish va olib chiqish jarayonida hujjatlarni rasmiylashtirish tartibi to‘g‘risida” bilan tartibga solinadi.

71. Korxona hududi, binolari va xonalarining jismoniy xavfsizligi bilan bog‘liq tashkiliy choralar kuzatuv nazorat va tahlil bo‘limi tomonidan amalga oshiriladi.

72. Ma’lumotni qayta ishlash, saqlash, uzatish va himoya qilish vositalari, xodimlarning ishchi stansiyalari tashqi korpuslarini plombalash KABT boshqarmasi tomonidan amalga oshiriladi.

11.3.4 Himoya qilinishi kerak bo‘lgan ma’lumotlarni axborot xavfsizligini ta’minlash bo‘yicha tashkiliy choralar

73. Korxonada himoya qilinishi kerak bo‘lganlar quyidagilardan iborat:

- xizmat (ish) faoliyatiga oid tarqatilishi cheklangan ma’lumotlar (“Xizmat uchun” grif qo‘yilgan ma’lumotlar);
- konfidensial ma’lumot, shu jumladan korxonaning tijorat siri;
- Korxonaga tegishli uchinchi tomon shaxslarning konfidensial ma’lumoti;
- xodimlar va mijozlarning shaxsga doir ma’lumotlari.

74. Konfidensial ma’lumotlarni himoya qilish bo‘yicha tashkiliy choralarga quyidagilar kiradi:

1) konfidensial ma’lumotni tashkil etuvchi ma’lumotlar ro‘yxatini shakillantirish hamda zarurat tug‘ilganda ushbu ro‘yxatga o‘zgartirish va qo‘shimchalar kiritish;

2) Himoyalanadigan axborotga ruxsat berilgan xodimlar ro‘yxatini shakllantirish;

3) Xodimlar tomonidan konfidensial ma’lumotni oshkor etmaslik majburiyatini olish (majburiatnoma rasmiylashtirish);

4) Kontragentlar bilan tuziladigan shartnomalarda konfidensial ma’lumotlarni oshkor etmaslik bo‘yicha shartlar, talablar, majburiyatlar va javobgarlikni belgilash (konfidensiallik kelishuvi);

5) Himoyalanadigan ma’lumotga va uning moddiy tashuvchilarida maxsus belgilar (griflar)dan foydalanish;

6) Qog‘oz shaklidagi himoyalanadigan ma’lumotni hamda konfidensial ma’lumotni o‘z ichiga olgan elektron tashuvchi (flash-xotira)larni ro‘yxatga olish va hisobini yuritish;

7) Himoyalanadigan ma’lumotni lokal va tashqi tarmoqlar, elektron pochta orqali yuborishda himoya talablari yoki cheklovlarini belgilash, shuningdek Internet tarmog‘i, ijtimoiy tarmoqlar, ommaviy axborot vositalari va boshqalarda konfidensial ma’lumotni tarqatishga cheklovlar joriy etish;

8) Himoyalanadigan ma’lumotni qog‘oz shaklida hamda elektron shaklda (axborotni qayta ishlash vositalari, elektron tashuvchi (flash-xotira)lar, mobil qurilmalar va boshqalar) saqlashda himoya talablari yoki cheklovlarini joriy etish;

9) Himoyalanadigan ma’lumotga kirish va undan foydalanish tartibini joriy etish;

10) Himoyalanadigan ma’lumot qayta ishlanadigan va saqlanadigan xonalar ro‘yxatini aniqlash hamda ularni ruxsatsiz jismoniy kirishdan himoya qilish bo‘yicha talablarni joriy etish;

11) Himoyalanadigan axborotni o‘z ichiga olgan elektron tashuvchi (flash-xotira)larni saqlash, uzatish, hisobdan chiqarish va yo‘q qilish (utilizatsiya) tartibi talablarini joriy etish;

12) Himoyalanadigan ma’lumotni elektron shaklda qayta ishlash va saqlash uchun foydalaniladigan axborotlashtirish obyektlarini aniqlash hamda ularni ruxsatsiz mantiqiy va jismoniy kirishdan himoya qilish talablarini joriy etish;

13) Xodimlarning mehnat faoliyati tugatilganda yoki o‘zgartirilganda, moddiy tashuvchidagi himoyalanadigan ma’lumotni qaytarish talablarini belgilash;

14) Himoyalanadigan ma’lumotni himoya qilish talablariga rioya etilishi ustidan nazoratni ta’minlash.

75. Korxonada himoya qilinishi kerak bo‘lgan ma’lumotni himoya qilish choralarini amalga oshirish tartibi mazkur Siyosatning 17-ilovasida keltirilgan “Himoya qilinishi kerak bo‘lgan ma’lumotlar bilan ishlash tartibi”da belgilangan.

“Xizmat uchun” grifi qo‘yilgan hujjatlar bilan ishlash tartibi O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025 yil 4 dekabrdagi 766-son qarori bilan tasdiqlangan qoidalarga

muvofiq amalga oshirilishi lozim.

76. Korxonada O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015 yil 16 oktyabrdagi 295-son qaroriga muvofiq konfidensial ma’lumotlarni tashkil etuvchi ma’lumotlar ro‘yxati, shuningdek 2025 yil 4 dekabrdagi 766-son qaroriga muvofiq “Xizmat uchun” toifasiga kiritilishi lozim bo‘lgan idoraviy hujjatlar ro‘yxati yuritilishi shart.

Mazkur ro‘yxatlarni tuzish tartibi mazkur Siyosatning 17-ilovasida keltirilgan “Himoya qilinishi kerak bo‘lgan ma’lumotlar bilan ishlash tartibi”da belgilangan.

77. Korxona xodimlarining, jumladan boshqarma, xodimlarining konfidensial ma’lumotlarni oshkor etmaslik majburiyatlari ularning mehnat shartnomalarida belgilangan bo‘lib, xodim ishga qabul qilinish jarayonida ushbu shartlar bilan tanishtiriladi. Korxona xodimlariga konfidensial ma’lumotlarni oshkor etmaslik majburiyatlarini yetkazish uchun mas’ul bo‘linma — korxonaning xodimlar bilan ishlash boshqarmasi hisoblanadi.

11.3.5. Ma’lumotlarni himoya qilish tizimi va vositalarini yaratish, ularni faoliyatini ta’minlash hamda rivojlantirish, shuningdek axborot xavfsizligini boshqarish bo‘yicha tashkiliy choralar

78. Korxonada ma’lumotlarni himoya qilish tizimi va vositalarini yaratish, ularni faoliyatini ta’minlash va rivojlantirish bo‘yicha tashkiliy choralar quyidagilarni o‘z ichiga oladi:

1) Axborot xavfsizligini ta’minlash tadbirlari doirasida ma’lumotlarni himoya qilish vositalarini korxona uchun alohida xarid qilish;

2) Xarid qilinadigan ma’lumotlarni himoya qilish vositalari uchun texnik talablarni belgilash;

3) Ma’lumotlarni himoya qilish tizimi va vositalarini joriy etishga tayyorgarlik va ularni foydalanishga topshirish bo‘yicha tashkiliy tadbirlarni amalga oshirish, jumladan: xonani ajratish, foydalanish bo‘yicha yo‘riqnomalarni ishlab chiqish, mas’ul xodimni belgilash va uni foydalanish bo‘yicha o‘qitish;

4) Ma’lumotlarni himoya qilish vositalarini joriy etishda tajriba asosida foydalanish va qabul-qilish bo‘yicha sinovlar o‘tkazish;

5) Himoya tizimini boshqarish (administratsiya qilish), unga quyidagilar kiradi: konfiguratsiya va sozlash parametrlarini nazorat qilish, zaxiralash va qayta tiklash, ishlash qobiliyatini tiklash, dasturiy ta’minotni o‘rnatish va yangilashni tekshirish, ekspluatatsiya hujjatlarini tuzatish, xavfsizlik insidentlarini nazorat qilish, voqealar jurnalini (log) yig‘ish va tahlil qilish, nazorat protseduralari va natijalarini hujjatlashtirish;

6) Axborotni himoya qilish tizimida kamchiliklar aniqlanganda tizimni takomillashtirish bo‘yicha takliflar tayyorlash va kiritish.

Korxonada ma’lumotlarni himoya qilish tizimi va vositalarini yaratish, ularni ishlatish va rivojlantirish bo‘yicha mazkur tashkiliy choralar KABT boshqarmasi tomonidan amalga oshiriladi.

79. Axborot xavfsizligini boshqarish bo‘yicha tashkiliy choralar, jumladan tarmoq xavfsizligini ta’minlash, kirish huquqlarini boshqarish, antivirus himoyasi va boshqa chora-tadbirlar mazkur Siyosatga ilova qilingan hujjatlarda belgilangan.

80. Axborot xavfsizligi insidentlariga javob berish bo‘yicha korxona quyidagi tashkiliy choralarni amalga oshiradi. Mazkur Siyosatning 12-bo‘limida belgilangan tartiblar. 20-ilovada keltirilgan Axborot xavfsizligi insidentlariga javob berish reglamentiga muvofiq.

11.3.6. Himoyalanish darajasini nazorat qilish va baholash bo‘yicha tashkiliy choralar

81. Himoyalanish darajasini nazorat qilish va baholash bo‘yicha tashkiliy chora-tadbirlar maqsadlari

Korxonada ushbu choralar quyidagi maqsadlarda qo‘llaniladi:

- AXBTdagi (Axborot xavfsizligini boshqarish tizimi) zaifliklar va kamchiliklarni aniqlash;

- himoya obyektlarining tahdidlardan himoyalanish darajasini obyektiv baholash;

- AXBT va undagi axborotni himoya qilish vositalari va metodlarining Siyosat va normativ hujjatlarga muvofiqligini aniqlash;

- ilova va tizim dasturiy ta’minoti hamda lokal tarmoqlardagi zaifliklarni aniqlash va boshqarish;

- amalga oshirilgan xavfsizlik choralarining samaradorligini baholash;

- axborot xavfsizligi maqsadlariga erishilganligini baholash.

82. Himoyalanish darajasini nazorat qilish va baholash bo‘yicha tashkiliy choralar:

1) Korxonada axborot xavfsizligi zaifliklarini aniqlash va tahlil qilish ishlarini olib borish;

2) Himoya obyektlarining himoyalanganlik darajasini baholash hamda mazkur Siyosatning dolzarbligi va samaradorligini baholash maqsadida ichki va tashqi audit o‘tkazish;

3) Axborotlashtirish obyektlari va MAI obyektlarini attestatsiyadan o‘tkazish;

4) O‘zbekiston Respublikasi Adliya vazirligida 2024-yil 14-noyabrda 3573-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati raisining 2024-yil 15-oktabrdagi 113-sonli buyrug‘i bilan tasdiqlangan “Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish tartibi to‘g‘risidagi nizomi”ga muvofiq Korxonaning axborot tizimlari va resurslari texnik topshiriqlarni hamda axborot tizimlari va resurslarini ekspertizadan o‘tkazish;

5) O‘zbekiston Respublikasi Adliya vazirligida 2024-yil 14-noyabrdagi 3574-son bilan ro‘yxatga olingan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati Raisining 2024-yil 15-oktyabrdagi 114-son buyrug‘i bilan tasdiqlangan “Axborot tizimlari va resurslarining kiberxavfsizligini ta’minlash uchun qo‘llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirish tartibi to‘g‘risidagi nizomi”ga muvofiq dasturiy va dasturiy-apparat vositalarni sertifikatlash;

6) Korxonaning AXBT (Axborot xavfsizligini boshqarish tizimi)ni xalqaro ISO 27001 standarti yoki O‘z MSt ISO/IEC 27001 milliy standartiga muvofiqligi bo‘yicha sertifikatlash ishlarini amalga oshirish;

7) Auditlar, ekspertizalar va attestatsiyalar natijalariga ko‘ra qabul qilingan tashkiliy, texnik va boshqa himoya choralarining samaradorligini baholash hamda aniqlangan kamchiliklarni bartaraf etish.

Mazkur choralar Korxona KABT boshqarmasi tomonidan, zarurat bo‘lganda boshqa bo‘lim mutaxassislari jalb qilingan holda ichki audit o‘tkazish ishlari amalga oshiriladi.

83. Korxonada ichki axborot xavfsizligi auditi yiliga kamida 1 marta, tashqi audit esa har 3 yilda kamida 1 marotaba o‘tkaziladi.

84. Ichki audit vazifalari:

- Korxonaning bo‘limlari va xodimlari tomonidan ushbu Siyosatda belgilangan axborot xavfsizligi talablariga rioya qilinishini tekshirish;

- axborot xavfsizligini boshqarish jarayonlarini to‘g‘ri bajarilishini nazorat qilish;

- Siyosatning dolzarbligi va samaradorligini 15-bo‘lim talablariga muvofiq baholash;

- axborot xavfsizligi talablariga mos kelmasliklar, zaifliklar va kamchiliklarni aniqlash.

85. Tashqi audit o‘tkazish maqsadida malakali xodimlari va tegishli vakolatga ega bo‘lgan korxonalar jalb qilinadi.

86. Auditlar va boshqa tekshiruvlar natijalari hujjatlashtiriladi, unda quyidagilar ko‘rsatiladi:

- zaifliklar, kamchiliklar va mos kelmasligini aniqlash;

- mos kelmaslik sabablarini tahlil qilish;

- zarur chora-tadbirlar va amalga oshirilgan ishlar;

- himoya choralarining samaradorligi bahosi va boshqa ma’lumotlar.

Auditlar va boshqa tekshiruvlar natijasida aniqlangan zaifliklar, kamchiliklar va mos kelmasliklarni bartaraf etish hamda himoya samaradorligini oshirish bo‘yicha choralar yoki amaliy ishlar amalga oshirilishi lozim.

11.4. Texnologik choralar

87. Korxonada texnologik chora-tadbirlar axborot tizimlari foydalanuvchilari tomonidan xatoliklar va qoidabuzarliklar sodir etilish ehtimolini kamaytirishga, shuningdek himoya obyektlarining konfiguratsiyasi va yaxlitligini nazorat qilish hamda boshqarishga qaratilgan.

88. Korxonaning axborot tizimlarida foydalanuvchilar tomonidan ma’lumotlarni kiritish va uzatishda yo‘l qo‘yilishi mumkin bo‘lgan xatolarni nazorat qilish hamda ularni xatoliklar haqida ogohlantirish choralarini nazarda tutish lozim. Mazkur nazorat axborot tizimlarining dasturiy ta’minoti orqali amalga oshirilishi kerak.

89. Korxonaning axborot tizimlari bilan ishlashda foydalanuvchilar xatolarining oldini olish maqsadida axborot tizimlaridan foydalanish tartibi va qoidalarini belgilovchi foydalanuvchi qo‘llanmalari ishlab chiqilishi lozim.

91. Dasturiy va apparat ta’minotining yaxlitligini nazorat qilish, shuningdek ularning konfiguratsiyasiga o‘zgartirishlar kiritish tartibi quyidagi himoya obyektlariga nisbatan amalga oshirilishi lozim:

1) Korxonada: lokal tarmoqning tarmoq uskunalari, axborotni himoya qilish vositalari hamda axborot tizimlarida axborotni qayta ishlash va saqlash vositalari, shu jumladan axborot almashish tizimlari va jismoniy xavfsizlik tizimlari;

2) Korxonada: lokal tarmoqning tarmoq uskunalari, axborotni himoya qilish vositalari hamda axborot tizimlarida axborotni qayta ishlash va saqlash vositalari, shu jumladan jismoniy xavfsizlik tizimlari.

92. Himoya obyektlarining dasturiy va dasturiy-apparat ta’minoti yaxlitligini nazorat qilish profilaktik tadbirlarni amalga oshirish jarayonida:

- Korxonada — KABT bo‘linmasi tomonidan amalga oshiriladi.

Profilaktik tadbirlar mazkur bo‘linmalar rahbarlari bilan kelishilgan holda tasdiqlangan reja-grafik asosida o‘tkaziladi.

93. Dasturiy ta’minotdan foydalanish jarayonida uning ishlashidagi xatolarni va ruxsatsiz o‘zgartirishlarni istisno etishga qaratilgan texnologik choralar ushbu Siyosatning 8-ilovasida keltirilgan “Dasturiy ta’minotni boshqarish bo‘yicha nizom”da belgilangan.

11.5. Muhandislik-texnik choralar

94. Muhandislik-texnik choralar axborot xavfsizligini ta’minlash talablari inobatga olingan holda bino va inshootlar, muhandislik tarmoqlari hamda transport kommunikatsiyalarini optimal tarzda loyihalash va tashkil etishga qaratilgan choralarni o‘z ichiga oladi.

Korxonada muhandislik-texnik choralar jismoniy xavfsizlikni ta’minlash hamda ma’lumotlarning texnik kanallar orqali sizib chiqishidan himoya qilishga yo‘naltirilgan.

95. Korxonada himoya obyektlariga begona shaxslarning jismoniy kirib kelishini oldini olish yoki cheklashga qaratilgan quyidagi muhandislik-texnik chora-tadbirlar qo‘llaniladi:

1) Korxona ishlab chiqarish hududi, binolari, xizmat xonalari hamda himoyalangan xonalariga kirishni turniketlar, eshiklar va boshqa muhandislik vositalari orqali chegaralash;

2) Korxonaning boshqarma binolarida jismoniy kirishni nazorat qilish va boshqarish uchun KBNT (kirishni boshqarish va nazorat qilish tizimi)ni qo‘llash;

3) Himoyalanadigan xonalarga, shu jumladan Korxona server xonalariga kirishda temir eshiklardan, shuningdek eshiklarda elektromagnit va kodli qulflardan foydalanish;

4) Bino perimetri hamda bino va xonalar ichida videonazoratni amalga oshirish uchun videokuzatuv tizimidan foydalanish;

5) Himoyalanadigan xonalarda ruxsatsiz jismoniy kirish holatlarini aniqlash uchun qo‘riqlash signalizatsiyasi va datchiklarni o‘rnatish;

6) Hujjatlashtirilgan himoyalanadigan ma’lumotlar va himoyalanadigan ma’lumotlar saqlangan raqamli ma’lumot tashuvchilarni saqlash uchun qulflanadigan, yong‘inga chidamli temir shkaflardan foydalanish.

99. Korxonada videokuzatuv tizimi quyidagilar ustidan nazoratni (monitoringini) ta’minlashi lozim:

- axborotlashtirish obyektlariga jismoniy ta’sir ko‘rsatish holatlari, shuningdek texnik uskunalar joylashgan bino va xonalarga kirish;
- serverlar va telekommunikatsiya uskunalari joylashgan xonalardagi ish jarayonlari, shu jumladan korxona server xonasi.

100. Server xonalarida, shuningdek kommutatsiya xonalarida o‘rnatilgan videokuzatuv tizimi quyidagi talablarga javob berishi lozim:

- serverlar bilan bevosita jismoniy aloqalarni video tasvirga olish;
- uzluksiz video kuzatuvni ta’minlash;
- serverlarning (server shkaflarining) orqa qismini kunduz va tun davomida tasvirga olish hamda nazorat qilish;
- videokameralar tasvir sifati texnologik uskunalarga xizmat ko‘rsatuvchi xodimlarning yuzlarini aniq ajratib olish imkonini beradigan darajada bo‘lishi.

Videokuzatuv qurilmalari elektr ta’minoti uzilgan paytdan boshlab kamida 12 soat davomida energiya manbaiga bog‘liq bo‘lmagan holda avtonom ishlash imkoniyatiga ega bo‘lishi lozim.

101. Korxonaning barcha videokuzatuv ma’lumotlarini saqlash muddati 3 oyni tashkil etadi.

102. Qo‘riqlash signalzatsiyasi tizimi, hududiy boshqarma xonalari, korxonaning xizmat xonalari qamrab olishi lozim.

103. Korxonada texnik kanallar orqali ma’lumotlarning oqib chiqishini oldini olishga qaratilgan quyidagi muhandislik-texnik choralar amalga oshiriladi:

1) Xonalar derazalarini vizual kuzatuvdan himoya qiluvchi vositalar bilan jihozlash (pardalar, jalyuzlar);

2) Axborotni ushlash, shovqinlar yoki shikastlanishdan himoyalangan kabellar va simlarni tortish;

3) Kabellarni tortishning oraliq va oxirgi nuqtalarini himoyalangan (yopiladigan) xonalar va shkaflarda joylashtirish, mustahkamlangan kabellarni ishlatish;

4) Kabellarni himoya qilish uchun elektromagnit ekranlashdan foydalanish va optik tolali kabellarni ishlatish;

5) Kabellarni har bir uchida yetarli miqdorda manba va manzil ma’lumotini ko‘rsatadigan belgilash, bu kabellarni jismoniy aniqlash va tekshirishga yordam beradi;

6) Himoyalanadigan xonalarda yong‘in va qo‘riqlash signalizatsiyasi tizimini faqat simli sxema asosida qurish.

11.6. Texnik choralar

104. Korxonadagi texnik choralar maxsus texnik vositalardan foydalanishga asoslangan bo‘lib, texnogen xavflar, tashqi muhit ta’siri bilan bog‘liq xavflarning oldini olish, himoya obyektlarining uzluksiz ishlashini va tiklanishini ta’minlash, shuningdek ma’lumotlarni xavfsiz saqlashga qaratilgan.

105. Korxonada texnogen xavflar va tashqi muhit ta’siridan himoya qilish uchun quyidagi choralar amalga oshiriladi:

1) Korxona server xonalarida harorat va namlikni monitoring qilish;

2) Korxona server xonalarida kerakli iqlim sharoitlarini ta’minlash vositalaridan foydalanish (konditsionerlar);

3) Korxonada xavfli yoki yonuvchan materiallarni qo‘riqlanadigan hududdan yetarlicha uzoq masofada ishonchli saqlash;

4) yong‘in signalizatsiyasi tizimlari va yong‘in o‘chirish vositalarini qo‘llash hamda ularni mos joylashtirish;

5) yong‘in holatida favqulodda chiqishlarni favqulodda signalizatsiya bilan jihozlash, evakuatsiya rejalarini ishlab chiqish;

6) sanitariya va yong‘in xavfsizligi qoidalariga rioya qilish;

7) server xonalaridagi uskunalarni yerga ulash (zemlyalash).

Ushbu choralar KABT boshqarmasi tomonidan amalga oshiriladi.

106. Korxonadagi himoya obyektlarining barqaror va uzluksiz ishlashini ta’minlash uchun quyidagi choralar amalga oshiriladi:

1) uskuna holatini doimiy tayyorlik va yaxlitlik holatida saqlash maqsadida uning texnik xizmat ko‘rsatish (ishlashini nazorat qilish, profilaktika, ta’mirlash)ni ta’minlash;

2) operatsion jarayonlarni (ishga tushirish, zaxira nusxa yaratish, sozlamalarni o‘zgartirish, korpuslarni ochish, qayta o‘rnatish, ta’mirlash, yangilash yoki dasturiy ta’minotni o‘zgartirish va boshqalar) hujjatlashtirish;

3) ma’muriy boshqarish hamda tizimlar va vositalardagi hodisalar jurnallarini tekshirish;

4) axborotni qayta ishlash vositalari va tizimlarida ishlamay qolish yoki xavfsizlik buzilishi holatlarining oldini olish uchun kiritiladigan o‘zgartirishlarni to‘g‘ri boshqarish;

5) quvvatlarni boshqarish – kelajakdagi quvvatga bo‘lgan ehtiyojlarni rejalashtirish yoki prognoz qilish, resurslardan foydalanishni monitoring qilish, resurslar yoki qo‘shimcha quvvatlar uchun zaxira yaratish;

6) sinov va foydalanish muhitlarini ajratish – test ishlari amaldagi tizimlardan alohida vositalarda amalga oshirilishi lozim;

7) axborotni qayta ishlash, saqlash, uzatish va himoya qilish vositalarini zaxiralash;

8) ma’lumotlar va dasturiy ta’minotni zaxira nusxasini yaratish;

9) dasturiy ta’minotni boshqarish – ushbu Siyosatning 8-ilovasidagi Dasturiy ta’minotni boshqarish nizomiga muvofiq dasturiy ta’minotni o‘rnatish, o‘zgartirish, sozlash va yangilash;

10) axborotni qayta ishlash vositalari yaqinida ovqatlanish, ichimlik ichish va tamaki mahsulotlaridan foydalanish bilan bog‘liq qoidalarni belgilash va ularga rioya qilish (sanitariya va yong‘in xavfsizligi talablari).

11) Korxonada axborotni qayta ishlash, saqlash, uzatish va himoya qilishning asosiy vositalari uchun uzluksiz elektr ta’minoti;

12) Aloqa kanallarini zaxiralash.

107. Korxonada texnik vositalarni, aloqa kanallarini zaxiralash, uzluksiz elektr ta’minotini ta’minlash hamda uzluksiz ishlashni ta’minlash bo‘yicha boshqa choralarni amalga oshirish talablari mazkur Siyosatinig 19-ilovasida “Uzluksiz ishlashni ta’minlash va ish faoliyatini tiklash bo‘yicha nizom”da belgilangan.

109. Zaxira nusxasini olishga quyidagilar kiradi: Korxonaning ma’lumotlar bazalari va jurnallari (log-fayllari), axborot tizimlari dasturiy ta’minoti, shuningdek tarmoq uskunalari, ma’lumotlar bazalari va axborotni himoya qilish vositalari sozlamalari (konfiguratsiya parametrlari). Zaxira nusxasini olish va ma’lumotlarni tiklash Korxonada ushbu Siyosatni 18-ilovasida keltirilgan “Ma’lumotlarni zaxiralash va tiklash bo‘yicha Nizom”ga muvofiq amalga oshiriladi.

110. Korxona server xonasi O’z DSt 2875 standartining quyidagi talablarini bajarishi shart:

- uzluksiz elektr ta’minotini ta’minlash;
- talab qilinadigan (harorat) iqlim sharoitlarini saqlash (sovutish tizimi);

- yong‘in xavfsizligini ta’minlash (yong‘indan ogoxlantiruvchi signalizatsiyasi va yong‘in o‘chirish vositalaridan foydalanish).

111. Korxonada ish faoliyatini tiklash choralari quyidagilardan iborat:

1) tiklash rejalari bo‘yicha tayyorgarlik, seminar-treninglar o‘tkazish va test sinovlarini amalga oshirish;

2) avariyaviy holatlarda zaxira uskunalar, aloqa kanallari, liniyalar yoki uzluksiz elektr ta’minoti manbalaridan foydalanish;

3) dasturiy ta’minot va ma’lumotlarni zaxira nusxalaridan tiklash;

4) uskunalarni ta’mirlash yoki almashtirish;

5) dasturiy ta’minotni qayta yuklash yoki qayta o‘rnatish va boshqa choralari.

Ish faoliyatini tiklash choralari mazkur Siyosatni 19-ilovasida keltirilgan “Uzluksiz ishlashni ta’minlash va ish faoliyatini tiklash bo‘yicha nizom”ga muvofiq tartibga solinadi.

112. Ma’lumotlarni xavfsiz saqlash, saqlanayotgan ma’lumotlarni sizib chiqishi va yo‘qotilishidan himoya qilish, shuningdek ma’lumot tashuvchi va saqlash qurilmalari (flash-xotira)ni o‘g‘irlik yoki yo‘qotilishdan himoya qilish choralari O‘zDSt ISO/IEC 27040 standarti bo‘yicha amalga oshirilishi shart.

113. Korxonada ma’lumotlarni ishonchli himoya qilish maqsadida quyidagi texnik choralari qo‘llanishi lozim:

- ma’lumot saqlash obyektlari va ma’lumot tashuvchilarni ruxsatsiz kirishdan himoya qilish;

- ma’lumot tashuvchilarini va saqlash qurilmalarini nazorat ostida to‘g‘ri yo‘q (utilizatsiya) qilish;

- saqlash qurilmalarini jismoniy himoya qilish;

- ma’lumot saqlash qurilmalariga kirishda autentifikatsiya va monitoringdan foydalanish;

- ma’lumotlarni qurilmalarda muntazam zaxira nusxasini olish;

- uzilishlarga bardoshli ma’lumotlar bazalari va ilovalarni, shuningdek ularga bog‘liq tizimlarni yagona ma’lumot nusxasi atrofida klasterlash.

116. Korxonaning ma’lum axborot tizimlari uchun administratorlar tayinlanadi. Ushbu administratorlar Korxonaning KABT boshqarmasi xodimlari hisoblanadi.

Administratorlar quyidagilarni ta’minlaydi:

- axborot tizimlari serverlarini sozlash va konfiguratsiyalash;

- foydalanuvchi qayd yozuvlarini yaratish va boshqarish qoidalarini, foydalanuvchilarga huquqlar (roller) tayinlash va yaratish qoidalarini o‘zgartirish;

- serverlarning parametrlarini va konfiguratsiyasini, shuningdek ularning ishlash va nosozlik jurnallarini tekshirish;

- axborot tizimlari serverlari (ma’lumotlar bazalari) ma’lumotlarini zaxiralash va tiklash;

- ma’lumotlar bazasi serverlarida yaxlitlikni tekshirish vositalaridan foydalangan holda axborot tizimlari serverlaridagi ma’lumotlar omborida ma’lumotlarning yaxlitligini tekshirish.

117. Korxonaning KABT boshqarmasidan alohida tayinlangan mas’ul xodim axborot tizimlari ma’lumotlar ombori xavfsizligini auditorlik qilish vazifalarini bajarishi lozim. Mas’ul xodimlarni vazifalari axborot xavfsizligi tahlilini o‘tkazish, foydalanuvchilarning huquq va vakolatlarini o‘rganish, xavfsizlik parametrlari va konfiguratsiyasini tekshirish, shuningdek voqea jurnallarini ko‘rib chiqishdan iborat.

118. Axborot tizimlari ma’lumotlar omboriga nisbatan xavfsizlik auditi, hisobga olish va monitoring ishlarini olib borish, ushbu jarayon quyidagilarni o‘z ichiga olishi lozim:

- saqlash boshqaruvida barcha muhim voqealarni qayd etish;

- voqealarni ro‘yxatga olish ma’lumotlarini saqlash;

- ma’lumotlarni zaxiralash siyosatiga muvofiq voqealarni ro‘yxatga olish ma’lumotlarini arxivlash va saqlash;

- qurilmaning vaqtini ishonchli tashqi manba bilan sinxronlashtirish.

Voqealarni ma’lumotlar omborlarida qayd etish va hisobga olish uchun syslog standarti (tizim voqealari haqidagi xabarlar jurnali) ishlatiladi.

119. Korxonaning axborot tizimlari ma’lumotlarini himoya qilishni kuchaytirish maqsadida quyidagi qo‘shimcha choralar amalga oshirilishi lozim:

- Serverda ishlatilmayotgan tarmoq portlarini yopish va faqat zarur portlardan foydalanish;
- Keraksiz va ishlatilmayotgan dasturiy ta’minotlarni o‘chirish;
- Keraksiz foydalanuvchilar qayd yozuvlarini o‘chirish;
- Standart bo‘yicha o‘rnatilgan yoki yaratilgan foydalanuvchilar qayd yozuvlarni qayta nomlash, o‘chirish yoki parolini o‘zgartirish;
- Axborot tizimi ishlashi uchun kerak bo‘lmagan xizmatlarni o‘chirish;
- Ishonchli manbalardan yangilanishlarni nazorat qilish mazkur Siyosatni 8-ilovasida keltirilgan “Dasturiy ta’minotni boshqarish bo‘yicha nizom”ga muvofiq amalga oshirish;
- Zararli dasturlardan himoyalanishni o‘rnatish va qo‘llab-quvvatlash.

11.7. Dasturiy-apparat choralari

120. Axborot xavfsizligini ta’minlashning dasturiy-apparat choralari ma’lumotni himoya qilish uchun dasturiy ta’minot va texnik vositalardan foydalanishga asoslanadi.

Axborot xavfsizligini ta’minlashda foydalaniladigan dasturiy ta’minot va texnik vositalar litsenziyalangan va axborot xavfsizligi talablariga muvofiq sertifikatlangan bo‘lishi kerak.

121. Dasturiy-apparat choralar, dasturiy va dasturiy-apparat vositalardan foydalanishga bog‘liq bo‘lib, quyidagilarni tashkil etishga qaratilgan:

- axborotni texnik himoya qilish;
- axborotni kriptografik himoya qilish.

122. Axborotni texnik himoya qilish bo‘yicha dasturiy-apparat choralarni qo‘llashning asosiy yo‘nalishlari:

- tarmoq xavfsizligi (tarmoq infratuzilmasi darajasidagi xavfsizlik);
- mantiqiy (texnik) kirishni boshqarish – identifikatsiya, autentifikatsiya va avtorizatsiya;
- antivirus himoyasi – zararli dasturlardan himoya;
- veb-resurslarni himoya qilish;
- himoyalanadigan ma’lumotlarning chiqib ketishidan himoya qilish;
- himoya darajasini nazorat qilish va baholash;
- axborot xavfsizligi insidentlarini boshqarish.

123. Tarmoqli xavfsizlik choralariga quyidagilar kiradi:

1) Korxona tarmoq infratuzilmasining xavfsiz arxitekturasini belgilash;

2) tarmoqlarni jismoniy va virtual tarzda ajratish;

3) tarmoqli xavfsizlik vositalarini qo‘llash (firewall, IDPS, VPN vositalari);

4) himoyalangan kanallar va tarmoq ulanishlarini tashkil etish.

124. Korxonaning lokal tarmog‘ining xavfsiz arxitekturasi, uning qurilish tamoyillari va himoyalangan tarmoq ulanishlari mazkur Siyosatning 1-ilovasida keltirilgan “Korxonaning lokal tarmog‘i va himoyalangan tarmoq ulanishlarini tashkil etish bo‘yicha nizom”da belgilangan.

126. Tarmoq infratuzilmasi xavfsizligini ta’minlash va tarmoq xavfsizligi vositalarini qo‘llash ushbu Siyosatni 2-ilovasida keltirilgan “Tarmoq infratuzilmasi darajasida axborot xavfsizligini ta’minlash va xavfsizlik devorlari to'g'risidagi nizom”ga muvofiq amalga oshiriladi.

127. Korxonada tarmoqqa bostirib kirish va hujumlardan himoya qilish choralari O‘zDSt ISO/IEC 27039 standarti talablariga muvofiq amalga oshirilishi kerak.

Axborot xavfsizligi bilan bog‘liq xavflar, xususan, korxona tarmoqlariga hujumlar va bostirib kirishlar amalga oshirilganda, lokal tarmoqlar hamda ularga ulangan vositalarni himoya qilish uchun IDPS tarmoqli vositalaridan foydalanish talab etiladi.

Korxonada oxirgi qurilmalarga va muhim serverlarga HIPS (Host-based Intrusion Prevention System) o‘rnatilishi shart.

Korxonada antivirus himoya vositalari ishlatiladi. Korxonada qo‘llaniladigan tarmoq IDPS va HIPSga bo‘lgan talablar ushbu Siyosatni 2-ilovasida keltirilgan “Tarmoq infratuzilmasi darajasida axborot xavfsizligini ta’minlash va t xavfsizlik devorlari to'g'risidagi nizom”da belgilangan.

128. Korxonaning axborot resurslari va tizimlariga kirishni chegaralash. Kirish huquqlarini belgilash uchun kirish matritsasini ishlab chiqiladi va u Ushbu Siyosatni 10-ilovasida keltirilgan “Kirish matritsasini ishlab chiqish va yangilash qoidalari”ga muvofiq bo‘lishi kerak.

129. Himoya obyektlariga kirishda foydalanuvchilarni autentifikatsiya qilishda parollar va boshqa identifikatorlar asosida amalga oshiriladi. Ularni shakllantirish va qo‘llash tartibi mazkur Siyosatni 9-ilovasida keltirilgan “Kirishni boshqarish, autentifikatsiya va parol himoyasi bo‘yicha yo‘riqnoma”ga muvofiq belgilanadi.

