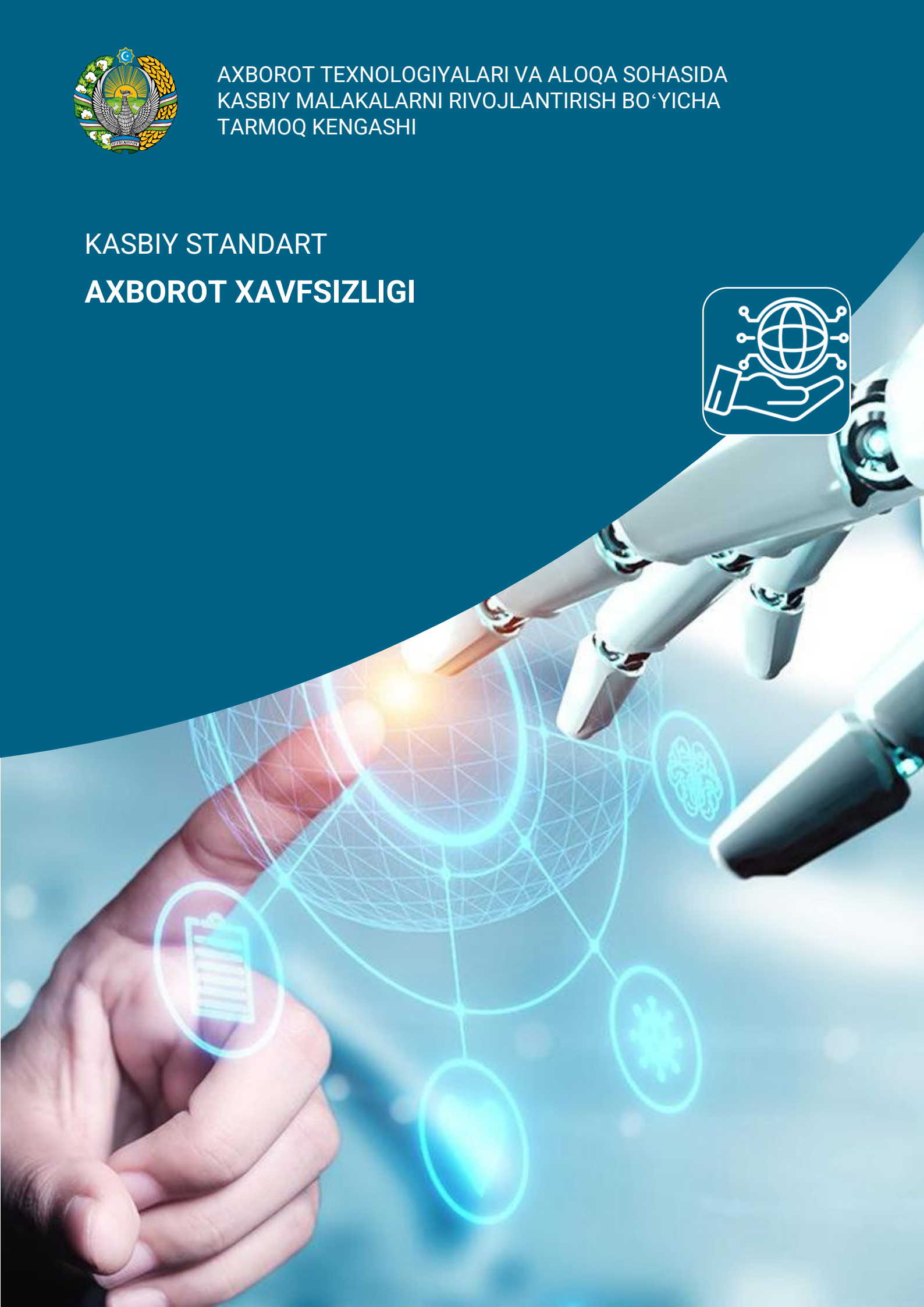
AXBOROT TEXNOLOGIYALARI VA ALOQA SOHASIDA
KASBIY MALAKALARNI RIVOJLANTIRISH BO‘YICHA
TARMOQ KENGASHI

KASBIY STANDART

AXBOROT XAVFSIZLIGI



“Axborot xavfsizligi” kasbiy standarti 2025-yil 18-dekabrdagi Kasbiy malakalarni rivojlantirish bo‘yicha Respublika kengashi majlisining 114-son bayoni bilan tasdiqlangan “Kasbiy standart shakli” hamda Milliy malaka tizimini rivojlantirish instituti direktorining 2025-yil 19-dekabrdagi 55-son buyrug‘i bilan tasdiqlangan “Kasbiy standartlarni ishlab chiqish va yangilash metodologiyasi”ga muvofiq, Axborot texnologiyalari va aloqa sohasida kasbiy malakalarni rivojlantirish bo‘yicha tarmoq kengashi tomonidan ishlab chiqilgan.

KASBIY STANDART

Axborot xavfsizligi

Reyestr raqami:

UZ-KS-2026-T1.0-0067

I. Umumiy ma’lumotlar

1. Kasbiy standartning qo‘llanilish sohasi: Ushbu Kasbiy standart “Axborot himoyasi bo‘yicha texnik” va “Axborot xavfsizligi bo‘yicha mutaxassis” kasblari uchun ta’lim dasturlarini ishlab chiqishda, kasbiy malakalarni mustaqil baholashda, shuningdek, tashkilotlarda xodimlarni boshqarish sohasida keng ko‘lamli masalalarni hal qilishda qo‘llaniladi.

2. Ushbu Kasbiy standartdac quyidagi asosiy tushunchalar va atamalar qo‘llaniladi:

axborot resursi – axborot tizimi tarkibidagi elektron shakldagi axborot, ma’lumotlar banki, ma’lumotlar bazasi, shu jumladan axborot tizimlarida ochiq shaklda joylashtiriladigan yoxud e’lon qilinadigan audio-, video-, grafik va matnli axborot;

axborot texnologiyasi – axborotni to‘plash, saqlash, izlash, unga ishlov berish va uni tarqatish uchun foydalaniladigan jami uslublar, qurilmalar, usullar va jarayonlar;

axborot tizimi – axborotni to‘plash, saqlash, izlash, unga ishlov berish hamda undan foydalanish imkonini beradigan, tashkiliy jihatdan tartibga solingan jami axborot resurslari, axborot texnologiyalari va aloqa vositalari;

axborot – manbalari va taqdim etilish shaklidan qat’i nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to‘g‘risidagi ma’lumotlar;

Axborotlashtirish – yuridik va jismoniy shaxslarning axborotga bo‘lgan ehtiyojlarini qondirish uchun axborot resurslari, axborot texnologiyalari hamda axborot tizimlaridan foydalangan holda sharoit yaratishning tashkiliy ijtimoiy-iqtisodiy va ilmiy-texnikaviy jarayoni;

axborotni muhofaza etish – axborot borasidagi xavfsizlikka tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish chora-tadbirlari;

bilim – kasbiy faoliyat doirasidagi vazifalarni bajarish uchun zarur bo‘ladigan, o‘rganilgan va o‘zlashtirilgan ma’lumotlar;

hujjatlashtirilgan axborot – identifikatsiya qilish imkonini beruvchi rekvizitlari qo‘yilgan holda moddiy jismda qayd etilgan axborot;

informal ta’lim – aniq maqsadga yo‘naltirilgan, ammo institutsionallashtirilmagan (muayyan qoidalar va normalarni

mujassamlashtirmagan), rasmiy yoki norasmiy ta’limdan ko‘ra kamroq tashkillashtirilgan va tarkiblashtirilgan hamda oiladagi, ish joyidagi, yashash joyidagi va kundalik hayotdagi o‘quv faoliyatini o‘z ichiga olgan ta’lim shakli;

