«Қ.И.Сатпаев атындағы Қазақ ұлттық техникалық зерттеу университеті»
КЕАҚ
Кибернетика және ақпараттық технологиялар институты
«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасы

7М06110-«АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ КЕШЕНДІ ҚАМТАМАСЫ»
Профильді оқыту(1,5 жыл)

«7М06110-Ақпараттық қауіпсіздіктің кешенді қамтамасы» білім беру бағдарламасы бойынша техника және технологиялар магистрі

БІЛІМ БЕРУ БАҒДАРЛАМАСЫ

ҚР 2018 жылғы жоғары оқу орнынан кейінгі ББМЖМС сәйкес

1-ші басылым

Алматы 2020

Бағдарлама жасалды және тараптар қол қойды:

Қ.И.Сатпаев атындағы ҚазҰТЗУ атынан:

Ақпараттық және телекоммуникациялық технологиялар Институтының директоры Т.Ф.Умаров

«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасының меңгерушісі Н.А.Сейлова

«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасының УМГ төрайымы Е.Ж.Айтхожаева

Жұмыс беруші атынан:

ЖШС « Казтелепорт» департамент директоры Толеулиев С.

Серіктес ЖОО атынан:
Ұлттық авиациялық университеті (ҰАУ, Киев, Украина)

Қ.И.Сатпаев атындағы Қазақ ұлттық техникалық зерттеу университетінің Оқу-әдістемелік кеңесі отырысында мақұлданды. № 3 хаттама 19.12.2018 ж.

Біліктілік:
7-деңгей: Ұлттық біліктілік шеңбері:

Кәсіби құзіреттілік: Ақпараттық қауіпсіздіктің кешенді қамтамасы, Ақпараттық қауіпсіздіктің аудиті, Ақпараттық қауіпсіздік жүйелерін ұйымдастыру.

Бағдарламаның қысқаша сипаттамасы:

1 Білім бағдарламасының мақсаты:

Білім бағдарламасының мақсаты магистранттарды профильді бағытта оқыту. Білім бағдарламасы тиісті құзыреттерге қол жеткізумен қатар, әртүрлі тәжірибе түрлерін (зерттеу, экспериментальдық, оқу және тәжірибе) өту арқылы базалық және арнайы пәндерді қамтиды.

Магистрлердің кәсіби қызметі ақпараттық қауіпсіздік және қорғау саласына, атап айтқанда ақпараттық қауіпсіздіктің кешенді қамтамасы және ақпараттың инженерлік -техникалық қорғалуына бағытталған.

Ақпараттық қауіпсіздіктегі профильді бағытта магистрлерді дайындау «Ақпараттық қауіпсіздіктің кешенді қамтамасы» атты жаңа білім беру бағдарламасы бойынша жүзеге асырылады. Білім бағдарламсы пәндері мен модульдер бағдарламары пәнаралық және көп салалы сипатта болады, әлемдік жетекші университеттердің білім бағдарламаларына және ақпараттық қауіпсіздік бағыты бойынша кәсіби қызметтің халықаралық жіктеушісін ескере отырып әзірленген.

Ақпараттық қауіпсіздіктің кешенді қамтамасы білім бағдарламасы негізгі нормативтік құжаттардың негізінде әзірленген:

- 24.10.2011ж № 487-VI ЗРК өзгертулер мен толықтыруларымен 27.07.2007 ж №319-III Қазақстан Республикасының «Білім туралы» заңы;

ҚР БҒМ Министрінің 2011 жылғы 20 сәуірдегі № 152 Бұйрығымен бекітілген білім берудің кредиттік технологиясы бойынша оқу үрдісін ұйымдастыру ережесі(соңғы өзгерістер Қазақстан Республикасы Білім және ғылым министрінің 2016 жылғы 28 қаңтардағы № 90 бұйрығымен бекітілген);

- білім берудің барлық деңгейлеріндегі мемлекеттік жалпыға міндетті білім беру стандарты, 31.10.2018 ж. № 604 бұйрығы және 05.05.2020 №.180.
- Ұлттық біліктілік жүйесі. 2016 жылғы 16 наурыздағы Әлеуметтік әріптестік және әлеуметтік -еңбек қатынастарын реттеу жөніндегі Республикалық үшжақты комиссияның хаттамасымен бекітілген;
- Өнеркәсіптің біліктілік шеңбері (ӨБШ). Әлеуметтік әріптестік және Әлеуметтік-еңбек қатынастарын реттеу жөніндегі салалық комиссияның 2016 жылғы 17 қарашадағы № 12-03-333 хаттамасымен бекітілген;
- ҚР БҒМ министрінің 2016 жылғы 05 шілдедегі № 425 бұйрығымен бекітілген 6М100200 – Ақпараттық қауіпсіздік жүйелері типтік оқу жоспары;
- Есептеу техникасы халықаралық Ассоциациясының компьютерлік ғылымдар саласында оқу бағдарламасы бойынша ұсынысы(серия CC2005).

