O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

70610201 – Kriptografiya va kriptoanaliz magistratura mutaxassisligining

MALAKA TALABI

Toshkent — 2024

ISHLAB CHIQILGAN VA KIRITILGAN:
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti.

TASDIQLANGAN VA AMALGA KIRITILGAN:
O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024-yil « 1 » avgust dagi 277 — sonli buyrug‘i bilan tasdiqlangan.

JORIY ETILGAN:
O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi.

Mazkur Malaka talablari “Oliy ta’limning davlat ta’lim standarti. Asosiy qoidalar”, “Oliy ta’limning davlat ta’lim standarti. Oliy ta’lim yo‘nalishlari va mutaxassisliklari klassifikatori”, O‘zbekiston Respublikasi Milliy va tarmoq malaka doiralari (ramkasi), kasbiy standartlar va kadrlar buyurtmachilari takliflariga muvofiq ishlab chiqilgan va rasmiy me’yoriy-uslubiy hujjat hisoblanadi.

O‘zbekiston Respublikasi hududida Malaka talablarini rasmiy chop etish huquqi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligiga tegishlidir.

MUNDARIJA

1. Umumiy tavsifi

70610201 – Kriptografiya va kriptoanaliz magistratura mutaxassisligi bo'yicha magistrlar tayyorlash kunduzgi ta'lim shaklida amalga oshiriladi. Mutaxassislik dasturining o'qish davomiyligi 2 yil.

1.1. Qo'llanish sohasi

1.1.1. Malaka talabining qo'llanilishi

Malaka talabi 70610201 – Kriptografiya va magistratura mutaxassisligi bo'yicha magistrlar tayyorlash o'quv reja va fan dasturlarining o'zlashtirilishini amalga oshirishda O'zbekiston Respublikasi hududidagi oliy ta'lim muassasalari uchun majburiy talablar majmuasini ifodalaydi.

1.1.2. Malaka talabining asosiy foydalanuvchilari:

mazkur magistratura mutaxassisligi bo'yicha malaka talablari, o'quv reja va o'quv dasturlarni ishlab chiqish va yangilash, ular asosida o'quv jarayonini samarali amalga oshirish uchun mas'ul hamda o'z vakolat doirasida bitiruvchilarning tayyorgarlik darajasiga javob beradigan oliy ta'lim tashkilotining boshqaruv xodimlari (rektor, prorektorlar, o'quv bo'limi boshlig'i, dekanlar va kafedra mudirlari) va professor-o'qituvchilari;

magistratura mutaxassisligining o'quv reja va fan dasturlarini o'zlashtiruvchi oliy ta'lim tashkilotining talabalari;

magistratura bitiruvchilarining tayyorgarlik darajasini baholashni amalga oshiruvchi davlat attestatsiya komissiyalari;

ta'limni boshqarish bo'yicha vakolatli davlat organlari;

oliy ta'lim tashkilotlarini moliyalashtirishni ta'minlovchi organlari;

oliy ta'lim tizimini akkreditatsiya va sifatini nazorat qiluvchi vakolatli davlat organlari;

kadrlar byurtmachilari, ish beruvchi tashkilot va korxonalar;

magistratura mutaxassisliklaridan birini ixtiyoriy tanlash huquqiga ega bo'lgan bakalavrlar va boshqa manfaatdor shaxslar.

1.2. Kasbiy faoliyatlarning tavsifi

1.2.1. Kasbiy faoliyatlarning sohalari:

"Axborot-kommunikatsion texnologiyalari" ta'lim sohasiga oid mutaxassislik bo'lib, ta'lim muassasalarida maxsus fanlarni o'qitish, ilmiy-tadqiqot institutlari, ilmiy-tadqiqot muassasa va tashkilotlarda, markazlarda, ilmiy-ishlab chiqarish birlashmalarida ilmiy-tadqiqot ishlarini olib borish, axborot-kommunikatsiya tizimlarida axborot xavfsizligini ta'minlash, xususan, axborotni kriptografik himoyasini amalga oshirish, kriptografik tizimlarni kriptotahlil usullariga nisbatan baholash, kriptografik tizimlarni dasturiy-apparat vositalar ko'rinishida amalga oshirish, axborot-kommunikatsiya texnologiyalari muhandisligi va tashkiliy boshqaruvga oid kompleks masalalarni yechishni qamrab oladi.