130. Korxonada antivirus himoyasini ta’minlash bo‘yicha quyidagi choralar va vositalar qo‘llaniladi:

1) Axborotni qayta ishlash vositalarida, shu jumladan mobil qurilmalarda, zararli dasturlarni aniqlash va bloklash, tizimning dastlabki holatini tiklash hamda foydalanuvchilarni xabardor qilish imkoniyatiga ega antivirus vositalarini qo‘llash;

2) Korxona xodimlari tomonidan zararli dasturlardan himoyalanish maqsadida, Siyosatda qabul qilingan antivirus himoyasi bo‘yicha talablarini bajarishlari shart.

3) Zararli dasturlar tomonidan foylanilishi mumkin bo‘lgan zaifliklarni aniqlash va bartaraf etish;

4) Lokal tarmoqqa, shuningdek korxonaning ichki ishlab chiqarish lokal tarmog‘iga ulangan oxirgi qurilmalarda har qanday olinadigan tashqi qurilmalar (USB, CD/DVD disklar) va Bluetooth dan foydalanishni bloklash.

131. Antivirus himoyasini tashkil etish va ta’minlash tartibi, shuningdek Korxona xodimlari tomonidan zararli dasturlardan himoyalanish talablariga rioya etish masalalari mazkur Siyosatni 11-ilovasida keltirilgan “Antivirus himoyasi bo‘yicha yo‘riqnoma”da belgilangan.

136. Korxonada foydalaniladigan axborotni texnik himoya qilish usullari va vositalari mazkur Siyosatni 15-ilovasida keltirilgan “Axborotni texnik himoya qilish bo‘yicha yo‘riqnoma”da belgilangan.

137. Korxonada axborotning kriptografik himoyasi, axborotni kriptografik himoya qilish vositalari (AKHV) ni qo‘llash orqali ta’minlanadi.

138. Korxonada axborotni kriptografik himoya qilish vositalari (AKHV) quyidagi maqsadlarda qo‘llaniladi:

1) Korxonaning ayrim xodimlari tomonidan tashqi tizimlardan foydalanilganda, himoyalangan elektron pochta tizimi EHAT, ijro intizomini nazorat qilish edo.ijro.uz tizimi hamda korxona uchun buxgalteriya hisobi va hisobot tizimi Faktura.uz. .

3) Korxona xodimlari tomonidan EHAT tizimiga kirish va unda ishlash jarayonida elektron raqamli imzodan (ERI) foydalanish.

4) himoyalangan aloqa kanallari va ulanishlarni tashkil etish;

5) Internet tarmog‘ida rasmiy veb-saytni identifikatsiya qilish, shuningdek, Internet foydalanuvchilarining unga himoyalangan ulanishlarini SSL-sertifikat orqali ta’minlash.

Korxonada (AKHV) ayrim xodimlar tomonidan himoyalangan elektron pochta tizimi EHATdan foydalanishi va shuningdek korxonaning veb-saytini SSL-sertifikat orqali himoya qilishda qo‘llaniladi.

139. Korxonada faqatgina O‘zbekiston Respublikasi Prezidentining 2007-yil 3-apreldagi 614-PQ-sonli Qaroriga muvofiq sertifikatsiyadan o‘tgan (AKHV)lardan foydalanilishi shart.

140. Korxonada qo‘llaniladigan usullar hamda (AKHV) mazkur Siyosatni 16-ilovasida keltirilgan “Axborotni kriptografik himoya qilishni tashkil etish bo‘yicha yo‘riqnoma”da keltirilgan.

11.8. Tashqi korxonalar va tashqi foydalanuvchilarga nisbatan choralar

141. Tashqi korxonalar va tashqi foydalanuvchilarga nisbatan choralar Korxona ular bilan o‘zaro aloqada bo‘lganida axborot xavfsizligi risklarini kamaytirishga yo‘naltirilgan bo‘lishi kerak. Ushbu choralar Korxonaning himoya obyektlari xavfsizligini ta’minlash maqsadida qo‘llanilishi kerak, ularga tashqi korxonalar va foydalanuvchilar kirish huquqiga ega bo‘lgan yoki ega bo‘lishi mumkin bo‘lgan obyektlar. Bunda tashqi korxonalar va foydalanuvchilar himoya obyektlariga nafaqat jismoniy, balki mantiqiy (elektron) kirish huquqiga ega bo‘lishi mumkin.

143. Axborot texnologiyalarini joriy etish va rivojlantirish bilan bog‘liq xizmatlar ko‘rsatadigan va ishlarni amalga oshiradigan uchinchi tomon korxonalari (pudratchilar, ishlab chiquvchilar, yetkazib beruvchilar), shuningdek, axborot xavfsizligini ta’minlash xizmatlarini ko‘rsatadigan autsorsing korxonalari bilan o‘zaro aloqada, Korxona quyidagi axborot xavfsizligi choralarini belgilaydi:

1) Korxonaning himoya obyektlariga kirish va ishlashga ruxsat berilgan uchinchi tomon korxonasi va uning mutaxassislariga qo‘yiladigan talablarni shartnoma tuzilishidan oldin belgilash;

2) Uchinchi tomon korxonalari bilan tuziladigan shartnomaga axborot xavfsizligi talablarini kiritish;

3) Uchinchi tomon korxonalari bilan konfidensiallik kelishuvlarni tuzish;

4) Uchinchi tomon korxonasi xizmat ko‘rsatish yoki ishlarni bajarish vaqtida kirish huquqiga ega bo‘ladigan ma’lumotlar va himoya obyektlari ro‘yxatini, shuningdek, kirishga ruxsat berilgan uchinchi tomon korxonasi va uning vakillari ro‘yxatini tuzish;

5) Uchinchi tomon korxonasi uchun kirish ruxsatini olish tartibini belgilash, kirish turlari va kirishni amalga oshirish tartibini ko‘rsatish;

6) Ishlarni boshlashdan oldin korxonaning axborot xavfsizligi talablarini uchinchi tomon korxonasi mutaxassislariga yetkazish;

7) Uchinchi tomon korxonasiga axborot va himoya obyektlariga kirishga ruxsat berishdan oldin nazorat va boshqaruv choralarini (jismoniy yoki mantiqiy) amalga oshirish;

8) Korxona boshqaruvidagi ma’lumotni qayta ishlash vositalarini uchinchi tomon korxonasi boshqaruvidagi vositalardan jismoniy ajratish;

9) Uchinchi tomon korxonasining korxonaning himoya obyektlari, axborotni qayta ishlash va uzatish tizimlariga kirishini nazorat-monitoring qilish hamda boshqarishni ta’minlash;

10) Uchinchi tomon korxonasi himoya obyektida ishlarni bajarayotganda korxona xodimining doimiy ishtirokini ta’minlash (yoki video nazorat orqali amalga oshirish);

11) Uchinchi tomon korxonasiga maxsus kirish identifikatorlarini taqdim etish, identifikatorlar himoya obyektiga kirishda afzalliklarga ega bo‘lgan huquqlarni bermasligi va Korxona xodimlariga ma’lum qilish;

12) Uchinchi tomon korxonasi ishlarini yakunlaganidan so‘ng kirish huquqlarini bekor qilish, axborot butunligini, vositalar sozlamalari va konfiguratsiyasini tekshirish;

13) Uchinchi tomon korxonasiga tegishli vositalarni qo‘llash va joylashtirishni kelishish;

14) Korxona tomonidan sotib olingan dasturiy va dasturiy-apparat vositalarni yetkazib beruvchi tomonidan to‘g‘ri xizmat ko‘rsatishni ta’minlash.

Yuqorida ko‘rsatilgan choralar, ularni bajarish tartiblari hamda korxonaning boshqa axborot xavfsizligi talablarini uchinchi tomon korxonasi bilan tuziladigan shartnomada aks

etish lozim.

144. Uchinchi tomon korxonasi bilan tuziladigan konfidensiallik kelishuvda uchinchi tomon korxonasining konfidensial ma’lumotlarini oshkor etmaslik bo‘yicha majburiyatlari va ushbu ma’lumotlarni uning aybi bilan oshkor etilgan taqdirda javobgarligi belgilanadi, jumladan, ushbu ma’lumotning oshkor etilishi natijasida korxona korxonaga yetkazilgan zararlarni qoplash majburiyati ham ko‘zda tutiladi.

Konfidensiallikni saqlashga oid kelishuv shartlari shartnoma amal qilayotgan davrda hamda uning bekor qilinishidan so‘ng kamida 5 yil davomida bajarilishi shart.

Axborot tizimlarini texnik xizmat ko‘rsatish (qo‘llab-quvvatlash) uchun uchinchi tomon korxonasi jalb qilingan taqdirda, qo‘shimcha ravishda quyidagi choralar ko‘rilishi shart:

1) Tegishli litsenziya yoki tegishli vakolatga ega korxonani jalb qilish;

2) Axborot tizimlarida ishlarni belgilangan tartibda avtorizatsiya asosida bajarish (rahbariyatdan ruxsat olish va KABT bo‘limi bilan ushbu ruxsatni kelishish);

3) Uchinchi tomon korxonasiga nazoratli kirish huquqini to‘g‘ridan-to‘g‘ri vositalarga yoki lokal tarmoq orqali taqdim etish zarurati tug‘ilganda masofaviy kirishni tashkil qilinishi mumkin, bu kirish himoyalangan ulanishlar orqali amalga oshirilishi lozim (VPN, SSH yoki RDP) va uchinchi tomon korxonaning vakillari uchun ikki faktorli autentifikatsiyadan foydalanilishi kerak;

4) Uchinchi tomon korxonasiga faqat obyektning ma’lum vositalariga va ishlarni bajarish uchun zarur bo‘lgan kirish huquqlari (vakolatlari) bilan kirish imkoniyatini taqdim etish;

5) Ishlarni boshlashdan oldin axborotni saqlash choralarini ko‘rish (ma’lumotlar, sozlamalar va dasturiy ta’minotning zaxira nusxasini yaratish);

6) Uchinchi tomon korxonasining harakatlarini qayd etish va boshqa tegishli choralar.

146. Korxonaning TJBAT tizimlariga uchinchi tomon korxonalariga, jumladan texnik qo‘llab-quvvatlash bilan bog‘liq korxonalarga masofaviy kirish berilishi taqiqlanadi. Ushbu ishlar faqat to‘g‘ridan-to‘g‘ri kirish lokal tarmoq orqali bajarilishi va korxona tomonidan nazorat qilinishi lozim.

147. Korxonaning hayotiy faoliyatini ta’minlash bilan bog‘liq tashqi xizmat ko‘rsatuvchi yetkazib beruvchilarga, jumladan telekommunikatsiya operatorlari va kommunal xizmatlar, nisbatan quyidagi choralar ko‘rilishi lozim:

1) Korxona obyektlarini tashqi yetkazib beruvchilar (telekommunikatsiya operatorlari va kommunal xizmatlar) tarmoqlariga ulashda talablarni bajarish;

2) Favqulodda vaziyatlar yuzaga kelganda barqarorlikni, uzluksiz ish faoliyatini va tiklashni ta’minlash bo‘yicha birgalikdagi choralarni ishlab chiqish;

3) Favqulodda vaziyatlarda tashqi yetkazib beruvchi bilan aloqani ta’minlash uchun mas’ul shaxslar va ular bilan bog‘lanish ma’lumotlarini shakllantirish;

4) Korxona xizmat yetkazib beruvchi o‘rtasida mas’uliyatni (risklarni) taqsimlash – yetkazib beruvchi o‘z majburiyatlarini bajarmagan taqdirda zararlarni qoplash va oqibatlarni bartaraf etish mas’uliyatini shartnomalar yoki kelishuvlarda belgilash.

150. Korxona axborot tizimlari uchinchi tomon korxonasining axborot tizimlari bilan integratsiyasida quyidagi axborot xavfsizligi choralari qo‘llaniladi:

1) Uchinchi tomon korxonaning axborot tizimlariga ulanishda axborot xavfsizligi talablarini belgilash;

2) Korxona tomonidan uchinchi tomon korxonasining o‘z axborot tizimiga ruxsatsiz mantiqiy kirishini istisno qiluvchi choralar va vositalarni belgilash;

3) Axborot tizimlari o‘rtasida ma’lumot almashish uchun himoyalangan ulanishlarni tashkil etish va boshqa tegishli choralar;

4) Korxonaning axborot tizimlari bilan uchinchi tomon korxonasining axborot tizimlari o‘rtasida ma’lumot almashish faqat veb-xizmat (API) orqali amalga oshirilishi, axborot tizimlarining ma’lumotlar bazalariga to‘g‘ridan-to‘g‘ri ulanish taqiqlanishi.

Yuqorida ko‘rsatilgan choralarning barchasi ikki tomonlama kelishuvlar yoki shartnomalarda bayon etiladi. Axborot tizimlari o‘rtasida himoyalangan ulanishlarni tashkil etish ushbu Siyosatning 1-ilovasida keltirilgan “Korxonaning lokal tarmog‘i va himoyalangan tarmoq ulanishlarini tashkil etish bo‘yicha nizom”da belgilangan tartibga muvofiq amalga oshiriladi.

Korxona axborot tizimlarini uchinchi tomon korxonasining axborot tizimlariga ulashda mazkur Siyosatning 2-ilovasida keltirilgan “Tarmoq infratuzilmasi darajasida axborot xavfsizligini ta’minlash va xavfsizlik devorlari to'g'risidagi nizom”ga muvofiq tarmoqlar aro ekranlash choralari qo‘llanilishi lozim.

153. Uchinchi tomon korxonalari vakillarini qabul qilish va ular bilan uchrashuvlar o‘tkazish jarayonida, ularning himoya obyektlariga ruxsatsiz jismoniy kirishini istisno etish maqsadida korxona tomonidan quyidagi choralar ko‘rilishi lozim:

1) Vakillarni qabul qilish va uchrashuvlarni qabul xonalarida (muzokara zallari va tashrif buyuruvchilarni qabul qilish xonasi) yoki yuqori xavfsizlik zonalaridan uzoqroqda joylashgan maxsus xonalarda o‘tkazish;

2) Korxonaning boshqarmasi binosiga tashrif buyuruvchilarning binoga kirish-chiqishni ro‘yxatga olish jurnalida qayd etish, shuningdek ularni kirib-chiqishini korxonaning KBNT tizimi orqali ro‘yxatga olish;

3) Korxona hududiga tashrif buyuruvchilarning kirishini faqat bir martalik ruxsatnomalar asosida amalga oshirish hamda ularning kirib-chiqishini maxsus jurnalga qayd etish;

4) Tashrif buyuruvchini bino ichida yoki hududda Korxona xodimlari tomonidan kuzatib borishi;

5) Uchinchi shaxslar tomonidan korxona ishlab chiqarish hududiga ma’lumotni qayta ishlash vositalari, mobil qurilmalar va raqamli ma’lumot tashuvchilarni olib kirishga cheklovlar o‘rnatish;

6) Tashrif buyuruvchiga lokal tarmoqqa yoxud Korxonaning axborot tizimlariga ulangan oxirgi qurilmalarda ishlash huquqini berishga cheklovlar o‘rnatish, shuningdek ularning qurilmalarini korxona tarmoqlari va axborot tizimlariga ulashga yo‘l qo‘ymaslik.

157. Tashqi korxonalar va tashqi foydalanuvchilarga nisbatan choralarni ta’minlash bo‘yicha talablar Korxonaning KABT boshqarmasi bilan birga korxonaning tegishli bo‘linmalari bilan birgalikda belgilanadi va ushbu talablarning bajarilishi korxona xodimlari tomonidan nazorat qilinadi.

Korxona tomonidan belgilangan, tashqi korxonalar va tashqi foydalanuvchilarga nisbatan choralarni ta’minlash bo‘yicha talablar KABT boshqarmasi bilan kelishilgan bo‘lishi shart.

12. Axborot xavfsizligi insidentlariga munosabat

158. Korxonada axborot xavfsizligi insidentlarini boshqarishda O‘z DSt 3386, O‘z DSt 3387, O‘z DSt 3361 hamda O‘z DSt ISO/IEC 27037 standart talablariga muvofiq mas’uliyatli, samarali va tizimli yondashuv qo‘llanilishi lozim.

159. Korxona axborot xavfsizligi insidentlarini boshqarishning maqsadlari quyidagilardan iborat:

- axborot xavfsizligi insidentlari oqibatida Korxonaga yetkazilgan zarar va yo‘qotishlarni minimallashtirish – xarajatlarni kamaytirish;
- tahdidlarni imkon qadar qisqa muddatda lokalizatsiya qilish va oldini olish maqsadida insidentlarga tezkor hamda samarali javob berish – to‘xtab qolish vaqtini kamaytirish;
- insidentlardan xulosa chiqarish orqali ularning takror yuzaga kelish riskini kamaytirish yoki kelgusida ularni oldini olish – insidentlar takrorlanishini bartaraf etish;
- Korxona va uning faoliyati uchun insidentlarning salbiy oqibatlarini imkon qadar kamaytirish – salbiy oqibatlarning oldini olish;

- eskalatsiya jarayoni (yuqori turuvchi korxonalarga murojaat qilish jarayoni) orqali inqirozli vaziyatlarni boshqarish hamda biznes uzluksizligini ta’minlashga tegishli elementlari bilan o‘zaro aloqani o‘rnatish – boshqaruvchanlikni saqlab qolish;

- axborot xavfsizligi zaifliklarini baholash va ularni bartaraf etish bo‘yicha tegishli choralarni ko‘rish orqali insidentlar sonini oldini olish yoki kamaytirish – zaifliklarni kamaytirish.

Korxona axborot xavfsizligi insidentlarini boshqarish bo‘yicha ko‘rsatilgan maqsadlar axborot xavfsizligi insidentlarini boshqarishda, insidentlarga javob berish bo‘yicha ustuvor yo‘nalishlarni to‘g‘ri anglab olishlari uchun mas’ul bo‘lgan xodimlarga yetkazilishi lozim.

160. Korxona insidentlarni boshqarish jarayonlarida rahbariyatdan quyi qatlamgacha barcha xodimlar ishtirok etishlari lozim.

161. Korxona rahbariyati axborot xavfsizligi insidentlarini boshqarish bo‘yicha vazifalariga quyidagilar kiradi:

1) Korxonada insidentlarni boshqarish maqsadlari va ustuvor yo‘nalishlarini belgilash;

2) Axborot xavfsizligi insidentlarini boshqarish protseduralari yoki jarayonlarini o‘tkazishga rozilik yoki ruxsat berish;

3) vazifalarni taqsimlash va insidentlarni boshqarish uchun mas’ullarni tayinlash;

4) insidentlarni bartaraf etish, ularning oqibatlarini bartaraf etish va insidentlarni qayta yuzaga kelishining oldini olish choralarini amalga oshirish uchun Korxona resurslarini ajratish yoki taqsimlash;

5) axborot xavfsizligi insidentlarini boshqarish jarayoniga tashqi korxonalarni jalb qilish va xabardor qilish bo‘yicha qarorlar qabul qilish;

6) insidentlarga sababchi bo‘lgan shaxslarga nisbatan jazo choralarini belgilash.

162. Korxona xodimlarining axborot xavfsizligi insidentlarini boshqarish jarayonlaridagi vazifalari quyidagilardan iborat:

1) axborot xavfsizligini ta’minlash bo‘yicha talab va qoidalarga rioya qilish;

2) o‘zlari tomonidan aniqlagan yoki ma’lum bo‘lgan axborot xavfsizligi insidentlari haqida darhol xabar berish;

3) insidentlarni bartaraf etishda qat’iy choralar ko‘rilmasa, salbiy oqibatlarga olib kelishi mumkin bo‘lgan buzilish faktlarini yashirishga yo‘l qo‘ymaslik;

4) Korxona xizmatlaridagi kuzatilgan yoki taxmin qilingan axborot xavfsizligi kamchiliklari haqida xabar berish;

5) Korxonaga katta zarar yetkazilishini oldini olish maqsadida, insidentlarning oqibatlarini bartaraf etish bo‘yicha kelishilmagan harakatlarni amalga oshirishga yo‘l qo‘ymaslik;

6) Insidentlarni tekshirish jarayonlarida ko‘maklashish.

163. Korxonada axborot xavfsizligi insidentlarni boshqarish jarayonlarida ishtirokchilar quyidagilar hisoblanadi:

1) KABT boshqarmasi — korxonada axborot xavfsizligi insidentlarini boshqarish jarayonlarini tashkil etish va amalga oshirish;

2) Axborot xavfsizligi administratori — Korxonada axborot xavfsizligini ta’minlash uchun mas’ul xodimi;

3) Kuzatuv nazorat va tahlil bo‘limi xodimlari — korxonada jismoniy xavfsizlikni ta’minlash uchun mas’ul xodimlar;

4) KABT boshqaruv bo‘linmasi xodimlari — himoya obyektlaridagi dasturiy va apparat vositalarni, shu jumladan axborot tizimlari, resurslar, lokal tarmoqlariga xizmat ko‘rsatish uchun mas’ul xodimlar.

Korxonada:

1) KABT bo‘linma — korxonada axborot xavfsizligi insidentlarini boshqarish jarayonlarini tashkil etish va amalga oshirish, shuningdek himoya ob’ektlaridagi dasturiy va dasturiy-apparat vositalarni, axborot tizimlari, resurslar va lokal tarmoqni xizmat ko‘rsatish;

2) TJBAT bo‘limi xodimlari — ishlab chiqarish hududidagi lokal tarmoq va unga bog‘langan TJBAT tizimlarining ishlashini ta’minlash uchun mas’ul xodimlar;

3) Korxonaning xavfsizlik xizmati xodimlari — Korxonada jismoniy xavfsizlikni ta’minlash uchun mas’ul xodimlar.

Shuningdek, Korxona axborot xavfsizligi insidentlarini boshqarish jarayonlariga qo‘shimcha ravishda quyidagilar jalb qilinishi mumkin:

1) Xodimlar bilan ishlash boshqarmasi xodimlari — insidentlarni boshqarishda xodimlarning mas’uliyatini kuchaytirish va xabardorligini oshirish bo‘yicha;

2) Yuridik boshqarmasi xodimlari — aybdorlarni javobgarlikka tortish bo‘yicha;

3) Buxgalteriya bo‘limi xodimlari — zarar va yo‘qotishlarni baholash bo‘yicha va boshqa masalalarda.

164. Korxonada axborot xavfsizligi insidentlariga tezkor javob qaytarishni ta’minlash maqsadida doimiy faoliyat yurituvchi hodisalarga javob berish guruhlari tashkil etiladi. Insidentlarga javob berish guruhlari Korxonaning buyruqlari bilan tuziladi hamda ularning tarkibi mazkur buyruqlar bilan belgilanadi.

165. Korxona insidentlarga javob berish guruhining vazifalariga quyidagilar kiradi:

1) axborot xavfsizligi tahdidining ta’sirini lokalizatsiya qilish va neytrallashtirish bo‘yicha chora-tadbirlarni amalga oshirish;

2) axborot xavfsizligi insidentining oqibatlarini baholash;

3) tiklash ishlarini tashkil etish va o‘tkazish hamda insident oqibatlarini bartaraf etish;

4) insident-tekshirish ishlarida insidentning kelib chiqish sabablarini aniqlash;

5) Shunga o‘xshash insidentlarning yuzaga kelishiga yo‘l qo‘ymaslik maqsadida insidentni tahlil qilish, insidentdan olingan tajriba va aniqlangan zaifliklarni belgilash.

166. Korxona axborot xavfsizligi insidentlarini boshqarishda quyidagi bosqichlar qo‘llanilishi lozim:

1) rejalashtirish va tayyorgarlik;

2) aniqlash va hisobot berish;

3) baholash va qaror qabul qilish;

4) javob choralarini ko‘rish;

5) tekshiruv o‘tkazish (zarurat bo‘lganda);

6) tajriba orttirish.

167. Korxonaning barcha himoya obyektlari axborot xavfsizligi insidentlarini aniqlash maqsadida monitoring qilinadi.

Korxonaning MAI obyektlari (TJBAT) uchun (24/7) rejimida monitoring amalga oshirilishi shart.

Korxonaning himoya obyektlarida axborot xavfsizligi insidentlari to‘g‘risidagi ma’lumotlar manbalari quyidagilardan iborat:

- axborot tizimlari, uskuna va dasturiy vositalarning tizim jurnallari (log-fayllar) ma’lumotlari, shuningdek funksionallik monitoringi tizimi ma’lumotlari;

- axborotni himoya qilish vositalarining chiqish ma’lumotlari (tarmoqlararo ekranlar, antivirus himoya vositalari va boshqalar);

- Korxona uskuna va tarmoq vositalari, axborot resurslari hamda axborot tizimlarining ish holatini vizual nazorat qilish;

- video kuzatuv kameralardan olingan ma’lumotlar;

- axborot xavfsizligi bo‘yicha ichki yoki tashqi audit natijalari;

- xodimlardan kelib tushgan axborot yoki xabarlar (axborot tizimlarining noto‘g‘ri ishlashi, aloqa uzilishi, yong‘in va qo‘riqlash xavfsizligi buzilishi, moddiy aktivlarning yo‘qolishi, himoyalangan axborot konfidensialligining buzilishi va boshqalar haqida);

- qo‘riqlash xavfsizligi buzilishlari (ruxsatsiz jismoniy kirish);

- o‘g‘rilik, talon-toroj, ma’lumotlar sizib chiqishi, ruxsatsiz ulanish va boshqa holatlar aniqlangan faktlar.

169. Korxona insidentlari to‘g‘risidagi ma’lumotlarni yig‘ish va tahlil qilish KABT boshqarmasi tomonidan, tizimosti korxonada esa – KABT boshqarmasi tomonidan amalga oshiriladi.

171. Korxonada quyidagi axborot xavfsizligi hodisalari insident sifatida qaralishi lozim:

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

2) himoya obyektlarining ishlash va funksionallikdagi nosozliklari — server va tarmoq uskunalari, dasturiy ta’minotdagi nosozliklar, texnik xatoliklar, xizmat ko‘rsatishdagi xatolar, dasturiy ta’minotdagi zaifliklar, ruxsatsiz mantiqiy yoki jismoniy kirishlar, zararli dasturiy ta’sirlar;

3) himoyalangan axborotning konfidensialligi, yaxlitligi va mavjudligi buzilishi hamda axborotni himoya qilish talablarining buzilishi;

4) o‘g‘rilik, talon-toroj, ma’lumotlar oqimi va boshqa ruxsatsiz harakatlar natijasida moddiy zarar, qimmatbaho moddiy aktivlar, vositalar, raqamli tashuvchilar va himoyalangan axborotning yo‘qolishi yoki o‘g‘irlanishi;

5) tashqi tarmoq, lokal tarmoq va lokal tarmoqlardagi aloqa uzilishi, tarmoq uskunalarining texnik nosozliklari, kabel uzilishi va shunga o‘xshash holatlar;

6) korporativ va lokal tarmoqlarga ruxsatsiz qurilmalar va tarmoq uzellarining ulanishi;

7) axborotni himoya qilish vositalarining har qanday sabablarga ko‘ra ishlamasligi, texnik nosozlik, inson omiliga bog‘liq xatolar yoki tarmoq hujumlari va zararli dasturlar natijasida;

8) ruxsatsiz yoki notog‘ri jismoniy kirish, shu jumladan hududga, binoga va himoyalangan xonalar yoki himoya obyektlariga kirish;

9) ruxsatsiz yoki notog‘ri mantiqiy kirish urinishlari va aniqlangan faktlar;

10) DoS (Denial of Service) va DDoS (Distributed Denial of Service) xizmat ko‘rsatishni rad etishi;

11) axborotni himoya qilish vositalari orqali aniqlangan tarmoq hujumlari va buzilishlar;

12) Aniqlangan xavfli viruslar va zararli dasturlar, shu jumladan josuslar va dasturiy ta’minotdagi e’lon qilinmagan funksiyalar;

13) Tashqi buzuvchilar yoki xodimlarning axborotni yig‘ish va olish bo‘yicha noqonuniy harakatlari.

172. Ish jarayonida insidentlar aniqlanganda, Korxona xodimi darhol KABT bo‘linmasiga xabar berishi lozim.

173. Korxonada KABT bo‘linmasi axborot xavfsizligi insidentlarini tahlil qilish va ularni tasniflash, shuningdek insidentlarni ro‘yxatga olish va hisobga olish uchun mas’uldir.

174. Ushbu bo‘limning 171-bandida ko‘rsatilgan barcha axborot xavfsizligi insidentlari, Korxonada sodir bo‘lgan bo‘lsa, ro‘yxatga olinishi va hisobga olinishi shart.

Axborot xavfsizligi insidentlarini korxonada ro‘yxatga olish va hisobga olish tartibi ushbu Siyosatning 20-ilovasida “”Axborot xavfsizligi insidentlariga javob berish reglamenti”da keltirilgan.

Axborot xavfsizligi insidentlarini hisobga olish ularning sabablarini aniqlash, insidentni tahlil qilish va axborot xavfsizligi riskini baholash maqsadida amalga oshiriladi.

175. Insidentlar haqida xabardor qilinishi yoki ogohlantirilishi lozim bo‘lgan shaxslar:

- Korxonada insident ta’sir ko‘rsatgan ishlab chiqarish bo‘limi yoki texnologik jarayon uchun mas’ul bo‘lgan tarkibiy bo‘linmalar rahbarlari;
- Himoya obyektiga xizmat ko‘rsatish uchun mas’ul bo‘lgan tarkibiy bo‘linma rahbari yoki mutaxassis (administrator);
- Korxona rahbariyati, agar axborot xavfsizligi insidenti «yuqori» xavf darajasiga ega bo‘lsa;
- Tashqi manfaatdor korxonalar;
- Korxona xodimlari.

176. Agar korxonaning TJABT tizimida axborot xavfsizligi insidenti yuzaga kelsa, korxona MAI subyekti sifatida darhol Kiberxavfsizlik Markazini xabardor qilishi shart.

Korxonaning KABT bo‘linmasi ushbu obyektlardagi insidentlar haqida xabar berish va insidentlarga javob berish bo‘yicha Kiberxavfsizlik Markazi bilan hamkorlik qilish uchun mas’uldir.

177. Insidentga javob choralarini amalga oshirish bosqichida insidentning yuzaga kelishiga sabab bo‘lgan tahdidning ta’siri cheklanishi yoki neytrallanishi lozim bo‘lib, bu insidentdan keladigan zararlarni minimallashtirish maqsadida amalga oshiriladi. Tahdidni cheklash yoki neytrallashdan so‘ng, insident sababli to‘xtatilgan jarayonlarni tiklash va insident oqibatlarini bartaraf etish ishlari amalga oshirilishi lozim.

Tahdidning ta’sirini cheklash va neytrallash, insident oqibatlarini baholash, tiklash va bartaraf etish ishlari uchun korxonada tashkil etilgan insidentlarga javob berish guruhlari mas’uldir. Insidentlarga javob berish bo‘yicha mazkur ishlar guruh rahbarlari tomonidan muvofiqlashtiriladi.

Zarurat tug‘ilganda va korxona rahbariyati bilan kelishilgan holda, axborot xavfsizligi insidentlariga javob berish ishlariga boshqa tarkibiy bo‘linma xodimlari yoki manfaatdor korxonalar xodimlari jalb qilinishi mumkin.

178. Zarurat tug‘ilganda yoki ma’lum turdagi insidentlar yuzaga kelganda, korxona quyidagi maqsadlarda tekshirish jarayonlarini boshlashi mumkin:

- Insidentning haqiqiy sabablarini aniqlash;
- Insidentning yuzaga kelishiga sababchi bo‘lgan shaxslarni javobgarlikka tortish;
- Dalillarni (guvohliklarni) yig‘ish, tahlil qilish va saqlash.

Korxona insident bo‘yicha tekshiruv o‘tkazish uchun maxsus guruh tuziladi, guruh tarkibi korxona rahbariyati bilan kelishiladi.

179. Axborot xavfsizligi insidentlarini boshqarish jarayonida dalillarni yig‘ish axborotni aniqlash, yig‘ish, olish va saqlashga qaratilgan bo‘lishi lozim, bu axborot sud va boshqa tekshiruvlarda dalil sifatida xizmat qilishi, aybdorlarni javobgarlikka tortish yoki intizomiy chora qo‘llash uchun asos bo‘lishi mumkin.

180. Tadqiqot bosqichida axborot xavfsizligi insidenti tahlil qilinishi lozim. Axborot xavfsizligi insidenti tahlili natijalariga ko‘ra quyidagilar aniqlanishi kerak:

- insidentga sabab bo‘lgan tahdidlarning xususiyatlari, aniqlangan tahdid turlarining yuzaga kelish chastotasi;
- insidentning sabablarini yoki tahdidlar manbalarini aniqlash;
- insident uchun foydalanilgan zaifliklar;
- insident oqibatlarini baholash - yetkazilgan zarar va yo‘qotishlar miqyosini aniqlash;
- insidentlarni va Axborot xavfsizligini boshqarish tizimidagi mavjud xatolar va kamchiliklar;
- Xodimlarning, shuningdek insidentlarni boshqarish protseduralari va jarayonlarining samaradorligini baholash.

181. Axborot xavfsizligi insidentlarini tahlil qilish natijalari hamda insidentdan olingan saboqlar quyidagi yo‘nalishlarda chora-tadbirlarni ishlab chiqish va qabul qilish uchun qo‘llanilishi lozim:

- kelgusida shunga o‘xshash insidentlarning qayta yuzaga kelishining oldini olish yoki ularning yuzaga kelish ehtimolini kamaytirish;
- aniqlangan zaiflik va kamchiliklarni bartaraf etish, himoya usul hamda vositalarini takomillashtirish, ularning samaradorligini oshirish;
- insidentlarni boshqarish usullari, vositalari va tartib-taomillarini yanada takomillashtirish.

182. Korxonadagi axborot xavfsizligi insidentlariga oid ma’lumotlar, jumladan:

- hodisalar va insidentlar to‘g‘risidagi ma’lumotlar, shuningdek ular bo‘yicha hisobotlar;
- insidentlar bilan bog‘liq zaifliklar to‘g‘risidagi ma’lumotlar;

- insidentlarni tahlil qilish natijalari;

- insidentlarni tekshirish (surishtiruv) natijalari;

- insidentni tekshirish jarayonida to‘plangan dalillar (isbot materiallari), konfidensial hisoblanadi.

Insidentlar bo‘yicha ma’lumotlar korxonaning KABT bo‘linmasida saqlanadi.

183. Axborot xavfsizligi insidentlarini boshqarish jarayonida korxona quyidagi tashqi korxonalar bilan hamkorlik qilishi mumkin:

1) insidentlar, ko‘rilgan choralar hamda ularni amalga oshirish jarayoni bo‘yicha axborot taqdim etish masalasida Kiberxavfsizlik markaz va boshqa vakolatli organlar;

2) Korxona o‘z faoliyati davomida hamkorlik qiladigan subyektlar bilan insidentlar haqida xabardor qilish, ularni bartaraf etish, oqibatlarini tugatish va kelgusida takrorlanishining oldini olish bo‘yicha qo‘shma choralarni ishlab chiqish masalasida manfaatdor uchinchi tomon korxonalar (telekommunikatsiya operatorlari, xizmat ko‘rsatuvchi provayderlar, yetkazib beruvchilar, mijozlar, o‘zaro integratsiyalashgan axborot tizimlariga ega uchinchi korxonalar hamda tashqi foydalanuvchilar – Ta’sischi);

3) jinoyat ishlarini qo‘zg‘atish va insidentlarni tergov qilishda ishtirok etish masalasida huquqni muhofaza qiluvchi organlar;

4) favqulodda vaziyatga olib kelgan insidentlar haqida xabardor qilish, ularning oqibatlarini bartaraf etishga jalb etish hamda sabablarini o‘rganish masalasida favqulodda vaziyatlar bo‘yicha organlar;

5) Insidentlar haqida ogohlantirish, ularni bartaraf etish, kamchiliklarni yo‘qotish yoki xizmatlar ko‘rsatishni qayta tiklash haqida axborot berish masalasida korxona mijozlari.