«Ақпараттық қауіпсіздіктің кешенді қамтамасы» білім беру бағдарламасының магистрі кәсіптік қызметтің мақсатын дербес анықтауға және оларға қол жеткізудің тиісті әдістерін және құралдарын таңдауды, жаңа білім алу үшін ғылыми, инновациялық қызметті жүзеге асыруға бағытталған. Бұдан басқа, барлық салалар, мемлекеттік ұйымдар және басқа да қызмет салалары үшін ақпараттық қорғау және қауіпсіздік жүйелерін ұйымдастыру, жобалау, әзірлеу, басқару және аудитіне баса назар аударылады.

Бағдарлама білім беруді басқарудың демократиялық сипатының қағидаттарын іске асыруға, білім беру мекемелерінің беделін арттыруға, академиялық бостандықтар мен білім берудің беделін арттыруға мүмкіндік береді, бұл инновациялық және ғылымды қажет ететін салалар үшін жоғары білікті мамандарды даярлауды қамтамасыз етеді.

Білім бағдарламасы магистранттерге жеке көзқарас, кәсіптік құзыреттіліктерді кәсіптік стандарттардан және біліктілік стандарттарынан оқу нәтижелеріне және оларға қол жеткізу жолдарына айналдыруды қарастырады.

Білім беру бағдарламасы ақпараттық қауіпсіздік басқарушысының, ақпараттық қауіпсіздік аудиторының және кәсіби стандарттарда көрсетілген ақпараттық қауіпсіздік қызметінің инженерінің еңбек функцияларын талдау негізінде әзірленген.

Білім беру бағдарламасын дамытуға қазақстандық компаниялар мен қауымдастықтардың өкілдері, қорғаныс және қауіпсіздік саласындағы ведомстволық құрылымдардың мамандары қатысты.

ББ мазмұны мен міндеті « Пәндердің сипаттамасы» 9 бөлімде көрсетілген.

Магистратура бағдарламалары бойынша оқуды аяқтаудың негізгі критериийі болып магистранттың оқу және ғылыми қызметінің барлық түрлерін меңгеру табылады.

Толық курсты сәтті аяқтаған жағдайда магистрге «Ақпараттық қауіпсіздіктің кешенді қамтамасы» білім бағдарламасы бойынша техника ғылымдарының магистрі дәрежесіне ие болады.

2 Еңбек қызметінің түрлері:

- Жоба- конструкторлық;
- Өндірісті- технологиялық;
- Экспериментальдік – зерттеу;
- Ұйымдастырушылық- басқарушылық;
- Эксплуатацилық;
- Ғылыми;
- Ғылыми- зерттеу.

3 Кәсіптік қызмет объектілері:

Магистрдің кәсіптік қызмет объектілері болып табылады: ақпараттық қауіпсіздіктің мониторингі және аудиті; ақпаратты қорғаудың ұйымдастырылуы және технологиясы; ақпаратты криптографиялық қорғаудың қамтамасы; ақпараттық қауіпсіздік оқиғаларына жауап; ақпараттық қауіпсіздікті басқару жүйелері; ақпараттық қауіпсіздік аудитін ұйымдастырушылық қамтамасыз ету; ақпараттық қауіпсіздік аудитін жоспарлау; ақпаратты қорғау жүйелерін оларды қолдану кезінде сүйемелдеу.

БІЛІМ БАҒДАРЛАМАСЫ ПАСПОРТЫ

1 Бағдарламаның мазмұны және көлемі

Магистратурада оқу мерзімі меңгерілген академиялық кредиттердің көлемімен анықталады.Магистр дәрежесін алу үшін күтілетін оқу нәтижесіне қол жеткізгенде және академиялық кредиттердің берілген көлемін меңгерген кезінде магистрдің білім беру бағдарламасы толығымен меңгерілген болып есептеледі.