iqtisodiy faoliyat turi – savdo uchun mo‘ljallangan mahsulot ishlab chiqarish (xizmat ko‘rsatish) maqsadida u yoki bu turdagi resurslarni (uskunalar, mehnat, texnologiya va boshqalar) birlashtirishga asoslangan ishlab chiqarish jarayoni;

kasb – ko‘nikma va bilimlarni talab qiladigan muayyan funksiyalar va vazifalarni bajarish bilan bog‘liq bo‘lgan faoliyat turi;

kasb xaritasi – kasb nomi, mehnat funksiyalari tavsifi, kasbga qo‘yiladigan asosiy xususiyatlar va talablarni o‘z ichiga olgan muayyan kasb to‘g‘risidagi tizimlashtirilgan ma’lumotlarni o‘z ichiga olgan kasbiy standartning tarkibiy elementi;

kasbiy standartlar reyestri – bu kasbiy standartlarning nomi, qamrab olingan kasblar, uni qabul qilishga oid qaror (buyruq) rekvizitlari hamda amal qilish muddatini o‘z ichiga olgan tizimlashtirilgan ro‘yxat;

kiberhimoya – kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma’lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmui;

kiberhujum – kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat.

kiberjinoyatchilik – axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi;

kibermakon – axborot texnologiyalari yordamida yaratilgan virtual muhit;

kibertahdid – kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui;

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

ko‘nikma – mehnat vazifasi doirasida alohida yoki yakka harakatlarni jismoniy va aqliy jihatdan bajarish;

ma’lumotlar butunligi – axborotni yo‘qotilishiga olib keluvchi buzilishlardan, shuningdek ma’lumotlarni mualliflik huquqi bo‘lmagan holda hosil qilish yoki yo‘q qilishdan himoya qilish;

maxfiy axborot – foydalanilishi qonun hujjatlariga muvofiq cheklab qo‘yiladigan hujjatlashtirilgan axborot;

mehnat funksiyasi — kasbiy faoliyat doirasida xodim tomonidan belgilangan natijaga erishish uchun amalga oshiriladigan mehnat vazifalari majmui;

mehnat harakatlari – xodimning mehnat predmeti bilan o‘zaro ta’sirida muayyan mehnat natijasiga erishiladigan jarayon;

mehnat vazifasi – mehnat funksiyasi doirasida xodimga yuklanadigan (topshiriladigan) ishning aniq turi;

norasmiy ta’lim – ta’lim xizmatlari taqdim etilishini ta’minlovchi shaxs yoki tashkilot tomonidan institutsionallashtirilgan (muayyan qoidalar va normalarni mujassamlashtiruvchi), aniq maqsadga yo‘naltirilgan va rejalashtirilgan, shaxsni butun hayoti davomida o‘qitishdagi rasmiy ta’limga qo‘shimcha va (yoki) uning muqobil shakli.

ommaviy axborot – cheklanmagan doiradagi shaxslar uchun mo‘ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar;

3. Kasbiy standartni ishlab chiqishga asos bo‘lgan normativ-huquqiy hujjatlar:

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

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-son Qarori;

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-son Qarori;

O‘zbekiston Respublikasi Prezidentining 2024-yil 30-sentabrdagi “O‘zbekiston Respublikasi milliy malaka tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PQ-345-son Qarori;

O‘zbekiston Respublikasi Prezidentining 2025-yil 20-yanvardagi ““Cyber university” davlat universitetini tashkil etish to‘g‘risida” PQ-14-son Qarori;

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

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2016-yil 24-avgustdagi 275-son “Iqtisodiy faoliyat turlarini tasniflashning xalqaro tizimiga o‘tish chora-tadbirlari to‘g‘risida”gi Qarori (IFUT-2.1);

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2018-yil 5-sentabrdagi “Butunjahon Internet tarmog‘ida axborot xavfsizligini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi 707-sonli Qarori.

4. Ushbu Kasbiy standartda quyidagi qisqartirishlar qo‘llaniladi:

MMR – Milliy malaka ramkasi;

TMR – Tarmoq malaka ramkasi;

IFUT – O‘zbekiston Respublikasi Iqtisodiy faoliyat turlarining umumdavlat tasniflagichi;

MMK – Mashg‘ulotlarning milliy klassifikatori.

II. Kasbiy standartning pasporti

1.	Kasbiy standartning nomi:	Axborot xavfsizligi	
2.	Faoliyatning asosiy maqsadi:	Axborot resurslari, tizimlari va infratuzilmalarining maxfiyligi, yaxlitligi va mavjudligini ta’minlash orqali axborot xavfsizligini ta’minlash.	
3.	IFUT bo‘yicha seksiya, bo‘lim, guruh, sinf va kichik sinf:	K syeksiyasi Aloqa, kompyuter dasturlashtirish, konsalting, hisoblash infratuzilmasi va boshqa axborot xizmatlar sohasidagi faoliyat; 62.9-Axborot texnologiyalari va kompyuter tizimlari sohasidagi boshqa faoliyat turlari; 62.90-Axborot texnologiyalari va kompyuter tizimlari sohasidagi boshqa faoliyat turlari; 62.09.0- Axborot texnologiyalari va kompyuter tizimlari sohasidagi boshqa faoliyat turlari	
4.	Kasbiy standartning qisqacha mazmuni:	Kasbiy standart axborot xavfsizligini ta’minlash sohasidagi mutaxassislarning mehnat faoliyati turlarini, kasbiy vazifa va funksiyalarini, zarur Bilimlar va Ko‘nikmalarlarni, shuningdek, malakalar darajasi bo‘yicha talablarni belgilaydi. Axborot resurslari va tizimlarini tahlil qilish, tahdid va xatarlarni baholash, himoya choralarini ishlab chiqish va joriy etish, axborot xavfsizligi siyosati va normativ hujjatlarini amalga oshirish kabi faoliyat yo‘nalishlarini qamrab oladi.	
5.	Qamrab olingan kasblar ro‘yxati va malaka darajasi:	**Kasblar kodi va nomi:**	**TMR dagi malaka darajasi:**
		35110002 Axborotni himoya qilish bo‘yicha texnik	5
		25291005 Axborot xavfsizligi bo‘yicha professional-mutaxassis	6

III. Kasbiy faoliyat turining funksional xaritasi

Kasblar		Mehnat funksiyalari		Mehnat vazifalari	
T/r	**Kodi va nomi**	**Kodi**	**Nomi**	**Kodi**	**Nomi**
1.	35110002-Axborotni himoya qilish bo‘yicha texnik	A1.5	Axborot tizimlarining xavfsizligini nazorat qilish va texnik himoya vositalarini qo‘llab-quvvatlash	A1.01.5	Texnik himoya vositalarini o‘rnatish va sozlash
				A1.02.5	Axborot tizimida texnik himoya vositalarining ishlash holatini muntazam tekshirish va nazorat qilish
				A1.03.5	Texnik himoya vositalarini yangilab borish va ishlashda yuzaga kelgan muammolarni bartaraf etish
		A2.5	Axborot xavfsizligiga tahdid soluvchi holatlarni aniqlash va bartaraf etishda ishtirok etish	A2.01.5	Axborot tizimlari jurnallarini (loglarini) tahlil qilish orqali shubhali faoliyatni aniqlash
				A2.02.5	Potensial tahdid va buzilish alomatlari yuzasidan axborot xavfsizligi bo‘yicha mutaxassislarga xabar berish
				A2.03.5	Standart ish algoritmi asosida avvaldan belgilangan choralarni qo‘llash orqali tahdidni bartaraf etishda ishtirok etish
2.	25291005-Axborot xavfsizligi bo‘yicha professional-mutaxassis	B1.6	Axborot xavfsizligi siyosati va tartib-qoidalarini ishlab chiqish va joriy etish	B1.01.6	Axborot xavfsizligi sohasidagi milliy va xalqaro standartlar asosida siyosat va tartib-qoidalarni tahlil qilish va loyihalash
				B1.02.6	Axborot xavfsizligi siyosati, qoidalar va protseduralar loyihasini ishlab chiqish va muvofiqlashtirish
				B1.03.6	Ishlab chiqilgan siyosat va qoidalarni tashkilot bo‘ylab joriy etish va ijrosini nazorat qilish
		B2.6	Axborot xavfsizligi holatini tahlil qilish va xatarlarni baholash	B2.01.6	Axborot tizimlarida mavjud xatarlar, zaif nuqtalar va tahdidlarni aniqlash bo‘yicha xavf tahlilini o‘tkazish
				B2.02.6	Xavflarning ehtimoliy ta’sir darajasini va ular yuzaga kelish ehtimolini baholash
				B2.03.6	Xavflarni kamaytirish bo‘yicha tavsiyalar ishlab chiqish va ustuvorlik darajasiga qarab chora-tadbirlar rejasini tuzish