1.2.2. Kasbiy faoliyatlarning obyektlari:

Oliy ta'lim, qayta tayyorlash va malaka oshirish, professional ta'lim muassasalarida.

O'zbekiston Respublikasi Fanlar akademiyasi va tarmoq ilmiy-tadqiqot institutlari va markazlari hamda oliy ta'lim muassasalarining ilmiy-tadqiqot faoliyatida.

Davlat va nodavlat tashkilotlarida.

O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi tasarrufidagi korxonalar va tashkilotlarida.

Faoliyati axborotni himoyalash bilan bog'liq bo'lgan idora va tashkilotlarda.

Vazirliklar va idoralar kompyuter va axborot texnologiyalari markazlarida.

Davlat va mahalliy boshqaruv organlari, mudofaa, ichki ishlar va xavfsizlik organlarida kompleks masalalarni yechishda.

Maktabgacha va maktab ta'limi tashkilotlarida, professional ta'lim muassasalarida.

1.2.3. Kasbiy faoliyatlarining turlari:

- ilmiy tadqiqot va pedagogik faoliyat;
- ekspluatatsiya faoliyati;
- tashkiliy-boshqaruv;
- eksperimental – tadqiqot faoliyati;
- axborot-tahliliy;
- ishlab chiqarish – boshqaruv faoliyati.

1.2.4. Kasbiy vazifalari:

70610201 – Kriptografiya va kriptoanaliz mutaxassisligi bo'yicha Milliy malaka ramkasining 7-malaka darajasi hamda magistr kasbiy faoliyatlarining sohalari, obyektlari va turlariga muvofiq magistratura bitiruvchisi quyidagi kasbiy vazifalarni bajarishga qodir bo'lishi lozim:

Ilmiy tadqiqot va pedagogik faoliyatda:

respublika va xorijda chop etilgan kompyuter texnologiyalariga oid ilmiy-texnik axborotning ilmiy manbalarini tadqiq etish;

mutaxassislikka mos ilmiy, amaliy tadqiqotlarni o'tkazish, tajriba natijalarini tahlil qilish va ular asosida ilmiy asoslangan xulosalar chiqarish, ilmiy yangiliklarni kashf etishi;

ilmiy maqolalar, ma'ruzalar, risola, o'quv adabiyotlar tayyorlash va tahrir qilish, o'tkazilayotgan tadqiqotlar mavzusi bo'yicha ilmiy sharhlarni ishlab chiqishi;

ilmiy adabiyotlar va internet tarmog'ida eng yangi ilmiy, konstruktorlik, texnologik va ekspluatatsion yutuqlar haqidagi ma'lumotlarni maqsadga yo'naltirilgan holda qidirish va tahlil qilishi;

ilmiy seminar, konferensiya va simpoziumlarni tashkil etish va o'tkazishda qatnashish hamda faol ishtirok etishi;

oliy ta'lim, qayta tayyorlash va malaka oshirish, professional ta'lim muassasalarida mutaxassisligi bo'yicha pedagogik faoliyat yuritishi;

o'quv jarayonini va ilmiy faoliyatni tashkil qilish, zamonaviy axborot va pedagogik texnologiyalardan va o'qitishning texnik vositalaridan foydalanib o'quv mashg'ulotlarini o'tkazishi;

o'tkazilayotgan ilmiy-tadqiqot loyihalari mavzusi bo'yicha modellar, algoritmlar, usullarni tadqiq qilishi va ishlab chiqishi;

pedagogik va ilmiy mahorati hamda malakasini muntazam oshirib borishi lozim.