Axborot xavfsizligi insidentlarini boshqarish jarayonida korxonaning tashqi korxonalar bilan o‘zaro hamkorlik qilish tartibi mazkur Siyosatning 20-ilovasida keltirilgan “Axborot xavfsizligi insidentlariga javob berish reglamenti”da belgilangan.

13. Aloqa kanallari xavfsizligini ta’minlash

184. Korxonada (boshqarma, ishlab chiqarish hududidagi binolar, ishlab chiqarish hududidan tashqaridagi binolar) hamda korxonada ma’lumotlarni uzatish uchun foydalaniladigan elektr ta’minoti kabellari va tarmoq kabellari axborotni tutib qolish hamda ularning shikastlanishini oldini olish maqsadida ruxsatsiz ochilishdan himoyalangan bo‘lishi lozim.

Mazkur xavflarni kamaytirish uchun quyidagi himoya choralari amalga oshiriladi:

1) tarmoq kabelini kanalizatsiya va kollektorlar orqali, binolarda esa tegishli tarzda noxush jismoniy kirishdan himoyalangan kanallarda, qutilarda yoki qoplamalarda o‘tkazish;

2) tarmoq kabelining o‘tkazilish marshrutini ommaviy foydalanish uchun mo‘ljallanmagan joylarga o‘tkazmaslik;

3) o‘zaro salbiy ta’sirini oldini olish uchun, tarmoq kabelini elektr kabelidan alohida o‘tkazish;

4) tarmoq kabeli rozetkalari ishlatilmasa, ularni maxsus tamg‘alar bilan yopish yoki yopishtirish;

5) krossli va ulanish uskunalarini, ularga ulanadigan tarmoq kabeli bilan, himoya qilingan xonalar yoki yopiladigan ulanish shkaflarida joylashtirish;

6) telekommunikatsion va server uskunalarini boshqarish vositalari orqali ishlatilmagan tarmoq portlarini o‘chirish;

7) kabel o‘tkazishning o‘rta va oxirgi nuqtalaridagi xonalar va shkaflarni yopish va himoya qilingan xonalarda armatura kabelarini ishlatish;

8) kabellarni elektromagnit ekranlashni yoki optik tolali kabellarni ishlatish;

9) kabelning har bir uchida manzil va manba haqida yetarli ma’lumotlarni ko‘rsatib belgilash, bu esa kabelni jismoniy aniqlash va tekshirishga yordam beradi;

10) ruxsatsiz qurilmalarning kabel tarmog‘iga ulanishi yuzasidan tekshiruvlar o‘tkazish (zondlash yoki jismoniy tekshirish).

186. Korxona ichida (boshqarma, ishlab chiqarish hududidagi binolar, ishlab chiqarish hududidan tashqaridagi binolar), korxona bilan, shuningdek tashqi korxonalar bilan himoyalangan axborot va yozishmalar almashinuvi uchun tashqi himoyalangan elektron pochta tizimi E-xat himoyalangan elektron pochta tizimidan foydalaniladi. Ushbu tizimga korxona devonxona xodimlari ulangan.

187. Korxona xodimlari uchun Internet tarmog‘iga markazlashtirilgan kirish korxona lokal tarmog‘ining Internet tarmog‘iga ulanish chegarasida o‘rnatilgan axborotni himoya qilish vositalari orqali tashkil etiladi.

Internet tarmog‘iga ulanish va undan foydalanish tartibi hamda talablari, shu jumladan Internetdan foydalanishda belgilangan cheklovlar, Korxona xodimlari uchun mazkur Siyosatning 14-ilovasida keltirilgan “Internet tarmog‘i va elektron pochta bilan ishlash bo‘yicha yo‘riqnoma”da belgilangan.

188. Korxonaning lokal tarmoqlarini (boshqarma, ishlab chiqarish hududidagi binolar, ishlab chiqarish hududidan tashqaridagi binolar) hamda korxonaning lokal tarmog‘ini qurishda, shuningdek ushbu tarmoqlarga kirish nuqtalarini tashkil etishda Wi-Fi simsiz aloqa texnologiyalaridan foydalanishga yo‘l qo‘yilmasligi lozim.

189. Korxona boshqarma (xodimlar uchun) hamda videokonferensiya zalida (xodimlar va tashrif buyuruvchilar uchun) Wi-Fi tarmog‘i quyidagi talablar asosida tashkil etiladi:

- Wi-Fi tarmog‘iga xavfsiz ulanish uchun Internet-provayder tomonidan alohida ulanish nuqtasi tashkil etilgan. Ushbu nuqtaga ulangan qurilmalardan korxona lokal tarmog‘iga ulanish imkoniyati mavjud emas.

190. Korxonaning ma’muriy binosida Wi-Fi tarmog‘i quyidagi talablar asosida tashkil etiladi:

- Wi-Fi tarmog‘i alohida fizik tarmoq sifatida tashkil etiladi (kirish nuqtalari idoraviy korxonaning lokal tarmog‘iga ulanmaydi);

- tarmoq faqat Internet tarmog‘iga kirish uchun ishlatiladi, bunda Wi-Fi tarmog‘ining Internetga alohida ulanishi ta’minlanadi (lokal tarmoqning Internetga ulanish kanali ishlatilmaydi);

- Wi-Fi tarmog‘iga korxona lokal tarmog‘iga ulangan oxirgi qurilmalarni ulash taqiqlanadi;

- Wi-Fi tarmog‘iga ulanish uchun alohida oxirgi qurilmalar ishlatiladi – korxonaga tegishli mobil hisob qaydnomali qurilmalar yoki xodimga tegishli qurilmalar;

- Wi-Fi tarmog‘iga ulanishda xodim oxirgi qurilmaning MAC-manzili va login-parol orqali autentifikatsiyadan o‘tishi shart.

191. Korxonaning ishlab chiqarish lokal tarmog‘iga va TJBAT tizimiga har qanday masofaviy kirish tashkil etilishi ham taqiqlanadi.

192. Quyidagi masofaviy kirishlar korxona xodimlari uchun tashqi tarmoq orqali tashkil etilishi mumkin:

1) Korxona xodimlarining xizmat safarida yoki korxona hududidan tashqarida bo‘lganida EHAT tizimiga ulanishi;

2) Imtiyozli foydalanuvchilarning Korxonadagi uskunalarni masofadan xizmat ko‘rsatish uchun ulanishi.

Masofaviy kirishni tashkil etishda va undan foydalanishda axborot xavfsizligini ta’minlash bo‘yicha talablar mazkur Siyosatning 1-ilovasida keltirilgan “Korxonaning lokal tarmog‘i va himoyalangan tarmoq ulanishlarini tashkil etish bo‘yicha nizom”da belgilangan.

14. Javobgarlikni taqsimlash

193. Vazifalar va mas’uliyatlar korxonada axborot xavfsizligini boshqarish bo‘yicha rahbariyat, tuzilma bo‘linmalari, alohida xodimlar va korxona xodimlari o‘rtasida aniq va hujjatlashtirilgan tarzda taqsimlanishi shart.

194. Vazifalar va mas’uliyatlarni taqsimlash hamda axborot xavfsizligi protseduralarini joriy etish korxona rahbariyati hamda ularning tuzilma bo‘linmalari rahbarlariga yuklatiladi.

195. Korxona rahbariyatining axborot xavfsizligini ta’minlashdagi asosiy vazifalari quyidagilardan iborat:

1) Axborot xavfsizligini ta’minlash maqsadlarini belgilash, ular korxona talablari bilan mos bo‘lishi;

2) Axborot xavfsizligi Siyosatini shakllantirish, ko‘rib chiqish va tasdiqlash;

3) Axborot xavfsizligi Siyosatini joriy etish samaradorligini nazorat qilish;

4) Xavfsizlikni oshirish bo‘yicha tashabbuslarni aniq rahbarlik va sezilarli ma’muriy qo‘llab-quvvatlash bilan ta’minlash;

5) Axborot xavfsizligini ta’minlash uchun zarur resurslarni ajratish;

6) Axborot xavfsizligi uchun javobgar shaxslarni tayinlash va ularning vazifalarini belgilash, Korxonaning axborot xavfsizligini boshqarish tuzilmasini aniqlash va o‘zgartirish;

7) Xodimlarning axborot xavfsizligi bo‘yicha xabardorligini oshirish bo‘yicha rejalari va dasturlarini yo‘lga qo‘yish;

8) Korxona doirasida axborot xavfsizligi loyihalarini tasdiqlash;

9) Axborot xavfsizligi talablarini barcha korxona loyihalariga kiritilganini hisobga olish;

10) Yangi va mavjud tizimlar uchun axborot xavfsizligini boshqarish bo‘yicha maxsus tadbirlarni joriy etishning yetarliligi va muvofiqligini baholash va muvofiqlashtirish;

11) Axborot xavfsizligi buzilish hodisalarini tekshirish natijalarini tahlil qilish va aybdorlarni javobgarlikka tortish;

12) Xodimlarni qo‘llab-quvvatlash, rag‘batlantirish va axborot xavfsizligi samaradorligini oshirishga hissa qo‘shganlarni rag‘batlantirish.

196. Korxonada axborot xavfsizligini boshqarish bo‘yicha faoliyat korxona rahbari tomonidan muvofiqlashtiriladi va boshqariladi.

197. Korxonada AXBTni bevosita tashkil etish va uning samarali faoliyat yuritishini ta’minlash KABT bo‘linmasiga yuklatiladi. Mazkur bo‘linmalarning axborot xavfsizligini ta’minlash sohasidagi vazifalari va majburiyatlari mazkur Siyosatning 5-ilovasida keltirilgan “Korxonaning KABT boshqarmasi to‘g‘risida nizom”ga muvofiq belgilangan.

198. Korxonada axborot xavfsizligini boshqarish jarayonlarida quyidagilar ishtirok etadi:

1) Korxonaning KABT boshqarmasi korxonada axborot xavfsizligini ta’minlash bo‘yicha barcha faoliyat uchun, shuningdek axborotni himoya qilish vositalarini joriy etish, ularga xizmat ko‘rsatish va ularning ishlashini tiklash uchun mas’ul hisoblanadi;

2) Korxonada axborot xavfsizligini ta’minlash bo‘yicha choralarni amalga oshirish hamda talablarni bajarish uchun korxonadagi axborot xavfsizligi administratorlari mas’uldir;

3) Korxonaning binolar, xonalar va moddiy aktivlarning jismoniy himoyasini ta’minlash, shuningdek jismoniy xavfsizlik tizimlari (KBNT va videokuzatuv tizimi)ning ishlashi uchun kuzatuv nazorati va tahlil bo‘limi mas’uldir;

4) Korxonaning axborot tizimlari va resurslarining uzluksiz ishlashini ta’minlash va ularning faoliyatini tiklash, axborot almashish tizimlari (korporativ elektron pochta, IP-telefon, videokonferensaloqa), lokal tarmoqlar, shuningdek oxirgi qurilmalarning ishlashi uchun KABT boshqaruvi bo‘linmasi mas’uldir.

199. Korxonada axborot xavfsizligini boshqarish jarayonlarida quyidagilar ishtirok etadi:

1) KABT bo‘linmasi quyidagilar uchun mas’uldir:

- korxonada axborot xavfsizligini ta’minlash bo‘yicha barcha faoliyat uchun;

- axborotni himoya qilish vositalarini joriy etish, ularga xizmat ko‘rsatish va ularning ishlashini tiklash uchun;

- axborot tizimlari va resurslarining uzluksiz ishlashini ta’minlash va ularni tiklash, IP-telefoniya tizimi, jismoniy xavfsizlik tizimlari (KBNT va videokuzatuv), lokal tarmoq hamda oxirgi qurilmalarning ishlashi uchun;

2) Korxonaning TJBAT ichki ishlab chiqarish lokal tarmog‘iga xizmat ko‘rsatish hamda ularning ishlashini tiklash uchun TJBAT bo‘linmasi mas’uldir;

3) Korxona hududi, binolari, xonalari va moddiy aktivlarining jismoniy himoyasini ta’minlash uchun qo‘riqlash xizmati mas’uldir.

200. Korxonada axborot xavfsizligini ta’minlash bo‘yicha mas’uliyat quyidagilarga ham yuklatiladi:

1) himoyalanadigan axborotning (har qanday shaklda) konfidensialligi buzilganligi uchun Korxona xodimlari, shuningdek axborot aktivlari egalari shaxsan javobgar hisoblanadi;

2) axborot tizimlarida amalga oshiriladigan harakatlar uchun axborot tizimlari foydalanuvchilari bo‘lgan Korxona xodimlari o‘zlariga biriktirilgan rollar va majburiyatlar doirasida javobgar hisoblanadi;

3) axborot xavfsizligi, jumladan ishchi stansiya va boshqa qurilmalarning jismoniy xavfsizligi, raqamli axborot tashuvchilarning saqlanishi uchun ushbu qurilmalar yoki raqamli tashuvchilar ish faoliyatida foydalanish uchun topshirilgan korxona xodimi javobgar hisoblanadi;

4) Korxona obyektlari hamda tarkibiy bo‘linmalari rahbarlari yong‘in xavfsizligi va har bir xonadagi uskunalarning saqlanishi uchun javobgar hisoblanadi;

202. Korxona rahbar buyruqlari bilan Axborot tizimlariga xizmat ko‘rsatish, texnik qo‘llab-quvvatlash va ularning uzluksiz ishlashini ta’minlash maqsadida Korxonaning KABT bo‘linmasi xodimlari va TJBAT bo‘linmasi xodimlari orasidan axborot tizimlari administratorlari tayinlanadi.

203. Axborot tizimlari administratorlarining vazifalari va majburiyatlari mazkur Siyosatning 4-ilovasida keltirilgan “Axborot tizimlari administratori uchun namunaviy lavozim yo‘riqnoma”da belgilangan.

204. Korxonaning KABT boshqarmasi xodimi bo‘lgan tarmoq administratori korxonaning lokal tarmog‘ining ishlashini, shuningdek lokal tarmoqqa kiruvchi tarmoq uskunalariga xizmat ko‘rsatadi. Korxona lokal tarmog‘ining tarmoq administratorining vazifalari va majburiyatlari mazkur Siyosatning 3-ilovasida keltirilgan “Lokal tarmog‘i bo‘yicha tarmoq administratori lavozim yo‘riqnomasi”da belgilangan.

205. Korxonaning KABT bo‘linmasi xodimi hisoblangan tizim administratori lokal tarmoqining ishlashini, shuningdek lokal tarmoqqa kiruvchi tarmoq uskunalariga xizmat ko‘rsatadi. Ushbu tizim administratorning vazifalari va majburiyatlari mazkur Siyosatning 3-ilovasida keltirilgan “Korxonaning lokal tarmog‘i bo‘yicha tarmoq administratori uchun lavozim yo‘riqnoma”da belgilangan.

206. Mas’ul xodimning ish joyida vaqtincha yo‘qligida (ta’til, kasallik, xizmat safari va h.k.) uning vazifalari belgilangan tartibda tayinlangan shaxs tomonidan bajariladi. Ushbu shaxs tegishli huquqlarga ega bo‘ladi va unga yuklatilgan vazifalarni to‘g‘ri bajarishi uchun javobgar hisoblanadi.

208. Korxonada KABT boshqarmasining vazifalarini boshqaruv raisning moliya, transformatsiya va xususiylashtirish bo‘yicha birinchi o‘rinbosari tomonidan amalga oshiriladi. Korxona xodimlarining axborot xavfsizligini ta’minlash bo‘yicha vazifalarni bajarishi va talablarni rioya etishini muvofiqlashtirish hamda nazorat qilish korxonaning bo‘linma va obyekt rahbarlari tomonidan amalga oshiriladi.

209. Korxonada vazifalar va mas’uliyatlarni taqsimlash uchun quyidagi chora-tadbirlar amalga oshiriladi:

1) Himoya obyektlariga, jumladan konfidensial axborot, server xonasi, boshqa yuqori xavfsizlikka ega xonalar, korporativ va lokal tarmoqlar, axborot tizimlari va resurslar, tarmoq uskunalari va korxona ma’lumotini himoya qilish vositalariga jismoniy va mantiqiy kirish huquqiga ega shaxslar ro‘yxati shakllantiriladi;

2) Axborot xavfsizligi bo‘yicha vazifalarni tayinlash va taqsimlash, shuningdek vaqtincha ish joyida yo‘qligi vaqtida xodim vazifalarini vaqtincha bajarish (vaqtinchalik o‘rinbosarlik) to‘g‘risida Korxona tomonidan tegishli buyruq, hujjatlar qabul qilinadi;

3) Korxona bo‘linmalari va xodimlariga aktivlar tegishli korxona-huquqiy hujjatlar orqali biriktiriladi;

4) Axborot xavfsizligini ta’minlash bo‘yicha bo‘linmalar va xodimlarga biriktirilgan vazifalarni bajarilishini nazorat qilish uchun mas’ul shaxslar tayinlanadi.

210. Korxona xodimlari tomonidan axborot xavfsizligi talablariga rioya etilishi ustidan nazorat KABT boshqarmasi tomonidan amalga oshiriladi. Axborot xavfsizligi talablarini buzgan shaxslarga nisbatan O‘zbekiston Respublikasi Mehnat kodeksiga muvofiq intizomiy choralar qo‘llanishi mumkin. Jiddiy axborot xavfsizligi buzilishlari holatlarida Korxona xodimlariga nisbatan amaldagi qonunchilikka muvofiq ma’muriy va jinoiy javobgarlik qo‘llanilishi mumkin.

15. Siyosatni qayta ko‘rib chiqish va aktuallashtirish tartibi

211. Korxonaning KABT boshqarmasi Axborot xavfsizligi siyosatining aktualligi va samaradorligini quyidagilarni aniqlash maqsadida baholaydi:

- Siyosatning amaldagi tashkiliy, texnologik va axborot infratuzilmasiga hamda ularning kelgusidagi rivojlanish istiqbollariga muvofiqligi;
- Siyosatning amaldagi normativ-huquqiy hujjatlar talablariga muvofiqligi;
- Siyosatda belgilangan talablarning muvofiqligi va yetarliligi;
- Siyosatda nazarda tutilgan usul va vositalarning samaradorligi.

212. Siyosatning aktualligi va samaradorligi kamida yiliga bir marotaba davriy ravishda baholanadi.

213. Baholash tasdiqlangan Siyosat talablariga muvofiqlik yuzasidan ichki yoki tashqi audit o‘tkazish orqali amalga oshirilishi mumkin.

Korxonada ichki audit KABT boshqarmasi tomonidan tashkil etiladi va o‘tkaziladi.

Tashqi auditni o‘tkazish uchun tegishli malakaga va vakolatga ega korxonalar jalb etiladi.

214. Baholash natijalariga ko‘ra Siyosatga o‘zgartirish va qo‘shimchalar kiritish yoki uni qayta ko‘rib chiqish bo‘yicha takliflar ishlab chiqilishi mumkin. Takliflar KABT boshqarmasi tomonidan tayyorlanib, Korxona rahbariyatiga kiritiladi. Korxona rahbariyati tomonidan o‘zgartirish yoki qayta ko‘rib chiqish to‘g‘risidagi qaror qabul qilinadi.

215. O‘zgartirish va qo‘shimchalar kiritish yoki qayta ko‘rib chiqish zarurati quyidagi hollarda yuzaga keladi:

- Siyosat talablarining infratuzilmaga nisbatan nomuvofiqligi aniqlanganda;
- Siyosat qoidalari yangi yoki o‘zgartirilgan normativ-huquqiy hujjatlarga zid kelganda;
- Talablar, usullar yoki himoya vositalarining yetarli emasligi yoki samarasizligi aniqlanganda;
- Axborot xavfsizligini boshqarish yondashuvlarini takomillashtirish zarurati tug‘ilganda;
- Korxona qayta tashkil etilganda;
- AXBT tuzilmasi o‘zgarganda;
- Axborot-kommunikatsiya infratuzilmasi modernizatsiya qilinganda;
- Faoliyat, texnologik yoki ishlab chiqarish jarayonlarida o‘zgarishlar yuz berganda.

216. Siyosatni o‘zgartirish yoki qayta ko‘rib chiqishda quyidagilar ta’minlanishi lozim:

- Axborot xavfsizligini boshqarish yondashuvi va jarayonlarini takomillashtirish;

- Nazorat, boshqaruv va himoya choralarini yaxshilash;
- Resurslar va mas’uliyatni oqilona taqsimlash;
- Axborot xavfsizligi risklarini kamaytirish.

217. Siyosatning ayrim bandlari yangi normativ-huquqiy hujjatlarga zid bo‘lib qolgan taqdirda, ular tegishli o‘zgartirishlar kiritilgunga qadar yuridik kuchini yo‘qotadi.

218. O‘zgartirish va qo‘shimchalar korxona buyrug‘i bilan kiritiladi hamda barcha xodimlarga yetkaziladi. Tasdiqlangan tahrir KABT boshqarmasida saqlanadi.

219. Agar o‘zgarishlar Siyosat mazmunining 30% dan ortig‘iga ta’sir qilsa, u to‘liq qayta ko‘rib chiqiladi va yangi tahrir ishlab chiqiladi.

220. Yangi tahrir O‘zMSt 816 standartiga muvofiq qayta kelishiladi.

221. Kelishuvdan so‘ng yangi tahrir Korxona rahbari tomonidan tasdiqlanadi va buyruq bilan kuchga kiritiladi. Zarur hollarda uni joriy etish rejasi ishlab chiqilib, buyruqqa ilova qilinadi.

222. Siyosat talablari KABT boshqarmasi (tizimosti korxonada — KABT boshqarmasi) tomonidan xodimlarga yetkaziladi. Oddiy xodimlarga ular uchun tegishli qoidalarni o‘z ichiga olgan eslatma (buklet) berilishi mumkin.

223. Barcha xodimlar Siyosat bilan tasdiqlangandan yoki qayta ko‘rib chiqilgandan so‘ng belgilangan shakldagi jurnalga imzo qo‘yish orqali tanishtiriladi. “Axborot xavfsizlik siyosati bilan tanishtirilganlikni ro‘yxatga olish jurnali” markaziy apparat, har bir hududiy boshqarma, xorijdagi vakolatxona va tizimosti korxonada alohida yuritiladi.

224. Ushbu jurnallar KABT boshqarmasi, hududiy administratorlar hamda tizimosti korxona KABT boshqarmasi tomonidan yuritiladi. Imzo qo‘yishdan oldin xodimga kirish instruktaji o‘tkaziladi va bilimlari tekshiriladi.

Axborot xavfsizligi
siyosatiga 5-ilova

Korxonaning KABT boshqarmasi to‘g‘risida nizom

1. Umumiy qoidalar

1.1. Ushbu nizom KABT boshqarmasining (keyingi o‘rinlarda – Boshqarma) tuzilmasi, vazifalari, funksiyalari, huquqlari va javobgarligini belgilaydi.

1.2. Korxonada axborot xavfsizligini ta’minlash bo‘yicha ishlarni tashkil etish va muvofiqlashtirish boshqarmaga yuklatiladi.

1.3. Boshqarma korxonaning mustaqil tarkibiy bo‘linmasi hisoblanadi.

1.4. Axborot xavfsizligini ta’minlash masalalari bo‘yicha boshqarma rahbari korxona rahbariga bo‘ysunadi.

1.5. Boshqarma faoliyatiga uning rahbari rahbarlik qiladi. Boshqarma rahbari korxona rahbarining buyrug‘iga asosan lavozimga tayinlanadi va lavozimdan ozod etiladi.

1.6. Boshqarma rahbari axborot xavfsizligi yoki axborot texnologiyalari sohasida oliy yoki o‘rta maxsus ma’lumotga, axborot xavfsizligi sohasida hamda rahbarlik lavozimlarida kamida 5 yil ish stajiga ega bo‘lishi kerak.

1.7. Boshqarma rahbari vaqtincha yo‘q bo‘lgan davrda (ta’til, kasallik, xizmat safari va boshqalar) uning vazifalari Korxona rahbarining buyrug‘iga muvofiq vaqtincha boshqarma rahbarining o‘rinbosari (bosh mutaxassis) zimmasiga yuklatiladi.

1.8. Boshqarma tarkibiga quyidagilar kiradi:

- Rahbar o‘rinbosari;
- Bosh mutaxassis;
- Yetakchi mutaxassis;
- I toifali mutaxassis, administratorlar va boshqa boshqarma xodimlari.

1.9. Boshqarmaning tuzilmasi va shtatlar jadvali korxona rahbari tomonidan tasdiqlanadi.

1.10. Boshqarma xodimlari lavozimga Korxona rahbarining buyrug‘iga asosan, Boshqarma rahbarining tavsiyasiga ko‘ra va amaldagi qonunchilikka muvofiq tayinlanadi hamda lavozimdan ozod etiladi.

1.11. Boshqarma o‘z faoliyatida quyidagilarga amal qiladi:

- korxonaning axborot xavfsizligi siyosatiga;
- axborot xavfsizligini ta’minlash bo‘yicha normativ hujjatlarga;
- korxona buyruq va farmoyishlariga;
- amaldagi qonunchilik hujjatlari, ichki mehnat tartibi qoidalariga;
- ushbu Nizomga.

2. Asosiy vazifalar

Boshqarmaning asosiy vazifalari quyidagilardan iborat:

1) Korxonada axborot xavfsizligini ta’minlash sohasida normativ-huquqiy choralarni amalga oshirish;

2) Korxonaning axborot aktivlarini boshqarish bo‘yicha chora-tadbirlarni amalga oshirish;

3) Xodimlarning axborot xavfsizligi sohasida xabardorligini oshirish, ularni o‘qitish hamda malakasini oshirish bo‘yicha xavfsizlik choralarini ta’minlash;

4) Korxonada axborotni texnik va kriptografik himoya qilish ishlarini tashkil etish va amalga oshirish;

5) Korxonada himoyalanganlik holatini nazorat qilish va baholash;

6) Korxonada axborot xavfsizligi insidentlariga javob choralarini tashkil etish va o‘tkazish;

7) Informatizatsiya obyektlarining uzluksiz ishlashini ta’minlash va ularni tiklash bo‘yicha choralarni nazorat qilish, favqulodda va avariya holatlarida tiklash ishlarini tashkil etish va o‘tkazish;

8) Korxona axborot xavfsizligi siyosatining dolzarbligi va samaradorligini baholash;

9) Axborot xavfsizligiga tahdidlarni prognoz qilish va oldini olish maqsadida tadqiqotlar o‘tkazish, Korxonada axborot xavfsizligini ta’minlash holatini tahlil qilish;

3. Funksiyalari

Boshqarma funksiyalariga quyidagilar kiradi:

1) Normativ-huquqiy choralar:

- korxonada axborot xavfsizligi sohasiga oid ichki normativ hujjatlarni ishlab chiqish;
- korxonaning axborot xavfsizligi sohasidagi normativ bazasini shakllantirish va yuritish;
- axborot xavfsizligini ta’minlash bo‘yicha ichki normativ hujjatlarni takomillashtirish yuzasidan rahbariyatga takliflar tayyorlash va kiritish;
- axborot xavfsizligi sohasidagi normativ hujjatlar talablarini Korxona xodimlariga yetkazish;
- korxonada axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlar rejalarini ishlab chiqish.

2) Axborot aktivlarini boshqarish:

- korxonaning konfidensial ma’lumotlar ro‘yxatini, axborot aktivlari reestrini yangilash bo‘yicha ishlarni tashkil etish va amalga oshirish, axborotni hamda korxonaning axborot resurslarini kategoriyalash;
- inventarizatsiya o‘tkazish, axborot aktivlari va himoya obyektlari ro‘yxatini aniqlash hamda yuritish, ularni himoyalanganlik darajasi bo‘yicha tasniflash, muhim va kritik himoya obyektlariga nisbatan tahdid modelini aniqlash;
- axborot tizimlari va boshqa himoya obyektlariga kirish huquqiga ega bo‘lgan xodimlar ro‘yxatini tuzish hamda ularning kirishini nazorat qilish;
- axborot aktivlari reyestriga kiritilgan axborot resurslaridan foydalanish, ularga kirish, ularni belgilash (markirovkalash) hamda axborot xavfsizligini ta’minlash bo‘yicha talablar bajarilishini nazorat qilish;
- korxona xodimlariga tegishli bo‘lgan tashkiliy-boshqaruv hujjatlari bilan hisobga olingan ko‘chma raqamli saqlash vositalari va ma’lumot tashuvchilarni biriktirish;
- himoyalanadigan ma’lumotlarni saqlash va uzatish uchun foydalaniladigan ko‘chma raqamli saqlash vositalari va ma’lumot tashuvchilar hisobini yuritish.

3) Xodimlar axborot xavfsizligi, ularning xabardorligi, o‘qitish va malakasini oshirish:

- korxona xodimlarini Korxonaning axborot xavfsizligi siyosati bilan, shuningdek internet tarmog‘idan, elektron pochta xizmatidan, ko‘chma axborot tashuvchilardan va axborotni kriptografik himoya qilish vositalaridan foydalanish bo‘yicha majburiyatlar bilan tanishtirish;
- korxona xodimlari uchun axborot xavfsizligini ta’minlash masalalari bo‘yicha yo‘riqnoma (ma’lumot berish), trening va seminarlar tashkil etish va o‘tkazish, shuningdek xodimlarni attestatsiya qilish, testdan o‘tkazish yoki so‘rovlar o‘tkazish orqali ularning bilimini baholash;
- korxona xodimlari bilan axborot xavfsizligini ta’minlashga oid tashkiliy-boshqaruv hujjatlari bilan tanishtirish va ularni o‘rganish bo‘yicha mashg‘ulotlar tashkil etish;
- axborot xavfsizligini ta’minlash uchun mas’ul bo‘lgan mutaxassislarning malakasini oshirish kurslarida ishtirok etishini tashkil etish;
- axborot xavfsizligi masalalarida tarkibiy bo‘linmalar va xodimlarga uslubiy hamda amaliy yordam ko‘rsatish.

4) Axborotni texnik va kriptografik himoya qilish:

- korxona axboroti va axborot tizimlarini himoya qilish bo‘yicha talablarni ishlab chiqish, axborotni himoya qilish tizimini, shu jumladan axborotni kriptografik himoya qilish tizimini joriy etish;

- axborotni himoya qilish tizimini joriy etish va rivojlantirish bo‘yicha amaliy tadbirlarni rejalashtirish va amalga oshirish;

- xarid qilinadigan texnik va kriptografik himoya vositalariga qo‘yiladigan texnik talablarni aniqlash;

- korxona axborot xavfsizligini ta’minlash tizimini joriy etish va rivojlantirish tadbirlari doirasida texnik va kriptografik himoya vositalarini xarid qilishni tashkil etish;

- axborotni himoya qilish tizimi va vositalarini joriy etish hamda ulardan foydalanishga tayyorlash bo‘yicha tashkiliy tadbirlarni amalga oshirish, jumladan, xonalarni ajratish, foydalanish yo‘riqnomalari va xizmat ko‘rsatish reglamentlarini qo‘llash;

- axborot himoya vositalarini joriy etishda tajriba-ekspluatatsiya va qabul-topshirish sinovlarini o‘tkazish;

- himoya tizimi hamda uning tarkibiga kiruvchi texnik va kriptografik himoya vositalaridan foydalanish (administratorlik qilish) uchun mas’ul xodimlarni belgilash;

- axborot himoya vositalarini boshqarish (administratorlik qilish), jumladan ularning konfiguratsiyasi va sozlamalarini nazorat qilish, ishlashini tiklash, dasturiy ta’minotni yangilash, ekspluatatsiya hujjatlarini tuzatish, xavfsizlik hodisalarini nazorat qilish hamda nazorat jarayonlari va natijalarini hujjatlashtirish;

- korxona xodimlarining internet tarmog‘iga ulanish bo‘yicha arizalarini qabul qilish, ko‘rib chiqish va kelishish hamda ularning internetdan foydalanishini nazorat qilish;

- korxonada axborot xavfsizligini ta’minlash maqsadida apparat va dasturiy vositalarni o‘rnatish hamda modernizatsiya qilish tartibini belgilash va qayta ko‘rib chiqish;

- dasturiy ta’minotni loyihalash, ishlab chiqish, sozlash, tekshirish, joriy etish va foydalanish jarayonlarida axborot xavfsizligini ta’minlash tartibini belgilash va qayta ko‘rib chiqish;

- korxonada AKHV va elektron raqamli imzo (ERI) vositalarini joriy etish bo‘yicha amaliy tadbirlarni rejalashtirish va amalga oshirish;

- xodimlarga ERI kriptografik kalitlarini berish tartibini reglamentlash va ta’minlash;

- xodimlar tomonidan ERI kriptografik kalitlarining saqlanishini ta’minlash bo‘yicha talablarni belgilash va nazorat qilish;

- korxonada qonunchilikda belgilangan tartibda sertifikatlangan kriptografik himoya vositalaridan foydalanish talablarini bajarish;

- axborot tizimlari himoyasi va xavfsizligini ta’minlash faoliyatida aniqlangan kamchiliklar yuzaga kelganda, tizimni takomillashtirish bo‘yicha rahbariyatga takliflar tayyorlash va kiritish.

5) Himoyalanganlik holatini nazorat qilish va baholash:

- korxonada axborot xavfsizligi risklarini tahlil qilish va baholashni amalga oshirish;

- texnik va kriptografik himoya choralarining ta’minlanishini tekshirish, himoyalanganlik darajasini baholash, himoya obyektlarida zaifliklar va axborot sizib chiqish kanallarini aniqlash maqsadida nazorat va tahlil vositalaridan foydalangan holda ichki auditni tashkil etish va o‘tkazish;

- korxonaning akkreditatsiyadan o‘tgan korxonalar tomonidan axborotlashtirish obyektlarining tashqi auditi va attestatsiyasini o‘tkazishni tashkil etish;

- korxonaning rasmiy veb-sayti va boshqa tashqi veb-resurslarining axborot xavfsizligi talablariga muvofiqligini ekspertizadan o‘tkazishni tashkil etish;

- mavjud axborot tizimlarini modernizatsiya qilish va yangi axborot tizimlari hamda resurslarni yaratish bo‘yicha texnik topshiriqlarni, shuningdek axborot xavfsizligi talablariga muvofiqligi nuqtai nazaridan axborot tizimlarining o‘zini ekspertizadan o‘tkazishni tashkil etish;

- qabul qilingan himoya choralarining samaradorligini baholash, audit, ekspertiza va attestatsiya natijalari bo‘yicha aniqlangan kamchiliklarni bartaraf etish;

- axborot xavfsizligini ta’minlash masalalari bo‘yicha Korxonaning uchinchi tomon korxonalari bilan tuzilgan shartnomalar va kelishuvlarni ekspertizadan o‘tkazish.

6) Axborot xavfsizligi hodisalariga javob choralarini ko‘rish:

- axborot xavfsizligi insidentlarini aniqlash va identifikatsiya qilish bo‘yicha ishlarni tashkil etish va amalga oshirish, ularni tahlil qilish va baholash;

- axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimlarini administratorlik qilish (boshqarish);

- axborot xavfsizligi hodisalarini hisobga olish va ro‘yxatga olish, ular haqida rahbariyat va manfaatdor tomonlarni xabardor qilish;

- axborot xavfsizligi insidentlariga javob choralarini ko‘rishni tashkil etish va muvofiqlashtirish, insidentlarni hamda ularning oqibatlarini bartaraf etish bo‘yicha choralarni rejalashtirish va amalga oshirish;

- axborot xavfsizligi insidentlari bo‘yicha tekshiruvlarni tashkil etish va o‘tkazish, rahbariyat ko‘rsatmasiga asosan axborot xavfsizligini ta’minlash qoidalari buzilishi holatlari bo‘yicha xizmat tekshiruvlarini tashkil etish va o‘tkazish;

- axborot xavfsizligi insidentlarining takrorlanishini oldini olish bo‘yicha choralarni rejalashtirish va amalga oshirish.