		B3.6	Texnik va tashkiliy himoya choralarini ishlab chiqish va amalga oshirish	B3.01.6	Axborot tizimlarini himoyalash uchun texnik vositalarni tanlash va joriy etish
				B3.02.6	Tashkiliy choralarni ishlab chiqish va joriy etish
				B3.03.6	Joriy qilingan himoya choralarining samaradorligini monitoring qilish va takomillashtirish bo‘yicha takliflar berish
		B4.6	Axborot xavfsizligi bo‘yicha xodimlarni o‘qitish va xabardorlikni oshirish	B4.01.6	Xodimlar uchun axborot xavfsizligiga oid o‘quv dasturlari va materiallarini ishlab chiqish
				B4.02.6	Axborot xavfsizligi bo‘yicha treninglar, seminarlar
				B4.03.6	Xodimlar xabardorlik darajasini baholash va muntazam ravishda tahlil qilish

IV. Kasblar xaritasi va mehnat funksiyalari tavsifi

Kasbning nomi:	Axborotni himoya qilish bo‘yicha texnik
Mashg‘ulot nomining kodi:	35110
TMR bo‘yicha malaka darajasi:	5
Malakani baholash bo`yicha talablar:	Tavsiya etiladi
Amaliy tajriba (ish staji)ga qo‘yilgan talablar:	5-daraja uchun 1 yil ish staji talab etiladi
Layoqatiga va shaxsiy kompetensiyalarga qo‘yilgan talablar:	- 18 yoshga to‘lgan bo‘lishi; - Erkak va ayol; - Ishga kirishda dastlabki tibbiy ko‘rikdan o‘tgan bo‘lishi; - Jismoniy jihatdan sog‘lom bo‘lishi kerak, yurak-qon tomir kasalliklari, orqa-miya muammolari va nafas yo‘llari kasalliklari bo‘lmasligi lozimж - Kasbiy faoliyat doirasida vujudga keladigan turli masalalar yechimini topish usullarini tanlay olish; - Rahbar tomonidan belgilangan maqsadga erishish uchun jamoada ishlay olish; - O‘zining kasbiy malakasini va shaxsiy kamolotini takomillashtirib borish; - Jamoada va ma’lum vazifani bajarishga yo‘naltirilgan guruhda ishlash, hamkasblar, rahbarlar va mijozlar bilan samimiy, xushmuomala hamda samarali muloqot qilish; - Ta’lim olgan tilida fikrini og‘zaki va yozma ravishda ravon bayon qilish; - Umuminsoniy fazilatlarga ega bo‘lish, o‘z millatini va Vatanini sevish, u bilan faxrlanish, milliy urf-odatlar, qadriyatlarni hurmat qilish; - Professional vazifalarni samarali bajarish uchun zarur bo‘ladigan ma’lumotlarni qidirish; - Kasbiy faoliyatida axborot-kommunikatsiya texnologiyalarini qo‘llash; - Kasbga doir hujjatlar bilan ishlash; - Kasbiy faoliyatda xavfsizlik texnikasi va mehnat muhofazasi qoidalariga amal qilish Ko‘nikmalarlariga ega bo‘lish; - Sanoat va nosanoat tashkilotlarda vujudga keladigan chiqindilarni atrof-muhitga zarar yetkazmaslik choralarini ko‘rish va utilizatsiya qilish; - Sohaga oid ekologik madaniyatga rioya qilgan holda faoliyat olib borish.
Ta’lim darajasiga qo‘yilgan talablar:	O‘rta maxsus professional ta’lim
Norasmiy va informal ta’lim bilan bog‘liqligi:	boshlang‘ich professional ta’lim yoki o‘rta professional ta’lim, norasmiy (informal) ta’lim yoki amaliy tajriba

Kasbiy standartlar reestrida mavjudligi:	-	
Kasbning boshqa mumkin bo‘lgan nomlari:	-	
Boshqa kasblar bilan aloqadorligi:	**TMR bo‘yicha malaka darajasi:**	**Kasbning nomi:**
	6	Axborot xavfsizligi bo‘yicha mutaxassis
	6	Axborot himoyasi bo‘yicha mutaxassis
	6	Axborot himoyasi bo‘yicha muhandis
	6	Kiberxavfsizlik bo‘yicha mutaxassis

Mehnat funksiyalarining tasnifi		
Kodi va nomi	**Mehnat vazifalari**	
	O`qitish natijalari	
A1.5 – Axborot tizimlarining xavfsizligini nazorat qilish va texnik himoya vositalarini qo‘llab-quvvatlash	A1.01.5 - Texnik himoya vositalarini o‘rnatish va sozlash	**Mehnat harakatlari:**
		1. Tizimga mos texnik himoya vositalarini tanlash
		2. Himoya vositalarini kompyuter va serverlarga o‘rnatish
		3. Dasturiy ta’minotni xavfsizlik siyosatiga muvofiq sozlash
		4. Foydalanilayotgan tizimlar bilan mosligini tekshirish
		5. O‘rnatilgan himoya vositalarining ishlashini testdan o‘tkazish
		6. Sozlangan tizimni ekspluatatsiyaga topshirish va hujjatlashtirish
		Ko‘nikmalar:
		Himoya dasturlarini o‘rnatish va konfiguratsiya qilish
		Tarmoq xavfsizligi vositalari bilan ishlash
		Operatsion tizim va dasturlar mosligini tekshirish
		Test sinovlarini o‘tkazish va natijalarni tahlil qilish
		Texnik hujjat tayyorlash va foydalanishga topshirish
		Bilimlar:
		Axborot xavfsizligi asoslari va xavf turlari
		Texnik himoya vositalari turlari va ularning ishlash tamoyillari
		Operatsion tizimlar asoslari
		Tizim xavfsizlik siyosatlari va sozlamalari
		Dasturiy ta’minot o‘rnatish va yangilash jarayonlari
		Tizimlararo moslik va nosozliklarni aniqlash tamoyillari
		Mehnat harakatlari:
		1. O‘rnatilgan texnik himoya vositalarining holatini tekshirish
		2. Himoya tizimlarining log va xatolik yozuvlarini tahlil qilish