Eksplutatsiya faoliyatida:

o'rnatilgan talablarni hisobga olgan holda axborot xavfsizligini ta'minlashning kriptografik himoya vositalarini o'rnatish, sozlash, ishlatish va texnik xizmat ko'rsatish;

axborot xavfsizligi talablariga muvofiq kriptografik tizimlarni kriptotahlillashda, qurilma va dasturlarni kriptotahlillashda ishtirok etish;

obyektning axborot xavfsizligi qismtizimlarini boshqarish;

Tashkiliy – boshqaruv faoliyatida:

muhofaza qilinadigan obyektning axborot xavfsizligini tashkiliy-huquqiy, kriptografik ta'minlashni amalga oshirish;

axborotni muxofaza qilish talablarini inobatga olgan holda ijrochilarning kichik guruhlari ishini tashkil etish;

axborot xavfsizligini boshqarish tizimini takomillashtirish;

axborotni muxofaza qilish samaradorligini oshirish, davlat va boshqa turdagi sirlarni saqlash sohasidagi boshqa muassasa, tashkilot va korxonalarning tajribasini o'rganish va umumlashtirish;

obyektning axborot xavfsizligi siyosatini amalga oshirish samaradorligini monitoring qilish.

Eksperimental – tadqiqot faoliyatida:

axborot-kommunikatsiya tarmoqlarida axborotni himoya qilishning kriptografik dasturiy-apparat vositalarini ishlab chiqish va tadqiq etishi;

kriptografik algoritmlarni loyihalash, kriptotahlil usullariga baholashni amalga oshirish;

mavjud kriptografik algoritmlarni o'zida mujassamlashtirgan kriptografik protokollarni loyihalash;

kvant kompyuterlarini yaratilishi bilan sodir bo'luvchi salbiy oqibatlarni bartaraf etuvchi kriptografik yechimlarni taklif etish;

kriptografik algoritmlarni maxsus holatlarda foydalanish uchun moslashtirish va muhitga qaratilgan kriptografik algoritmlarni ishlab chiqish.

Axborot-tahliliy faoliyatida:

loyihalar samaradorligini baholash;

axborot-tahlil faoliyati natijalari bo'yicha hisobot tayyorlash;

boshqaruv qarorlarining samaradorligini baholash.

Ishlab chiqarish - boshqaruv faoliyatida:

axborot tizimi himoyasi uchun mos kriptografik algoritmlarni tanlash;

mavjud kriptografik himoya vositalaridan oqilona foydalanib, belgilangan vazifani bajarish va yuqori samaradorlikka erishishga qaratilgan chora-tadbirlar majmuini ishlab chiqish;

soha-korxonalarida talab etiluvchi axborotni himoyalashning kriptografik vositalarini tadqiq etish;

boshqarish sohasida axborot-kommunikatsiya tarmoqlarida himoya

tizimini boshqara bilish;

axborot xavfsizligi sohasida bo'lishi mumkin bo'lgan xavflarni oldindan bashorat qilgan holda, ularga qarshi kriptografik himoya vositalarini qo'llashni tadqiq etish.

2. Kasbiy kompetensiyalariga qo'yiladigan talablar

ilmiy dunyoqarashga doir bilimlarni egallagan bo'lishi, umummetodologik fanlar asosi, axborot xavfsizligi muammolari va jarayonlarini mustaqil tahlil qilish qobiliyatiga ega bo'lishi;

xorijiy tillardan birini ilmiy muloqot va kasbiy malaka almashish vositasi sifatida egallagan bo'lishi;

yangi bilimlarni mustaqil egallay bilishi, o'z ustida ishlashi va mehnat faoliyatini ilmiy asosda tashkil qila olishi;

o'zlashtirilgan bilimlarni ijodiy tanqidiy ko'rib chiqish va tahlil qilishi, ulardan ilmiy faoliyatida foydalana olishi;

o'z faoliyatida meyoriy – huquqiy hujjatlardan foydalana olishi, o'zining kasbiy faoliyatida asosli mustaqil qarorlar qabul qila bilishi;