Білім беру мазмұнын, оқу процессін өткізу және ұйымдастыру әдістерін жобалау университеттің білім берудің кредиттік технологиясының негізінде дербес жүзеге асырылады.

Профильді бағыттағы магистратура тереңдетілген кәсіби дайындыққа ие басқару кадрларын дайындау бойынша жоғары оқу орнынан кейінгі білім беру бағдарламаларын жүзеге асырады.

Магистратураның білім беру бағдарламасының мазмұны:

1) базалық және профильдік пәндер циклдерін оқуды қамтитын теориялық оқытудан;

2) магистранттарды тәжірибелік дайындау: тәжірибенің әртүрлі түрлерінен;

3) магистрлік жобаны орындауды қоса алғанда, экспериментальды – зерттеу жұмыстарынан ;

4) қорытынды атттестациядан тұрады.

Атауы: Ақпараттық қауіпсіздіктің кешенді қамтамасы

Білім беру бағдарламасының мақсаты:

- Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ақпаратты қорғау жүйелерін жобалау және басқару,ұйымдастыруда түрлі технологияларды, білімдерді, дағдылар мен құзіреттілікті қолдана алатын ғылыми қызметтің және өндірістің мамандарын даярлауды қамтамасыз ету.
- Өндіріс мамандарын аудиттің, мониторингтің, күтілетін нәтижелерге бағдарланған ақпараттық қауіпсіздіктің инциденттерін зерттеуге байланысты өндірістік қызметке дайындау.
- Ақпараттық қауіпсіздікті және қорғау процестерін жоспарлау, әзірлеу, пайдалану және қолдау бойынша ұйымдастырушылық және басқарушылық қызметке қабілетті басшыларды дайындау.
- Еңбек нарығында үздіксіз кәсіби дамуға, әлеуметтік және жеке құзыреттерді дамытуға, әлеуметтік ұтқырлық пен бәсекеге қабілеттілікке жағдай жасау.

Білім беру бағдарламасының міндеті:

Келесі мәселелерді шеше алатын жоғары білікті мамандарды даярлау:

- Ақпараттық қауіпсіздік аудиті бойынша жұмыстарды жоспарлау;
- Ақпараттық қауіпсіздік аудитін ұйымдастырущылық қамтамасыз ету;
- ақпараттық қауіпсіздікті қамтамасыз ету объектісіне ақпараттық-коммуникациялық технологиялар саласындағы талаптарға сәйкес жобалау, операциялық және техникалық құжаттаманың сәйкестігіне талдау жасау;
- АҚ аудиті объектісінің қауіпсіздігінің ағымдағы жай-күйін талдау;
- Осалдықтарды анықтау және жою;

- АҚ оқиғаларын зерттеу және бақылау;
- Кәсіпорындардағы ақпараттық қауіпсіздік қатерлерінің моделін жасау;
- Ақпаратты қорғау жүйелерін құру үшін техникалық тапсырмаларды жасау.

2 Өтініш берушіге қойылатын талаптар

Өтініш берушілердің жоғары білім деңгейі жоғары кәсіби білім (бакалавриат) болып табылады. Өтініш беруші бекітілген үлгідегі дипломға ие болуы тиіс және ағылшын тілін білу деңгейін сертификатпен немесе белгілі үлгідегі дипломмен растауы тиіс.

Азаматтарды магистратураға қабылдау тәртібі «Жоғары оқу орнынан кейінгі білім берудің білім беру бағдарламаларын жүзеге асыратын білім беру ұйымдарында оқуға қабылдаудың үлгі ережесіне» сәйкес белгіленеді.

Магистранттардың контингентін қалыптастыру ғылыми және педагогикалық кадрларды даярлауға мемлекеттік білім беру тапсырысы арқылы, сондай-ақ оқу ақысын азаматтардың өз қаражаты және басқа да көздердің есебінен төлеу арқылы жүзеге асырылады. Қазақстан Республикасының азаматтарына мемлекет мемлекеттік білім беру туралы бұйрыққа сәйкес конкурстық негізде ақысыз жоғары оқу орнынан кейінгі білім беру ережелеріне сәйкес, егер олар осы деңгейде бірінші рет білім алса, құқық беруді қамтамасыз етеді.

Магистрант магистратураның білім бағдарламасын меңгеруге қажет барлық пререквизитттерге ие болуы керек. Қажет пререквизиттердің тізімі жоғары оқу орнымен дербес анықталады.