	A1.02.5 - Axborot tizimida texnik himoya vositalarining ishlash holatini muntazam tekshirish va nazorat qilish	3. Aniqlangan nosozliklar yoki xavflar yuzasidan ma’lumotlarni yig‘ish va hisobot tayyorlash
		4. Himoya vositalarini yangilash va ularning holatini testdan o‘tkazish
		5. Tizim xavfsizligi bo‘yicha rejali monitoringni amalga oshirish va natijalarni hujjatlashtirish
		Ko‘nikmalar:
		Himoya vositalarining ishlashini monitoring qilish
		Log-fayllar va tahlil vositalaridan foydalanish
		Nosozliklarni aniqlash va hujjatlashtirish
		Yangilash va texnik xizmat ko‘rsatishni amalga oshirish
		Xavfsizlik holati bo‘yicha hisobot tayyorlash
		Bilimlar:
		Texnik himoya vositalari ishlash prinsiplari
		Tizim monitoringi va log-fayllarni o‘qish asoslari
		Operatsion tizimlar va tarmoq xavfsizligi asoslari
		Texnik xizmat reglamentlari va xavfsizlik siyosatlari
		Axborot xavfsizligi muammolarini aniqlash metodlari
	A1.03.5- Texnik himoya vositalarini yangilab borish va ishlashda yuzaga kelgan muammolarni bartaraf etish	**Mehnat harakatlari:**
		1. O‘rnatilgan texnik himoya vositalarining versiyalarini tekshirish va yangilanish zaruriyatini aniqlash
		2. Dasturiy ta’minotni yangilash yoki patchlarni o‘rnatish orqali tizimni aktual holatga keltirish
		3. Yuzaga kelgan xatolik va nosozliklarni aniqlab, diagnostika qilish
		4. Nosozliklarni bartaraf etish uchun mos texnik choralarni ko‘rish
		5. Ko‘rilgan choralar natijasini sinovdan o‘tkazish va ish faoliyatini tiklash
		6. Amalga oshirilgan ishlarga oid hisobot va texnik hujjatlarni tayyorlash
		Ko‘nikmalar:
		Himoya dasturlarini yangilash va sozlash
		Patch o‘rnatish orqali xavfsizlikni ta’minlash
		Nosozliklarni tahlil qilish va bartaraf etish
		Tizim holatini sinovdan o‘tkazish va monitoring qilish
		Amalga oshirilgan ishlarga oid texnik hisobot tuzish
		Bilimlar:
		Texnik himoya vositalari ishlash prinsiplari
		Dasturiy yangilanishlar va patch tushunchasi
		Diagnostika vositalari va muammolarni aniqlash usullari
		Operatsion tizim va tarmoq arxitekturasi asoslari
		Texnik himoya vositalari ishlash prinsiplari
		1. Xavfsizlikka tahdid soluvchi holatlarni aniqlashda faol ishtirok etish va tegishli choralarni ko‘rish

	Mas’uliyat va mustaqillik:	2. Amalga oshirilgan ishlar haqida hujjatlashtirish va axborot xavfsizligiga oid talablarni rioya qilish uchun javobgarlik
		3. Belgilangan texnik reglamentlar asosida o‘z vazifalarini mustaqil bajarish
		4. Oddiy va o‘rtacha darajadagi texnik muammolarni hal qilishda mustaqil qaror qabul qilish
		5. Tahdid holatlarini baholash va dastlabki texnik choralarni ko‘rish
A2.5- Axborot xavfsizligiga tahdid soluvchi holatlarni aniqlash va bartaraf etishda ishtirok etish	A2.01.5- Axborot tizimlari jurnallarini (loglarini) tahlil qilish orqali shubhali faoliyatni aniqlash	**Mehnat harakatlari:**
		1. Axborot tizimlariga oid log fayllarni muntazam yig‘ish va saqlash
		2. Tizim jurnallarini tahlil qilish uchun vositalardan foydalanish
		3. Shubhali harakatlar, kirish urinishlari va xavfsizlik buzilish belgilarini aniqlash
		4. Aniqlangan tahdidlar haqida axborot xavfsizligi bo‘yicha mas’ullarga xabar berish
		5. Tahlil natijalarini hujjatlashtirish va hisobot tayyorlash
		Ko‘nikmalar:
		Tizim loglarini o‘qish va tahlil qilish
		SIEM (Security Information and Event Management) tizimlaridan foydalanish
		Shubhali faoliyat belgilarini aniqlash va ularni hujjatlashtirish
		Anomaliyalar asosida xavfsizlik tahdidlarini baholash
		Tahlil natijalarini tushunarli shaklda ifodalash va hisobot tuzish
		Bilimlar:
		Axborot tizimlarining ishlash tamoyillari va jurnal (log) yozuvlari tuzilmasi
		Xavfsizlik tahdidlari, buzilish belgilari va hujum turlari
		Log tahlili vositalari va dasturlarining ishlash prinsiplari
		Korxona axborot xavfsizligi siyosatlari va tartib-qoidalari
		Maxfiylik, yaxlitlik va mavjudlik (CIA triadasi) prinsiplari
	A2.02.5- Potensial tahdid va buzilish alomatlari yuzasidan axborot xavfsizligi bo‘yicha mutaxassislarga xabar berish	**Mehnat harakatlari:**
		1. Tizim monitoringi orqali aniqlangan shubhali faoliyatlarni qayd etish
		2. Tahdidga oid dalillarni yig‘ish va dastlabki tahlilini o‘tkazish
		3. Buzilish yoki tahdid alomatlarini axborot xavfsizligi mutaxassisiga belgilangan tartibda yetkazish
		4. Axborot uzatishda maxfiylik va aniqlik talablariga rioya qilish
		5. Xabarnomalar va rasmiy hisobotlarni rasmiylashtirish va topshirish
		Ko‘nikmalar:
		Axborotni tahlil asosida aniq va lo‘nda tarzda ifodalash

		Axborot xavfsizligi bo‘yicha aloqalarni tezkor tashkil etish
		Hodisalarni hujjatlashtirish va ustuvorlik bo‘yicha tasniflash
		Xabarnoma va ogohlantirishlarni tegishli formatda rasmiylashtirish
		Zudlik bilan xabar yetkazish bo‘yicha ichki tartiblarni qo‘llay bilish
		Bilimlar:
		Tashkilotda tahdid holatlari bo‘yicha xabar berish protokollari
		Favqulodda vaziyatlarda aloqa kanallaridan foydalanish qoidalari
		Xavfsizlik insidentlari turlari va ularning ustuvorlik darajalari
		Mutasaddi mutaxassislar va bo‘linmalarning vakolat doirasi
		Tizimli hisobot berish va hujjat aylanishi asoslari
	A2.03.5-Standart ish algoritmi asosida avvaldan belgilangan choralarni qo‘llash orqali tahdidni bartaraf etishda ishtirok etish	**Mehnat harakatlari:**
		1. Tahdid holatini aniqlab, unga mos choralar algoritmini tanlash
		2. Belgilangan instruktsiyalar asosida tizim resurslariga vaqtinchalik cheklovlar qo‘yish
		3. Muammoli foydalanuvchi seansini yakunlash yoki bloklash
		4. Tizimdagi xavfli xizmatlarni vaqtincha to‘xtatish orqali tarqalishni cheklash
		5. Ko‘rilgan chora-tadbirlar bo‘yicha hisobot tayyorlash va tegishli mutaxassislarga yetkazish
		Ko‘nikmalar:
		Belgilangan xavfsizlik algoritmlarini amalda qo‘llash
		Xavfni cheklovchi choralarni tizimli va izchil bajara olish
		Muammoli foydalanuvchilar va resurslar bilan ishlashni muvofiqlashtirish
		Vaqtli hisoboti va to‘plangan ma’lumotlarni to‘g‘ri taqdim eta olish
		Bilimlar:
		Axborot xavfsizligi hodisalariga nisbatan tezkor chora ko‘rish algoritmlari
		Tizimni izolyatsiya qilish usullari va vaqtinchalik xavfsizlik rejimlari
		Xavfsizlik devori, kirish nazorati va monitoring vositalari bilan ishlash asoslari
		Hodisalar tarixini qayd etuvchi jurnal (log) yozuvlari
		Muvofiqlikni saqlagan holda xavfsizlik bo‘limi bilan o‘zaro hamkorlik qilish qoidalari