Internet tarmog'idan axborotni olish, saqlash, qayta ishlashning asosiy usullari bilishi va vositalaridan foydalana olishi, axborotni boshqarish vositasi sifatida kompyuter bilan ishlash ko'nikmalariga ega bo'lishi;

axborot texnologiyalaridan foydalana olishi, axborotlashgan jamiyat sharoitida axborot texnologiyalarining mohiyati va ahamiyatini tushunish, axborot xuruji va tahdidlarini anglash, axborot xavfsizligining asosiy talablariga rioya qilish qobiliyatiga ega bo'lishi;

ijtimoiy muammolar va jarayonlarni mustaqil tahlil qilish qobiliyatiga ega bo'lishi;

o'zining individual bilimlariga tayangan holda ilmiy-texnikaviy, ijtimoiy va shaxsiy ahamiyatga ega bo'lgan muammolarni tushunishi va ularni tahlil qilishi;

tabiat, ilmiy-texnikaviy taraqqiyot va jamiyatda yuz berayotgan jarayon va hodisalar haqida yaxlit tasavvurga ega bo'lishi, insonning ma'naviy qiyofasi haqida bilimlarga ega bo'lishi, ulardan hayotda va kasbiy faoliyatida hamda zamonaviy ilmiy tadqiqotlarda foydalana olishi;

shaxsning inson, jamiyat, atrof muhitga bo'lgan munosabatini tartibga soluvchi huquqiy va axloqiy meyorlarni kasbiy faoliyatida qo'llay olishi;

pedagogik faoliyatida axborot va pedagogik texnologiyalardan samarali foydalanishi;

ta'lim, ilmiy-texnikaviy ijodiy faoliyati sifati va samaradorligini oshirishga innovatsion yondashishi;

kasbiy muammolarni hal etishda matematik tahlil, diskret matematika, ehtimollar nazariyasi, matematik statistika va sonlar nazariyasi usullaridan foydalanish qobiliyatiga ega bo'lishi;

kasbiy faoliyatida informatika va kompyuter texnologiyalari rivojlanishining zamonaviy tendensiyalarini hisobga olish, umumiy va maxsus dasturiy ta'minotlar bilan ishlash qobiliyatiga ega bo'lish;

dasturlash tillari va tizimlaridan, professional, tadqiqot va amaliy muammolarni hal qilishda foydalanish qobiliyatiga ega bo'lishi;

mustaqil ravishda kriptografik algoritmlar tuzish, ularni kriptotahlillash va zamonaviy dasturiy vositalar ko'rinishida amalga oshirish qobiliyati;

axborot xavfsizligi, axborotning kriptografik himoyasi, kriptotahlil masalalari bo'yicha ilmiy va texnik ma'lumotlarni, meyoriy, huquqiy va uslubiy materiallarni, mahalliy va xorijiy tajribalarni o'rganish va umumlashtirish qobiliyati;

axborot xavfsizligini, xususan, kriptografik algoritmlarni baholash bo'yicha nazariy va amaliy eksperimental tadqiqot ishlarida qatnashish, tadqiqot natijalari bo'yicha ilmiy hisobotlar, sharhlar yozish qobiliyatiga ega bo'lish;

kompyuter tizimlari xavfsizligini axborot xavfsizligi, axborotni kriptografik himoyasiga oid mahalliy va xorijiy standartlarga muvofiqligi bo'yicha tahlillash;

kompyuter tizimlari xavfsizligini kriptografik mexanizmlarini tahlil qilish va ishlab chiqishda qatnashish qobiliyati;

loyiha va texnik hujjatlarni ishlab chiqishda ishtirok etish qobiliyati;

axborot xavfsizligini ta'minlash, mos kriptografik himoyani amalga oshirish uchun loyihalar yechimlarini ishlab chiqish va tahlil qilish qobiliyati;

ijrochilardan mehnatkash jamoani tashkil qilish, kasbiy faoliyat sohasida boshqaruv qarorlarini topish va qabul qilish qobiliyati;

axborot xavfsizligi, axborotni kriptografik vositalariga oid ishlarni tartibga soluvchi meyoriy, huquqiy va uslubiy materiallarni ishlab chiqish;

kriptotahlil usullari yordamida kriptografik algoritmlar va kriptografik himoya tizimini samaradorligini, xavfsizligini baholash qobiliyati;

zamonaviy kriptografiya yo'nalishlari, kvant hisoblash tizimlariga bardoshli bo'lgan post-kvant kriptografik algoritmlarni tadqiq etish, kriptografik algoritmlardan turli maqsadlarga qarab foydalanish qobiliyatiga ega bo'lish.