7) Uzluksiz ishlash va tiklash:

- axborotni himoya qilish tizimi va uning tarkibiga kiruvchi himoya vositalariga profilaktik, ta’mirlash va avariya ishlarini o‘tkazish tartibini belgilash hamda jadvalini tasdiqlash;

- axborot xavfsizligi vositalarini zaxiralash, ularning sozlamalari, dasturiy ta’minoti va ma’lumotlar bazalarining zaxira nusxalarini yaratishni ta’minlash;

- korxona KABT boshqarmasi xodimlari tomonidan kritik ahamiyatga ega bo‘lgan informatizatsiya obyektlarining apparat-dasturiy vositalarini zaxiralash, dasturiy ta’minot va ma’lumotlarni zaxiralash ishlarini nazorat qilish;

- korxona xodimlari bilan birgalikda favqulodda va avariya holatlarida harakat qilish bo‘yicha treninglar tashkil etish;

- favqulodda va avariya holatlari yuzaga kelganda kritik informatizatsiya obyektlarida tiklash ishlarini o‘tkazilishini nazorat qilish.

8) Korxona axborot xavfsizligi siyosatining dolzarbligi va samaradorligini baholash:

- korxona axborot xavfsizligi siyosatining dolzarbligi va samaradorligini baholashni amalga oshirish;

- korxona rahbariyatiga axborot xavfsizligi siyosatiga o‘zgartirish va qo‘shimchalar kiritish yoki uni qayta ko‘rib chiqish zarurligi bo‘yicha takliflar tayyorlash;

- korxona axborot xavfsizligi siyosatiga o‘zgartirish va qo‘shimchalar kiritish yoki uni qayta ko‘rib chiqish.

9) Axborot xavfsizligi ta’minotini tadqiq qilish va tahlil qilish:

- axborot xavfsizligi tahdidlarini bartaraf etish bo‘yicha choralarni ishlab chiqish va amalga oshirish, ularning yuzaga kelishiga sabab bo‘ladigan omillarni o‘rganish;

- axborot xavfsizligini ta’minlash sohasida ilg‘or milliy va xorijiy tajriba, usullar va vositalarni o‘rganish hamda ularni Korxona faoliyatida qo‘llash imkoniyatlarini ko‘rib chiqish;

- korxonada axborot xavfsizligini ta’minlash holatini tahlil qilish hamda tegishli axborot-tahliliy materiallarni tayyorlash;

- bo‘linma faoliyati natijalarini umumlashtirib, Korxona rahbariyatiga hisobot berish.

4. Huquqlar

Boshqarma o‘ziga yuklatilgan vazifalar va funksiyalarni bajarish uchun quyidagi huquqlarga ega:

- korxona tarkibiy bo‘linmalaridan ish faoliyati uchun zarur bo‘lgan ma’lumotlarni so‘rash va olish;
- korxonada axborot xavfsizligini ta’minlashga doir barcha rejalarni boshqarish;
- korxona axborot xavfsizligi siyosatini o‘zgartirish bo‘yicha takliflar ishlab chiqish va kiritish;
- korxonada axborot xavfsizligini ta’minlash bo‘yicha mavjud normativ-uslubiy hujjatlarga o‘zgartirishlar kiritish hamda yangi hujjatlarni qabul qilish;
- korxona rahbariyati bilan kelishgan holda, axborot xavfsizligini ta’minlash jarayoniga qo‘shimcha xodimlarni jalb qilish hamda ularning vazifalari va vakolatlarini belgilash;
- axborotni texnik va kriptografik himoya qilish talablarining bajarilishini tekshirish;
- korxona xodimlari, birinchi navbatda, imtiyozli vakolatlarga ega xodimlar tomonidan axborot xavfsizligi talablariga rioya etilishini nazorat qilish;
- axborot texnologiyalaridan foydalanish, axborotni qayta ishlash texnologiyalarini qo‘llash va axborot resurslari hamda tizimlaridan foydalanish masalalari bo‘yicha xodimlardan ma’lumot olish;
- axborot tizimlarini yaratish va rivojlantirish bo‘yicha texnik topshiriqlar hamda loyihalarni ko‘rib chiqish, ularga axborot xavfsizligini ta’minlash bo‘yicha takliflar kiritish;
- axborot tizimlarida axborot xavfsizligi tizimlarini ishlab chiqish, sinovdan o‘tkazish va qabul qilishda ishtirok etish, shu jarayonlarda maxfiy ma’lumotlarning sizib chiqishini oldini olish bo‘yicha amaliy choralar ko‘rish;
- o‘z vakolatlari doirasida Korxona axborot xavfsizligini boshqarish, ta’minlash va nazorat qilish usullari, vositalari va mexanizmlarini tanlash, joriy etish va qo‘llash;
- korxona xodimlarining axborot xavfsizligi talablariga rioya etishini nazorat qilish;
- axborot xavfsizligini boshqarish usullari, vositalari va mexanizmlarini o‘z vakolatlari doirasida tanlash, joriy etish va qo‘llash;
- axborot xavfsizligini ta’minlash bilan bog‘liq materiallar va ishlarni qabul qilish bo‘yicha komissiyalar tarkibida ishtirok etish;
- axborot xavfsizligi buzilishi bilan bog‘liq hodisalar yuzasidan xizmat tekshiruvlarini tashkil etish, axborot xavfsizligi talablarini buzgan shaxslarni javobgarlikka tortish bo‘yicha rahbariyatga takliflar kiritish.

5. Javobgarlik

Boshqarma boshlig‘i va xodimlari quyidagilar uchun javobgar hisoblanadi:

- mazkur nizomda nazarda tutilgan o‘z xizmat vazifalarini bajarmaganligi yoki lozim darajada bajarmaganligi uchun;
- korxonada axborot xavfsizligini ta’minlash bo‘yicha amalga oshirilgan ishlar sifati uchun;
- korxona tarmoqlari, axborot resurslari va tizimlari, shuningdek jismoniy obyektlarning himoyalanganlik darajasini saqlash va belgilangan himoya darajasini ta’minlash holati uchun.

Axborot xavfsizligi
siyosatiga 6-ilova

Axborot xavfsizligi administratorining namunaviy lavozim yo‘riqnomasi

1. Umumiy qoidalar

1.1. Ushbu yo‘riqnoma Korxonada axborot xavfsizligini ta’minlash uchun mas’ul bo‘lgan xodimning (keyingi o‘rinlarda — axborot xavfsizligi administratori) majburiyatlari, huquqlari va javobgarligini belgilash maqsadida ishlab chiqilgan.

1.2. Korxona axborot xavfsizligi administratori korxona KABT boshqarmasi xodimi hisoblanadi.

1.3. Axborot xavfsizligi administratorining majburiyatlari, huquqlari va javobgarligi mazkur yo‘riqnoma bilan belgilanadi hamda uning lavozim yo‘riqnomasida qayd etiladi.

1.4. Korxona axborot xavfsizligi administratori Korxona rahbarining buyrug‘i bilan tayinlanadi.

1.5. Korxona axborot xavfsizligi administratori lavozimiga tayinlanadigan xodimlar nomzodlari KABT boshqarmasi rahbari tomonidan taqdim etiladi.

1.6. Axborot xavfsizligi administratori oliy yoki o‘rta maxsus ma’lumotga hamda axborot xavfsizligi sohasida kamida 3 yil ish tajribasiga ega bo‘lishi kerak.

1.7. O‘z xizmat vazifalarini bajarishda axborot xavfsizligi administratori KABT boshqarmasi rahbariga bo‘ysunadi.

1.8. Axborot xavfsizligi administratori tomonidan o‘z funksiyalarini bajarish bilan bog‘liq qo‘yilgan talablar Korxonaning barcha xodimlari tomonidan bajarilishi majburiy hisoblanadi.

1.9 Axborot xavfsizligi administratori kasallik yoki mehnat ta’tili sababli ishda bo‘lmagan davrda, mazkur yo‘riqnoma bilan belgilangan uning huquqlari, majburiyatlari va javobgarligi Korxonaning AT-mutaxassisi zimmasiga yuklatiladi.

1.10. Axborot xavfsizligi administratori o‘z faoliyatida quyidagilarga amal qiladi:

- korxonaning axborot xavfsizligi siyosatiga;
- axborot va kiberxavfsizlikni ta’minlash sohasidagi normativ hujjatlarga;
- korxona buyruq va farmoyishlariga;
- amaldagi qonunchilik hujjatlari, ichki mehnat tartibi qoidalariga;
- ushbu Yo‘riqnomaga.

2. Majburiyatlar

2.1. Axborot xavfsizligi administratori KABT boshqarmasiga yuklatilgan vazifalarni bevosita amalga oshirishda ishtirok etishi shart.

2.2. Axborot xavfsizligi administratori quyidagilarni bilishi kerak:

- korxonaning axborot xavfsizligi siyosati qoidalarini;
- axborot xavfsizligini ta’minlash bo‘yicha, jumladan Korxona ichki normativ hujjatlarini;
- korxona uchun mavjud bo‘lgan axborot xavfsizligi tahdidlari va risklarini;
- korxona axborot xavfsizligi boshqaruv tizimini (AXBT) tashkil etish tartibi va talablarini;
- korxonada qo‘llaniladigan axborot xavfsizligini ta’minlash choralari;
- korxonada axborot xavfsizligini boshqarish jarayonlari;
- korxonada ekspluatatsiya qilinadigan axborotni himoya qilish vositalarini;
- korxonada foydalaniladigan axborotni himoya qilish vositalari.

2.3. Axborot xavfsizligi administratori majburiyatlari:

- Korxona xodimlarini axborot xavfsizligi siyosati bilan tanishtirish, yangi xodimlar uchun axborot xavfsizligini ta’minlash masalalari bo‘yicha yo‘riqnoma (instruktaj) o‘tkazish;

- Korxona axborot xavfsizligi siyosati bilan tanishtirish, yangi ishga qabul qilingan xodimlar uchun axborot xavfsizligini ta’minlash masalalari bo‘yicha yo‘riqnoma o‘tkazish;

- Korxona xodimlariga axborot xavfsizligi masalalari bo‘yicha ko‘mak va maslahatlar berish;

- axborot xavfsizligiga oid ichki normativ hujjatlarni hududiy boshqarma xodimlariga yetkazish;

- tasdiqlangan rejalar asosida hududiy boshqarmada axborot xavfsizligini ta’minlash bo‘yicha tadbirlarni tashkil etish va amalga oshirish;

- Korxona xodimlari tomonidan Korxona axborot xavfsizligi siyosati talablariga rioya etilishini monitoring qilish;

- Korxona xodimlarga axborot xavfsizligi siyosati talablarini bajarish bo‘yicha yo‘riqnoma o‘tkazish, ularning bilim va amaliy ko‘nikmalarini baholash;

- axborot xavfsizligi masalalarida korxonada muvofiqlashtirilgan hamkorlikni tashkil etish.

- Korxonada axborot xavfsizligi bo‘yicha ichki auditni tashkil etish va o‘tkazish, zaifliklar hamda axborot sizib chiqish kanallarini aniqlash;

- Korxonada himoyalanganlikni ta’minlash tizimining ishlashidagi kamchiliklarni aniqlash, axborot himoya tizimini takomillashtirish bo‘yicha takliflar kiritish;

- Korxonada axborot xavfsizligining umumiy holatini doimiy monitoring qilish;

- axborot xavfsizligi holati bo‘yicha KABT boshqarmasi talabiga muvofiq hisobotlar va boshqa ma’lumotlarni taqdim etish;

- Korxonada aniqlangan axborot xavfsizligi insidentlari to‘g‘risida ma’lumotlarni to‘plash;

- axborot xavfsizligi hodisalarini hisobga olish jurnalini yuritish;

- Korxonada axborot xavfsizligi hodisalari yuzaga kelganda KABT boshqarmasini o‘z vaqtida xabardor qilish;

- axborot xavfsizligi hodisalarini tahlil qilish va ular bo‘yicha tekshiruvlarda ishtirok etish.

3. Huquqlar

Axborot xavfsizligi administratori o‘ziga yuklatilgan vazifalarni bajarish uchun quyidagi huquqlarga ega:

- axborotni himoya qilish vositalarini xarid qilish bo‘yicha takliflar kiritish hamda xarid qilishdan oldin ularga qo‘yiladigan texnik talablarni ishlab chiqish;

- Korxonada axborot himoya vositalarini loyihalash, qabul qilish va sanoat ekspluatatsiyasiga topshirish jarayonlarida ishtirok etish;

- axborot tizimlarida hamda umuman Korxona bo‘yicha axborot xavfsizligi tizimlarini ishlab chiqish, sinovdan o‘tkazish va qabul qilish jarayonlarida ishtirok etish, ushbu jarayonlarda himoyalangan ma’lumotlarning sizib chiqishini oldini olish bo‘yicha amaliy choralar ko‘rish;

- axborot xavfsizligini ta’minlash masalalariga oid Korxona axborot xavfsizligi siyosati va ichki normativ hujjatlarini o‘zgartirish bo‘yicha takliflar kiritish, shu jumladan korxona xodimlari faoliyatini tartibga soluvchi hujjatlar yuzasidan ham;

- Korxona yoki xorijiy vakolatxona xodimlaridan axborotni qayta ishlash texnologiyalaridan foydalanish hamda axborot resurslari va tizimlaridan ekspluatatsiya qilish masalalari bo‘yicha ma’lumot olish;

- Korxona xodimlari tomonidan axborot xavfsizligi talablariga rioya etilishini nazorat qilish;

- korxona mablag‘lari hisobidan axborot xavfsizligi sohasida malaka oshirish va o‘quv kurslarida ishtirok etish.

4. Javobgarlik

Axborot xavfsizligi administratori quyidagilar uchun javobgar hisoblanadi:

- ushbu Yo‘riqnomada nazarda tutilgan o‘z xizmat vazifalarini bajarmaganligi yoki lozim darajada bajarmaganligi uchun;

- korxonada axborot xavfsizligini ta’minlash bo‘yicha amalga oshirgan ishlarining sifati uchun.

Axborot xavfsizligi
siyosatiga 11-ilova

Antivirusdan himoya qilish bo‘yicha ko‘rsatmalar

1. Umumiy qoidalar

1. Ushbu Yo‘riqnoma quyidagilarni belgilaydi:

- Korxona ichida zararli dasturlardan himoya qilishni tashkil etish talablari;
- Korxona ichida qo‘llaniladigan zararli dasturlardan himoya qilish usullari va vositalari;
- Antivirus himoyasini ta’minlash uchun mas’ul xodimlar va Korxonaning oddiy xodimlari tomonidan amalga oshirish tartiblari (qoidalari) va tartiblari;
- Antivirus himoyasi talablari, shuningdek, xodimlarning ularga rioya qilish bo‘yicha majburiyatlari va mas’uliyati.

2. Ushbu Yo‘riqnoma Korxonaning barcha xodimlari, shuningdek Korxona ichida antivirus himoyasini ta’minlash uchun mas’ul xodimlar uchun majburiydir.

2. Atamalar, ta'riflar va qisqartmalar

3. Ushbu Yo‘riqnomada quyidagi atamalar va ularning ta'riflari qo‘llaniladi:

1) antivirus himoyasi: antivirus dasturlari yordamida kompyuter virusi ta’sirining oldini olish, aniqlash va zararsizlantirishga qaratilgan chora-tadbirlar majmui;

2) antivirus dasturi: zararli dasturlarni, shu jumladan viruslar, tarmoq “qurtlari”, troyanlar, fishing havolalari va boshqalarni aniqlash, davolash va yo‘q qilish mexanizmini o‘z ichiga olgan maxsus dasturiy ta’minot.

3) antivirus nazorati: ish stansiyalari va serverlarda zararli dasturlarni mavjudligini muntazam tekshirish, kunlik yangilanishlarni amalga oshirish, har oyda ish stansiyalari va serverlarni zararli dasturlarga nisbatan to‘liq skanerlash, zararli dasturlarni aniqlash bilan bog‘liq insidentlarga javob qaytarish.

4) zararli dastur: apparat, dasturiy-apparat yoki dasturiy usullar yordamida amalga oshirilgan va har qanday ruxsatsiz yoki zararli faoliyatni amalga oshirish uchun mo‘ljallangan dastur.

5) antivirus nazorati vositasi: parametrlarni, virusga qarshi vositaning yangilanishini va antivirus himoyasi sohasida sodir bo‘lgan insidentlarni markazlashtirilgan tartibda nazorat qilishning avtomatlashtirilgan tizimi.

4. Ushbu tartibda quyidagi qisqartmalar qo‘llaniladi:

IDPS (Intrusion Detection & Prevention System) – buzib kirishlarni aniqlash va oldini olish vositalari (tizimi);

HIPS (Host Intrusion Prevention System) - uzellarda buzib kirishlarning oldini olish tizimi;

AT – axborot tizimi.

3. Antivirus himoyasini tashkil qilish talablari

5. Korxonada antivirus himoyasi axborot va axborotni qayta ishlash uskunalarini (dasturiy ta'minotini) zararli dasturlardan himoya qilishni ta’minlash uchun tashkil etilgan.

6. Korxonada quyidagi antivirus himoya choralari qo‘llaniladi:

- zararli dasturlardan himoya vositalarini qo‘llash;
- Korxona xodimlari tomonidan bajarilishi kerak bo‘lgan antivirus himoyasi qoidalarini (talablarini) belgilash, shu jumladan tashqi tarmoqlardan yoki ular orqali yoki har qanday saqlash vositalari orqali fayllar va dasturlarni qabul qilish va yuklab olish;
- zararli dasturlar tomonidan ishlatilishi mumkin bo‘lgan zaifliklarni aniqlash va yo‘q qilish;
- zararli veb-resurslarga kirishni blokirovka qilish (URL filtrlash), bunday veb-resurslar ro‘yxatini tuzish va yuritish ("qora ro‘yxat");

- olinadigan vositalarni, axborotni qayta ishlash uskunalaridagi disk drayverlarini ulash uchun portlardan foydalanishni blokirovka qilish, shuningdek, Wi-Fi va Bluetooth funksiyalarini o‘chirib qo‘yish;

- xodimlarning o‘z so‘nggi qurilmalariga ruxsatsiz dasturlarni mustaqil ravishda o‘rnatish imkoniyatini cheklash;

- xavfsizlikni oshirish uchun veb-brauzerlarni shunga mos ravishda sozlash;

- xodimlarni antivirusdan himoya qilish majburiyatlari bilan tanishtirish va/yoki xodimlarning antivirusdan himoya qilish bo‘yicha xabardorligini oshirish uchun treninglar o‘tkazish;

- yangi zararli dasturlar haqida muntazam ravishda ma’lumot to‘plash tartiblarini joriy etish (elektron pochta xabarnomalariga obuna bo‘lish yoki tegishli veb-saytlarni ko‘rish).

7. KABT boshqarmasi antivirusdan himoya qilish choralarini amalga oshirish uchun javobgardir.

8. Korxona quyidagi zararli dasturlardan himoya qilish vositalaridan foydalanadilar:

- ma’lumotlarni qayta ishlash uskunalaridagi antivirus dasturi;

- tarmoq trafikidagi zararli dasturlarni aniqlash vositalari (IDPS tizimlari);

- ma’lumotlarni qayta ishlash uskunalaridagi buzg‘unchiliklarni aniqlash va oldini olish vositalari (HIPS vositalari).

9. Korxonada antivirus sifatida markazlashtirilgan antivirus himoya tizimi qo‘llaniladi, u Korxonaning lokal tarmog‘ida tashkil etiladi. Antivirus tizimi lokal tarmoqqa ulangan yakuniy qurilmalar (serverlar, ishchi stansiyalar, hisobga olingan mobil qurilmalar)ni zararli dasturlar hamda boshqa tahdidlarni (HIPS funksiyasi – anti-hacker) aniqlash maqsadida doimiy monitoring qilib borishni ta’minlaydi.

Korxonada antivirus tizimidan foydalanish (ekspluatatsiya qilish) KABT boshqarmasi tomonidan amalga oshiriladi.

10. Bundan tashqari, Korxonada tashqi tarmoqlarga ulanish chegarasida IDPS vositalari qo‘llaniladi, ular kiruvchi tashqi trafikni zararli dasturlar mavjudligiga tekshirishni ta’minlaydi.

11. Korxonada antivirus himoyasini tashkil qilishda quyidagi talablarga rioya qilinishi kerak:

- barcha oxirgi qurilmalar, shu jumladan mobil qurilmalar, shuningdek, korporativ yoki lokal tarmoqlarga ulangan serverlar, shuningdek, tashqi tarmoq trafiki majburiy antivirus monitoringidan o‘tkaziladi;

- antivirus dasturi o‘rnatilmagan oxirgi qurilmalar va serverlarga Korxonaning axborot va kommunikatsiya infratuzilmasiga ulanishga ruxsat berilmaydi;

- litsenziyalangan antivirus dasturidan foydalanish va uning o‘z vaqtida yangilanishini ta’minlash;

- antivirus dasturini markazlashtirilgan boshqarish;

- antivirus dasturi ma’lumotlar bazasini muntazam ravishda yangilab turish;

- antivirus dasturining yangilanganligini (eskirgan emasligini) tekshirish;

- zararli dasturlar va boshqa tahdidlarni doimiy ravishda kuzatib borish va aniqlash uchun antivirus dasturining avtomatik ishlashini ta’minlash.

4. Antivirus himoyasini ta’minlash talablari

12. Axborot xavfsizligi bo‘limi Korxona ichida antivirus himoyasi tadbirlarini tashkil qilish antivirus himoyasi tadbirlarini tashkil qilish uchun javobgardir.

13. Korxonaning KABT boshqarmasi antivirus himoyasini ta’minlash bo‘yicha majburiyatlari quyidagilarni o‘z ichiga oladi:

- antivirus himoyasini tashkil qilish – antivirus himoyasi choralari va vositalarini amalga oshirish;

- antivirus himoyasi vositalarini boshqarish (o‘rnatish, sozlash, ishlashni kuzatish, profilaktika choralarini amalga oshirish va zaxira nusxasini yaratish);

- antivirus himoyasi holatini doimiy ravishda kuzatib borish va antivirus himoyasi vositalari tomonidan aniqlangan antivirus himoyasi buzilishlari holatlariga javob berish;

- antivirus sozlamalarining to‘g‘riligini, shuningdek, xodimlarning so‘nggi qurilmalarida yoki muhim biznes jarayonlarini qo‘llab-quvvatlovchi axborotni qayta ishlash vositalarida dasturiy ta'minot inventarizatsiyasini muntazam ravishda tekshirish;

- zararli dasturlar tomonidan foydalaniladigan zaifliklarni aniqlash va yo‘q qilish;

- xodimlarning antivirus himoyasi talablariga rioya qilishini monitoring qilish.

14. Korxonadagi antivirus tizimi KABT boshqarmasi xodimi tomonidan boshqariladi, uning vazifalari quyidagilarni o‘z ichiga oladi:

- Antivirus himoyasi serverini boshqarish – tizimning ishlashini kuzatish va antivirus ma’lumotlar bazasini yangilash, serverning uzluksiz ishlashini ta’minlash uchun profilaktika choralari, antivirus dasturini qayta o‘rnatish (agar kerak bo‘lsa) va konfiguratsiya qilish;

- So‘nggi qurilmaarga (ish stantsiyalari, mobil qurilmalar) va serverlarga o‘rnatilgan antivirus dasturini markazlashtirilgan konfiguratsiya qilish;

- Antivirus himoyasi holatini doimiy ravishda kuzatib borish va KABT boshqarmasi boshlig‘ini aniqlangan antivirus himoyasi buzilishlari haqida xabardor qilish;

- Markazlashtirilgan antivirus himoyasi serverining zaxira nusxasini yaratish;

- Zararli dasturlarni bartaraf etish jarayonlarida ishtirok etish.

15. Korxonada yakuniy qurilmalar va serverlarga antivirus dasturlarini o‘rnatish KABT boshqarmasi xodimlari tomonidan amalga oshiriladi.

16. Markazlashtirilgan antivirus himoya vositalarini yakuniy qurilmalarda sozlashda quyidagi talablar bajarilishi lozim:

- antivirus ma’lumotlar bazasi doimiy ravishda yangilanib turishini ta’minlash;

- antivirusdan himoya qilish vositalarining ishlashini monitoring qilish;

- Korxona xodimlari va administratorlariga antivirus dasturini o‘chirib qo‘yishni, antivirus dasturi sozlamalarini o‘zgartirishni yoki uni o‘chirishni taqiqlash;

- antivirus dasturida HIPS funksiyasini yoqish;

- so‘nggi qurilmalarda USB portlari va boshqa olinadigan media portlarini bloklash;

- vaqti-vaqti bilan axborotni qayta ishlash qurilmasini to‘liq skanerlash;

- zararli dastur aniqlanganda xabar berish;

- zararli dastur ta’sirini lokalizatsiya qilish va bartaraf etish, zararli dastur bilan zararlangan vositalarni izolyatsiya qilish.

Ushbu talablarning bajarilishi ustidan nazorat Korxonada KABT boshqarmasi tomonidan amalga oshiriladi.

17. Korxona xodimlari so‘nggi qurilmalarida antivirus himoyasi yordamida axborot tashuvchi va saqlovchi qurilmalarni ulash portlari bloklanadi.

Ishlab chiqarish zarurati tug‘ilganda Korxona rahbariyati tomonidan belgilangan ayrim ishchi o‘rinlarda ko‘chma raqamli tashuvchilardan foydalanishga ruxsat beriladi. Bunda ushbu ishchi o‘rinlardagi antivirus himoya vositalari ko‘chma raqamli tashuvchilar ulanishi bilan ularni avtomatik tekshirishga sozlangan bo‘lishi kerak. Ishonchsiz ko‘chma raqamli tashuvchilar ulanadigan bo‘lsa, ularni ulashdan oldin ishchi o‘rinni mahalliy tarmoqdan uzib qo‘yish (tarmoq kabelini uzib tashlash orqali) lozim.

18. Korxonada KABT boshqarmasi tomonidan amalga oshiriladigan IDPS vositasi sozlamalarida zararli dasturlar mavjudligini aniqlash uchun trafik nazorati hamda imzolar bazasini avtomatik yangilash funksiyasi yoqilgan bo‘lishi shart.

19. Disklarning barcha yuklash sektorlari va oxirgi qurilmalardagi fayllarning antivirus monitoringi oxirgi qurilmalar dastlabki yuklanganda yoki belgilangan vaqtda (tushlik tanaffusi) har kuni avtomatik ravishda, serverlar uchun esa ularni qayta ishga tushirgandan so‘ng amalga oshirilishi kerak.

20. Oxirgi qurilmalar va serverlarga o‘rnatilgan antivirus ma’lumotlar bazalari antivirus tizimidan muntazam va avtomatik ravishda yangilanishi kerak. Antivirus tizimi antivirus dasturi ishlab chiqaruvchisining yangilash serverlariga kirish uchun sozlangan bo‘lishi kerak.

21. Korxonaning lokal tarmog‘i orqali, shuningdek, axborot tashuvchilarda qabul qilingan va uzatilgan har qanday ma’lumot (har qanday formatdagi matnli fayllar, ma’lumotlar fayllari, bajariladigan fayllar) majburiy antivirus monitoringidan o‘tkazilishi kerak.

22. Elektron arxivga joylashtirilgan fayllar majburiy antivirus skanerlashdan o‘tkazilishi kerak. Elektron arxivlarni davriy tekshirish oyiga kamida bir marta o‘tkazilishi kerak.

23. Axborotni qayta ishlash uskunasiga o‘rnatilgan (o‘zgartirilgan) dasturiy ta'minot zararli dasturlar mavjudligini oldindan tekshirishi kerak. Tizim dasturini o‘rnatgandan (o‘zgartirgandan) so‘ng darhol antivirus tekshiruvi o‘tkazilishi kerak.

24. Korxona xodimlari tomonidan yakuniy qurilmalarga dasturiy ta’minotni mustaqil o‘rnatib yuborishning oldini olish uchun ularga o‘z yakuniy qurilmalariga faqat foydalanuvchi (administrator bo‘lmagan) kirish huquqi taqdim etilishi lozim.

5. Antivirus himoyasi ishtirokchilarining majburiyatlari

25. Korxonada o‘rnatilgan antivirus dasturisiz so‘nggi qurilmalar va serverlardan foydalanishni taqiqlaydi.

26. Agar zararli dastur mavjudligiga shubha qilinsa (g‘ayrioddiy dastur xatti-harakati, grafik va ovoz effektlarining paydo bo‘lishi, ma’lumotlarning buzilishi, fayllarning yo‘qolishi yoki tizim xatolari haqidagi tez-tez xabarlar), Korxona xodimi mustaqil ravishda yoki Korxonaning KABT boshqarmasi xodimi bilan birgalikda ularning so‘nggi qurilmasini antivirus skanerlashi kerak.

27. Agar antivirus skanerlash paytida kompyuter viruslari bilan zararlangan fayllar aniqlansa, Korxona xodimlari quyidagilarga majburdirlar:

- ishni to‘xtatib turish;
- Korxonaning KABT boshqarmasi shuningdek, ushbu fayllardan o‘z ishlarida foydalanadigan Korxona xodimlariga virus bilan zararlangan fayllar aniqlanganligi haqida darhol xabar berish;
- undan keyingi foydalanishni tahlil qilish;
- zararlangan fayllarni dezinfeksiya qilish yoki yo‘q qilish;
- Agar mavjud antivirus dasturi tomonidan davolab bo‘lmaydigan yangi virus aniqlansa, Korxonaning KABT boshqarmasiga xabar berish.

28. Agar oxirgi qurilma yoki server kompyuter virusi bilan zararlangan bo‘lsa, uning Korxona yoki tizim korxonasi tarmog‘i bo‘ylab tarqalishining oldini olish uchun quyidagi shoshilinch choralar ko‘rilishi kerak:

- Zararlangan oxirgi qurilma yoki serverdagi ishlashni to‘xtatib qo‘yish va tarmoq kabelini uzib, uni lokal tarmoqdan uzish;
- Litsenziyalangan antivirus dasturi yordamida virusni skanerlash va o‘chirish;
- Agar antivirus dasturi virusni olib tashlay olmasa, oxirgi qurilma yoki serverdagi operatsion tizim va dasturlar qayta o‘rnatilishi kerak.

29. So‘nggi qurilma foydalanuvchisiga quyidagilar taqiqlanadi:

- antivirusdan himoya qilish vositalarining sozlamalari va konfiguratsiyasini o‘zgartirish;
- tizimga boshqa antivirusdan himoya qilish vositalarini olib tashlash yoki qo‘shish;
- oxirgi qurilmada o‘rnatilgan antivirusdan himoya qilish vositalari bilan avval skanerlamasdan olinadigan saqlash vositalaridan foydalanish;
- elektron pochta orqali olingan yoki internetdan yuklab olingan noma’lum ilovalarni yoki fayllarni ishga tushirish.

30. Korxona xodimi quyidagilarga majburdir:

- noma’lum, shubhali yoki ishonchsiz manbalardan olingan elektron pochta xabarlariga ilovalarni ochmaslik va bunday ilovalar darhol o‘chirilishi kerak;

- noma’lum yoki shubhali manbalardan ma’lumotlarni yuklab olmaslik;

- asosiy faoliyatni bajarish uchun zarur bo‘lmagan hollarda, o‘qish/yozish ruxsatnomalari bilan oxirgi qurilmaning mantiqiy disklari va fayl papkalariga umumiy kirishni ta’minlashdan qochish;

- noma’lum yoki shubhali manbalardan olingan saqlash vositalarini ulardan foydalanishdan oldin viruslarga tekshirish;

- So‘nggi qurilmani dastlabki ishga tushirishda har kuni rezident antivirus monitorining mavjudligiga ishonch hosil qilish va agar bittasi yo‘q bo‘lsa, Korxonaning KABT boshqarmasiga xabar berish;

- Korxonaning KABT boshqarmasi tizimda virus mavjudligi haqida bildirishnoma olgandan so‘ng yoki virusga shubha tug‘ilganda, oxirgi qurilma qurilmasini rejadan tashqari antivirus skanerlashni boshlash.

6. Javobgarlik

31. Ushbu Yo‘riqnoma talablariga muvofiq antivirus nazoratini tashkil etish uchun javobgarlik Korxonaning KABT boshqarmasi zimmasiga yuklatiladi.

32. Ushbu Yo‘riqnoma talablariga rioya qilish uchun javobgarlik Korxona xodimlariga yuklatiladi.

33. Antivirus himoyasi holatini, shuningdek, belgilangan antivirus nazorati tartibiga rioya qilinishini va Korxona xodimlari tomonidan ushbu Yo‘riqnoma talablarining bajarilishini davriy monitoring qilish KABT boshqarmasi tomonidan amalga oshiriladi.

Axborot xavfsizligi
siyosatiga 12-ilova

Mobil qurilmalar bilan ishlashda xavfsizlikni ta’minlash bo‘yicha yo‘riqnoma

1. Umumiy qoidalar

1. Ushbu Yo‘riqnoma ruxsatsiz kirishning oldini olish uchun mobil qurilmalardan foydalanish talablari va qoidalarini hamda ulardan Korxona ichida tahdidni amalga oshirish uchun foydalanish imkoniyatini belgilaydi.

2. Korxona ichida mobil qurilmalardan foydalanish deganda, Korxonaning axborot-kommunikatsiya infratuzilmasi va mobil qurilmalar o‘rtasida ma’lumotlarni qayta ishlash, qabul qilish va uzatish maqsadida ularning qurilmalar, tarmoqlar va axborot resurslari va tizimlariga ulanishi tushuniladi.

3. Ushbu Yo‘riqnoma Korxonaning barcha tarkibiy bo‘linmalari va xodimlariga qo‘llaniladi.

2. Atamalar, ta’riflar va qisqartmalar

4. Ushbu Yo‘riqnomada quyidagi atamalar va ularning ta'riflari qo‘llaniladi: nazorat qilinadigan zona - Doimiy yoki bir martalik ruxsati bo‘lmagan begona shaxslar va transport vositalarining nazoratsiz bo‘lishi ta’qiqlangan joy (hudud, binolar, xonalarning bir qismi); mobil qurilmalar - smartfonlar, planshetlar, elektron kitoblar, telefonlar, shaxsiy raqamli yordamchilar, operatsion tizimga ega netbuklar va mobil tarmoqlarga, Wi-Fi va internetga ulanish imkonini beradigan mobil qurilmalar, shuningdek ish stansiyalari va boshqa shunga o‘xshash qurilmalar;

5. Ushbu Yo‘riqnomada quyidagi qisqartmalar qo‘llaniladi:

DLP (Data Leak Prevention) — axborot oqishining oldini olish tizimi;

VPN (Virtual Private Network) - virtual xususiy tarmoq;

EHAT – elektron hujjat aylanish tizimi;

ERI – elektron raqamli imzo.

3. Mobil qurilmalardan foydalanish qoidalari

6. Korxona ichida mobil qurilmalardan foydalanishga qo‘yiladigan ushbu talablar mobil qurilmalar axborot xavfsizligi tahdidlariga ko‘proq moyil ekanligi va axborotning chiqib ketishi uchun samarali ishlatilishi mumkinligi (video yozuv, fotosuratga olish, audio yozuv, ma’lumotlarni saqlash) asosida belgilanadi.