	Mas’uliyat va mustaqillik:	1. Axborot tizimlarining ishlash holatini muntazam kuzatib borish va tahdid alomatlarini aniqlash uchun javobgar
		2. Avvaldan belgilangan choralarni (standart operatsion algoritm asosida) aniq va to‘g‘ri qo‘llash orqali hodisaga tezkor javob berish
		3. Oddiy tahdid holatlarida – texnik himoya vositalari (antivirus, fayrvol, IDS/IPS) orqali aniqlangan shubhali faoliyatga nisbatan mustaqil tarzda standart choralarni qo‘llash
		4. O‘z faoliyati doirasida qaror qabul qilish vakolatiga ega
Texnik va/yoki texnologik talab		- Firewall (tarmoqlararo himoya devorlari); - IDS/IPS tizimlari (xavfsizlikni buzishlarni aniqlash va oldini olish); - VPN (Virtual shaxsiy tarmoq qurilmalari); - SIEM (Security Information and Event Management) tizimlari: Splunk, QRadar, ELK Stack; - Log tahlilchi dasturlar: Graylog, SolarWinds; - Kaspersky Endpoint Security, ESET, Symantec, Bitdefender; - Serverlar, router va switchlar; - Maxsus xavfsizlik modullari (HSM – Hardware Security Module); - Patch management tizimlari: WSUS, ManageEngine Patch Manager; - Tarmoq skanerlari: Nmap, Wireshark; - Konfiguratsiyani boshqarish vositalari: Ansible, Puppet (soddalashtirilgan foydalanuvchi uchun); - GRC (Governance, Risk, and Compliance) platformalari; - Elektron pochta xavfsizligi tizimlari (Mail Gateway, SPF/DKIM/DMARC); - Operatsion tizimlar: Windows Server, Linux distributivlari (Debian, CentOS); - Virtualizatsiya vositalari: VMware, VirtualBox (sinov muhitida); - Incident response toolkit (sozlangan skriptlar, avtomatlashtirish vositalari); - Backup va tiklash vositalari: Acronis, Veeam.

Kasbning nomi:	Axborot xavfsizligi bo‘yicha professional-mutaxassis
Mashg‘ulot nomining kodi:	25291
TMR bo‘yicha malaka darajasi:	6
Malakani baholash bo`yicha talablar:	Malakani baholash markazlarida tavsiya etilmaydi
Amaliy tajriba (ish staji)ga qo‘yilgan talablar:	6-daraja uchun 1 yil ish staji talab etiladi
Layoqatiga va shaxsiy kompetensiyalarga qo‘yilgan talablar:	- 18 yoshga to‘lgan bo‘lishi; - erkak va ayol; - Ishga kirishda dastlabki tibbiy ko‘rikdan o‘tgan bo‘lishi; - Jismonan sog‘lom va stressga chidamli bo‘lishi kerak, uzoq vaqt ishlash qobiliyatiga ega bo‘lish; - Kasbiy faoliyat doirasida vujudga keladigan turli masalalar yechimini topish usullarini tanlay olish; - Rahbar tomonidan belgilangan maqsadga erishish uchun jamoada ishlay olish; - O‘zining kasbiy malakasini va shaxsiy kamolotini takomillashtirib borish; - Jamoada va ma’lum vazifani bajarishga yo‘naltirilgan guruhda ishlash, hamkasblar, rahbarlar va mijozlar bilan samimiy, xushmuomala hamda samarali muloqot qilish; - Ta’lim olgan tilida fikrini og‘zaki va yozma ravishda ravon bayon qilish; - Umuminsoniy fazilatlarga ega bo‘lish, o‘z millatini va Vatanini sevish, u bilan faxrlanish, milliy urf-odatlar, qadriyatlarni hurmat qilish; - Professional vazifalarni samarali bajarish uchun zarur bo‘ladigan ma’lumotlarni qidirish; - Kasbiy faoliyatida axborot-kommunikatsiya texnologiyalarini qo‘llash; - Kasbga doir hujjatlar bilan ishlash; - Kasbiy faoliyatda xavfsizlik texnikasi va mehnat muhofazasi qoidalariga amal qilish Ko‘nikmalarlariga ega bo‘lish; - Sanoat va nosanoat tashkilotlarda vujudga keladigan chiqindilarni atrof-muhitga zarar yetkazmaslik choralarini ko‘rish va utilizatsiya qilish; - Sohaga oid ekologik madaniyatga rioya qilgan holda faoliyat olib borish
Ta’lim darajasiga qo‘yilgan talablar:	Bakalavriat
Norasmiy va informal ta’lim bilan bog‘liqligi:	o‘rta maxsus professional ta’lim va amaliy tajriba
Kasbiy standartlar reestrida mavjudligi:	-

Kasbning boshqa mumkin bo‘lgan nomlari:	Axborot xavfsizligi bo‘yicha mutaxassis	
Boshqa kasblar bilan aloqadorligi:	**TMR bo‘yicha malaka darajasi:**	**Kasbning nomi:**
	6	Axborot himoyasi bo‘yicha mutaxassis
	6	Axborot himoyasi bo‘yicha muhandis
	6	Axborot va psixologiya xavfsizligi bo‘yicha mutaxassis

Mehnat funksiyalarining tasnifi		
Kodi va nomi	**Mehnat vazifalari**	
	O`qitish natijalari	
B1.6- Axborot xavfsizligi siyosati va tartib-qoidalarini ishlab chiqish va joriy etish	B1.01.6- Axborot xavfsizligi sohasidagi milliy va xalqaro standartlar asosida siyosat va tartib-qoidalarni tahlil qilish va loyihalash	**Mehnat harakatlari:**
		1. Amaldagi milliy va xalqaro axborot xavfsizligi standartlarini (masalan, ISO/IEC 27001, ISO/IEC 27002, GOST) o‘rganish va tahlil qilish
		2. Tashkilot faoliyatiga mos axborot xavfsizligi siyosati va tartib-qoidalarining loyihasini ishlab chiqish
		3. Siyosat loyihalarini manfaatdor tomonlar bilan muvofiqlashtirish va hujjatlashtirish
		4. Tavsiya etilgan siyosat va tartib-qoidalarni xavflarni baholash natijalari asosida optimallashtirish
		5. Loyiha hujjatlarini rahbariyat ko‘rib chiqishi va tasdiqlashi uchun tayyorlash
		Ko‘nikmalar:
		Axborot xavfsizligiga oid siyosiy va normativ hujjatlarni tahlil qilish
		ISO/IEC 27001 va boshqa xalqaro standartlar asosida siyosat loyihalash
		Hujjatlar bilan aniq ishlash va ularni rasmiylashtirish
		Manfaatdor tomonlar bilan samarali aloqa o‘rnatish va fikr almashish
		Axborot xavfsizligi risklarini aniqlash va baholashga asoslangan yondashuvdan foydalanish
		Axborot xavfsizligiga oid siyosiy va normativ hujjatlarni tahlil qilish
		Bilimlar:
		Axborot xavfsizligi bo‘yicha milliy me’yoriy hujjatlar
		Xalqaro standartlar
		Siyosat hujjatlari tuzilmasi va ularga qo‘yiladigan talablar
		Tashkilot axborot tizimlari va ulardagi xavfsizlik ehtiyojlari
		Axborot xavfsizligiga oid muammolarni huquqiy va texnik nuqtayi nazardan baholash asoslari