3. Amaliyotlarga qo'yiladigan talablar.

Ilmiy amaliyot - umumkasbiy va mutaxassislik fanlaridan nazariy bilimlarni mustahkamlash va ishlab chiqarish hamda ilmiy tadqiqot jarayonlari bilan uyg'unlashtirish, tegishli amaliy ko'nikmalar, kompetensiyalar va malakalarni shakllantirishga qaratiladi.

Mutaxassislik bo'yicha ilmiy amaliyot o'tkaziladi.

4. Fanlar katalogining tuzilishi

T.r.	Fanning malakaviy kodi	O'quv fanlari, bloklar va faoliyat turlari	Umumiy yuklamaning hajmi, soatlarda	Kredit miqdori	Semestri
1.00		**Majburiy fanlar**	**1200**	**40**	**1-3**
1.01	ITM1104	Ilmiy tadqiqot metodologiyasi	120	4	1
1.02	AIA1104	Axborotlarni izlash va ajratib olish	120	4	1
1.03	ILB1204	Innovatsiya va loyihalarni boshqarish	120	4	2
1.04	ALT1204	Algoritmlarni loyihalashtirish va tahlil qilish	120	4	2
1.05	MFO1304	Maxsus fanlarni o'qitish metodikasi	120	4	3
1.06	CRA1206	Kriptotahlil	180	6	2
1.07	MCR1306	Zamonaviy kriptografiya	180	6	3
1.08	IPI1108	Ilmiy pedagogik ish	240	8	1, 2, 3
2.00		**Tanlov fanlar**	**480**	**16**	**1, 3**
		Jami:	**1680**	**56**	**1-3**
Kvalifikatsiya		Kriptograf-kriptoanalitik, pedagog-tadqiqotchi			
	ILA1412	Ilmiy amaliyot	360	12	4
	MDH1152	Magistrlik dissertasiyasini tayorlash	1560	52	1-4
		Jami:	**1920**	**64**	**1-4**
		Jami	**3600**	**120**	

Bibliografik ma'lumotlar

UDK: 002:651.1/7 Guruh T 55

OKS 01.040.01

Tayanch so'zlar: Kasbiy faoliyat turi, kompetensiya, modul, ta'lim yo'nalishi, kasbiy faoliyat obyekti, kasbiy faoliyat sohasi, axborotni izlash, blokcheyn, kriptovalyuta, kriptografiya, xavfsiz dasturlash, shifrlash, kodlash, elektron raqamli imzo, rasshifirofka, kriptobardoshlilik, qonun, qoida, qaror, oliy ta'lim, o'quv jarayoni, magistratura, konsalting, loyiha-qidiruv, pedagogik, ilmiy-pedagogik ish, malaka amaliyoti, bitiruv malakaviy ish, magistrlik dissertatsiyasi, baholash, sifat nazorat, davlat attestatsiyasi, mustaqil ta'lim, o'quv fanlari bloki, mundarija, oliy ta'lim muassasasi, ta'lim jarayoni, profil, amaliyot obyekti, kadrlar sifati, yuklama, yuklama hajmi, ilmiy faoliyat, ichki nazorat, yakuniy davlat nazorati, davlat-jamoatchilik nazorati, tashqi nazorat, moddiy-texnik baza, kriptologiya, kriptografiya, kriptoanaliz, kriptografiyaning matematik asosi.

Ishlab chiquvchilar, kelishilgan asosiy turdosh oliy ta'lim muassasalari hamda kadrlar iste'molchilari

ISHLAB CHIQILGAN:

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Rektor _____ **B.Maxkamov**

2024-yil «14» iyun

M.O'.

KELISHILGAN:

O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Oliy ta'limni rivojlantirish tadqiqotlari markazi

Direktor _____ **M.Boltabayev**

2024-yil «1» avgust

M.O'.

Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Boshlig'i _____ **B.Raximov**

2024-yil «14» iyun

M.O'.

«Kiberxavfsizlik markazi» DUK

Direktor _____ **O.Mirzayev**

2024-yil «13» iyun

M.O'.

«UNICON.UZ» – Fan-texnika va marketing tadqiqotlari markazi MCHJ

Direktor _____ **M.Maxmudov**

2024-yil «13» iyun

M.O'.