7. Ushbu hujjatda belgilangan talablar quyidagilarga tegishli bo‘lgan mobil qurilmalardan foydalanishga nisbatan qo‘llaniladi:

- Korxona xodimlari bo‘lmagan shaxslar (mijozlar va tashrif buyuruvchilar);
- Korxona xodimlari;
- Korxona va xodimlarga o‘z xizmat vazifalarini bajarish uchun taqdim etiladigan.

8. Ushbu Yo‘riqnoma maqsadlari uchun mobil qurilmalarga (axborot tashuvchilar uchun portlar va Bluetooth orqali), Korxonaning korporativ va lokal tarmoqlariga simli yoki simsiz Wi-Fi orqali ulanishi mumkin bo‘lgan va mobil tarmoqlarga yoki Internetga ulanish imkoniyatiga ega bo‘lgan mobil telefonlar, smartfonlar, planshetlar, netbuklar va noutbuklar kabi qurilmalar kiradi.

9. Uchinchi shaxslarga tegishli barcha turdagi mobil qurilmalarni asosiy ishlab chiqarish maydoniga olib kirish, shuningdek, Korxona majlislar zalida foydalanish taqiqlanadi.

10. Uchinchi shaxslarga va Korxona xodimlariga tegishli barcha turdagi mobil qurilmalarga quyidagilar taqiqlanadi:

- ularni qurilmalarga, Korxonaning korporativ yoki lokal tarmog‘iga ulash;
- umumiy foydalanishdagi telekommunikatsiya tarmog‘i va Internet orqali ularni Korxonaning lokal tarmog‘i hamda axborot tizimlariga masofadan ulash; ulardan

konfidensial yoki boshqa himoya qilinadigan axborotni qayta ishlash va saqlash uchun, shu jumladan parollar hamda ERIning kriptografik kalitlarini saqlash va ulardan foydalanish uchun foydalanish.

11. Uchinchi shaxslarga (yoki tashrif buyuruvchilarga) tegishli mobil qurilmalar faqat Korxonaning faqatgina internetga kirish uchun o‘rnatilgan Wi-Fi tarmog‘iga ulanishi mumkin. Ushbu simsiz tarmoq Korxonaning lokal tarmog‘iga yoki uning ichki axborot tizimlari va resurslariga ulanmagan. Ushbu ulanish Korxona rahbariyatining ruxsati bilan KABT boshqarmasi tomonidan amalga oshiriladi.

12. Korxonaning mulki bo‘lgan va Korxona xodimlariga o‘z xizmat vazifalarini bajarish uchun taqdim etilgan ro‘yxatdan o‘tgan mobil qurilmalardan - noutbuklar va planshetlardan (bundan keyin ro‘yxatdan o‘tgan mobil qurilmalar deb yuritiladi) Korxonaning axborot-kommunikatsiya infratuzilmasida foydalanishga ruxsat beriladi.

13. Korxona xodimlariga ro‘yxatdan o‘tgan mobil qurilmalarni ro‘yxatdan o‘tkazish va tayinlash KABT boshqarmasi tomonidan amalga oshiriladi.

Korxonada ro‘yxatdan o‘tgan mobil qurilmalar o‘z xodimlariga doimiy foydalanish yoki vaqtinchalik foydalanish uchun (xizmat safarlari paytida) Korxona rahbariyatining ruxsati bilan beriladi. Foydalanilmayotganda, mobil ma’lumotlarni saqlash qurilmalari Korxonaning KABT boshqarmasiga qaytariladi va saqlanadi.

14. Mobil ma’lumotlarni saqlash qurilmalari faqat Korxona ichida ishlatilishi mumkin:

- Korxona xodimlari tomonidan xizmat safarlari paytida;
- Internetga kirish uchun Korxonada tashkil etilgan Wi-Fi tarmog‘iga ulanish uchun;
- VPN yordamida himoyalangan ulanish talablariga muvofiq, Korxonadan tashqarida Internet orqali faqat Korxonaning EHATga masofadan ulanish uchun.

Hisobga olingan mobil qurilmalarni Internet tarmog‘i orqali EHATga masofadan ulash Korxonada belgilangan himoyalangan ulanish talablariga rioya etgan holda amalga oshirilishi shart.

15. Korxona xodimlari hisobga olingan mobil qurilmalardan foydalanganda quyidagi talablarni bajarishlari shart:

- ulardan belgilangan maqsadda foydalanish;
- ushbu Yo‘riqnoma talablarining buzilishi holatlari, shuningdek hisobga olingan mobil qurilmaning yo‘qolishi (o‘g‘irlanishi) haqida KABT boshqarmasini xabardor qilish;
- hisobga olingan mobil qurilmaning jismoniy xavfsizligini barcha oqilona usullar bilan ta’minlash;
- hisobga olingan mobil qurilmani Korxona xodimi bo‘lmagan boshqa shaxslarga vaqtincha foydalanish uchun bermaslik;
- foydalanilmayotgan holatlarda, shuningdek ishdan bo‘shash yoki boshqa ishga o‘tish vaqtida hisobga olingan mobil qurilmani qaytarish.

16. Korxona xodimlariga foydalanish uchun beriladigan hisobga olingan mobil qurilmalarda quyidagi axborot xavfsizligi talablari bajarilishi shart:

- operatsion tizim orqali hisobga olingan mobil qurilmalarga kirish parollarini o‘rnatish;
- hisobga olingan mobil qurilmalarga antivirus himoya vositalarini o‘rnatish.

17. Masofadan EHATga kirish uchun foydalaniladigan mobil qurilmalarda (noutbuklarda) qo‘shimcha ravishda himoyalanadigan axborotning sizib chiqishini oldini olish uchun DLP himoya vositalari o‘rnatilishi lozim.

18. Zarurat tug‘ilganda va Korxona rahbariyati yoki KABT boshqarmasi rahbari bilan kelishilgan holda hisobga olingan mobil qurilmalarni (noutbuklarni) Korxonaning lokal tarmog‘iga ulashga ruxsat beriladi. Bunda hisobga olingan mobil qurilmalar Korxona xodimlarining ishchi stansiyalari uchun belgilangan axborot xavfsizligi talablariga javob berishi shart, ya’ni:

- antivirus himoya vositalari hamda himoyalanadigan axborotning sizib chiqishini oldini oluvchi DLP vositalarini o‘rnatish;

- hisobga olingan mobil qurilmani markazlashtirilgan tarzda boshqarish va unga kirishni nazorat qilish;

- hisobga olingan mobil qurilmaga faqat foydalanishga ruxsat etilgan dasturiy ta’minotni o‘rnatish;

- hisobga olingan mobil qurilmada xodim uchun foydalanuvchi huquqlarini belgilash;

- Korxonaning ichki axborot tizimlari va resurslariga kirishni cheklash.

19. Hisobga olingan mobil qurilmalardan Korxonaning har qanday himoya qilinadigan axborotini saqlash va qayta ishlash uchun foydalanish taqiqlanadi.

20. Ushbu Yo‘riqnomada bayon etilgan axborot xavfsizligi talablarining hisobga olingan mobil qurilmalarda ta’minlanishi Korxonada KABT boshqarmasi tomonidan amalga oshiriladi.

4. Javobgarlik

21. Korxona xodimlari ushbu Yo‘riqnoma talablarini buzganlik uchun shaxsan javobgardirlar.

22. Ushbu Yo‘riqnomada belgilangan ro‘yxatdan o‘tgan mobil qurilmalardan foydalanish talablarini buzish O‘zbekiston Respublikasining ichki mehnat qoidalari va mehnat qonunchiligiga muvofiq intizomiy choralar ko‘rishga olib keladi.

21. Korxonaning KABT boshqarmasi ushbu Yo‘riqnoma talablariga rioya qilish uchun javobgardir.

Axborot xavfsizligi
siyosatiga 13-ilova

Axborot tashuvchi vositalar va ma’lumotlarni saqlash qurilmalari bilan ishlashda xavfsizlikni ta’minlash bo‘yicha yo‘riqnoma

1. Umumiy qoidalar

1. Ushbu Yo‘riqnoma ruxsatsiz kirishning oldini olish va ularda saqlanadigan ma’lumotlarning xavfsizligini ta’minlash maqsadida Axborot tashuvchi vositalar va ma’lumotlarni saqlash qurilmalari (bundan buyon matnda raqamli axborot tashuvchilar deb yuritiladi) foydalanish talablari va qoidalarini belgilaydi.

2. Korxonaning axborot-kommunikatsiya infratuzilmasida raqamli saqlash vositalaridan foydalanish deganda, ularning Korxonaning axborot-kommunikatsiya infratuzilmasi va raqamli axborot tashuvchilar o‘rtasida ma’lumotlarni qayta ishlash, qabul qilish/uzatish maqsadida qurilmalarga, lokal yoki lokal tarmoqqa ulanishi tushuniladi.

3. Ushbu Yo‘riqnoma Korxonaning barcha tarkibiy bo‘linmalari va xodimlariga qo‘llaniladi.

2. Atamalar, ta’riflar va qisqartmalar

4. Ushbu Yo‘riqnomada quyidagi atamalar va ularning ta'riflari qo‘llaniladi: nazorat qilinadigan zona - Doimiy yoki bir martalik ruxsati bo‘lmagan begona shaxslar va transport vositalarining nazoratsiz bo‘lishi ta’qiqlangan joy (hudud, binolar, xonalarning bir qismi);

2) ma’lumotlarni saqlash qurilmasi: ma’lumotni o‘qiydigan va/yoki yozadigan hamda ma’lumotlarni zaxiralash, saqlash va tashish uchun axborotni qayta ishlash vositalaridan tashqarida ishlatiladigan qurilma;

3) ma’lumotlarni tashish qurilmasi - oflayn rejimida saqlash uchun mo‘ljallangan qurilma. Ular quyidagi shaklda bo‘lishi mumkin: qattiq disklar (HDD), flesh-xotira (USB flash), optik lazer disklari (CD, DVD), disketalar.

5. Ushbu hujjatda quyidagi qisqartmalar qo‘llaniladi:

DLP (Data Leak Prevention) — axborot sizib chiqishini oldini olish tizimi;

3. Raqamli saqlash vositalaridan foydalanish qoidalari

6. Ma’lumotlarni saqlash qurilmalari ma’lumotlarni qayta ishlash va saqlash vositalarida ishlatiladigan HDD va SSD disklarni, shuningdek, olinadigan saqlash portlari (USB va Type-C) orqali ma’lumotlarni qayta ishlash va saqlash vositalariga ulangan tashqi qurilmalarni o‘z ichiga oladi.

Raqamli saqlash vositalari ma’lumotlarni avtonom saqlash va yozib olish joyidan mustaqil ravishda foydalanish uchun mo‘ljallangan. Ular flesh-xotira, optik disklar, magnit lentalar, floppi disklar, raqamli xotira kartalari (SD kartalar) va boshqalar bo‘lishi mumkin.

7. Ushbu hujjatda belgilangan talablar quyidagilarga tegishli bo‘lgan raqamli saqlash vositalaridan foydalanishga nisbatan qo‘llaniladi:

- Korxona xodimlari bo‘lmagan shaxslar (mijozlar va tashrif buyuruvchilar);
- Korxona xodimlari;
- Korxona xodimlarga o‘z xizmat vazifalarini bajarish uchun taqdim etiladigan.

8. Tashqi shaxslarga tegishli barcha turdagi raqamli axborot tashuvchilarni Korxonaning hududiy boshqarmalariga olib kirish taqiqlanadi.

Tashqi shaxslar tomonidan raqamli axborot tashuvchilarning olib kirilishi ustidan nazorat qo‘riqlash xizmati tomonidan amalga oshiriladi.

9. Tashqi shaxslarga hamda Korxona xodimlariga tegishli barcha turdagi raqamli axborot tashuvchilardan Korxonaning maxfiy va boshqa himoya qilinadigan axborotini saqlash uchun foydalanish taqiqlanadi.

10. Korxonada lokal tarmoqqa ulangan yakuniy qurilmalarda ko‘chma raqamli axborot tashuvchilarni ulash uchun mo‘ljallangan portlar va drayvlarning ishlatilishi bloklanadi.

Ishlab chiqarish zarurati tug‘ilganda Korxona rahbariyati tomonidan belgilangan ayrim ishchi o‘rinlarda ko‘chma raqamli axborot tashuvchilardan foydalanishga ruxsat beriladi.

11. Tashqi shaxslarga yoki Korxona xodimlariga tegishli bo‘lgan ko‘chma raqamli axborot tashuvchilarni faqat ko‘chma tashuvchilarni ulash portlaridan foydalanishga ruxsat berilgan va antivirus himoya vositalari hamda himoyalanadigan axborotning sizib chiqishini oldini oluvchi DLP vositalari o‘rnatilgan qurilmalarga ulashga ruxsat etiladi.

Tashqi shaxslarga tegishli va ishonchsiz deb hisoblangan ko‘chma raqamli axborot tashuvchilar hamda ma’lumot saqlovchi qurilmalar Korxonada foydalanishdan oldin zararli dasturlar mavjudligiga tekshiruvdan o‘tkazilishi mumkin. Mazkur tekshiruv Korxonaning KABT boshqarmasi axborot xavfsizligi administratorlari tomonidan, maxsus ish joyida amalga oshiriladi. Ushbu ish joyida yangilangan antivirus bazasiga ega antivirus himoya vositasi o‘rnatilgan bo‘lishi shart. Tashqi raqamli tashuvchilar va ma’lumot saqlovchi qurilmalar tekshirilayotgan davrda maxsus ish joyi Korxonaning lokal va lokal tarmog‘idan uzilgan bo‘lishi lozim.

12. Korxona xodimlari shaxsiy, mulkiy ma’lumotlarni saqlash uchun o‘zlarining raqamli axborot tashuvchilardan foydalanishlari mumkin. Biroq, ularni Korxonaning har qanday konfidensial yoki boshqa himoyalangan ma’lumotlarini olib chiqish uchun saqlash yoki ulardan foydalanish taqiqlanadi. Ushbu talabga rioya qilish uchun javobgarlik butunlay Korxona xodimiga yuklatiladi va ularning lavozim tavsifida ko‘rsatilgan.

13. Korxonaning axborot va kommunikatsiya infratuzilmasida faqat Korxonaning mulki bo‘lgan va Korxona xodimlariga o‘z xizmat vazifalarini bajarish uchun taqdim etilgan raqamli saqlash vositalaridan foydalanish mumkin.

14. Korxona xodimlariga raqamli axborot tashuvchilarni hisobga olish va tayinlash Axborot xavfsizligi bo‘limi tomonidan amalga oshiriladi.

Korxonadagi raqamli axborot tashuvchilar o‘z xodimlariga doimiy foydalanish yoki vaqtincha foydalanish uchun Korxona rahbariyatining ruxsati bilan beriladi. Foydalanilmaganda, raqamli axborot tashuvchilar topshiriladi va Korxonaning KABT boshqarmasida saqlanadi.

Xodimlarga (bo‘limlarga) raqamli saqlash vositalarini tayinlash, shuningdek, ularning Korxona ichidagi harakati Korxonaning raqamli saqlash vositalari jurnalida qayd etiladi, uning shakli ushbu Yo‘riqnomaning 1-ilovasida keltirilgan.

Ushbu jurnal Korxonaning Axborot xavfsizligi bo‘limi tomonidan yuritiladi.

15. Raqamli axborot tashuvchilar Korxonaning Axborot xavfsizligi bo‘limi tomonidan muntazam audit va monitoringdan o‘tkaziladi.

16. Korxonada hisobga olingan ko‘chma raqamli axborot tashuvchilar quyidagi maqsadlarda qo‘llaniladi:

- xizmat axborotini saqlash uchun;

- himoya qilinadigan axborotni saqlash uchun (masalan, “xizmatda foydalanish uchun” belgilangan hujjatlarni devonxonada saqlash);

- ishlab chiqarish-texnologik maqsadlarda foydalanish uchun (masalan, zaxira nusxalarni saqlash, dasturlarni saqlash yoki o‘rnatish, dastur manba kodlari va test ma’lumotlarini saqlash va boshqalar).

17. Korxonada ishlab chiqarish-texnologik maqsadlarda foydalaniladigan hisobga olingan ko‘chma raqamli axborot tashuvchilar KABT boshqarmasi mutaxassislar va axborot xavfsizligi administratorlari tomonidan qo‘llaniladi.

18. Korxonaning nazorat qilinadigan zonadan tashqarida konfidensial va boshqa himoyalangan ma’lumotlarni o‘z ichiga olgan saqlash vositalarini chiqish faqat Korxona rahbariyatining ruxsati bilan ruxsat beriladi. Konfidensial ma’lumotlarni o‘z ichiga olgan saqlash vositalarini kiritish va olib chiqish to‘g‘risidagi ma’lumotlar ushbu Yo‘riqnomaning

2-ilovasida keltirilgan maxsus jurnalda qayd etiladi.

19. Korxona xodimlari vaqti-vaqti bilan ularga taqdim etilgan raqamli axborot tashuvchilarni antivirus dasturi yordamida zararli dasturlar bor-yo‘qligini tekshirib turishlari shart. Bundan tashqari, antivirus dasturi xodimning oxirgi qurilmasiga ulanganida raqamli saqlash vositalarni avtomatik ravishda skanerlash uchun sozlangan bo‘lishi kerak.

20. Raqamli saqlash vositalaridan foydalanganda Korxona xodimlari quyidagi talablarga rioya qilishlari shart:

- ulardan maqsadli foydalanish;
- Korxonaning KABT boshqarmasiga raqamli axborot tashuvchilarning yo‘qolishi (o‘g‘irlanishi) yoki ishdan chiqishi haqida xabar berish;
- ish va ishdan tashqari vaqtlarda raqamli saqlash vositalarining jismoniy xavfsizligini barcha oqilona vositalar bilan ta’minlash;
- raqamli saqlash vositalarini boshqa shaxslarga bermaslik;
- ushbu Yo‘riqnomada belgilangan saqlash vositalari bilan harakatlar uchun tegishli ruxsatnoma olish;
- ma’lumotlarni saqlash vositalarini zararli dasturlar bor-yo‘qligini vaqti-vaqti bilan tekshirish;
- foydalanilmayotgan paytda, shuningdek, ishdan bo‘shatish yoki boshqa ishga o‘tkazish holatlarida raqamli saqlash vositalarini qaytarish.

21. KABT boshqarmasi ruxsatisiz Korxonaning lokal tarmog‘iga ulangan ishchi stansiyalar va serverlarga ma’lumot saqlovchi qurilmalarni ulashga ruxsat etilmaydi.

22. Korxonada zaxira nusxalar va elektron arxivlarni saqlash uchun ko‘chma raqamli axborot tashuvchilardan foydalanilmaydi.

Korxonaning server zaxira nusxalarini saqlash uchun hisobga olingan ko‘chma axborot tashuvchilar qo‘llaniladi. Ularni hisobga olish va xavfsiz saqlash KABT boshqarmasining axborot xavfsizligi administratori tomonidan amalga oshiriladi.

Korxonada zaxira nusxasi mavjud bo‘lgan hisobga olingan ko‘chma axborot tashuvchidagi ma’lumotlarning to‘liqligi va yaxlitligi muntazam ravishda tekshirib borilishi lozim.

23. Zarurat tug‘ilganda yakuniy qurilma yoki serverni tashqi korxonalar tomonidan ta’mirlashdan oldin ma’lumot saqlovchi qurilma (disk) chiqarib olinishi shart. Agar ta’mirlash ishlarini ma’lumot saqlovchi qurilmasiz amalga oshirish imkonsiz bo‘lsa, bunday ta’mirlash ishlari Korxona KABT boshqarmasi vakili ishtirokida va uning nazorati ostida bajarilishi lozim.

24. Yakuniy qurilmalar va serverlardan yechib olingan ma’lumot saqlovchi qurilmalar foydalanilmayotgan davrda Korxona KABT boshqarmasining himoyalangan shkaflarida saqlanishi lozim.

25. Korxonada konfidensial axborotni o‘z ichiga olgan ma’lumot saqlovchi qurilmalarni nazorat qilinadigan zona tashqarisiga olib chiqish faqat Korxona rahbariyati ruxsati bilan hamda maxsus jurnalda (ushbu Yo‘riqnomaning 2-ilovasida keltirilgan shakl bo‘yicha) hisobga olish yozuvlarini kiritgan holda amalga oshiriladi.

Bunda konfidensial axborotga ega ma’lumot saqlovchi qurilmalarni tashish Korxona xodimi tomonidan shaxsan amalga oshiriladi.

4. Ko‘chma raqamli axborot tashuvchilar va ma’lumot saqlovchi qurilmalarni utilizatsiya qilish hamda qayta foydalanishga qo‘yiladigan talablar

26. Korxona xodimi ishdan bo‘shatilgan yoki boshqa ish joyiga o‘tkazilgan taqdirda, ularga taqdim etilgan raqamli saqlash vositalari Korxonaning KABT boshqarmasiga qaytarib topshirilishi kerak.

27. Axborot tashuvchi vositalar shu bilan birga ishchi stansiyalar bir xodimdan boshqa xodimga foydalanish uchun taqdim etilganda vositada saqlangan har qanday axborot KABT boshqarmasi tomonidan o‘chirilishi shart.

Himoyalangan ma’lumotlarni qayta ishlash uchun ishlatilmagan (konfidensial ma’lumotlarni o‘z ichiga olmaydigan) va hisobdan chiqarilishi kerak bo‘lgan raqamli saqlash qurilmalarida, ish stansiyalarida yoki mobil saqlash qurilmalarida ishlatiladigan raqamli saqlash vositalari ham o‘chirishga majburdir.

29. Axborot tashuvchi vositalardagi ma’lumotlarni tozalash uchun o‘chirish uchun dasturiy ta’minot yoki apparat vositalaridan foydalanish maqsadga muvofiq. Qayta yozish ATA/SCSI buyrug‘i mantiqiy manzilli va mantiqiy bo‘lmagan jismoniy qurilma uchun ishlatiladi.

Qurilma interfeysini qo‘llab-quvvatlash (ATA yoki SSD) bilan tekshirish barcha kirish mumkin bo‘lgan joylarni to‘liq o‘qib chiqish orqali barcha manzilli joylarda o‘chirish kutilgan natijalarni berganligini tekshirish orqali amalga oshiriladi.

30. Qattiq disklardagi qoldiq ma’lumotlarni o‘chirib tashlaganidan keyin o‘qish imkoniyatini oldini olish uchun yo‘q qilinayotgan ma’lumotlarni saqlash joylarida ma’lumotlarni 7 marta yozib olish va o‘chirish tavsiya etiladi.

Korxonada raqamli axborot tashuvchilarda saqlanayotgan himoyalanadigan axborotni kafolatli yo‘q qilish uchun raqamli qayta yozish (overwrite) usuli qo‘llaniladi. Buning uchun raqamli tashuvchidan himoyalanadigan axborot o‘chirilgandan so‘ng, axborot saqlangan joylarga uch marta ma’lumot yozish va o‘chirish amaliyoti bajariladi.

Raqamli axborot tashuvchilardagi kafolatlangan ma’lumotlarni yo‘q qilish Korxonadagi KABT boshqarmasi tomonidan amalga oshiriladi.

31. Ma’lumotlarni saqlash qurilmalari (serverlar), ish stantsiyalari yoki mobil qurilmalardan yaroqsiz holga kelgan (bundan keyin foydalanib bo‘lmaydigan) raqamli saqlash vositalari yo‘q qilinishi va hisobdan chiqarilishi kerak.

Ma’lumotlarni saqlash qurilmalari va ish stansiyalarida himoyalangan ma’lumotlarni qayta ishlash uchun ishlatilgan va hisobdan chiqarilishi kerak bo‘lgan saqlash vositalari ham yo‘q qilinishi va hisobdan chiqarilishi kerak.

32. Saqlash vositalari parchalanish yo‘li bilan yo‘q qilinadi, bu esa vositalarni parchalanish (undagi ma’lumotlarni o‘qish imkoniyatisiz jismoniy yo‘q qilish) orqali to‘liq yo‘q qilishni o‘z ichiga oladi.

33. Yo‘q qilish va hisobdan chiqarish uchun mo‘ljallangan raqamli saqlash vositalari Korxonaning KABT boshqarmasiga topshirilishi kerak.

Yo‘q qilish uchun mo‘ljallangan raqamli saqlash vositalari qulflangan metall shkaflarda (seyflarda) saqlanishi kerak.

34. Raqamli saqlash vositalari yo‘q qilingandan so‘ng, Korxonaning KABT boshqarmasiga tegishli ma’lumotlarni ushbu Yo‘riqnomaning 3-ilovasida keltirilgan maxsus jurnalga kiritadi.

35. Raqamli saqlash vositalarini hisobdan chiqarish Korxona tomonidan belgilangan tartibda, hisobdan chiqarish to‘g‘risidagi dalolatnoma tayyorlash bilan amalga oshiriladi.

6. Javobgarlik

36. Korxona xodimlari ushbu Yo‘riqnoma talablarini buzganlik uchun shaxsiy javobgarlikka tortiladilar.

37. Ushbu Yo‘riqnomada belgilangan raqamli saqlash vositalaridan foydalanish talablarini buzish O‘zbekiston Respublikasining ichki mehnat qoidalari va mehnat qonunchiligiga muvofiq intizomiy choralar ko‘rishga olib keladi.

38. Ushbu Yo‘riqnoma talablariga rioya qilinishi uchun Korxonaning KABT boshqarmasi javobgardir.

Axborot xavfsizligi
siyosatiga 14-ilova

Internet, elektron pochta va tezkor xabar almashish ilovalaridan foydalanish bo‘yicha yo‘riqnoma

1. Asosiy qoidalar

1. Ushbu Yo‘riqnoma xodimlar Internetga kirish va undan foydalanishda, shuningdek, elektron pochta va tezkor xabar almashish tizimlari, fayllar va media (keyingi o‘rinlarda – messenjer) orqali ma’lumot almashishda Korxona uchun axborot xavfsizligini ta’minlash talablarini belgilaydi.

2. Ushbu hujjat quyidagilarga oid talablarni belgilaydi:

- Internetdan ma’lumot olish yoki yuklab olish;
- Internet veb-resurslariga tashrif buyurish;
- Internetda ma’lumot joylashtirish;
- Internet resurslaridan foydalanish (ijtimoiy tarmoqlar, elektron pochta xizmatlari, messenjerlar).

3. Ushbu hujjat talablari quyidagilar orqali ma’lumot almashishga nisbatan qo‘llaniladi:

- tashqi elektron pochta, shu jumladan Internet elektron pochta xizmatlari (Gmail, Mail.ru, Yahoo Mail);
- korporativ elektron pochta;
- tashqi tezkor xabar almashish vositalari (WhatsApp, WeChat, Facebook Messenger, Telegram va boshqalar);
- korporativ tezkor xabar almashish vositalari.

4. Markazlashtirilgan Internetga kirish Korxonaning xodimlariga Korxona lokal tarmog‘ining Internetga ulanish chegarasida o‘rnatilgan axborotni himoya qilish vositalari orqali taqdim etiladi.

5. Korxonada proksi-server orqali markaziy apparat va hududiy boshqarmalar xodimlari uchun Internet-resurslarning ayrim toifalariga kirish quyidagi kategoriyalar bo‘yicha cheklanadi:

- Birinchi toifadagi xodimlarga internetga kirish huquqi beriladi, ammo ma'lum resurslarga kirish cheklovlari bilan ("qora ro‘yxat"), bu tashqi messenjerlar, ijtimoiy tarmoqlar, tashqi proksi-serverlar, VPN serverlari, TOR tarmoqlari va tengdosh tarmoqlarini o‘z ichiga oladi;
- Ikkinchi toifa xodimlariga Internet tarmog‘iga to‘liq kirish huquqi beriladi (faqat zararli, fishing va firibgarlik resurslari hamda shunga o‘xshash xavfli manbalarga kirish cheklanadi).

6 . Korxonada korporativ elektron pochta uchun o‘z serveri tashkil etilgan. Bu server korxonaning ichki lokal tarmog'ida yoki tashqi himoyalangan datamarkazda bo'lishi mumkin. Korporativ elektron pochta rahbariyat tomonidan ruxsat etilgan korxona xodimlariga Internet tarmog‘i orqali tashqi foydalanuvchilar bilan elektron pochta almashish imkonini beradi. Korxonaning korporativ elektron pochta shaxsiy manzili bo'lim yoki sex nomi bilan ochiladi. Pochta qutisi birinchi marta tizimga kirilgandan va pochta serveriga ulanish sozlangandan so‘ng foydalanish uchun ochiladi.

Korxona xodimlarini, korporativ elektron pochta tizimiga ulash KABT boshqarmasi tomonidan ta’minlanadi.

7 . Korxonada elektron pochta xizmat axborotini matnli xabarlar yoki elektron hujjatlar ko‘rinishida Korxona xodimlari o‘rtasida hamda tashqi foydalanuvchilar bilan almashish uchun qo‘llaniladi.

8 . Elektron pochta orqali tashqi foydalanuvchilar bilan har qanday himoya qilinadigan axborotni shifrlanmagan holda uzatish taqiqlanadi. Mazkur himoya qilinadigan axborotni uzatish faqat axborotni kriptografik himoya qilish vositalari (keyingi o‘rinlarda – AKHV)

yordamida shifrlangan holda yoki Korxona KABT boshqarmasi bilan kelishilgan hamda Korxona rahbariyati tomonidan tasdiqlangan boshqa usulda amalga oshirilishi mumkin.

9 . Korxonaning himoya qilinadigan axborotini “E-xat” himoyalangan elektron pochta tizimi orqali uzatishga ruxsat etiladi, ushbu tizimga Korxonaning ayrim xodimlari ulangan bo‘ladi.

10. Korxona xodimlari o‘rtasida tezkor xabar almashish uchun korporativ tezkor messenjer xizmatini tashkil qiladi.

11. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2024-yil 24-oktabrdagi 699-sonli qaroriga muvofiq, Lochin aloqa platformasi Korxona xodimlari tomonidan davlat idoralari va korxonalari bilan tezkor xabar almashish uchun ishlatilishi kerak.

Shuningdek, Korxonaning ayrim toifadagi xodimlariga o‘z xizmat vazifalarini bajarish uchun bunday ruxsat talab qilinadigan tashqi tezkor xabar almashish vositalaridan foydalanish huquqi berilishi mumkin.

12. Korporativ messenjer, Lochin messenjeri, tashqi messenjerlar yoki boshqa Internet axborot almashinuv tizimlari (masalan, Internet pochtasi, ijtimoiy tarmoqlar, onlayn video konferensiyalar va boshqalar) orqali konfidensial va boshqa himoyalangan ma’lumotlarni uzatish taqiqlanadi.

13. Internetdan, elektron pochta yoki tezkor messenjer orqali olingan har qanday elektron ma’lumot Korxonada qo‘llaniladigan antivirus himoyasi va elektron pochta xavfsizlik vositalari yordamida zararli dasturlarga tekshirilishi kerak.

2. Atamalar, ta’riflar va qisqartmalar

14. Ushbu Yo‘riqnomada quyidagi atamalar va ta'riflar qo‘llaniladi:

1) Internet resurslari: veb-saytlar va mobil ilovalardan tortib ma’lumotlar bazalari va bulutli saqlashgacha Internetda mavjud bo‘lgan ma’lumotlar va xizmatlar to‘plami;

2) Messenger: foydalanuvchilar o‘rtasida tezkor xabar almashish, fayllar va media almashinuvi tizimi;

3) Elektron pochta: kompyuter tarmog‘i orqali foydalanuvchilar o‘rtasida raqamli xabarlar va fayllarni yuborish texnologiyasi va xizmati..

15. Ushbu hujjatda quyidagi qisqartmalar qo‘llaniladi:

DLP (Data Leak Prevention) — axborot oqishining oldini olish tizimi;

3. Internetga kirishni ta’minlash va elektron pochta va tezkor xabar almashish vositalaridan foydalanish tartibi

16. Korxona ichida ayrim xodimlarga ularning ish majburiyatlariga qarab Internetga kirish imkoniyati taqdim etiladi.

17. Korxona xodimlariga Internetga kirish imkoniyati tarkibiy bo‘linma rahbarining Korxona rahbariyati tomonidan tasdiqlangan arizasi asosida taqdim etiladi.

Korxonada arizada Internetga kirish toifasi ko‘rsatilishi kerak.

Tasdiqlangan arizalar Korxonaning KABT boshqarmasiga yuboriladi.

18. Korxona xodimlariga, Internet tarmog‘iga kirish huquqi KABT boshqarmasi (lokal tarmoq tarmoq administratori) tomonidan taqdim etiladi.

19. Internetga kirish imkoniyatini taqdim etishdan oldin, Korxona xodimlari ushbu Yo‘riqnoma bilan tanishib chiqishlari kerak.

20. Korxona xodimi tomonidan Internetga kirish ularning oxirgi qurilmasidan amalga oshiriladi. Boshqa shaxsning oxirgi qurilmasidagi harakatlar uchun javobgarlik harakat amalga oshirilgan oxirgi qurilma foydalanuvchisi zimmasidadir.

21. Korxona rahbariyatining roziligisiz Internetga kirishni mustaqil ravishda tashkil etish taqiqlanadi. Korxonaning KABT boshqarmasi tomonidan tasdiqlanmagan boshqa texnik ulanish usullaridan foydalangan holda Internetga kirishni mustaqil ravishda tashkil etish ham taqiqlanadi.

22. Korxona xodimlari uchun Internetga kirishni tashkil qilishda ularning tashqi Internet tarmog‘iga ulanish chegarasida o‘rnatilgan proksi-server va xavfsizlik shlyuzi orqali, xodimlar uchun esa tashqi Internet tarmog‘iga ulanish chegarasida o‘rnatilgan xavfsizlik shlyuzi orqali ulanish talabi bajarilishi kerak.

23. Korxonada korporativ elektron pochta tizimiga kirish huquqi beriladigan xodimlar ro‘yxati KABT boshqarmasi tomonidan belgilanadi va Korxona rahbariyati bilan kelishiladi. Korxona xodimlarining korporativ elektron pochta tizimiga kirish huquqi Korxonaning kirish matritsasida aks ettirilishi shart.

24. Tashqi foydalanuvchilar bilan elektron pochta almashish huquqi Korxona xodimiga tarkibiy bo‘linma rahbari tomonidan berilgan, Korxona rahbariyati bilan kelishilgan ariza asosida taqdim etiladi.

Kelishilgandan so‘ng mazkur ariza Korxonaning KABT boshqarmasiga yuboriladi.

25. Korxonaning korporativ messenjeriga kirish huquqiga ega bo‘lgan xodimlar ro‘yxati KABT boshqarmasi tomonidan belgilanadi va Korxona rahbariyati bilan kelishiladi. Korxona xodimlarining, messenjerga kirish huquqi Korxonaning kirish matritsasida aks ettirilishi shart.

26. “Lochin” messenjeri va boshqa tashqi messenjerlardan foydalanish huquqi ro‘yxati Korxona rahbariyati tomonidan belgilanadigan xodimlarga taqdim etiladi.

27. Korxona faoliyati to‘g‘risidagi axborotni tarqatish hamda reklama maqsadlarida Korxonaning rasmiy veb-sayti va ijtimoiy tarmoqlardan foydalaniladi.

Yuqorida ko‘rsatilgan axborotni tarqatish huquqi Korxona marketing bo‘linmasi xodimlariga beriladi. Boshqa xodimlar esa Korxona nomidan Internet tarmog‘ida axborotlarni faqat Korxona rahbariyati bilan kelishilgandan so‘ng e’lon qilishlari mumkin.

4. Internetdan foydalanish qoidalari

28. Korxona xodimlari ma’lumot olish va tarqatish maqsadida o‘zlarining oxirgi qurilmalaridan Internetga kirishlari mumkin.

29. Korxona xodimlari o‘zlarining xizmat vazifalarini bajarish uchun zarur bo‘lgan har qanday ma’lumotni Internetdan qidiruv tizimlari orqali Internet axborot resurslariga kirish yoki URL manzilini kiritish orqali olishlari mumkin.