	B1.02.6- Axborot xavfsizligi siyosati, qoidalar va protseduralar loyihasini ishlab chiqish va muvofiqlashtirish	**Mehnat harakatlari:**
		1. Tashkilot xavfsizlik ehtiyojlarini aniqlash va hujjatlashtirish
		2. Axborot xavfsizligi siyosatining loyihasini ishlab chiqish
		3. Amaliy qoidalar va protseduralarni siyosat bilan muvofiqlashtirib ishlab chiqish
		4. Loyiha hujjatlarini manfaatdor tomonlar bilan kelishish
		5. Tavsiyalar va fikrlar asosida hujjat loyihasini takomillashtirish
		6. Tasdiqlangan siyosat va protseduralarni ichki tizimlarga joriy qilish bo‘yicha ko‘rsatmalar tayyorlash
		Ko‘nikmalar:
		Axborot xavfsizligi hujjatlarini loyihalash va tuzish
		Siyosat, qoidalar va protseduralarni tashkilot ehtiyojlariga moslashtirish
		Manfaatdor tomonlar bilan muvofiqlashtirish va kelishish jarayonini olib borish
		Axborot xavfsizligi bo‘yicha me’yoriy hujjatlar bilan ishlash
		Hujjatlar aylanishini boshqarish va rasmiylashtirish
		Bilimlar:
		Milliy va xalqaro axborot xavfsizligi standartlari
		Tashkilotning axborot xavfsizligi siyosatiga qo‘yiladigan talablar
		Siyosat va protseduralar hujjatlarini tuzishning metodologiyasi
		Huquqiy va tartibga soluvchi asoslar
		Axborot xavfsizligida risklarni boshqarish tamoyillari
	B1.03.6- Ishlab chiqilgan siyosat va qoidalarni tashkilot bo‘ylab joriy etish va ijrosini nazorat qilish	**Mehnat harakatlari:**
		1. Axborot xavfsizligi siyosati va qoidalarini tashkilot bo‘limlariga yetkazish
		2. Siyosat va qoidalarning joriy etilishi bo‘yicha reja tuzish va amalga oshirish
		3. Hodimlarga axborot xavfsizligi bo‘yicha amaliy ko‘rsatmalar berish
		4. Siyosat ijrosini monitoring qilish va aniqlangan kamchiliklarni tahlil qilish
		5. Amalga oshirish natijalari yuzasidan rahbariyatga hisobot tayyorlash
		Ko‘nikmalar:
		Siyosat va tartib-qoidalarni joriy etish bosqichlarini tashkil etish va muvofiqlashtirish
		Hodimlarga amaliy yo‘riqnomalar berish va nazorat qilish
		Jarayonlar monitoringi asosida tahlil va xulosa chiqarish

		Rahbariyatga aniq va tizimli hisobotlar tayyorlash
		Bilimlar:
		Axborot xavfsizligi bo‘yicha milliy va xalqaro siyosatlar asoslari
		Siyosatlarni joriy etish metodologiyasi va tartiblari
		Axborot xavfsizligi auditi va nazorat vositalari
		Korporativ kommunikatsiya asoslari va jamoa bilan ishlash madaniyati
	Mas’uliyat va mustaqillik:	1. Siyosat va qoidalarning barcha bo‘limlarda to‘g‘ri joriy etilishi va bajarilishini ta’minlash.
		2. Siyosatni amaliyotga joriy etishda tashkil etish va nazorat qilish ishlarini mustaqil olib boradi.
B2.6- Axborot xavfsizligi holatini tahlil qilish va xatarlarni baholash	B2.01.6- Axborot tizimlarida mavjud xatarlar, zaif nuqtalar va tahdidlarni aniqlash bo‘yicha xavf tahlilini o‘tkazish	**Mehnat harakatlari:**
		1. Axborot tizimlarining tuzilmasi va ishlashini tahlil qilish
		2. Tizimdagi zaif nuqtalarni aniqlash uchun skanerlash vositalaridan foydalanish
		3. Potensial tahdidlar va ularga mos xatar ssenariylarini aniqlash
		4. Topilgan xatarlar bo‘yicha xavf darajasini baholash
		5. Tahlil natijalarini hujjatlashtirish va tegishli mutasaddilarga taqdim etish
		Ko‘nikmalar:
		Tizim arxitekturasi va xavfsizlik holatini tahlil qilish.
		Zaifliklarni aniqlash uchun skanerlash va diagnostika vositalaridan foydalanish.
		Xatar darajasini aniqlash va xavf ssenariylarini tuzish.
		Tahlil natijalarini hujjatlashtirish va tushunarli tarzda taqdim etish
		Bilimlar:
		Axborot xavfsizligi bo‘yicha xavf tahlili usullari
		Zaifliklar bazalari va standartlari
		Tarmoq va tizim xavfsizligi asoslari
		Skanerlash vositalari
		Tashkilotning texnik infratuzilmasi va xavfsizlik siyosatiga oid asosiy talablar
	B2.02.6- Xavflarning ehtimoliy ta’sir darajasini va ular yuzaga kelish ehtimolini baholash	**Mehnat harakatlari:**
		1. Har bir aniqlangan xavf uchun zararning miqyosini baholash
		2. Tahdidlarning yuzaga kelish ehtimolligini aniqlash
		3. Ehtimollik va ta’sir darajasi asosida xavf prioritetlarini belgilash
		4. Baholash natijalarini xavf xaritasi yoki jadvalda aks ettirish
		5. Tavakkal darajasiga qarab xavfsizlik choralari bo‘yicha tavsiyalar ishlab chiqish

		Ko‘nikmalar:
		Tahdidlarning ta’sir doirasini va yuzaga kelish ehtimolini tahlil qilish
		Risk darajasini ustuvorlikka qarab baholash va saralash
		Baholash natijalarini vizual vositalar orqali ifodalash
		Olingan natijalar asosida xavfsizlik tavsiyalari ishlab chiqish
		Bilimlar:
		Axborot xavfsizligida xavf baholash modellari
		Kvant va sifat baholash usullari
		Xavflarni tavsiflash va tasniflash mezonlari
		Tashkilotdagi axborot aktivlarining qiymati va ularning zaiflik darajalari
		Risklarni kamaytirish strategiyalari
	B2.03.6-Xavflarni kamaytirish bo‘yicha tavsiyalar ishlab chiqish va ustuvorlik darajasiga qarab chora-tadbirlar rejasini tuzish	**Mehnat harakatlari:**
		1.Xavf tahlili natijalariga asoslanib, bartaraf etish variantlarini ishlab chiqish
		2.Har bir xavf bo‘yicha ustuvorlikni aniqlab, chora-tadbirlarni tartiblash
		3.Texnik, tashkiliy yoki yondashuvga oid xavfsizlik choralarini rejalashtirish
		4.Chora-tadbirlar rejasini manfaatdor tomonlarga taqdim etish va kelishish
		5.Amalga oshirish bosqichlarini aniqlab, ijro nazorat mexanizmini belgilash
		Ko‘nikmalar:
		Xavflarni bartaraf etish va kamaytirish strategiyalarini ishlab chiqish
		Chora-tadbirlarni ustuvorlikka qarab tartiblash va rejalashtirish
		Rejani amaliy bosqichlarga bo‘lish va monitoring mexanizmini belgilash
		Tavsiyalarni manfaatdor tomonlarga asosli tarzda taqdim etish
		Bilimlar:
		Xavf menejmenti bosqichlari va tavakkalni kamaytirish strategiyalari
		Xavfsizlik bo‘yicha xalqaro tavsiyalar
		Texnik va tashkiliy xavfsizlik choralarining farqlari va qo‘llash shartlari
		Qaror qabul qilishda ustuvorlik baholash metodlari
		Loyihalashtirilgan choralarni amalga oshirishga oid nazorat va baholash usullari