Қажет пререквизиттер болмаған жағдайда магистрантқа оларды ақылы түрде меңгеруге рұқсат етіледі.

3 Оқуды аяқтау үшін және диплом алу үшін қойылатын талаптар

Біліктілігі / дәрежесі: Осы білім бағдарламасы түлегіне «Ақпараттық қауіпсіздіктің кешенді қамтамасы» білім бағдарламасы бойынша техникалық ғылымдар магистрі дәрежесі беріледі.

Магистратура бағдарламасын меңгерген түлек келесі кәсіби біліктілікке ие болуы керек:

- жаңа білімдер мен дағдыларды өз бетінше меңгере білу, түсіну, қалыптастыру және кәсіби қызметте пайдалану, өзінің инновациялық қабілеттерін дамыту;
- зерттеу мақсатын өз бетінше қалыптастыра білу, кәсіби міндеттерді шешу кезегін белгілеу
- магистратура бағдарламасының бағытын (бейінін) анықтайтын пәндердің фундаменталды және қолданбалы бөлімдері білімдерін тәжірибеде қолдану;
- ғылыми және тәжірибелік міндеттерді шешу үшін заманауй ғылыми - техникалық құрылғыны кәсіби түрде таңдауға және шығармашылық пайдалануға қабілеті;
- өзінің кәсіби қызметінің нәтижелерін сыни талдау,ұсыну, қорғау,талқылау және тарату қабілеті;

- ғылыми-техникалық құжаттарды, ғылыми баяндамалар, шолулар, есептер мен мақалаларды дайындау және орындау дағдыларына ие болу;

- команданы кәсіби қызметінде басқаруға дайын, әлеуметтік, этникалық, конфессиялық және мәдени айырмашылықтарды толерантты түрде қабылдау;

- кәсіби қызметтің мәселелерін шешу үшін шет тіліндегі ауызша және жазбаша түрдегі қарым-қатынасқа дайындық.

Магистратураны меңгерген магистр магистратура бағдарламасына бағытталған кәсіптік қызмет түрлеріне сәйкес келетін кәсіби біліктілікке ие болуға тиіс:

- *өндірістік қызмет:*

- Тәжірбиелік мәселелерді шешуде өндірістік, өрістік, зертханалық және интерпретациялық жұмыстарды өз бетінше жүргізу қабілеті;

- Магистратураның меңгерілген бағдарламасы саласында заманауи далалық және зертханалық жабдықтар мен аспаптарды кәсіптік пайдалану мүмкіндігі;

- өндірістік мәселелерді шешу үшін күрделі ақпаратты өңдеу мен интерпретациялаудың заманауи әдістерін қолдану мүмкіндігі;

- *Жобалық қызмет:*

- Ақпараттық қауіпсіздік саласында ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстардың жобаларын өз бетімен жасау және ұсыну мүмкіндігі;

- кәсіби мәселелерді шешуде кешенді ғылыми-зерттеу және өндірістік жұмыстарды жобалауға дайындық;

- кәсіби мәселлерді шешуде ғылыми-зерттеу және ғылыми-өндірістік жұмыстарды басқару және ұйымдастыру тәжірибелік дағдыларын пайдалану;

- ақпараттық қауіпсіздікті қамтамасыз ету саласында ғылыми- өндірістік жұмыстарды жоспарлау мен ұйымдастыруда нормативтік құжаттарды практикалық қолданудың дайындығы;

- *ұйымдастыру –басқарушылық қызмет:*

- кәсіби мәселлерді шешуде ғылыми-зерттеу және ғылыми-өндірістік жұмыстарды басқару және ұйымдастыру тәжірибелік дағдыларын пайдалану;

- ақпараттық қауіпсіздікті қамтамасыз ету саласында ғылыми- өндірістік жұмыстарды жоспарлау мен ұйымдастыруда нормативтік құжаттарды практикалық қолданудың дайындығы;

Магистратураның бағдарламасын әзірлеу кезінде магистратура бағдарламасына бағдарланған кәсіби қызмет түрлеріне байланысты барлық жалпы мәдени және жалпы кәсіби құзыреттілік, сондай-ақ кәсіби құзыреттілік талап етілетін мастер-класс бағдарламаларының жиынтығына кіреді.