Ushbu Yo‘riqnoma bilan taqiqlangan va Korxonaning Axborot xavfsizligi siyosatiga zid bo‘lgan Internet resurslariga xodimlarning kirishiga cheklovlar Korxonaning proksi-serveri va Korxonaning xavfsizlik shlyuzlari orqali o‘rnatiladi.

30. Internetdan foydalanishda quyidagilar zarur:

- ushbu Yo‘riqnoma talablariga rioya qilish;
- Internetdan faqat o‘z xizmat vazifalarini bajarish uchun foydalanish;
- Korxonaning KABT boshqarmasiga ushbu Yo‘riqnoma talablarining har qanday buzilishi haqida xabar berish.

31. Internetdan foydalanishda Korxona xodimlariga quyidagilar taqiqlanadi:

- taqdim etilgan Internetga kirishdan shaxsiy yoki ko‘ngilochar maqsadlarda foydalanish;
- qonun bilan taqiqlangan kontentni ko‘rish yoki tarqatish;
- Internetga ruxsatsiz kirish huquqini olish;
- konfidensial yoki boshqa himoyalangan ma’lumotlarni shifrlanmagan shaklda va Korxonaning KABT boshqarmasi yoki Korxona rahbariyatining roziligisiz uzatish;
- konfidensial hujjatlarni Internetdagi bulutli xizmatlarga yuklash;
- Internetdagi ko‘ngilochar, shubhali, zararli yoki noqonuniy veb-saytlarga tashrif buyurish;
- Internetdan dasturlarni yuklab olish va o‘rnatish;
- Xodimlarga Internetga ruxsatsiz kirish imkonini beruvchi maxsus apparat va dasturiy ta’minotdan foydalanish;

- Korxonaning KABT boshqarmasi tomonidan ruxsat etilganlardan tashqari, Internetga kirishning boshqa shakllaridan foydalanish, shuningdek, anonim Internetga kirish uchun turli veb-saytlar va dasturlardan foydalanish;

- Onlayn ishlayotganda tashqi proksi-serverlardan, VPN serverlaridan, TOR tarmoqlaridan, tengdosh tarmoqlaridan va anonimlashtiruvchilardan foydalanish;

- Korxona shu jumladan elektron pochta manzillarini e'lonlar taxtalarida yoki mehmonlar kitoblarida e'lon qilish;

- Rasmiy va himoyalangan ma’lumotlarni yuborish uchun elektron pochta, ijtimoiy tarmoqlar va tashqi internet-messenjerlardan foydalanish;

- Korxonaning himoyalangan obyektlariga foydalanuvchi qayd yozuvlari, parollar va boshqa kirish ma’lumotlarini ulashish;

- Tarmoqqa katta yuk keltiradigan va boshqa foydalanuvchilarning normal ishlashiga xalaqit beradigan oqimli resurslarga kirish;

- Internetda qonun bilan va ushbu Yo‘riqnomaga zid bo‘lgan noqonuniy tranzaksiyalarni amalga oshirish va boshqa harakatlarni amalga oshirish.

32. Korxona xodimlari quyidagi huquqlarga ega:

- Internet tarmog‘iga kirish imkonini bermaydigan texnik xatoliklar yuzaga kelganda KABT boshqarmasiga murojaat qilish;

- Ushbu Yo‘riqnoma talablarining har qanday buzilishi holatlari haqida Korxonaning KABT boshqarmasini xabardor qilish;

- Internet tarmog‘iga kirishda kontent filtrlash qoidalarini o‘zgartirish bo‘yicha takliflar kiritish.

5. Elektron pochta va tezkor xabar almashish dasturlaridan foydalanish qoidalari

33. Korxona xodimlari elektron pochta va messenjerlar bilan ishlashda, hatto ma'lum jo‘natuvchidan olingan har qanday elektron pochta xabarlari xavf tug‘dirishi mumkinligini tushunishlari kerak.

Shuning uchun, elektron pochta va messenjerlar foydalanuvchilari, hatto jo‘natuvchini shaxsan bilsalar ham, har qanday shubhali xabardan ilovalar yoki havolalarni ochishda juda ehtiyot bo‘lishlari kerak.

34. Foydalanuvchi pochta qutisi hajmi va uzatiladigan ma’lumotlar hajmiga cheklov o‘rnatiladi. Agar saqlangan yoki uzatiladigan ma’lumotlar hajmi belgilangan chegaradan oshsa, elektron pochtaga kirish bloklanadi. Elektron pochtaga kirish bloklanganda, pochta qutisi chegarasi oshib ketganligi va foydalanuvchi pochta qutisini tozalashi kerakligi haqida xabar ko‘rsatiladi.

35. Elektron pochta va tezkor xabar almashish foydalanuvchilariga quyidagilar taqiqlanadi:

- ulardan shaxsiy yozishmalar uchun, har qanday shaxsiy yoki tijorat maqsadlarida foydalanish;

- shubhali ilovalar va havolalarni ochish;

- konfidensial va boshqa himoyalangan ma’lumotlarni shifrlanmagan shaklda yuborish va uzatish;

- siyosiy, diniy yoki g‘ayriinsoniy xarakterdagi ma’lumotlarni, shuningdek, odobsiz, tuhmat qiluvchi, haqoratli, tahdidli yoki noqonuniy materiallarni uzatish, namoyish qilish yoki saqlash. Agar bunday ma’lumotlar paydo bo‘lsa, foydalanuvchi darhol o‘zining bevosita rahbariga xabar berishi kerak;

- axloqsiz, haqoratli yoki noqonuniy kontentga ega yozishmalarni yuborish yoki tahdidlar yoki haqoratlarni o‘z ichiga olish;

- reklama (xizmat faoliyatiga mos bo‘lmagan) yoki ko‘ngilochar materiallarni yuborish;

- professional faoliyat yoki ish majburiyatlari bilan bog‘liq bo‘lmagan ko‘ngilochar kontentga yoki davriy onlayn reklama materiallariga obuna bo‘lish uchun ish elektron pochta

manzilidan foydalanish;

- elektron pochta xabarlarini yuborishda mavjud bo‘lmagan qaytish manzillaridan foydalanish;

- biznes bilan bog‘liq bo‘lmagan elektron pochta xabarlarini ommaviy ravishda yuborish;

- viruslar bilan zararlangan zararli dasturlarni yoki fayllarni, shuningdek, *.exe, *.com, *.scr, *.js, *.vbs, *.dll, *.bat va boshqalar kengaytmali bajariladigan fayllarni tarqatish;

- rasmiy yozishmalar uchun bepul Internet elektron pochta xizmatlaridan (mail.ru, yandex.ru va boshqalar) foydalanish;

- parollar yoki Korxonaning himoyalangan obyektlariga kirishning boshqa ma’lumotlarini uchinchi shaxslarga taqdim etish.

36. Elektron pochta va messenjer foydalanuvchilari quyidagilarni bajarishlari shart:

- ishbilarmonlik uslubi va xushmuomala ohangni saqlash;
- hissiy, ziddiyatli va noaniq so‘zlardan qochish;
- ma’lumotlarning grammatikasi va aniqligini tekshirish;
- xabarning mohiyatini aks ettiruvchi mavzu qatorini ko‘rsatish;
- qo‘shimchalarning ruxsat etilgan hajmiga rioya qilish;
- yuborishdan oldin qabul qiluvchilar ro‘yxatini tekshirish.

6. Internet, elektron pochta va xabar almashishdan foydalanishni monitoring qilish

37. Korxona xodimlarining toifasiga qarab, ularga ushbu Yo‘riqnomaning 1-bo‘limiga muvofiq tegishli Internet resurslariga kirish huquqi beriladi. Internetga kirishda “qora” ro‘yxatda ko‘rsatilgan tashqi resurslarga kirish taqiqlanadi va “oq” ro‘yxatda ko‘rsatilgan tashqi resurslarga kirishga ruxsat beriladi.

38. Korxona xodimlarining har bir toifasi uchun muayyan Internet resurslariga kirish cheklovlari ("qora" va "oq" ro‘yxatlar) ro‘yxati Korxonaning KABT boshqarmasi tomonidan Korxona rahbariyati bilan kelishilgan holda tuziladi.

39. Tashqi Internet resurslariga kirish proksi-server va xavfsizlik shlyuzlari orqali cheklanadi. Tegishli konfiguratsiya Korxonaning KABT boshqarmasi tomonidan amalga oshiriladi.

40. Kirish proksi-server va xavfsizlik shlyuzidagi so‘rovlar va trafikni filtrlash orqali cheklanadi.

41. Korxonaning lokal tarmog‘i tarmoq administratori Korxona xodimlari tomonidan Internet tarmog‘i resurslaridan foydalanishni hisobga olishni yuritadi, ushbu Yo‘riqnomaga rioya etilishini nazorat qiladi hamda Internet resurslaridan xavfsiz foydalanishni ta’minlaydi.

42. Korxonaning KABT boshqarmasi axborot xavfsizligi xodimlari tomonidan internetdan maqsadli foydalanishning tasodifiy va to‘liq auditini o‘tkazish huquqiga ega.

Ushbu audit proksi-server va xavfsizlik shlyuzidagi yoki xodimlarning so‘nggi qurilmalaridagi brauzerlardagi tarix jurnallarini ko‘rib chiqish orqali amalga oshiriladi.

43. Xodimlar tomonidan tashrif buyurilgan internet-resurslar haqidagi ma’lumotlar keyingi tahlil qilish uchun qayd etiladi, zarur hollarda, tarkibiy bo‘linmalar rahbarlariga, shuningdek, ko‘rib chiqish uchun Korxona rahbariyatiga taqdim etilishi mumkin.

44. Internetdan maqsadli foydalanishning rejadan tashqari va to‘liq auditlari natijalariga ko‘ra, ushbu Yo‘riqnomani eng doimiy ravishda buzuvchilar aniqlanadi.

45. Noto‘g‘ri foydalanish holatlari Korxonaning KABT boshqarmasi tomonidan tayyorlangan “Internetdan noto‘g‘ri foydalanish to‘g‘risidagi hisobot”da qayd etiladi.

Agar yovuz niyatli huquqbuzar Internetdan noto‘g‘ri foydalanayotgani aniqlansa, undan tushuntirish xati shaklida yozma bayonot olinadi.

Internetdan noto‘g‘ri foydalanish to‘g‘risidagi hisobot Korxona rahbariyatiga taqdim etiladi.

Qayta qoidabuzarlik qilganlarning Internetga kirishi bloklanishi yoki cheklanishi yoki intizomiy choralar ko‘rilishi mumkin.

46. Agar Korxona xodimi Internetdan noto‘g‘ri foydalanishda gumon qilinsa, Korxonaning KABT boshqarmasi ichki tekshruvni boshlaydi.

47. Korxona xodimlarning elektron pochta va tezkor xabar almashish ilovalaridan foydalanish qoidalariga rioya qilishini nazorat qilish uchun quyidagi choralarni amalga oshirishlari shart:

- DLP tizimidan foydalangan holda elektron pochta va tezkor xabar almashish ilovalari orqali himoyalangan ma’lumotlarning oqishini kuzatish;
- xodimning kiruvchi va chiquvchi elektron pochta yoki messenjer yozishmalarini vaqti-vaqti bilan ko‘rib chiqish;
- elektron pochta yoki tezkor xabar almashish siyosati talablarining buzilishi bo‘yicha ichki tekshiruvlarni boshlash va o‘tkazish;
- foydalanish shartlari buzilgan taqdirda yoki boshqa intizomiy choralar qo‘llanilgan taqdirda xodimning elektron pochta yoki tezkor xabar almashishga kirishini blokirovka qilish.

48. Xodimlarning elektron pochta va tezkor xabar almashishdan foydalanish qoidalariga rioya qilishini nazorat qilish Korxonaning KABT boshqarmasi tomonidan amalga oshiriladi.

7. Javobgarlik

49. Korxona xodimlari ushbu Yo‘riqnomani buzganlik uchun shaxsiy javobgarlikka tortiladilar.

50. Ushbu Yo‘riqnomada belgilangan Internet va elektron pochtadan foydalanish qoidalarini buzish O‘zbekiston Respublikasining ichki mehnat qoidalari va mehnat qonunchiligiga muvofiq intizomiy choralar ko‘rishga olib keladi.

51. Korxona xodimlari tomonidan ushbu Yo‘riqnomaga rioya qilinishini ta’minlash uchun Korxonaning KABT boshqarmasi javobgardir.

Axborot xavfsizligi
siyosatiga 17-ilova

Himoya qilinadigan axborot bilan ishlash tartibi

1. Umumiy qoidalar

1) Ushbu hujjat O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”, “Tijorat siri to‘g‘risida”, “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonunlari, O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi 295-sonli qarori hamda 2025-yil 4-dekabrdagi 766-sonli qaroriga muvofiq himoya qilinishi lozim bo‘lgan axborot (keyingi o‘rinlarda – himoyalanadigan axborot) xavfsizligini ta’minlash chora-tadbirlarini tashkil etish va amalga oshirish tartibini belgilaydi.

2) Himoyalanadigan axborot xavfsizligi choralari ularning konfidensialligini (kirishni cheklash, oshkor etmaslik va tarqatmaslik, sizib chiqishining oldini olish) hamda saqlanishini (yo‘qotish, yo‘q qilib yuborish va yaxlitligini buzishni istisno etish) ta’minlashga qaratilgan.

3) Ushbu Yo‘riqnoma talablari davlat sirlarini o‘z ichiga olgan axborotga tatbiq etilmaydi. Bunday axborotni himoya qilish qonunchilikda belgilangan tartibda amalga oshiriladi.

4) Ushbu hujjat Korxonaning barcha xodimlari uchun og‘zaki shakldagi, moddiy tashuvchilardagi hamda axborotlashtirish obyektlarida (axborot tizimlari ma’lumotlar bazalari, yakuniy qurilmalar tashuvchilari, olinadigan raqamli tashuvchilar va boshqalar) saqlanadigan yoki aloqa kanallari orqali uzatiladigan elektron ko‘rinishdagi himoyalanadigan axborot xavfsizligini ta’minlashning yagona tartibini belgilaydi.

5) Korxonaning quyidagi axborotlari himoya qilinishi lozim:

- xizmat doirasida foydalanish uchun mo‘ljallangan, tarqatilishi cheklangan axborot xizmati (“XDFU” belgisi qo‘yilgan axborot);
- korxonaning tijorat sirini tashkil etuvchi axborot;
- xodimlar va mijozlarning shaxsga doir ma’lumotlari;
- uchinchi tomon korxonalaridan hamkorlik doirasida olingan konfidensial axborot.

2. Atamalar, ta’riflar va qisqartmalar

6. Ushbu tartibda quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

1) “Xizmatda doirasida foydalanish uchun” grifi qo‘yilgan hujjatlar – moddiy tashuvchiga yozilgan, ularni identifikatsiya qilish imkonini beruvchi rekvizitlarga ega hamda belgilangan tartibda xizmat doirasida foydalanish bilan cheklangan hujjatlar;

2) konfidensial axborotga kirish – konfidensiallik saqlanishi sharti bilan, axborot egasining roziligi yoki boshqa qonuniy asosga ko‘ra, muayyan shaxslarning konfidensial axborot bilan tanishish huquqi;

3) XDFU – axborot tashuvchilarida joylashtiriladigan yoki elektron faylga kiritiladigan, xizmat doirasida foydalanishni cheklash uchun mo‘ljallangan maxsus belgi (grif);

4) tijorat siri – ilmiy-texnikaviy, texnologik, ishlab chiqarish, moliyaviy-iqtisodiy va boshqa sohalarda tijorat qiymatiga ega bo‘lgan, uchinchi shaxslarga noma’lumligi sababli ahamiyat kasb etuvchi, qonuniy asosda erkin foydalanish imkoni bo‘lmagan hamda egasi tomonidan uni himoya qilish choralari ko‘rilgan axborot;

5) nazorat qilinadigan zona – doimiy yoki bir martalik ruxsatnomaga ega bo‘lmagan begona shaxslar va transport vositalarining nazoratsiz bo‘lishi istisno etilgan hudud (territoriya, bino yoki binoning bir qismi).

Izoh: Nazorat qilinadigan zonaning chegaralari quyidagilar bo‘lishi mumkin:

- korxonaning qo‘riqlanadigan hududi perimetri;
- agar bino qo‘riqlanmaydigan hududda joylashgan bo‘lsa, qo‘riqlanadigan bino yoki uning qo‘riqlanadigan qismining to‘siq konstruksiyalari;

6) konfidensial axborot – davlat sirlarini o‘z ichiga olmaydigan, hujjatlashtirilgan hamda qonunchilikka muvofiq kirish cheklangan axborot;

7) axborotning konfidensialligi – axborotning ruxsatsiz shaxslarga taqdim etilmasligi yoki oshkor etilmasligini ta’minlovchi xususiyat;

8) mobil qurilmalar – Internet-planshetlar, elektron kitoblar, mobil telefonlar, noutbuklar, netbuklar kabi operatsion tizim va/yoki mobil ilovalarga ega bo‘lgan, mobil aloqa tarmoqlari, Wi-Fi va Internetga, shuningdek ishchi stansiyalar va boshqa o‘xshash qurilmalarga ulanish imkonini beruvchi qurilmalar.

9) axborotlashtirish obyekti – turli daraja va maqsadga ega axborot tizimlari, telekommunikatsiya tarmoqlari, axborotni qayta ishlashning texnik vositalari, ushbu vositalar o‘rnatilgan va ekspluatatsiya qilinadigan binolar, shuningdek muzokaralar o‘tkazish uchun mo‘ljallangan alohida xonalar (shu jumladan maxfiy xonalar);

10) shaxsga doir ma’lumotlar – fuqaroning shaxsini identifikatsiya qilish imkonini beruvchi uning hayotiga oid faktlar, voqealar va holatlar to‘g‘risidagi ma’lumotlar; 1 1) XDFU hujjatlari bilan ishlash qoidalari – axborotni saqlash, qidirish, tizimlashtirish, bog‘lash va qayta ishlash bo‘yicha, uni foydalanish uchun qulay shaklda taqdim etish maqsadida amalga oshiriladigan operatsiyalar majmui;

12) konfidensial axborotni oshkor etish – konfidensial axborot egasining roziligisiz, har qanday shaklda (og‘zaki, yozma yoki boshqa shaklda, shu jumladan texnik vositalardan foydalangan holda) uchinchi shaxslarga ma’lum bo‘lishiga olib kelgan harakat yoki harakatsizlik;

13) axborot tashuvchisi vositalar – axborotni mustaqil saqlash va yozilgan joyidan qat’i nazar foydalanish uchun mo‘ljallangan tashuvchi. Ular quyidagi ko‘rinishlarda bo‘lishi mumkin: magnit lentalar, olinadigan qattiq disklar, qattiq holatli disklar (SSD), flesh-xotira, optik lazer disklari (CD, DVD), disketalar;

14) uchinchi shaxs – amaldagi qonunchilikka muvofiq yuridik shaxs hisoblanmaydigan xorijiy korxonalar, shuningdek har qanday jismoniy yoki yuridik shaxs.

7) Ushbu hujjatda quyidagi qisqartmalar qo‘llaniladi:

RAM (Privileged Account Management) – imtiyozli foydalanuvchilarni boshqarish va nazorat qilish tizimi;

AKHV – axborotni kriptografik himoya qilish vositasi;

KBNT – kirishni boshqarish va nazorat qilish tizimi;

MBBT – ma’lumotlar bazasini boshqarish tizimi;

EHAT – elektron hujjat aylanishi tizimi.

3. Himoya qilinishi lozim bo‘lgan axborotni aniqlash tartibi

8. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi 295-sonli qaroriga muvofiq, Korxonada konfidensial axborot ro‘yxati shakllantirilishi lozim.

Shuningdek, O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025-yil 4-dekabrdagi 766-sonli qaroriga muvofiq, Korxonada “XDFU” toifasiga kiritilishi lozim bo‘lgan tarmoq (tizim osti) hujjatlar ro‘yxati shakllantirilishi shart.

9. Konfidensial axborotlar ro‘yxatini shakllantirish hamda “xizmatda foydalanish uchun” toifasiga kiritilishi lozim bo‘lgan tarmoq (ichki idoraviy) hujjatlar ro‘yxatini tuzish ishlari Korxona rahbariyati tomonidan tashkil etiladi.

10. Korxonaning qog‘oz va elektron shakldagi konfidensial axborot ro‘yxati (shu jumladan tijorat sirini tashkil etuvchi axborot, shaxsga doir ma’lumotlar va “XDFU” toifasidagi axborot) maxfiy axborotni tashkil etuvchi ma’lumotlar ro‘yxatini aniqlash bo‘yicha komissiya (keyingi o‘rinlarda – Komissiya) tomonidan belgilanadi.

Komissiya tarkibi Korxona buyrug‘i bilan esa tegishli buyruq bilan tasdiqlanadi.

11. Komissiyaning vazifalariga quyidagilar kiradi:

- korxona faoliyatining barcha yo‘nalishlarini tahlil qilish hamda ularning obyektlari va tarkibiy bo‘linmalarida foydalaniladigan axborotni inventarizatsiyadan o‘tkazish;

- inventarizatsiya natijalariga ko‘ra konfidensial axborot ro‘yxatini aniqlash;

- konfidensial axborot ro‘yxatini Korxona rahbariyatiga tasdiqlash uchun kiritish va uni kuchga kiritish;

- yiliga kamida bir marta konfidensial axborot ro‘yxatining dolzarbligini baholash hamda unga o‘zgartirish va qo‘shimchalar kiritish zarurati yuzasidan rahbariyatga takliflar kiritish.

12. Komissiya o‘z faoliyatida quyidagilarga amal qiladi:

- “Tijorat siri to‘g‘risida” va “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonunlarga;

- O‘zbekiston Respublikasi Vazirlar Mahkamasining 2011-yil 7-noyabrdagi 296-sonli qaroriga;

- O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi 295-sonli qaroriga;

- O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025-yil 4-dekabrdagi 766-sonli qaroriga;

- korxona to‘g‘risidagi Nizomga korxona ustaviga;

- boshqa amaldagi normativ-huquqiy hujjatlarga.

13. Konfidensial axborot ro‘yxati, shuningdek unga kiritiladigan o‘zgartirish va qo‘shimchalar Korxona buyrug‘i bilan kuchga kiritiladi hamda himoyalanadigan axborotni qayta ishlashga ruxsat etilgan xodimlarga o‘zlariga tegishli qismi bo‘yicha yetkaziladi.

14. Konfidensial axborot ro‘yxatida belgilangan har qanday shakl va ko‘rinishdagi himoyalanadigan axborot himoya qilinishi va oshkor etilmasligi lozim.

4. Himoyalanadigan axborotni himoya qilishning umumiy talablari

15. Korxonaning konfidensial axborot ro‘yxatiga kiritilgan himoyalanadigan axborot Korxona xodimlari bo‘lmagan uchinchi shaxslarga hech qanday shaklda oshkor etilmasligi hamda uchinchi shaxslar mulkiga aylanishi mumkin emas.

16. Himoyalanadigan axborot xodim tomonidan uchinchi shaxslarga faqat rahbariyat roziligi bilan yoki qonunchilikda belgilangan tartibda oshkor etilishi mumkin.

17. Himoyalanadigan axborot rahbariyat roziligisiz ushbu axborotga kirish huquqiga ega bo‘lmagan xodimlarga berilishi yoki oshkor qilinishi taqiqlanadi.

18. Himoyalanadigan axborotni internet tarmog‘ida, ochiq matbuotda, radio, televideniye hamda boshqa ommaviy axborot vositalarida tarqatish taqiqlanadi.

19. “XDFU” grifi qo‘yilgan axborot bundan mustasno holda, himoyalanadigan axborot Korxonaning axborot tizimlari, korporativ va lokal tarmoqlarida qayta ishlanishi mumkin.

20. Himoyalanadigan axborot Korxonaning nazorat qilinadigan zonasi tashqarisida aloqa kanallari orqali uzatilganda mazkur Tartibning 13-bo‘limida ko‘rsatilgan talablar bajarilishi lozim.

21. Rahbariyatning ruxsatisiz himoyalanadigan axborotni moddiy tashuvchilarda nazorat qilinadigan zona tashqarisiga olib chiqish taqiqlanadi.

22. Korxonada konfidensial axborotni himoya qilish ishlarini tashkil etish O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi 295-sonli qarori talablariga muvofiq amalga oshiriladi.

5. Xodimlar tomonidan konfidensiallikni ta’minlash

23. Korxona xodimi ish faoliyati davomida unga ma’lum bo‘lgan himoyalanadigan axborotni oshkor etmaslik majburiyatini o‘z zimmasiga oladi.

Mazkur talabni ta’minlash maqsadida har bir xodim bilan himoyalanadigan axborotni oshkor etmaslik to‘g‘risida kelishuv tuziladi. Ushbu kelishuvda xodimning majburiyatlari hamda himoyalanadigan axborotni oshkor etganlik uchun javobgarligi belgilanadi.

24. Xodim korxonada ishlash davrida konfidensial axborot ro‘yxatiga kiritilgan himoyalanadigan axborotni oshkor qilmasligi, shuningdek mehnat shartnomasi bekor qilingan sanadan boshlab kamida 5 (besh) yil davomida ushbu majburiyatga rioya etishi shart.

25. Korxona xodimlarining himoyalanadigan axborotni oshkor qilmaslik bo‘yicha majburiyatlari mehnat shartnomalari va kontraktlarda belgilanadi.

26. Korxonaning kadrlar bo‘linmasi xodimlarni himoyalanadigan axborotni oshkor qilganlik uchun javobgarlik to‘g‘risida xabardor qilishi hamda mehnat shartnomasi yoki kontraktning konfidensiallik shartlari bilan imzolashdan oldin tanishtirishi shart.

6. Kontragentlar tomonidan konfidensiallikni ta’minlash

27. Yuridik va jismoniy shaxslar (keyingi o‘rinlarda – kontragentlar) bilan ishlarni bajarish yoki xizmatlar ko‘rsatish bo‘yicha tuziladigan shartnomalarda (kontraktlarda) himoyalanadigan axborot sizib chiqishining oldini olish maqsadida maxfiylik shartlari nazarda tutilishi lozim.

28. Kontragentlar bilan tuziladigan shartnomalarda (kontraktlarda) konfidensiallik shartlari quyidagilarni o‘z ichiga olishi kerak:

- kontragent shartnoma (kontrakt) tuzish yoki uni bajarish natijasida unga ma’lum bo‘lgan yoki ma’lum bo‘ladigan har qanday axborot yoki ma’lumotlarning konfidensialligini saqlash majburiyatini oladi;
- kontragent shartnoma (kontrakt) amal qilish muddati davomida va u bekor qilingandan keyin kamida 5 yil davomida axborot konfidensialligini ta’minlashi shart.

29. Kontragentlar bilan tuzilgan shartnomalar (kontraktlar) doirasida beriladigan moliyaviy, iqtisodiy, ishlab chiqarish, texnik va boshqa turdagi har qanday axborotning konfidensialligini ta’minlanishi lozim.

30. Agar kontragent bilan tuzilgan shartnomada (kontraktda) konfidensial axborot almashinuvi nazarda tutilgan bo‘lsa, ushbu kontragent bilan qo‘shimcha ravishda konfidensiallik to‘g‘risidagi kelishuv (Non-disclosure agreement, NDA) tuzilishi lozim. Ushbu kelishuv shartnomaning ajralmas qismi hisoblanadi.

31. Konfidensiallik to‘g‘risidagi kelishuvda shartnoma tomonlarining himoyalanadigan axborotni oshkor etmaslik majburiyatlari hamda kontragentning aybi bilan axborot oshkor etilgan taqdirda uning javobgarligi belgilanadi.

32. Shartnomalar (kontraktlar) tuzishda ushbu bo‘lim talablari Korxona yuristlari tomonidan ta’minlanishi shart.

7. Himoyalangan axborotni himoya qilish talablari

33. Korxonada ilmiy-texnik, texnologik, ishlab chiqarish, moliyaviy-iqtisodiy hamda boshqa sohalarda ular uchun tijorat qiymatiga ega bo‘lgan Korxonaning, shuningdek mijozlar va kontragentlarning tijorat siri himoya qilinishi lozim.

34. Korxonaning himoyalanadigan shaxsga doir ma’lumotlari — bu ularning xodimlari, mijozlari yoki kontragentlariga tegishli bo‘lib, ularni identifikatsiya qilish imkonini beradigan ma’lumotlardir.

35. Korxonaning “XDFU” grifi bilan belgilangan himoyalanadigan axboroti “XDFU” toifasiga kiritilishi lozim bo‘lgan tarmoq (tizim osti ichki) hujjatlar ro‘yxatida belgilanadi. “XDFU” toifasiga kiruvchi hujjatlar tarkibiga shaxsga doir ma’lumotlar ham kiradi.

36. Tijorat sirini tashkil etuvchi himoyalanadigan axborot, shaxsga doir ma’lumotlar va “XDFU” grifi bilan belgilangan hujjatlar Korxonaning konfidensial axborot ro‘yxatiga kiritiladi hamda mazkur Tartib talablariga muvofiq himoya qilinadi.

37. Tijorat siri va shaxsga doir ma’lumotlar elektron yoki moddiy tashuvchida qayd etilishi mumkin. “XDFU” grifi bilan belgilangan hujjatlar moddiy tashuvchida rasmiylashtiriladi.

38. Tijorat sirini tashkil etuvchi axborot mavjud bo‘lgan moddiy tashuvchiga «tijorat siri» grifi qo‘yilishi mumkin. Shaxsga doir ma’lumotlarni o‘z ichiga olgan axborotning moddiy tashuvchisiga “XDFU” grifi qo‘yilishi shart.

39. “XDFU” grifi bilan belgilangan hujjatlar mazkur Tartibning 14-bo‘limi talablariga muvofiq hisobga olinishi va saqlanishi lozim.

40. Xodimlar va kontragentlar mazkur tartibning 4 va 5-bo‘limlari talablariga rioya etgan holda, Korxonaning tijorat siri hisoblangan axborotning konfidensialligini ta’minlashlari shart.

41. Tijorat siri hisoblangan axborot Korxona rahbariyatining roziligisiz uchinchi shaxslarga har qanday shaklda (og‘zaki, yozma yoki elektron ko‘rinishda) oshkor etilmasligi lozim.

Tijorat sirini o‘z ichiga olgan hujjatlar, shuningdek elektron ko‘rinishdagi tijorat siri hisoblangan axborot boshqa tarkibiy bo‘linmalar xodimlariga tanishish uchun faqat Korxona rahbariyatining ruxsati bilan yoki qonunchilikda belgilangan tartibda taqdim etilishi mumkin. Aks holda, mazkur axborotni ko‘rsatilgan shaxslarga taqdim etish tijorat sirini oshkor etish deb baholanadi.

42. Korxona xodimlarining shaxsga doir ma’lumotlarini qayta ishlash, tizimlashtirish, hisobga olish, saqlash va ularning xavfsizligini ta’minlash kadrlar boshqaruvi bo‘linmalari tomonidan amalga oshirilishi lozim.

43. Korxona xodimlari va mijozlarining shaxsga doir ma’lumotlariga ishlov berishni amalga oshiruvchi axborot tizimlari Korxonaning Axborot xavfsizligi siyosatidagi 1-jadvalda ko‘rsatilgan.

44. Korxonada shaxsga doir ma’lumotlarga ishlov berish O‘zbekiston Respublikasining "Shaxsga doir ma’lumotlar to‘g‘risida"gi Qonuni, O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 5-oktabrdagi 570-son qarori hamda Shaxsga doir ma’lumotlarga ishlov berishning namunaviy tartibi (O‘zbekiston Respublikasi Adliya vazirligida 2023-yil 15-noyabrda 3478-son bilan ro‘yxatga olingan) talablariga muvofiq amalga oshirilishi lozim.

45. Shaxsga doir ma’lumotlarga ishlov berish, jumladan ularni tarqatish va uzatish subyektning yoki uning qonuniy vakilining roziligi asosida amalga oshiriladi.

Korxona xodimlari, kontragentlari (jismoniy shaxslar) va mijozlarining shaxsga doir ma’lumotlariga ishlov berish ulardan rozilik olingandan so‘ng amalga oshiriladi.

Mazkur rozilik xodim bilan tuziladigan mehnat shartnomasida, kontragent bilan tuziladigan kontraktda hamda mijoz bilan tuziladigan xizmat ko‘rsatish shartnomasida aks ettiriladi.

46. Korxona shaxsga doir ma’lumotlarni qayta ishlash jarayonida ruxsatsiz, shu jumladan tasodifiy kirish, yo‘q qilish, o‘zgartirish, bloklash, nusxa ko‘chirish, uchinchi shaxslarga ruxsatsiz taqdim etish, ruxsatsiz tarqatish va boshqa noqonuniy harakatlardan himoya qilish maqsadida huquqiy, tashkiliy va texnik choralarni ko‘rishi shart.

Shaxsga doir ma’lumotlarni himoya qilish bo‘yicha quyidagi choralar qo‘llaniladi:

1) subyektning shaxsiy hayotiga aralashuvdan himoyalanish huquqini ta’minlash;

2) shaxsga doir ma’lumotlarning yaxlitligi va saqlanishini ta’minlash;

3) shaxsga doir ma’lumotlarning konfidensialligini ta’minlash;

4) shaxsga doir ma’lumotlarga noqonuniy ishlov berilishining oldini olish;

5) shaxsga doir ma’lumotlarni ommaga ochiq va ommaga ochiq bo‘lmagan axborotga ajratish;

6) shaxsga doir ma’lumotlarga ishlov berish va ulardan foydalanish tartibini belgilash;

7) shaxsga doir ma’lumotlarga ishlov berish yoki ularga kirish huquqiga ega bo‘lgan shaxslarni aniqlash;

8) har kim foydalana olmaydigan axborotni himoya qilish vositalarini o‘rnatish hamda shaxsga doir ma’lumotlarga ishlov beruvchi texnik vositalarning dasturiy ta’minotini muntazam yangilab borishni ta’minlash;

9) ma’lumotlar bazasini boshqarish tizimlari hodisalari jurnalini yuritish;

10) har kim foydalana olmaydigan shaxsga doir ma’lumotlarga kirish huquqiga ega foydalanuvchilarning harakatlarini qayd etishni ta’minlash;

11) har kim foydalana olmaydigan shaxsga doir ma’lumotlarning yaxlitligini nazorat qilish vositalaridan foydalanish;

12) qonunchilikda nazarda tutilgan hollar bundan mustasno, subyektning roziligi bilan shaxsga doir ma’lumotlarni boshqa shaxslarga himoyalangan aloqa kanallari va (yoki) shifrlash vositalari orqali taqdim etish;

13) har kimga ochiq bo‘lmagan shaxsga doir ma’lumotlar bilan ishlashda xodimlarni identifikatsiya va (yoki) autentifikatsiya qilish vositalaridan foydalanish;

14) Korxonaning shaxsga doir ma’lumotlarga ishlov berish va ularni himoya qilish siyosatini belgilovchi ichki hujjatlarni tasdiqlash;

15) shaxsga doir ma’lumotlar subyektining so‘rovi asosida shaxsga doir ma’lumotlarni bloklash va yo‘q qilish tartibini belgilash.

47. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2020-yil 8-fevraldagi 71-son qaroriga muvofiq, Korxonaning shaxsga doir ma’lumotlarga ishlov berishni amalga oshiruvchi axborot tizimlari ma’lumotlar bazalari shaxsga doir ma’lumotlar bazalarining davlat reyestriga kiritilishi lozim.