	Mas’uliyat va mustaqillik:	1. Tahlil natijalarini rasmiy ravishda hujjatlashtirish va manfaatdor tomonlarga yetkazish
		2. Risklarni noto‘g‘ri baholash oqibatida yuzaga kelishi mumkin bo‘lgan salbiy holatlarga nisbatan mas’ul bo‘lish
		3. Xavf tahlili va baholash jarayonlarini tanqidiy fikrlash asosida mustaqil amalga oshiradi
		4. Chora-tadbirlar rejasini ishlab chiqishda tashqi bosimlarsiz, faqat tahlil natijalariga tayangan holda qaror qabul qiladi
		5. Faqat strategik tavsiyalar bo‘yicha rahbariyat bilan muvofiqlashtiradi, tahlil va texnik xulosalarda to‘liq mustaqillikka ega
B3.6- Texnik va tashkiliy himoya choralarini ishlab chiqish va amalga oshirish	B3.01.6- Axborot tizimlarini himoyalash uchun texnik vositalarni tanlash va joriy etish	**Mehnat harakatlari:**
		1. Tizim tahlili asosida zarur xavfsizlik vositalari ro‘yxatini shakllantirish
		2. Mos texnik himoya yechimlarini funksional va muvofiqlik jihatidan baholash
		3. Tanlangan vositalarni sinovdan o‘tkazish va joriy qilish jarayonini rejalashtirish
		4. Himoya vositalarini tizimga integratsiya qilish va sozlash ishlarini amalga oshirish
		5. Texnik choralar ishlashini tekshirish va monitoring mexanizmini yo‘lga qo‘yish
		Ko‘nikmalar:
		Himoya vositalarining texnik xususiyatlarini baholash va tanlash
		Texnik vositalarni tizimga integratsiya qilish va sozlash
		Sinovdan o‘tkazilgan himoya yechimlarining samaradorligini tahlil qilish
		Turli ishlab chiqaruvchilarning xavfsizlik vositalarini solishtirish va amaliy qo‘llash
		Bilimlar:
		Tarmoq xavfsizligi vositalari: IDS/IPS, DLP, WAF, NGFW ishlash prinsipi
		Operatsion tizimlar va axborot tizimlarining himoyalanish talablari
		Texnik vositalarning standartlari va sertifikatsiya mezonlari
		Texnik xavfsizlik vositalarini joriy etish bosqichlari va hujjatlashtirish talablari
		Tashkilot infratuzilmasi bilan muvofiqlikni ta’minlash uchun texnik tahlil

	B3.02.6- Tashkiliy choralarni ishlab chiqish va joriy etish	**Mehnat harakatlari:**
		1. Xavfsizlik siyosati, tartib va protseduralar asosida tashkiliy choralar loyihasini ishlab chiqish
		2. Xodimlar uchun axborot xavfsizligi bo‘yicha majburiy amaliy qoidalarni belgilash
		3. Tashkilotdagi rollar va javobgarliklarni xavfsizlik nuqtai nazaridan taqsimlash
		4. Amalga oshirilayotgan choralarni tegishli bo‘limlar bilan muvofiqlashtirish
		5. Joriy etilgan tashkiliy choralar ijrosini monitoring qilish va baholash
		Ko‘nikmalar:
		Himoya choralarining ishlash natijalarini tahlil qilish
		Monitoring vositalaridan foydalangan holda xavfsizlik darajasini baholash
		Kamchiliklarni aniqlab, takomillashtirish bo‘yicha asosli takliflar tayyorlash
		Xavfsizlik ko‘rsatkichlarini muntazam kuzatish va hujjatlashtirish
		Bilimlar:
		Axborot xavfsizligi samaradorligini o‘lchovchi indikatorlar
		Monitoring tizimlari ishlash prinsipi
		Tahlil asosida chora-tadbirlarni optimallashtirish metodlari
		Takomillashtirish sikli: rejalashtirish, bajarish, tekshirish va harakat
		Texnik va tashkiliy choralar o‘rtasidagi uzviy bog‘liqlik va ularning samaradorlik tahlili
	B3.03.6- Joriy qilingan himoya choralarining samaradorligini monitoring qilish va takomillashtirish bo‘yicha takliflar berish	**Mehnat harakatlari:**
		1. Amalga oshirilgan himoya choralarining ishlashini monitoring qilish
		2. Kamchilik va zaif jihatlarni aniqlash bo‘yicha tahlillar o‘tkazish
		3. Takomillashtirish uchun texnik yoki tashkiliy choralar yuzasidan takliflar ishlab chiqish
		Ko‘nikmalar:
		Monitoring tizimlaridan (SIEM, IDS/IPS) foydalanish
		Tahliliy fikrlash va nosozliklarni aniqlash
		Takliflarni hujjatlashtirish va asoslash
		Bilimlar:
		Axborot xavfsizligi standartlari
		Himoya choralarining texnik va tashkiliy turlari
		Xavfsizlik monitoringi va tahlil uslublari

	Mas’uliyat va mustaqillik:	1. Texnik va tashkiliy choralarni tashkilotning xavfsizlik talablariga muvofiq ishlab chiqish va joriy etishga mas’ul
		2. Tashkilot miqyosida xavfsizlikni ta’minlashga xizmat qiluvchi taklif va yechimlar uchun javobgar
		3. Tashkiliy choralarni ishlab chiqishda mavjud siyosatlarga asoslangan holda o‘z tashabbuslarini ilgari surish
		4. Monitoring natijalariga tayangan holda mustaqil tahlil qilish va takomillashtirish bo‘yicha takliflar berish
B4.6- Axborot xavfsizligi bo‘yicha xodimlarni o‘qitish va xabardorlikni oshirish	B4.01.6- Xodimlar uchun axborot xavfsizligiga oid o‘quv dasturlari va materiallarini ishlab chiqish	**Mehnat harakatlari:**
		1. Tashkilot ehtiyojlariga mos axborot xavfsizligi mavzularini aniqlash
		2. Amaliy va nazariy qamrovga ega o‘quv dasturi tarkibini ishlab chiqish
		3. Treninglar, prezentatsiyalar va test materiallarini tayyorlash
		4. O‘quv materiallarini aktual holatda saqlash va muntazam yangilab borish
		5. O‘quv materiallarini tashkilotdagi tegishli bo‘limlar bilan kelishish
		Ko‘nikmalar:
		Mavjud xavfsizlik siyosati asosida o‘quv materiallarini loyihalash
		Murakkab texnik tushunchalarni sodda va tushunarli shaklda ifodalash
		Trening materiallarini tayyorlashda vizual va interaktiv vositalardan foydalanish
		Turli darajadagi xodimlar uchun moslashtirilgan o‘quv kontentini ishlab chiqish
		Bilimlar:
		Axborot xavfsizligi asoslari va xodimlar uchun muhim xavfsizlik qoidalari
		O‘quv metodikasi, taqdimot va trening vositalari bilan ishlash tamoyillari
		Yetakchi xalqaro standartlar bo‘yicha xodimlar xabardorligini oshirish usullari
		Tashkilotda o‘quv ehtiyojlarini aniqlash va ularga mos o‘quv yechimlarini ishlab chiqish usullari
		E-learning va offline ta’lim shakllari uchun mos formatlarni tanlash va loyihalash asoslari
		Mehnat harakatlari:
		1. Trening va seminar mavzularini tashkilot ehtiyojlariga muvofiq rejalashtirish
		2. Tadbir o‘tkazish formatini belgilash