4 Білім бағдарламасының оқу жоспары

4.1. Оқу мерзімі 1,5 жыл

ЖҰМЫС ОҚУ ЖОСПАРЫ

7М06110- «Ақпараттық қауіпсіздіктің кешенді қамтамасы» білім бағдарламасы

Академиялық дәрежесі: Техника және технология магистрі
Оқу мерзімі:1,5ж.

оқу жылы	**Код**	**Пән атауы**	**Компонент**	**Кредиттер**		**Дс/зж/пр/СӨЖ**	**Пререквизиттер**	**Код**	**Пән атауы**	**Компонент**	**Кредиттер**		**Дс/зж/пр/СӨЖ**	**Пререквизиттер**
				ECTS	**РК**						**ECTS**	**РК**		
1	**1 семестр**							**2 семестр**						
	LNG202	Шет тілі (Кәсіби)	LNG202	6	3	0/0/3/3			Электив	БП ТК	4	2		
	MNG274	Басқару	MNG274	6	3	2/0/1/3			Электив	ПП ТК	6	3		
	HUM204	Басқару психологиясы	HUM204	4	2	1/0/2/2			Электив	ПП ТК	6	3		
		Электив	БП ТК	6	3				Электив	ПП ТК	6	3		
		Электив	ПП ТК	6	3				Электив	ПП ТК	6	3		
									Электив	ПП ТК	6	3		
								AAP221	Магистранттың тәжірибелік-зерттеу жұмыстары (магистерлік диссертацияны орындауды қоса алғанда)	МЭЗЖ	4			
		Барлығы		**28**							**38**			
2	**3 семестр**							**4 семестр**						
	AAP246	Өндірістік практика	ПП	9										

	AAP220	Магистранттың тәжірибелік-зерттеу жұмыстары (магистерлік диссертацияны орындауды қоса алғанда)	МЭЗЖ	14										
	ECA205	Магистрлік диссертацияны рәсімдеу және қорғау (МДРжҚ)	ҚА	12										
		Барлығы		**30**										
									Жалпы		**101**			

7M06110- «Ақпараттық қауіпсіздіктің кешенді қамтамасы» білім бағдарламасының

ЭЛЕКТИВТІ ПӘНДЕР КАТАЛОГІ

		БП Таңдау компонентері - 10 кредит			
	Код	**Пәннің аты**	**Кредит**	**Дәр/зертх/прак/СӨЖ**	**Семестр**
	SEC221	Желілік ОЖ-дің қауіпсіздік құралдары	6	2/0/1/3	1
	CSE749	ОЖ қорғау әдістері мен құралдары	6	1/1/1/3	1
	SEC 238	Стеганографиялық ақпаратты қорғау әдістері	4	1/0/1/2	2
	SEC244	Виртуализация және бұлт жүйелерінің қауіпсіздіг	4	1/1/0/2	2
		Барлығы	**18**		
		ПП Таңдау компонентері - 36 кредит			
	SEC210	Жасанды зияткерлік модельдері мен әдістері	6	2/1/0/3	1
	SEC246	Big Data және деректер анализы	6	2/1/0/3	3
	SEC222	Сімсіз желілер мен мобильді қолданбалардың қорғау технологиялары	6	2/1/0/3	2
	SEC 215	Ақпараттық қауіпсіздік жүйелерін ұйымдастыру	6	1/1/1/3	2
	SEC204	Ақпараттық қауіпсіздіктің аудиті	6	2/1/0/3	3
	SEC245	Киберқауіпсіздікте рисктерді басқару	6	2/0/1/3	3
	SEC247	Зияткерлік тану және кибершабуылдарға қарсы шаралар	6	1/1/1/3	3
	SEC239	Аналитикалық деректер қоймалары және OLAP технологиялары	6	1/1/1/3	3
	SEC218	Шағын контроллерді бағдарламалау	6	2/1/0/3	3
	CSE720	Киберқылмыс пен компьютерлік сот сараптамасы	6	2/1/0/3	3
		Барлығы	**36**		

МОДУЛДІК БІЛІМ БЕРУ БАҒДАРЛАМАСЫ

Білім беру бағдарламасы: 7М**06110-«Ақпараттық қауіпсіздіктің кешенді қамтамасы»**

Оқу түрі: Күндізгі   Оқу мерзімі:1,5ж.   Академиялық дәрежесі: Техника және технология магистрі