Shaxsga doir ma’lumotlar bazalarini himoya qilish uchun quyidagi shaxsga doir ma’lumotlarni himoya qilish talablari bajarilishi shart:

1) Korxonaning shaxsga doir ma’lumotlar bazalari joylashgan server xonalarida xavfsizlik rejimini tashkil etish, ularga kirish huquqiga ega bo‘lmagan shaxslarning ruxsatsiz kirishi yoki bo‘lishining oldini olish;

2) shaxsga doir ma’lumotlarni o‘z ichiga olgan moddiy obyektlarning saqlanishini ta’minlash;

3) shaxsga doir ma’lumotlarga ishlov berish bazalariga kirish huquqiga ega bo‘lgan shaxslar ro‘yxatini, shuningdek ularning mazkur ishlov berish bo‘yicha majburiyatlarini belgilash;

4) axborot xavfsizligi sohasidagi talablarga muvofiqligi baholash jarayonidan o‘tgan axborot xavfsizligi vositalaridan foydalangan holda shaxsga doir ma’lumotlarni mavjud tahdidlardan himoya qilish;

5) ma’lumotlar bazasidagi shaxsga doir ma’lumotlar xavfsizligini ta’minlash uchun mas’ul bo‘lgan mansabdor shaxsni (xodimni) tayinlash.

Korxonada shaxsga doir ma’lumotlar bazalarining xavfsizligini ta’minlash uchun mas’ul xodim sifatida KABT boshqarmasi mutaxassisi (axborot tizimlari administrator) tayinlanadi.

48. Tijorat siri, shaxsga doir ma’lumotlar hamda “XDFU” grifi bilan belgilangan moddiy tashuvchidagi hujjatlar Korxonaning tarkibiy bo‘linmalarida seyflarda yoki qulflanadigan shkaflarda saqlanishi lozim, ularga faqat mazkur axborotdan foydalanishga ruxsat etilgan xodimlargina kirish huquqiga ega bo‘lishi kerak.

Mazkur hujjatlarning konfidensialligini ta’minlash uchun tarkibiy bo‘linmalar rahbarlari hamda ushbu axborotga ruxsat etilgan xodimlar javobgar hisoblanadi.

49. Tijorat siri, shaxsga doir ma’lumotlar va “XDFU” grifi bilan belgilangan elektron ko‘rinishdagi axborotga kirish ham cheklangan bo‘lishi lozim.

Tijorat siri mavjud bo‘lgan axborotni oxirgi qurilmalarda (end-point qurilmalar) va raqamli tashuvchilarda saqlash, shuningdek uni aloqa kanallari orqali uzatish mazkur Tartibning 11, 12 va 13-bo‘limlari talablariga muvofiq amalga oshirilishi shart.

8. Xodimlarni himoyalanadigan axborotga ruxsat berish tartibi

50. Korxonaning himoyalanadigan axborotiga ishlov berish, uni saqlash va unga kirish faqat ushbu himoyalanadigan axborotdan foydalanishga ruxsat berilgan xodimlar tomonidan amalga oshirilishi lozim.

51. Korxonaning himoyalanadigan axborotiga ruxsat etilgan xodimlar ro‘yxati ularning rahbariyati tomonidan belgilanadi va mazkur xodimlar Korxonaning konfidensial axborot ro‘yxatida himoyalanadigan axborotning har bir turi qarshisida ko‘rsatilishi shart.

52. Konfidensial axborotlar ro‘yxatida ko‘rsatilmagan hamda unga ruxsat etilmagan Korxonaning boshqa xodimlarining himoyalanadigan axborot bilan tanishishiga va undan foydalanishiga faqat Korxona rahbariyatining ruxsati bilan yo‘l qo‘yiladi.

53. Himoyalanadigan axborot qayta ishlanadigan xonalar, moddiy tashuvchida saqlanadigan himoyalanadigan axborot joylashgan seyflar va qulflanadigan shkaflar, shuningdek elektron ko‘rinishda himoyalanadigan axborot saqlanadigan va unga ishlov beriladigan oxirgi qurilmalar hamda axborot tizimlariga kirish faqat ushbu himoyalanadigan axborotdan foydalanishga ruxsat etilgan xodimlar tomonidan amalga oshiriladi.

9. Himoyalanadigan axborotga ishlov beriladigan xonalarga qo‘yiladigan talablar

54. Korxonada himoyalanadigan axborotga ishlov beriladigan va saqlanadigan xonalar ro‘yxati hujjat bilan belgilanadi (bundan buyon — himoyalanadigan xonalar).

55. Himoyalanadigan xonalarga xizmat xonalari va server xonalari kiradi.

56. Begona shaxslarning himoyalanadigan xonalarga ruxsatsiz kirishiga yo‘l qo‘yilmaydi.

Begona shaxsning himoyalanadigan xonada bo‘lishiga faqat Korxona xodimi kuzatuvi ostida ruxsat etiladi.

57. Himoyalanadigan xonalarga nisbatan begona shaxslarning nazoratsiz kirishini hamda ularda qayta ishlanadigan va saqlanadigan himoyalanadigan axborotga ruxsatsiz kirishni istisno etuvchi quyidagi choralar ko‘rilishi lozim:

- himoyalanadigan xonalarning eshiklari tadbirlar oralig‘ida va ish vaqtidan tashqari paytda elektron yoki mexanik qulflar bilan yopilishi hamda (yoki) elektron kodli qulflar yoki kirishni nazorat qilish va boshqarish tizimlari (KNB tizimi) qo‘llanilishi lozim;
- himoyalanadigan xonalarda qo‘riqlash signalizatsiyasi datchiklari, jumladan, bostirib kirishni aniqlash datchiklari o‘rnatilishi va ular ish vaqtidan tashqari yoqilgan holatda bo‘lishi kerak;
- yo‘laklarda videokuzatuv kameralari o‘rnatilishi lozim bo‘lib, ularning ko‘rish maydoni himoyalanadigan xonalar kirish qismini qamrab olishi kerak; yuqori darajadagi xavfsizlik talab etiladigan xonalarda videokameralar xona ichiga ham o‘rnatilishi mumkin;
- derazalar orqali matnli va grafik himoyalanadigan axborotni ko‘rish imkoniyatini istisno qilish uchun himoyalanadigan xonalar tegishli vositalar (jalyuzi yoki pardalar) bilan jihozlanishi lozim;
- himoyalanadigan xonalar yong‘in va qo‘riqlash signalizatsiyasi tizimlari faqat simli axborot yig‘ish (aloqa pulti bilan bog‘lanish) sxemasi bo‘yicha qurilishi hamda himoyalanadigan xonalar bilan bir nazorat qilinadigan zonada joylashtirilishi kerak;
- himoyalanadigan xonalarda himoyalanadigan axborot moddiy tashuvchilarda seyflarda yoki qulflanadigan shkaflarda saqlanishi lozim.

“XDFU” grifi bilan belgilangan hujjatlar bilan ishlash, ularni ro‘yxatga olish, ko‘paytirish (nusxalash), hisobga olish, saqlash va yo‘q qilish ishlari olib boriladigan xizmat xonalari hujjat yo‘qolishi, oshkor etilishi yoki begona shaxslar nazoratisiz kirishining oldini oluvchi vositalar bilan jihozlangan bo‘lishi lozim.

58. Himoyalanadigan xonalarda uskunalarni o‘rnatish, ta’mirlash va almashtirish, shuningdek mebellarni joylashtirish va ta’mirlash ishlari Korxona rahbariyati bilan kelishilgan holda, server xonalarida esa Korxonaning KABT boshqarmasi xodimi nazorati ostida amalga oshiriladi.

59. Ushbu tartibning ushbu bo‘limida ko‘rsatilgan himoyalanadigan xonalarni ruxsatsiz kirishdan himoya qilish va xavfsizlik talablarini tashkil etish hamda ta’minlash bo‘yicha javobgarlik Korxonaning kuzatuv nazorati bo‘limi zimmasiga yuklanadi.

10. Himoyalangan ma’lumotlar qayta ishlanadigan axborot texnologiyalari obyektlariga qo‘yiladigan talablar

60. Korxonaning himoyalangan ma’lumotlarni qayta ishlaydigan va saqlaydigan axborot tizimlari va resurslari Korxonaning Axborot aktivlari reestrida keltirilgan bo‘lib, u Korxonaning Axborot xavfsizligi siyosatining 7-ilovasida keltirilgan.

61. Korxonaning himoyalangan ma’lumotlarni qayta ishlaydigan va saqlaydigan axborot tizimlarining serverlari va ma’lumotlar bazasi omborlari server xonasida joylashgan bo‘lib, unga ruxsatsiz shaxslar kirishi cheklangan.

62. Axborot tizimlarida himoyalangan ma’lumotlarni himoya qilish uchun quyidagi chora-tadbirlar majmuini ta’minlaydigan axborot xavfsizligi tizimi joriy etilishi kerak:

- Korxonaning Axborot xavfsizligi siyosatining 9-ilovasida keltirilgan Kirish boshqaruvi, autentifikatsiya va parolni himoya qilish bo‘yicha yo‘riqnomalarga muvofiq foydalanuvchilarning axborot tizimlariga kirishini cheklash;
- Korxonaning Axborot xavfsizligi siyosatining 2-ilovasida keltirilgan Tarmoq infratuzilmasi darajasida axborot xavfsizligini ta’minlash va tarmoqlararo ekran to‘g‘risidagi Nizomga muvofiq xavfsizlik devorlari, buzg‘unchiliklarni aniqlash va oldini olish tizimlari (IDPS) yordamida ruxsatsiz tarmoqqa kirish, tarmoqqa kirish va hujumlardan himoya qilish;
- Korxonaning Axborot xavfsizligi siyosatining 11-ilovasida keltirilgan Antivirus himoyasi bo‘yicha yo‘riqnomalarga muvofiq zararli dasturlardan himoya qilish;
- foydalanuvchilar va imtiyozli foydalanuvchilarning (administratorlarning) masofaviy ulanishlari uchun himoyalangan ulanishlarni tashkil qilish;
- ma’lumotlar bazasi serverlarining zaxira nusxasi va/yoki axborot tizimi ma’lumotlarining zaxira nusxasi.

63. Profilaktik va ta'mirlash ishlarini bajarish, zaxira nusxasini yaratish va arxivlash, konfiguratsiya qilish va kirishni boshqarish maqsadida axborot tizimining server uskunasiga jismoniy va masofaviy kirish Korxona ayrim xodimlariga (bundan keyin administratorlar deb yuritiladi) beriladi.

64. Axborot tizimi server uskunasiga administratorning masofaviy kirishi faqat administratorga ma’lum bo‘lishi va ruxsatsiz shaxslarga oshkor qilinmasligi kerak bo‘lgan parol yordamida ta’minlanadi. Administrator paroli va uni o‘zgartirishga qo‘yiladigan talablar Korxonaning Axborot xavfsizligi siyosatining 9-ilovasida keltirilgan Kirish boshqaruvi, autentifikatsiya va parolni himoya qilish bo‘yicha ko‘rsatmalarda belgilangan.

65. Axborot tizimlarida himoyalangan ma’lumotlarning himoyasini ta’minlash uchun administrator quyidagilarga majburdir:

- axborot tizimi ma’lumotlar bazasida saqlangan ma’lumotlarni uchinchi shaxslarga tarqatmaslik;
- zaxiralash va arxivlash choralari bilan ko‘zda tutilmagan bo‘lsa, axborot tizimi ma’lumotlar bazasida saqlangan ma’lumotlarning nusxalarini yaratmaslik;
- axborot tizimi ma’lumotlar bazasida saqlangan ma’lumotlarning nusxalarini zaxira ma’lumotlari va elektron arxivlarni saqlash uchun mo‘ljallanmagan joylarda saqlamaslik.

66. Axborot tizimlari uchun zaxira ma’lumotlari xavfsiz joylarda saqlanishi kerak.

67. Axborot tizimi ma’lumotlar bazalariga kirishda administratorning harakatlarini kuzatish va qayd etish uchun MBBT, shuningdek, operativ xotira tizimidan foydalanish kerak. Buxgalteriya hisobi jurnalidagi ma’lumotlar kamida bir yil davomida saqlanishi kerak.

68. Administrator ishdan bo‘shatilgandan so‘ng, uning kirish parollarini va axborot tizimi foydalanuvchilarining kirish parollarini tezda o‘zgartirish choralari ko‘riladi.

69. Axborot tizimlarida axborotni qayta ishlashning texnologik jarayonida, shu jumladan nusxalar va arxiv ma’lumotlarini saqlash uchun ishlatiladigan barcha raqamli saqlash vositalari hisobga olinishi kerak. Ushbu hisobga olish Korxonaning KABT boshqarmasi tomonidan amalga oshiriladi.

Ruxsatsiz shaxslarning bunday vositalarga kirishi cheklanishi kerak.

11. Himoyalangan ma’lumotlarni oxirgi qurilmalarda saqlash va qayta ishlash talablari

70. Korxonaning konfidensial ma’lumotlari ro‘yxatiga kiritilgan himoyalangan ma’lumotlar, “XDFU” deb belgilangan ma’lumotlardan tashqari, elektron shaklda oxirgi qurilmalarda saqlanishi mumkin.

Ushbu oxirgi qurilmalar himoyalangan binolarda joylashgan bo‘lishi kerak.

71. Himoyalangan ma’lumotlarga elektron shaklda kirish huquqiga ega xodimlar uni oxirgi qurilmalarda qayta ishlash va saqlashga ruxsatga ega.

72. Himoyalangan ma’lumotlar elektron shaklda quyidagilarda saqlanishi mumkin emas:

- oxirgi qurilmalardagi ommaga ochiq tarmoq papkalari;
- xodimga tegishli har qanday mobil qurilmalar;
- xodimga tegishli hisob bermaydigan olinadigan raqamli saqlash qurilmalari;
- bulutli xizmatlar (saqlash).

73. Himoyalangan ma’lumotlarni, xususan, tijorat siri yoki shaxsga doir ma’lumotlarni tashkil etuvchi ma’lumotlarni saqlaydigan oxirgi qurilmalarga quyidagi talablar qo‘yilishi kerak:

- oxirgi qurilmalarga kirish parol bilan himoyalangan bo‘lishi kerak, parolni o‘zgartirish oralig‘i va murakkabligi Korxonaning Axborot xavfsizligi siyosatining 9-ilovasida keltirilgan Kirish boshqaruvi, autentifikatsiya va parolni himoya qilish bo‘yicha yo‘riqnomalar talablariga javob berishi kerak;
- foydalanuvchi 5 daqiqa davomida faol bo‘lmagan taqdirda, oxirgi qurilmalar ekranni avtomatik ravishda qulflash uchun sozlangan bo‘lishi kerak va kirish paroli yordamida qulfni ochish amalga oshirilishi kerak;
- oxirgi qurilmalarga kirish paroli faqat oxirgi qurilma xodimiga ma’lum bo‘lishi kerak;
- oxirgi qurilmalarga antivirus himoyasi o‘rnatilgan bo‘lishi kerak;
- raqamli tashuvchi qurilma, Bluetooth va boshqa oqish kanallarini ulash uchun portlar oxirgi qurilmalarda bloklangan bo‘lishi kerak;
- oxirgi qurilmalarga DLP oqishining oldini olish tizimi o‘rnatilgan bo‘lishi kerak;
- Himoyalangan ma’lumotlarni ish stollarida va oxirgi qurilmalarning ommaga ochiq papkalarida elektron shaklda saqlash taqiqlangan;
- Oxirgi qurilmalar Korxona ichida foydalanish uchun tasdiqlangan standart dasturiy ta’minot to‘plami bilan jihozlangan bo‘lishi kerak.

74. Himoyalangan ma’lumotlarni saqlaydigan oxirgi qurilmalarning apparat yoki dasturiy ta’minot konfiguratsiyasidagi har qanday o‘zgarishlar Korxonaning KABT boshqarmasi tomonidan tasdiqlanishi va amalga oshirilishi kerak.

75. “XDFU”deb belgilangan oxirgi qurilmalarda tayyorlangan himoyalangan ma’lumotlar chop etish va qayta ishlashdan (ma’lumotlarni imzolash va o‘rnatish) keyin yo‘q qilinishi kerak. “XDFU” deb belgilangan ma’lumotlarni elektron shaklda oxirgi qurilmalarda saqlash taqiqlanadi.

76. Oxirgi qurilmadagi har qanday himoyalangan ma’lumotlarni, shu jumladan “XDFU”ni qayta ishlashda xodimlar uchinchi shaxslarning monitor ekranlaridan matnli va grafik himoyalangan ma’lumotlarni ko‘rishiga yo‘l qo‘ymaslik choralarini ko‘rishlari shart.

77. Agar uchinchi tomon korxonalari tomonidan himoyalangan ma’lumotlarni saqlaydigan oxirgi qurilmalarni ta'mirlash talab qilinsa, ta'mirlash boshlanishidan oldin ma’lumotlarni saqlash qurilmasi olib tashlanishi kerak. Agar ma’lumotlarni saqlash qurilmasini olib tashlashning iloji bo‘lmasa, undagi himoyalangan ma’lumotlar o‘chirilishi kerak.

78. Himoyalangan ma’lumotlarni elektron shaklda qayta ishlaydigan, saqlaydigan va uzatadigan xodimlar quyidagi talablarga rioya qilishlari kerak:

- o‘z hisob qaydnomasi parolini hech kimga oshkor qilmaslik;

- Korxonaning KABT boshqarmasining roziligisiz oxirgi qurilmalarning apparat konfiguratsiyasi va dasturiy ta’minot sozlamalarini o‘zboshimchalik bilan o‘zgartirish taqiqlanadi;

- “XDFU” deb belgilangan elektron shakldagi himoyalangan ma’lumotlarni yoki endi kerak bo‘lmagan boshqa himoyalangan ma’lumotlarni aniqlash va yo‘q qilish uchun ish stoli papkalarini haftalik ko‘rib chiqish;

- ishdan bo‘shatilgandan so‘ng, tarkibiy bo‘linma rahbariga himoyalangan ma’lumotlarning oxirgi qurilmada joylashganligi haqida xabar berish va unga himoyalangan ma’lumotlarni o‘z ichiga olgan barcha raqamli tashuvchilarni o‘tkazish.

12. Himoyalangan ma’lumotlarni raqamli tashuvchilarda saqlash talablari

79. Korxonaning himoyalangan ma’lumotlarini saqlash uchun tashrif buyuruvchilarga yoki xodimlarga tegishli raqamli tashuvchi vositalardan foydalanishni taqiqlaydi.

80. Himoyalangan ma’lumotlarni saqlashga quyidagilarga ruxsat beriladi:

- Korxonaning hisobga olingan raqamli tashuvchi vositalarida;

- Himoyalangan ma’lumotlar qayta ishlanadigan axborot tizimlarining oxirgi qurilmalari va serverlarining raqamli saqlash qurilmalarida.

81. Ko‘chma raqamli axborot tashuvchilar va ma’lumot saqlovchi qurilmalarni hisobga olish Korxona axborot xavfsizligi siyosatiga 13-ilovada keltirilgan “Axborot tashuvchi ko‘chma vositalar va ma’lumot saqlovchi qurilmalar bilan ishlashda xavfsizlikni ta’minlash bo‘yicha Yo‘riqnoma”ga muvofiq amalga oshiriladi.

82. Himoya qilinadigan axborotga ega hisobga olingan ko‘chma tashuvchilar seyflarda yoki qulflanadigan temir shkaflarda saqlanishi lozim.

83. Himoyalangan ma’lumotlarni o‘z ichiga olgan raqamli tashuvchi vositalar va saqlash qurilmalarini binolaridan Korxona rahbariyatining ruxsatisiz olib chiqish taqiqlanadi.

“XDFU” belgisi qo‘yilgan himoyalangan ma’lumotlarni Korxonadan tashqariga o‘tkazishga faqat O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025-yil 4-dekabrdagi 766-sonli qaroriga muvofiq axborot xavfsizligi talablariga muvofiqligi baholangan moddiy vositalar yordamida ruxsat etiladi.

Himoyalangan ma’lumotlarni o‘z ichiga olgan raqamli tashuvchi vositalar va saqlash moslamalarini Korxonadan tashqariga olib chiqish Korxonaning Axborot xavfsizligi siyosatining 13-ilovasida keltirilgan talablarga muvofiq amalga oshirilishi kerak.

84. Yakuniy qurilma yoki serverni, hisobga olingan ko‘chma axborot tashuvchini hisobdan chiqarish to‘g‘risida qaror qabul qilinganda, shuningdek ularni boshqa maqsadlarda foydalanish bo‘yicha qaror qabul qilinganda, ularning tashuvchilarida saqlanayotgan himoya qilinadigan axborot o‘chirilishi lozim. Bunda axborotni qayta tiklash imkoniyatini istisno etuvchi usullar qo‘llanilishi kerak hamda ular Korxona axborot xavfsizligi siyosatiga 13-ilovada keltirilgan “Axborot tashuvchi ko‘chma vositalar va ma’lumot saqlovchi qurilmalar bilan ishlashda xavfsizlikni ta’minlash bo‘yicha Yo‘riqnoma”da belgilangan talablarga muvofiq bo‘lishi lozim.

85. Ishdan chiqqan va yo‘q qilish uchun mo‘ljallangan, himoya qilinadigan axborotni o‘z ichiga olgan raqamli axborot tashuvchilar ushbu Yo‘riqnoma talablariga muvofiq, ulardan qoldiq axborotni o‘qib olish imkonini bermaydigan tarzda jismoniy yo‘q qilinishi lozim (Korxona axborot xavfsizligi siyosatiga 13-ilovada keltirilgan “Axborot tashuvchi ko‘chma vositalar va ma’lumot saqlovchi qurilmalar bilan ishlashda xavfsizlikni ta’minlash bo‘yicha Yo‘riqnoma”ga muvofiq).

13. Himoyalangan ma’lumotlarni aloqa kanallari orqali uzatish talablari

86. Himoyalangan ma’lumotlar, “XDFU” deb belgilangan himoyalangan ma’lumotlardan tashqari, aloqa kanallari orqali AKHVdan foydalanmasdan, Korxonaning lokal tarmog‘i orqali axborot almashish tizimlari (korporativ elektron pochta, korporativ messenjer, elektron hujjat aylanish tizimi va boshqalar) yordamida uzatilishi mumkin.

87. “XDFU” deb belgilangan himoyalangan ma’lumotlarni Korxonaning lokal tarmog`i yoki aloqa kanallari, tashqi tarmoq yoki elektron pochta orqali “XDFU” deb belgilangan elektron shaklda uzatish taqiqlanadi.

88. Aloqa kanallari orqali “XDFU” belgisi qo‘yilgan hujjatlar almashinuviga faqat AKHVdan foydalanadigan va O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025-yil 4-dekabrdagi 766-sonli qaroriga muvofiq axborot xavfsizligi talablariga muvofiqligi baholangan himoyalangan elektron hujjat aylanishi tizimidan foydalanish orqali ruxsat beriladi.

89. Korxonaning himoyalangan ma’lumotlarini, jumladan, “XDFU” belgisi qo‘yilgan ma’lumotlarni AKHVdan foydalanmasdan quyidagi tashqi aloqa kanallari orqali uzatish taqiqlanadi:

- elektron pochta va internet, shu jumladan internet pochta xizmatlari (mail.ru, yandex.ru va boshqalar) va ijtimoiy tarmoqlar orqali;
- tashqi tezkor xabar almashish tizimlari (messenjerlar) orqali;
- tashqi himoyalanmagan elektron pochta tizimlari va elektron hujjat aylanishi tizimlari.

90. Korxonaning tijorat siri bo‘lgan himoyalangan ma’lumotlar Korxonaning KABT boshqarmasi tomonidan belgilangan AKHVdan foydalangan holda tashqi kanallar orqali uzatilishi mumkin. AKHVdan foydalanmasdan, tijorat sirlarini yuborish faqat Korxona rahbariyatining ruxsati bilan, yuborish usuli bo‘yicha kelishilganidan so‘ng, masalan, elektron pochta orqali va hokazolarga yo‘l qo‘yiladi.

91. Uchinchi tomon korxonasi (kontragent) bilan ular bilan tuzilgan shartnomalar (shartnomalar) bo‘yicha tijorat siri bo‘lgan himoyalangan ma’lumotlarni almashishda ushbu ma’lumotlarni o‘tkazish usuli shartnomada (shartnomada) ko‘rsatilishi va himoyalangan bo‘lishi kerak.

92. Himoyalangan ma’lumotlarni shifrlash uchun ishlatiladigan kriptografik axborotni himoya qilish vositalari belgilangan tartibda sertifikatlangan bo‘lishi kerak.

14. Himoyalangan ma’lumotlarni hisobga olish, qayta ishlash va saqlash

93. Tijorat siri yoki shaxsga doir ma’lumotlarni tashkil etuvchi himoyalangan ma’lumotlar ushbu himoyalangan ma’lumotlarni qayta ishlashga vakolatli xodimlarga berilgan tarkibiy bo‘linmalar tomonidan qayd etiladi va saqlanadi.

94. “XDFU” belgisi qo‘yilgan hujjatlar bilan ishlash O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025-yil 4-dekabrdagi 766-sonli qarori bilan tasdiqlangan “Faqat rasmiy foydalanish uchun hujjatlar bilan ishlash qoidalari”ga muvofiq amalga oshiriladi.

95. Korxonada “XDFU” belgisi qo‘yilgan hujjatlar bilan ishlash uchun tarkibiy bo‘linmalar rahbarlari, ofis xodimlari va rasmiy foydalanish uchun hujjatlar bilan ishlashga vakolatli rahbar shaxslar javobgardir.

95. “XDFU” belgisi qo‘yilgan hujjatlarni qabul qilish, qayd etish va saqlash Korxona tomonidan amalga oshiriladi.

96. “XDFU” hujjatlar bilan ishlashga vakolatli Korxona xodimlariga ushbu hujjatlardagi ma’lumotlarni rasmiy zarurat talab qilmasa, og‘zaki yoki yozma ravishda hech kimga yetkazish taqiqlanadi.

97. Himoyalangan ma’lumotlar bilan ishlashga jalb qilingan Korxona xodimlari ushbu Tartib bilan tanishib chiqishlari shart, “XDFU” hujjatlar bilan ishlashga vakolatli xodimlar esa qo‘shimcha ravishda O‘zbekiston Respublikasi Vazirlar Mahkamasining 2025-yil 4-dekabrdagi 766-sonli qarori bilan tasdiqlangan Faqat rasmiy foydalanish uchun hujjatlar

bilan ishlash qoidalari bilan tanishib chiqishlari shart.

15. Himoyalangan ma’lumotlarni himoya qilish talablariga rioya qilinishini monitoring qilish

98. Ushbu Tartibda belgilangan himoyalangan axborotni himoya qilish talablariga rioya qilinishini monitoring qilish himoyalangan axborotning haqiqiy xavfsizligi holatini o‘rganish va baholash hamda ushbu Tartib talablarining kamchiliklari va buzilishini aniqlash maqsadida amalga oshiriladi.

99. Korxonaning tarkibiy bo‘linmalari rahbarlari o‘zlariga bevosita bo‘ysunadigan xodimlar tomonidan himoyalangan axborotni himoya qilish talablariga rioya qilinishini doimiy ravishda kuzatib borishlari shart.

100. Korxonaning KABT boshqarmasi himoyalangan axborotni himoya qilish talablariga rioya qilinishini rejali yoki rejadan tashqari tekshirishlarni amalga oshiradilar.

101. Himoyalangan axborotni himoya qilish talablariga rioya qilinishini rejali tekshirishlar yiliga kamida bir marta o‘tkaziladi.

Rejadan tashqari tekshirishlar Korxona rahbariyati tomonidan boshlanadi va/yoki himoyalangan axborotning konfidensialligi yoki xavfsizligini buzish holatlarini tekshirish doirasida o‘tkaziladi.

102. Rejalashtirilgan va rejadan tashqari tekshirishlar doirasida quyidagilar tekshiriladi:

- himoyalangan ma’lumotlarni elektron va moddiy vositalarda saqlash va uzatish talablariga rioya qilish;
- himoyalangan ma’lumotlarni to‘g‘ri saqlash va ulardan foydalanish;
- “XDFU” belgisi qo‘yilgan hujjatlarni saqlash va ular bilan ishlash talablariga rioya qilish;
- himoyalangan ma’lumotlarga oid xodim bilan oshkor qilmaslik to‘g‘risidagi shartnomaning mavjudligi;
- kontragentlar bilan tuzilgan shartnomalarga konfidensiallik bandlarini kiritish;
- konfidensiallik yorliqlarini to‘g‘ri belgilash;
- xodimlarning ushbu Tartib talablaridan xabardorligi va boshqalar.

103. Inspektorlar obyektda va tarkibiy bo‘linmada ishlatiladigan barcha hujjatlarni ko‘rib chiqish, oxirgi qurilmalarni tekshirish, shuningdek, xodimlar bilan suhbatlar va maslahatlashuvlar o‘tkazish, tekshirish mavzusiga oid masalalar bo‘yicha yozma tushuntirishlar, sertifikatlar va hisobotlarni so‘rash huquqiga ega.

104. Tekshiruv natijalariga ko‘ra, himoyalangan ma’lumotlarni himoya qilish holati, aniqlangan kamchiliklar va qoidabuzarliklar hamda ularni bartaraf etish bo‘yicha takliflarni aks ettiruvchi hisobot tuziladi.

105. Korxonaning tarkibiy bo‘linmalari rahbarlari himoyalangan ma’lumotlarni himoya qilishda aniqlangan har qanday kamchiliklar va qoidabuzarliklarni, shuningdek, ularning yuzaga kelishiga sabab bo‘lgan sabablar va shart-sharoitlarni hisobotda ko‘rsatilgan muddatlarda bartaraf etishlari shart.

106. Himoyalangan ma’lumotlarning sizib chiqishi yoki oshkor bo‘lishi holatida, ushbu voqea sodir bo‘lgan Korxonaning tarkibiy bo‘linmasi rahbari darhol Korxona rahbariyatiga xabar berishi shart.

107. Himoyalangan ma’lumotlarning sizib chiqishi yoki oshkor bo‘lishi holatida Korxona rahbariyati ichki tekshiruvni boshlashi mumkin. Ichki tekshiruv natijalariga ko‘ra, rahbariyat aybdor shaxslarni javobgarlikka tortish va bunday qoidabuzarliklarning takrorlanishining oldini olish choralarini ko‘rish to‘g‘risida tegishli qaror qabul qiladi.

16. Himoyalangan ma’lumotlarning konfidensialligini saqlash majburiyatlari

108. Korxona xodimlari quyidagilarga majburdirlar:

- ish paytida va mehnat shartnomasi bekor qilingan kundan boshlab 5 (besh) yil davomida himoyalangan ma’lumotlarni oshkor qilmaslik va himoyalangan ma’lumotlarni uchinchi shaxslar tomonidan buzilishdan yoki ularni o‘tkazish yoki oshkor qilishga urinishlardan himoya qilish;

- ish paytida o‘rganilgan himoyalangan ma’lumotlardan faqat Korxona manfaatlari yo‘lida foydalanish;

- himoyalangan ma’lumotlardan shaxsiy maqsadlarda, shu jumladan boshqa korxonada ishlayotganda yoki yakka tartibdagi tadbirkor sifatida tadbirkorlik faoliyatini amalga oshirayotganda, ilmiy yoki pedagogik faoliyatda yoki omma oldida nutq so‘zlash yoki intervyular paytida foydalanmaslik;

- o‘zlari vakolat bermagan himoyalangan ma’lumotlarga kirish huquqiga ega bo‘lmaslik;

- uchinchi shaxslar, shuningdek, himoyalangan ma’lumotlarga kirish huquqiga ega bo‘lmagan Korxona xodimlari tomonidan Korxonaning har qanday himoyalangan ma’lumotlariga kirishni cheklash;

- ushbu Tartibda ko‘rsatilgan himoyalangan ma’lumotlarni himoya qilishni ta’minlash talablari va qoidalariga rioya qilish;

- himoyalangan ma’lumotlar bilan ishlashda Korxona tomonidan belgilangan ko‘rsatmalarga rioya qilish;

- himoyalangan ma’lumotlarning oshkor bo‘lishi, shu jumladan o‘z aybi bilan ham, darhol Korxona rahbariyatiga xabar berish.

109. Himoyalangan ma’lumotlar xodim tomonidan Korxona rahbariyatining roziligisiz oshkor qilinishi mumkin, agar xodim ushbu himoyalangan ma’lumotlarni O‘zbekiston Respublikasi qonunchiligiga muvofiq davlat organlariga topshirishi shart bo‘lsa. Bu holda, xodim himoyalangan ma’lumotlarning faqat davlat organining qonuniy talabi tufayli oshkor qilinishi zarur bo‘lgan qismini O‘zbekiston Respublikasi qonunchiligiga muvofiq ruxsat etilgan doirada oshkor qilishga majburdir. Bu holda, xodim bunday so‘rovlar va ushbu organlarga O‘zbekiston Respublikasi qonunchiligi talablariga muvofiq himoyalangan ma’lumotlarni taqdim etish zarurati haqida Korxona rahbariyatiga darhol xabar berishga majburdir.

110. Mehnat shartnomasi bekor qilinganda, Korxonaning xodimi birinchi so‘rovidan keyin bir kun ichida moddiy tashuvchida himoyalangan ma’lumotlarni, shuningdek ularning nusxalarini qaytarishga yoki Korxona rahbariyatining qaroriga ko‘ra bunday tashuvchilarni (nusxalarni) yo‘q qilishga majburdir.

111. Korxona rahbariyati quyidagilarni amalga oshirishga majburdir:

- xodimlarga konfidensial ma’lumotlar ro‘yxatini, shuningdek, himoyalangan ma’lumotlarga kirish huquqiga ega bo‘lgan xodimlar ro‘yxatini yetkazish;

- xodimlarni ushbu Tartib bilan tanishtirish;

- himoyalangan ma’lumotlarning oshkor bo‘lishining aniqlangan holatlari bo‘yicha aybdor shaxslarni aniqlash uchun tekshiruv o‘tkazish;

- xodimni o‘z aybi bilan himoyalangan ma’lumotlarni oshkor qilgani uchun javobgarlikka tortish.

17. Javobgarlik

112. Korxona xodimlari tomonidan himoyalangan ma’lumotlarni elektron vositalar orqali ruxsatsiz to‘plash yoki ruxsatsiz uzatish, xodimlar tomonidan bunday ma’lumotlarni o‘z ichiga olgan hujjatlarni oshkor qilish yoki yo‘qotish, yoki himoyalangan ma’lumotlarni olish yoki qasddan yo‘q qilish uchun serverlar va ma’lumotlar bazalarini buzish O‘zbekiston Respublikasining amaldagi qonunchiligiga muvofiq intizomiy, ma'muriy yoki jinoiy javobgarlikka sabab bo‘ladi.

113. Himoyalangan ma’lumotlar oshkor qilingan taqdirda, Korxona xodimi O‘zbekiston Respublikasi qonunchiligiga muvofiq bunday oshkor qilish natijasida ko‘rilgan har qanday

zararni Korxonaga to‘liq qoplashi shart.

114. Himoyalangan ma’lumotlarning sizib chiqishi yoki yo‘qolishi holatlarida ichki tekshiruv o‘tkaziladi. Ichki tekshiruv natijalari konfidensial ma’lumotlarning sizib chiqishi yoki yo‘qolishi uchun aybdor shaxslarni javobgarlikka tortish to‘g‘risida qaror qabul qilish uchun Korxona rahbariyatiga xabar qilinadi.

115. Himoyalangan ma’lumotlarni oshkor qilmaslik bo‘yicha ushbu Tartibning talablariga qasddan rioya qilmaslik mehnat majburiyatlarini buzish hisoblanadi va mehnat shartnomasining bekor qilinishiga olib kelishi mumkin.