	B4.02.6- Axborot xavfsizligi bo‘yicha treninglar, seminarlar va interaktiv mashg‘ulotlarni tashkil etish va o‘tkazish	3. Mashg‘ulotlar uchun texnik vositalar va o‘quv muhitini tayyorlash
		4. Ishtirokchilarni ro‘yxatga olish va jadval bo‘yicha xabardor qilish
		5. Trening va mashg‘ulotlarni o‘tkazish, baholash va ishtirokchilar fikrini yig‘ish
		Ko‘nikmalar:
		Trening va seminarlarni tashkiliy jihatdan rejalashtirish va o‘tkazish
		Texnik va interaktiv o‘quv uslublarini qo‘llash
		Ishtirokchilar bilan samarali muloqot o‘rnatish va bilimlarini baholash
		O‘quv materiallarini amaliy mashg‘ulotlarga moslashtirish
		Bilimlar:
		Axborot xavfsizligi sohasidagi asosiy xavf-xatarlar va foydalanuvchi xatti-harakatlari
		Pedagogik metodlar: yetkazish uslublari, didaktik vositalar, interaktiv yondashuvlar
		Trening samaradorligini baholash usullari
		Voqea-senariliy mashg‘ulotlar, test va viktorinalar tashkiloti
		Xodimlar bilimini oshirish bo‘yicha xalqaro tajribalar va tendensiyalar
	B4.03.6- Xodimlar xabardorlik darajasini baholash va muntazam ravishda tahlil qilish	**Mehnat harakatlari:**
		Xodimlar uchun testlar, so‘rovnomalar yoki baholovchi topshiriqlarni ishlab chiqish
		Baholash natijalarini tizimli tarzda yig‘ish va tahlil qilish
		Xabardorlikdagi bo‘shliqlarni aniqlash va ularni bartaraf etish bo‘yicha tavsiyalar tayyorlash
		Hisobotlar tayyorlash va rahbariyatga taqdim etish
		Baholash natijalariga asoslangan holda o‘quv dasturlarini qayta ko‘rib chiqish
		Ko‘nikmalar:
		Baholash vositalarini tuzish va qo‘llash
		Tahliliy dasturlar yoki elektron platformalar yordamida ma’lumotlarni qayta ishlash
		Olingan natijalarni tahlil qilish va ularga asoslangan xulosa chiqarish
		Xodimlar samaradorligini monitoring qilish va takomillashtirish rejasini ishlab chiqish
		Bilimlar:
		Axborot xavfsizligiga oid xodimlar uchun zarur bilim darajasi mezonlari
		Baholash metodlari va diagnostika usullari

		Statistik tahlil asoslari va hisoboti shakllari
		O‘quv samaradorligini o‘lchash mezonlari
		Tahlil asosida xavfsizlik bo‘yicha qaror qabul qilish mexanizmlari
	Mas’uliyat va mustaqillik:	1. O‘quv dasturlari va trening materiallarining aniqligi, dolzarbligi va tashkilot siyosatiga muvofiqligi uchun javobgarlik
		2. Mashg‘ulotlar sifati va xodimlarning bilim darajasini oshirish natijalari uchun javob berish
		3. Xabardorlik darajasi bo‘yicha olingan ma’lumotlarning tahliliy aniqligi va asoslangan xulosalar uchun javobgarlik
		4. O‘quv mazmuni, metodikasi va baholash shakllarini tanlashda mustaqil qaror qabul qilish
		5. Trening va seminarlarni tashkil qilish va o‘tkazishda tashkiliy erkinlik
		6. Xodimlar o‘rganish ehtiyojlariga mos yechimlar ishlab chiqish va taklif etishda mustaqillik bilan harakat qilish
Texnik va/yoki texnologik talab		- Microsoft Word, Google Docs – siyosat va reglamentlarni yozish; - ISO 27001 Toolkit (CertiKit, ISMS.online) – siyosat va standartlar asosida hujjatlar tayyorlash; - SharePoint, Confluence – hujjatlarni saqlash, ulashish va hamkorlikda ishlash; - Nessus, OpenVAS – avtomatik zaifliklarni aniqlash; - Splunk, IBM QRadar – xavfsizlik hodisalarini SIEM asosida tahlil qilish; - RiskLens, RSA Archer – xavf baholash va ustuvorliklarni aniqlash; - Firewall: Cisco ASA, pfSense – kiruvchi/chiquvchi axborotni nazorat qilish; - IDS/IPS: Snort, Suricata – hujumlarni aniqlash va to‘xtatish; - EDR: CrowdStrike, Kaspersky EDR – kompyuterlar uchun ilg‘or himoya; - DLP: Symantec, McAfee – ma’lumotlar oqishini oldini olish; - MDM: Microsoft Intune – mobil qurilmalarni boshqarish;

V. Kasbiy standartning texnik ma’lumotlari

5.1. Kasbiy standartning rekvizitlari

1.	Kasbiy malakalarni rivojlantirish bo‘yicha tarmoq kengashining tasdiqlash hujjatlari:	Axborot texnologiyalari va aloqa sohasida kasbiy malakalarni rivojlantirish bo‘yicha tarmoq kengashining 2026-yil 13-fevraldagi 3/29-son bayoni
2.	Milliy malaka tizimini rivojlantirish institutining xulosasi:	KS-0057-son xulosa, 20.02.2026
3.	Kasbiy standart talqini va ishlab chiqilgan sanasi:	1.0-talqin, 12.01.2026
4.	Taxminiy qayta ko‘rib chiqish sanasi:	20.01.2031

5.2. Kasbiy standartni ishlab chiqishga mas’ul tashkilot

“Raqamli hukumat loyihalarini boshqarish markazi” DM

(tashkilot nomi)

Direktori **Mansurov Anvar Rustamovich**

(rahbarning lavozimi, imzosi va F.I.O.)

5.3. Kasbiy standartni ishlab chiqishda ishtirok etgan tashkilot (korxona)lar to‘g‘risida ma’lumot

T/r	Ishlab chiquvchilar to‘g‘risida ma’lumot	
	Ish joyi va lavozimi	**Familiyasi, ismi, otasining ismi**
1.	Raqamli texnologiyalar vazirligi Kasbiy malakalarni rivojlantirish bo‘yicha bosh mutaxassisi	Axmedov B.R.
2.	“Respublika maxsus aloqa bog‘lamasi” DUK kadrlar bo‘limi boshlig‘i	Kasimova G.T.
3.	“O‘zkomnazorat” inspeksiyasi “Raqamli texnologiyalar sohasida nazorat qilish” boshqarmasi boshlig‘i	Ashirbayev E.
4.	“Dasturiy mahsulotlar va axborot texnologiyalari texnologik parki direksiyasi” MCHJ yetakchi iqtisodchisi	Ergashev A.Y.
5.	"O‘zbekiston pochtasi" aksiyadorlik jamiyati “Xalqaro tezkor pochta” filiali direktori	Tadjibayeva X.Sh.
6.	“Radioaloqa, radioeshittirish va televideniye markazi” mas’uliyati cheklangan jamiyati “Iqtisodiy rejalashtirish va tahlil” bo‘limi boshlig‘i	Axmedov S.U.
7.	Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kiberxavfsizlik fakulteti O‘quv ishlari bo‘yicha dekan muovuni	Shukurov O.P.

AXBOROT TEXNOLOGIYALARI VA ALOQA SOHASIDA KASBIY MALAKALARNI RIVOJLANTIRISH BO‘YICHA TARMOQ KENGASHI

KASBIY STANDART

AXBOROT XAVFSIZLIGI