Axborot xavfsizligi
siyosatiga 20-ilova

Axborot xavfsizligi insidentlariga javob berish reglamenti

1. Umumiy qoidalar

1. Axborot xavfsizligi insidentlariga javob berish reglamenti quyidagilarni belgilaydi:

- Korxonada axborot xavfsizligi insidentlarini boshqarish jarayonlarini amalga oshirish tartibi;
- axborot xavfsizligi insidentlarini boshqarish jarayonlarini amalga oshirishda Korxonaning tarkibiy bo‘linmalari hamda mutaxassislarining o‘zaro hamkorlik qilish tartibi;
- Korxonaning axborot xavfsizligi insidentlarini boshqarish jarayonida tashqi korxonalar bilan o‘zaro hamkorlik qilish tartibi;
- axborot xavfsizligi insidentlarini boshqarish jarayonlarini hujjatlashtirish tartibi.

2. Korxonaning tarkibiy bo‘linmalari hamda mutaxassislari axborot xavfsizligi insidentlarini boshqarish jarayonlarini amalga oshirishda mazkur Reglamentga muvofiq aniq va izchil harakatlarni bajarishlari hamda o‘zaro hamkorlik qilishlari shart.

3. Mazkur Reglamentning amal qilishi Axborot xavfsizligi siyosatida belgilangan himoya obyektlariga nisbatan yuzaga keladigan barcha insidentlarga tatbiq etiladi.

4. Mazkur Reglament talablari Korxonaning barcha himoya obyektlarida axborot xavfsizligi insidentlarini boshqarishda majburiy hisoblanadi.

5. Mazkur Reglament bilan Korxonada axborot xavfsizligi insidentlarini boshqarish jarayonlarida ishtirok etuvchi barcha xodimlar tanishtirilishi lozim.

6. Korxonada axborot xavfsizligi insidentlariga javob berish, insidentlarni boshqarishning tegishli protseduralarini bajarish orqali quyidagi tartibda amalga oshiriladi:

1) Rejalashtirish va tayyorgarlik:

- axborot xavfsizligi insidentlarini boshqarish bo‘yicha xabardorlikni oshirish, o‘qitish va treninglar o‘tkazish;
- ichki va tashqi korxonalar bilan hamkorlik qilish – aloqalarni o‘rnatish, “ishonch telefoni”ni tashkil etish;
- favqulodda tiklash (avariyaviy tiklash) rejalarini ishlab chiqish;
- insidentlarga javob berish bo‘yicha muntazam mashg‘ulotlar o‘tkazish hamda favqulodda tiklash rejalarini sinovdan o‘tkazish, mas’ul xodimlarda amaliy ko‘nikmalarni shakllantirish va tezkor javob berish darajasini oshirish;
- insidentlar yuzaga kelgan taqdirda foydalanish uchun ichki va tashqi resurslarni zaxiralash;
- himoya obyektlarining ishlashini monitoring va nazorat qilish vositalarini joriy etish.

2) Aniqlash va hisobot berish:

- jarayonlarni monitoring qilish;
- axborot xavfsizligi bilan bog‘liq salbiy hodisalarni aniqlash;
- axborot xavfsizligi hodisalari to‘g‘risidagi ma’lumotlarni foydalanuvchilar, yetkazib beruvchilar, hamkorlar, xodimlar, axborotni himoya qilish vositalari yoki axborot xavfsizligi hodisalarini monitoring qilish vositalaridan yig‘ish va umumlashtirish;
- axborot xavfsizligi hodisalari bo‘yicha hisobotlarni shakllantirish.

3) Baholash va qaror qabul qilish:

- axborot xavfsizligi insidentini aniqlash;
- insidentni ro‘yxatdan o‘tkazish va hisobga olish;
- insident oqibatlarini baholash;
- insidentlar to‘g‘risida xabardor qilish, bildirish va axborot berish.

4) Javob choralarini ko‘rish:

- axborot xavfsizligi insidentining nazorat ostida ekanligini aniqlash;
- insidentni lokalizatsiya qilish va bartaraf etish;

- insidentdan keyin faoliyatni tiklash va uning oqibatlarini bartaraf etish.

5) Tekshiruv o‘tkazish (zarur hollarda):

- insident sabablarini aniqlash;
- dalillarni (isbotlarni) yig‘ish, tahlil qilish va saqlash;
- insident kelib chiqishiga sababchi bo‘lgan shaxslarni javobgarlikka tortish.

6) Tajribani o‘zlashtirish:

- insidentlar natijalarini hisobga olish;
- insidentlar va aniqlangan zaifliklarni tahlil qilish hamda ulardan olingan tajribani belgilash;
- insidentlarning takroran yuzaga kelishiga yo‘l qo‘ymaslik choralarini ishlab chiqish va qabul qilish;
- insidentga javob berish samaradorligini baholash;
- insidentlarni boshqarish tizimini takomillashtirish bo‘yicha choralarni ishlab chiqish va qabul qilish.

2. Atamalar, ta’riflar va qisqartmalar.

7. Mazkur hujjatda quyidagi atamalar va ularning ta’riflari qo‘llanilgan:

1) Axborot xavfsizligi insidenti – axborot va axborot tizimining konfidensialligi, yaxlitligi yoki mavjudligiga putur yetkazish ehtimoliga ega bo‘lgan hodisa yoki jarayon;

2) Axborot xavfsizligi insidentiga javob berish: axborot xavfsizligi insidentining oqibatlarini bartaraf etish yoki yumshatish maqsadida ko‘riladigan chora-tadbirlar, shu jumladan axborot tizimi va unda saqlanayotgan axborotning normal ish rejimini himoya qilish va tiklash bo‘yicha choralar;

3) Axborot xavfsizligi hodisasi: tizim, xizmat yoki tarmoq holatining aniqlangan ko‘rinishi bo‘lib, axborot xavfsizligi siyosatining buzilishi, himoya vositalarining ishdan chiqishi yoki axborot xavfsizligiga salbiy ta’sir ko‘rsatishi mumkin bo‘lgan ilgari noma’lum vaziyatni ko‘rsatadi;

4) Axborot xavfsizligi insidentlarini boshqarish: axborot xavfsizligi insidentlarini aniqlash, ro‘yxatga olish, baholash, ularga javob berish va tekshirish jarayonlari majmui.

8. Axborot xavfsizligi insidentlariga javob berish Reglamentida quyidagi qisqartmalar qo‘llaniladi:

IDPS (Intrusion Detection & Prevention System) hujumlarni aniqlash va oldini olish tizimi;

DLP (Data Leak Prevention) – ma’motlarni ruxsatsiz chiqib ketishini oldini olish tizimi;

PAM (Privileged Account Management) – imtiyozli foydalanuvchilarni boshqarish tizimi;

AT – axborot tizimi;

MAI – muhim axborot infratuzilmasi;

MBBT – ma’lumotlar bazasini boshqarish tizimi;

KBNT – kirishni boshqarish va nazorat qilish tizimi.

3. Insidentlarni boshqarishga tayyorgarlik ko‘rish tartibi.

9. Korxonada axborot xavfsizligi insidentlarini samarali boshqarish uchun quyidagi tayyorgarlik choralari ko‘rilishi lozim:

1) ularga javob berish uchun mas’ul bo‘lgan xodimlarni insidentlarni boshqarish bo‘yicha o‘qitish;

2) xodimlarni insidentlarni boshqarish tartib-taomillari bilan tanishtirish;

3) xodimlarda amaliy ko‘nikmalarni shakllantirish va tezkor javob berish darajasini oshirish maqsadida belgilangan insidentlarni boshqarish tartib-taomillarini muntazam mashq qilish yoki favqulodda tiklash rejalarini sinovdan o‘tkazish;

4) insidentlarni boshqarish jarayonida xodimlarni ularning vazifalari va javobgarligi haqida xabardor qilish;

5) insidentlar yuzaga kelganda foydalanish uchun ichki va tashqi resurslarni zaxiralash;

6) insidentlarni boshqarish jarayonida hamkorlik qilish zarur bo‘lgan tashqi korxonalar bilan aloqalarni o‘rnatish;

- Korxonaning KABT boshqarmasi tomonidan obyektlar va tarkibiy bo‘linmalardan insidentlar to‘g‘risidagi ma’lumotlarni yig‘ish uchun “ishonch telefoni”ni tashkil etish hamda ushbu “ishonch telefoni” haqida Korxona xodimlariga ma’lumot yetkazish.

10. Axborot xavfsizligi insidentlarini boshqarish bo‘yicha tayyorgarlik choralarini amalga oshirish Korxonaning KABT boshqarmasi tomonidan ta’minlanadi.

11. Korxonaning KABT boshqarmasi hududlardagi kadrlar boshqaruvi bo‘linmalari bilan hamkorlikda davriy ravishda (kamida yiliga bir marotaba):

- mazkur hujjatda belgilangan insidentlarni boshqarish jarayonidagi ularning vazifalari va javobgarligi yuzasidan Korxona xodimlari o‘rtasida tushuntirish ishlarini olib boradilar;

- ularga javob berish uchun mas’ul bo‘lgan xodimlarni insidentlarni boshqarish bo‘yicha o‘qitadilar;

- Axborot xavfsizligi siyosatining 12-bo‘limida belgilangan axborot xavfsizligi insidentlarini boshqarishdagi xodimlarning vazifalari haqida xabardor qiladilar.

12. Insidentlarni boshqarish bo‘yicha o‘qitish jarayonida ularga javob berish uchun mas’ul bo‘lgan xodimlarga insidentlarni boshqarishdagi ularning vazifalari va javobgarligi yetkazilishi, shuningdek o‘zaro hamkorlik tartibi yuzasidan tushuntirish berilishi lozim.

13. Korxonaning KABT boshqarmasi muntazam ravishda, kamida yiliga bir marotaba, mazkur hujjatda belgilangan insidentlarni boshqarish tartib-taomillarini amalga oshirish bo‘yicha mashg‘ulotlar hamda favqulodda tiklash rejalarini sinovdan o‘tkazishni Korxonada tashkil etadi va o‘tkazadi.

14. Korxonaning KABT boshqarmasi insidentlarni boshqarish jarayonida hamkorlik qilish zarur bo‘lgan barcha tashqi korxonalarning aloqa ma’lumotlariga ega bo‘lishi shart.

4. Axborot xavfsizligi insidentlarini boshqarish tartibi

4.1. Aniqlash va hisobot berish

15. Axborot xavfsizligi hodisalarini aniqlash uchun monitoring tartibida quyidagi shaxslar ishtirok etishi lozim:

1) Korxona xodimlari, quyidagi himoya ob’ektlari bo‘yicha:

- ulardan foydalanilayotgan oxirgi qurilmalar va ularga o‘rnatilgan dasturiy ta’minot;

- ularga foydalanish uchun berilgan raqamli axborot vositalari;

- ular foydalanuvchilari bo‘lgan axborot tizimlari.

2) Korxonaning himoyalanadigan axborotga egalik qiluvchi tarkibiy bo‘linmalari hamda himoyalanadigan axborotga kirish huquqi berilgan xodimlar, quyidagi himoya obyektlari bo‘yicha:

- himoyalanadigan axborot, jumladan tijorat siri, shaxsiy ma’lumotlar va “Faqat xizmat uchun” belgisi bo‘lgan hujjatlar;

- konfodensial axborot bilan ishlash amalga oshiriladigan himoyalangan xonalar va himoyalanadigan hujjatlar saqlanadigan joylar (qog‘oz shaklida).

3) Korxonaning IT-bo‘linmasi quyidagi ob’ektlar bo‘yicha:

- server uskunalari, ma’lumotlar bazasini boshqarish tizimlari MBBT va axborot tizimlari operatsion tizimlari hamda Korxona resurslari;

- Korxona lokal tarmog‘i va uning tarkibidagi tarmoq uskunalari;

- tashqi aloqalar kanallari va lokal tarmoqni tashkil etishda ishlatiladigan kanallar;

- axborot almashish tizimlari, jumladan korporativ elektron pochta, IP-telefoniya, Call-markaz, videokonferensiya, korporativ messenjer;

- rasmiy veb-sayt, fayl serveri;

- Korxona markaziy apparatidagi xodimlarning oxirgi qurilmalari.

4) Hududiy boshqarmalardagi axborot xavfsizligi administratorlari, quyidagi obyektlar bo‘yicha:

- hududiy boshqarmaning lokal tarmog‘i va uning tarkibidagi tarmoq uskunalari;
- tashqi aloqalar kanallari va hududiy boshqarma lokal tarmoqqa ulanish kanallari;
- hududiy boshqarma xodimlarining oxirgi qurilmalari.

5) KABT boshqarmasi, axborotni himoya qilish vositalari bo‘yicha.

6) Jismoniy xavfsizlik bo‘limi, quyidagi obyektlar bo‘yicha:

- jismoniy xavfsizlikni ta’minlash tizimlari (KBNT va videokuzatuv);
- himoyalanadigan xonalar, obyektlar va moddiy aktivlar.

7) Korxona rahbariyati, obro‘ va imidj bo‘yicha.

16. […]

17. Axborot xavfsizligi hodisalari bo‘yicha qo‘shimcha ma’lumotlarni yig‘ish maqsadida Korxonaning KABT boshqarmasi tomonidan Korxonada qo‘llaniladigan ma’lumotlarni himoya qilish vositalarining chiqish ma’lumotlaridan ham foydalaniladi.

18. […]

Korxonada axborot xavfsizligi holatini monitoring qilish bo‘yicha ishlar sutka davomida (24/7) uzluksiz rejimda tashkil etiladi.

19. Korxona himoya qilinadigan obyektlarida yuzaga kelgan va axborotni himoya qilish vositalari tomonidan aniqlanmagan hodisalar haqida darhol “issiq liniya” orqali KABT boshqarmasiga xabar beriladi.

20. Axborot xavfsizligi hodisalari haqida xabar berishda Korxona xodimi KABT boshqarmasiga quyidagilarni ma’lum qilishi shart:

- hodisa aniqlangan vaqt;
- hodisa sodir bo‘lgan himoya obyekti;
- yuzaga kelgan oqibatlar va ularning tavsifi;
- agar xodimga ma’lum bo‘lsa, hodisaning sabablari;
- sodir bo‘lgan hodisa haqida xabardor bo‘lgan shaxslar.

4.2. Baholash va qaror qabul qilish.

21. Korxonada Axborot xavfsizligi siyosatining 12-bo‘limida ko‘rsatilgan axborot xavfsizligi hodisalarini insident sifatida ko‘rib chiqilishi lozim.

22. Hodisa to‘g‘risida olingan ma’lumotlar asosida Korxonaning KABT boshqarmasining AT bo‘linmasi tomonidan hodisani tahlil qilish va baholash amalga oshiriladi, uning natijasida:

- hodisa axborot xavfsizligi insidenti sifatida tasniflanadi;
- axborot xavfsizligi insidentining xavflilik darajasi aniqlanadi;
- xodimga uning keyingi harakatlari bo‘yicha ma’lumot beriladi.

23. Axborot xavfsizligi hodisasini baholash jarayonida uning oqibatlari darajasi aniqlanadi. Oqibatlar darajasidan kelib chiqib, jadvalda belgilangan qoidalarga muvofiq insidentning xavflilik darajasi belgilanadi.

Jadval. Axborot xavfsizligi insidentining xavflilik darajasini aniqlash

Xavflilik darajasi	Insident tavsifi	Javob choralari mezonlari
Yuqori	Muhim himoya obyektida yuz bergan, Korxona faoliyati yoki uning muhim texnologik va ishlab chiqarish jarayonlari buzilishiga yoki to‘xtatilishiga olib kelgan, yoxud Korxonaga sezilarli moddiy zarar, imij va obro‘siga putur yetkazgan, shuningdek mijozlar yoki hamkorlarga jiddiy moddiy yoki ma’naviy zarar yetkazgan muhim insident.	Insident haqida Korxona rahbariyatini xabardor qilish. Uni bartaraf etish uchun Korxonaning barcha zarur kuch va vositalarini jalb etish. Insident sabablarini tekshirish. Yetkazilgan zararni baholash.
O‘rta	Himoya obyektida yuz bergan, Korxonaning ayrim texnologik va ishlab chiqarish jarayonlari buzilishiga yoki vaqtincha to‘xtashiga olib kelgan, biroq asosiy ishlab chiqarish vazifalari va funksiyalariga ta’sir ko‘rsatmagan, yoki Korxona uchun sezilarli bo‘lmagan moddiy zarar, alohida mijoz yoki hamkor uchun sezilarli bo‘lmagan ma’naviy yoki moddiy zarar yetkazgan insident.	Insident yuz bergan tarkibiy bo‘linma rahbarini xabardor qilish. Insidentni bartaraf etish uchun tegishli tarkibiy bo‘linma resurs va vositalarini jalb etish. Axborot xavfsizligi insidentini tahlil qilish va baholash.
Past	Himoya obyektining keyingi faoliyatiga ta’sir ko‘rsatmagan yoki Korxona, uning mijozlari va hamkorlariga moddiy yoki ma’naviy zarar yetkazmagan insident.	Insidentni hisobga olish. Takrorlanishini aniqlash uchun monitoring olib borish. Insident takrorlanganda, uni tahlil qilish va baholash hamda tegishli choralarni ko‘rish.

24. Qo‘shimcha ravishda, Korxonaning KABT boshqarmasining AT bo‘linmasi tomonidan qo‘shimcha ma’lumotlar yig‘iladi, jumladan axborot tizimlari hamda axborotni qayta ishlash va himoya qilish vositalarining hodisalar jurnallaridan foydalaniladi. Ushbu qo‘shimcha ma’lumotlarni yig‘ish jarayoniga Korxonaning boshqa tarkibiy bo‘linmalari xodimlari ham jalb etilishi mumkin.

25. Agar hodisa axborot xavfsizligi insidenti sifatida aniqlansa, u majburiy ravishda ro‘yxatdan o‘tkazilishi va hisobga olinishi lozim. Insidentlar mazkur Reglamentning 1-ilovasida belgilangan shaklga muvofiq axborot xavfsizligi insidentlarining elektron bazasini yuritish orqali ro‘yxatdan o‘tkaziladi va hisobga olinadi.

26. “Yuqori” xavflilik darajasiga ega insident mazkur Reglamentning 2-ilovasida belgilangan shaklga muvofiq navbatdan tashqari holatlar hisob jurnali (reestri)da ro‘yxatdan o‘tkazilishi lozim.

27. Axborot xavfsizligi insidentlarining elektron bazasi hamda navbatdan tashqari holatlar hisob jurnali Korxonada KABT boshqarmasi tomonidan alohida yuritiladi.

28. Korxonaning axborot xavfsizligi insidentlari elektron bazasidagi hamda navbatdan tashqari holatlar hisob jurnalidagi ma’lumotlarni saqlash muddati cheklanmaydi. Bu ma’lumotlar insidentlar bo‘yicha statistik ma’lumotlarni shakllantirish hamda axborot xavfsizligi risklarini tahlil qilish va baholash maqsadida foydalaniladi.

Axborot xavfsizligi insidentlari elektron bazasi va navbatdan tashqari holatlar hisob jurnalidagi ma’lumotlarga kirish cheklangan bo‘lishi hamda faqat KABT boshqarmasi xodimlariga taqdim etilishi lozim.

29. Aniqlangan insident to‘g‘risida Korxonaning KABT boshqarmasi quyidagilarni xabardor qiladi:

- o‘z bo‘linmasi rahbarini;
- insident ta’sir ko‘rsatgan ishlab chiqarish uchastkasi yoki texnologik jarayon uchun mas’ul tarkibiy bo‘linma rahbariyatini;

- himoya obyektiga xizmat ko‘rsatish uchun mas’ul mutaxassisni (administratorni).

Agar insident oqibatlari “yuqori” xavflilik darajasiga ega bo‘lsa, KABT boshqarmasi yoki tizimosti korxonaning AT bo‘linmasi bu haqda Korxona rahbariyatiga xabar beradi.

“Yuqori” xavflilik darajasiga ega insident yuzaga kelgan taqdirda, bu haqda “ishonch telefoni” orqali Korxonaning KABT boshqarmasiga ham xabar berishi shart.

30) Axborot xavfsizligi insidenti haqida xabardor qilishda quyidagi ma’lumotlar ko‘rsatilishi lozim:

- insident aniqlangan vaqt;
- insident sodir bo‘lgan himoya obyekti;
- insidentning xavflilik darajasi;
- insidentning tavsifi va uning oqibatlari;
- insident sabablari yoki aybdor shaxslar (agar ma’lum bo‘lsa);
- insidentga nisbatan ko‘rilgan choralar.

31. Muhim axborot infratuzilmasi (MAI) obyektida (axborot tizimi) axborot xavfsizligi insidenti yoki Korxonada “yuqori” xavf darajasiga ega insident yuzaga kelgan taqdirda, KABT boshqarmasi bu haqda Kiberxavfsizlik markazini xabardor qilishi shart.

Korxonada axborot xavfsizligi insidentlari to‘g‘risida Kiberxavfsizlik markazini xabardor qilish tartibi Kiberxavfsizlik markazi tomonidan belgilangan tartibda amalga oshiriladi.

32. Tashqi manfaatdor korxonalar, hamkorlar va mijozlarni xabardor qilish to‘g‘risidagi qaror Korxona rahbariyati tomonidan qabul qilinadi.

Tashqi korxonalarni xabardor qilish vazifasi tashqi korxona darajasi hamda yuzaga kelgan oqibatlar xususiyatidan kelib chiqib, Korxonaning KABT boshqarmasi rahbariga yuklatiladi.

4.3. Javob choralarini ko‘rish.

33. “Yuqori” va “o‘rta” xavflilik darajasiga ega insident yuzaga kelgan taqdirda, insidentga sabab bo‘lgan tahdid harakatlarini lokalizatsiya qilish va bartaraf etish, shuningdek insident oqibatlarini tugatish jarayonlariga Korxonada insidentlarga javob berish guruhi jalb etiladi.

Korxonada insidentlarga javob berish guruhi faoliyatiga KABT boshqarmasi boshlig‘i rahbarlik qiladi.

Korxonada jismoniy xavfsizlik buzilishi bilan bog‘liq insidentlar yuzaga kelgan taqdirda, javob choralarini ko‘rish jarayonlariga jismoniy xavfsizlik bo‘linmasi jalb etiladi.

Korxonaning hududiy boshqarmasi insident yuzaga kelgan taqdirda, ularga javob choralarini ko‘rish jarayonida hududiy boshqarmaning axborot xavfsizligi administratori hamda AT mutaxassisi ishtirok etishi shart.

Korxonaning mazkur jarayonlarda ishtirok etuvchi vakillari sifatida axborot xavfsizligi bo‘yicha administrator hamda hududiy boshqarmaning AT mutaxassisi jalb etilishi lozim.

Mazkur ishlarga, shuningdek, Korxona rahbariyati bilan kelishilgan holda boshqa tarkibiy bo‘linmalar va mutaxassislar ham jalb qilinishi mumkin.

34. Axborot xavfsizligiga tahdidlar ta’siri bilan bog‘liq insident yuzaga kelganda quyidagi choralar ko‘rilishi lozim:

- tahdidning sababi yoki manbasini baholash;
- tahdidni to‘liq bartaraf etilgunga qadar uning tarqalishini cheklash va yetkazilishi mumkin bo‘lgan zararni minimallashtirishga qaratilgan lokalizatsiya qilish.

35. Lokalizatsiya choralari quyidagilarga qaratilishi lozim:

- zararlangan tizimlarni izolyatsiya qilish yoki tahdid manbasini bartaraf etish (zararlangan qurilmani tarmoqdan uzish, tashqi tarmoqdan uzish yoki zaxira tashqi aloqa kanallarini ishga tushirish, IP-manzilni o‘zgartirish, masofaviy kirishni o‘chirish va boshqalar);

- kirishni bloklash (buzilgan va oshkor bo‘lgan qayd yozuvlarni bloklash yoki o‘chirish, parollar va kirish identifikatorlarini almashtirish, kirish huquqlarini cheklash va boshqalar);

- trafikni filtrlash va cheklash (zararli IP-manzillarni bloklash, portlarni yopish, tarmoqlararo ekran sozlamalariga o‘zgartirish kiritish va boshqalar).

36. Tahdid lokalizatsiya qilingandan so‘ng insident oqibatlarini bartaraf etish bo‘yicha quyidagi choralar ko‘rilishi lozim:

- axborotni va/yoki tizimlar faoliyatini tiklash;
- zaifliklarni bartaraf etish;
- xavfsizlik sozlamalarini o‘zgartirish;
- monitoringni kuchaytirish va boshqalar.

37. Texnik nosozliklar bilan bog‘liq insidentlar yuzaga kelganda tizimlar faoliyatini tiklash ishlari amalga oshiriladi. Tiklash ishlari himoya obyektining favqulodda tiklash rejasiga muvofiq olib borilishi lozim.

38. Korxonada insidentni bartaraf etish va uning oqibatlarini tugatish bo‘yicha ishlarning borishi haqida muntazam ravishda “issiq liniya” orqali KABT boshqarmasi rahbariga xabar berib borilishi lozim.

Agar insidentni bartaraf etish va uning oqibatlarini tugatish jarayoni Korxona rahbariyati tomonidan nazorat qilinsa, u holda ishlarning borishi to‘g‘risida KABT boshqarmasi rahbariyati Korxona rahbariyatiga hisobot beradi.

39. Kiberxavfsizlik markazi tomonidan nazoratga olingan insidentlar bo‘yicha Korxona insident sabablarini aniqlash, tahdidni lokalizatsiya qilish va oqibatlarini bartaraf etish yuzasidan talab etilgan ma’lumotlarni Kiberxavfsizlik markaziga u belgilagan tartibda taqdim etishi lozim.

4.4. Tekshiruv o‘tkazish.

40. Insident sabablarini aniqlash va/yoki insidentda aybdor shaxslarni javobgarlikka tortish maqsadida Korxona rahbariyati tomonidan insident yuzasidan tekshiruv o‘tkazish jarayoni tashabbus qilinishi mumkin.

41. Insident bo‘yicha tekshiruv quyidagi maqsadlarda o‘tkaziladi:

- sabablarni aniqlash;
- aybdorlarni aniqlash;
- aybdorlarni javobgarlikka tortish uchun dalil va isbotlarni to‘plash;
- aybdor harakatlarining xususiyatini aniqlash (qasddan, ehtiyotsizlik oqibatida, maqsadli va boshqalar).

42. Insident bo‘yicha tekshiruv o‘tkazish uchun KABT boshqarmasi tomonidan maxsus guruh tuziladi, uning tarkibi Korxona rahbariyati bilan kelishiladi. Ushbu guruh tarkibiga Korxona vakillari kiritilishi mumkin.

43. Insidentni tekshirish doirasida tekshiruv guruhi vakillari quyidagi huquqlarga ega:

- zarur dalillarni to‘plash maqsadida insident sodir bo‘lgan xonalarga, jumladan xodimlarning ish joylariga yoki boshqa jihozlarga bevosita kirish;
- tekshiruvga taalluqli hujjatlar yoki boshqa ma’lumotlarni ko‘rib chiqish va ularni tekshiruv materiallariga qo‘shish uchun xodimlardan taqdim etishni talab qilish;
- insidentda bevosita yoki bilvosita ishtiroki yuzasidan xodimlardan tushuntirish xatlari yozishni talab qilish;
- insidentda bevosita yoki bilvosita ishtiroki bo‘yicha shaxsiy suhbat o‘tkazish uchun xodimlarni chaqirish.

44. Insidentni tekshirish jarayonida Korxona xodimlari tekshiruv guruhi vakili talabiga ko‘ra quyidagilarni taqdim etishi shart:

- so‘ralgan ma’lumotlarni;
- yozma tushuntirishlarni;
- xonalarga, shu jumladan o‘z ish joyiga hamda boshqa jihozlarga kirish imkoniyatini.

45. Tekshiruv davomida tekshiruv guruhi vakillari tomonidan dalillar to‘planadi. Quyidagilar dalil sifatida xizmat qilishi mumkin:

- himoya obyektlari va ular bilan bog‘liq vositalarning hodisalar jurnali ma’lumotlari (loglar);
- axborotni himoya qilish vositalari ma’lumotlari;
- raqamli tashuvchilarda va xotirada saqlangan ma’lumotlar;
- elektron yozishmalar va xabarlar;
- videokuzatuv kameralaridan olingan tasvirlar;
- tarmoq ma’lumotlari (IP-manzil, port, protokol va boshqalar);
- xodimlarning ko‘rsatmalari va boshqalar.

46. Aybdorlarni jinoiy javobgarlikka tortish zarurati tug‘ilganda, insident bo‘yicha tekshiruvga huquqni muhofaza qiluvchi organlar jalb etilishi mumkin.

Huquqni muhofaza qiluvchi organlarni tekshiruvga jalb etish to‘g‘risidagi qaror Korxona rahbariyati tomonidan qabul qilinadi.

47. Insident bo‘yicha tekshiruv natijalari Korxona rahbariyatiga taqdim etiladi.

48. Aybdorlarga nisbatan jazo choralari Korxona rahbariyati tomonidan amaldagi qonunchilik, ichki mehnat tartibi qoidalari hamda mehnat shartnomasiga muvofiq qo‘llaniladi.

4.5. Tajribadan xulosa chiqarish.

49. Korxonada “yuqori” yoki “o‘rta” xavf darajasiga ega insident tahlili KABT boshqarmasi tomonidan insidentlarga javob berish guruhi, shuningdek manfaatdor tarkibiy bo‘linmalar va mutaxassislarni jalb qilgan holda amalga oshiriladi.

50. Tahlil jarayonida:

- insident sabablari va zaifliklar aniqlanadi;
- tahdidni lokalizatsiya qilish va oqibatlarni bartaraf etish bo‘yicha ko‘rilgan choralar hamda ularning natijalari baholanadi.

51. Agar insident natijasida Korxonaga zarar yetkazilgan bo‘lsa, tahlil jarayonida yetkazilgan zarar va ko‘rilgan moliyaviy yo‘qotishlar miqdori aniqlanishi lozim. Yetkazilgan zarar yoki yo‘qotishlar miqdorini aniqlash uchun tahlilga Korxonaning buxgalteriya xodimlari jalb etilishi mumkin.

52. Insidentlar tahlili yakunlari bo‘yicha quyidagilarni o‘z ichiga olgan hisobot tayyorlanadi:

- insidentga olib kelgan tahdidlar tavsifi va oxirgi davrda shunga o‘xshash tahdidlarning yuzaga kelish chastotasi;
- insident sabablari va tahdid manbalari;
- insidentni amalga oshirishda foydalanilgan zaifliklar;
- insident yoki uning ko‘lami va oqibatlariga olib kelgan mavjud xatolar va kamchiliklar;
- insident sabablari va/yoki oqibatlarida aybdor shaxslar;
- oqibatlarning tavsifi, yetkazilgan zarar yoki yo‘qotishlar miqdori;
- tahdidni lokalizatsiya qilish va tiklash bo‘yicha ko‘rilgan choralar hamda ularning natijalari;
- insidentga javob berish samaradorligining bahosi;
- insidentning takroran yuzaga kelishining oldini olish uchun ko‘rilishi lozim bo‘lgan chora-tadbirlar;
- Korxonada insidentlarni boshqarish tizimini takomillashtirish bo‘yicha chora-tadbirlar.

Mazkur hisobot Korxonaning KABT boshqarmasi xodimlari, axborot xavfsizligi insidentlariga javob berish guruhi a’zolari hamda insident tahlilida ishtirok etgan boshqa shaxslar tomonidan imzolanadi va Korxona rahbariyatiga taqdim etiladi.

53. Insident tahlili bo‘yicha hisobot rahbariyat tomonidan ma’qullangan taqdirda, Korxonaning KABT boshqarmasi zarur choralarni ko‘rish yuzasidan qaror loyihasini

tayyorlaydi.

5. Tashqi korxonalar bilan hamkorlik tartibi.

54. Axborot xavfsizligi insidentlarini boshqarish jarayonida Korxona quyidagi tashqi korxonalar bilan o‘zaro faoliyat olib borishi mumkin:

1) Kiberxavfsizlik markazi va boshqa vakolatli organlar: insidentlar bo‘yicha hamda ularga qarshi ko‘rilgan chora-tadbirlar va ularning amalga oshirilishi to‘g‘risida xabardor qilish;

2) Manfaatdor tashqi korxonalar (telekommunikatsiya operatorlari, xizmat provayderlari, yetkazib beruvchilar, mijozlar, o‘zaro ishlaydigan axborot tizimlari va tashqi foydalanuvchilar – Asoschi): insidentlar haqida xabardor qilish, oqibatlarni bartaraf etish, ularni kamaytirish va takroriy insidentlarning oldini olish bo‘yicha hamkorlik;

3) Huquqni muhofaza qiluvchi organlar: jinoyat ishlarini qo‘zg‘atish va insidentlarni tekshirish o‘tkazishda ishtirok etish;

4) Favqulodda vaziyatlar organlari: favqulodda vaziyatlarga olib kelgan insidentlar haqida xabardor qilish, oqibatlarini bartaraf etishga jalb qilish va sabablarini tekshirish;

5) Korxona mijozlari: insidentlar, ularni bartaraf etish, kamchiliklarni yo‘qotish yoki xizmatlarni tiklash haqida xabardor qilish.

54. Kiberxavfsizlik markazi bilan Korxona va idoraviy korxona MAI obyektlarida (AT tizimi), yuzaga kelgan insidentlar shuningdek, Korxona “yuqori” xavf darajasiga ega insidentlar yuzaga kelganda o‘zaro faoliyat olib borishi shart. Ta’minlanadigan ma’lumotlar va o‘zaro faoliyat tartibi Kiberxavfsizlik markazi tomonidan belgilanadi.

Ushbu o‘zaro faoliyat Korxonaga insident sabablarini aniqlash, tahdidni lokalizatsiya qilish, oqibatlarni bartaraf etish, tekshiruv o‘tkazish va himoya choralarini ko‘rishda yordam ko‘rsatishga qaratilgan.

55. Insident haqida xabardor qilish yoki insidentlarni boshqarish jarayoniga boshqa tashqi korxonalarni jalb qilish to‘g‘risidagi qaror Korxona rahbariyati tomonidan qabul qilinadi.

56. Og‘ir oqibatlarga olib kelgan axborot xavfsizligi insidentlarini tekshirishda aybdorlarni jinoiy javobgarlikka tortish maqsadida huquqni muhofaza qiluvchi organlar jalb qilinadi.

57. Agar insident natijasida favqulodda vaziyat yuzaga kelsa (yong‘in, suv toshqini, bino qulash va boshqalar), Korxona ushbu insidentlar haqida favqulodda vaziyatlar organlarini xabardor qiladi, ularni oqibatlarni bartaraf etishga va sabablarini tekshirishga jalb qiladi.

58. Insidentlar Korxonaning hamkorlar, yetkazib beruvchilar va boshqa o‘zaro faoliyat olib boradigan korxonalar bilan ishlash jarayonini buzilishiga olib kelishi mumkin. Bu buzilishlar Korxonadagi yoki u bilan o‘zaro faoliyat qiluvchi korxonadagi insidentlar natijasida yuzaga kelishi mumkin. Bunday vaziyatlarda Korxona uchinchi tomon korxonalar bilan insidentlar haqida xabardor qilish, oqibatlarni bartaraf etish va tiklash bo‘yicha birgalikda chora-tadbirlarni ishlab chiqish, tiklash ishlari va uzilgan hamkorlik jarayonlari haqida xabardor qilish uchun o‘zaro faoliyat olib borishi kerak.

59. Agar insidentlar raqamli xizmatlarni ko‘rsatishni imkonsiz qilsa, Korxona mijozlarni bu haqda xabardor qilishi shart.

60. Insidentlarni boshqarish bo‘yicha tashqi korxonalar va mijozlar bilan bog‘lanish Korxonaning ushbu o‘zaro faoliyat bilan shug‘ullanuvchi tarkibiy bo‘linmalari tomonidan amalga oshiriladi.