Пәннің циклі	**Пәннің коды**	**Пәннің аты**	**Семестр**	**Акад. кредиттер**	**Дәр**	**зерт**	**прак.**	**ОӨЖ**	**Бақылау түрі**	**Каф**
Профиль бойынша оқыту модулі										
Базалық пәндер (БП)										
ЖОО компоненті										
БП 1.1.1	LNG202	Шет тілі (Кәсіби)	1	6	0	0	3	3	Емтихан	АТ
БП 1.2.1	MNG274	Басқару	1	6	2	0	1	3	Емтихан	ЖБҒББО
БП 1.3.1	HUM204	Басқару психологиясы	1	4	1	0	1	2	Емтихан	ЖБҒББО
Таңдауы бойынша компонент (10 кредит)										
Желілік қауіпсіздікті, бұлтты технологиялар мен деректер қорының қауіпсіздігін қамтамасыз ету модулі										
БП	CSE749	ОЖ қорғау әдістері мен құралдары	1	6	1	1	1	3	Емтихан	КАӨжС
БП	SEC221	Желілік ОЖ-дің қауіпсіздік құралдары	1	6	2	0	1	3	Емтихан	КАӨжС
БП	SEC 238	Стеганографиялық ақпаратты қорғау әдістері	2	4	1	0	1	2	Емтихан	КАӨжС
БП	SEC205	Бұлтты есептеулер мен телекоммуникациялардың қорғауы мен қауіпсіздігі	2	4	1	1	0	2	Емтихан	КАӨжС
Профильді пәндер (ПП)										
Таңдауы бойынша компонент (36 кредит)										
Деректерді талдау, АҚ-да жасанды интеллектті қолдану және ақпаратты қорғау мен қауіпсіздігін қамтамасыз ету модулі										
ПП	SEC210	Жасанды зияткерлік модельдері мен әдістері	1	6	2	1	0	3	Емтихан	КАӨжС
ПП	SEC246	Big Data және деректерді талдау	1	6	2	1	0	3	Емтихан	КАӨжС
ПП	SEC222	Сімсіз желілер мен мобильді қолданбалардың қорғау технологиялары	2	6	2	1	0	3	Емтихан	КАӨжС
ПП	SEC 215	Ақпараттық қауіпсіздік жүйелерін ұйымдастыру	2	6	1	1	1	3	Емтихан	КАӨжС
ПП	SEC204	Ақпараттық қауіпсіздіктің аудиті	2	6	2	1	0	3	Емтихан	КАӨжС
ПП	SEC245	Киберқауіпсіздікте рисктерді басқару	2	6	2	0	1	3	Емтихан	КАӨжС
ПП	SEC247	Зияткерлік тану және кибершабуылдарға қарсы шаралар	2	6	1	1	1	3	Емтихан	КАӨжС

ПП	SEC239	Аналитикалық деректер қоймалары және OLAP технологиялары	2	6	1	1	1	3	Емтихан	КАӨжС
ПП	SEC240	Киберқылмыс пен компьютерлік сот сараптамасы	2	6	1	1	0	3	Емтихан	КАӨжС
ПП	SEC218	Шағын контроллерді бағдарламалау	2	6	2	1	0	3	Емтихан	КАӨжС
Практикалық-бағдарланған модуль										
ПП	AAP246	Өндірістік практика	3	9					Есеп	
Ғылыми-зерттеу модулі										
МЭЗЖ	AAP221	Магистранттың тәжірибелік-зерттеу жұмыстары (магистерлік диссертацияны орындауды қоса алғанда)	2	4					Есеп	
МЭЗЖ	AAP220	Магистранттың тәжірибелік-зерттеу жұмыстары (магистерлік диссертацияны орындауды қоса алғанда)	3	14					Есеп	
Қорытынды аттестациялау модулі (12 кредит)										
ҚА	ECA205	Магистрлік диссертацияны рәсімдеу және қорғау	3	12					Диссертация қорғау	
Барлығы				**101**						

5 Білім, білік, дағды және құзыреттілік деңгейі мен көлемінің дескрипторлары

Магистранттың дайындық деңгейіне қойылатын талаптар Жоғары білімнің екінші деңгейіндегі Дублиндік дескрипторлар (магистратура) негізінде анықталады және қол жеткізілген оқыту нәтижелерінде көрсетілген игерілген құзыреттіліктерді көрсетеді.

Оқыту нәтижелері магистратураның барлық білім беру бағдарламасы деңгейінде де, жеке модульдер немесе оқу пәні деңгейінде де тұжырымдалады.

Дескрипторлар білім алушының қабілетін сипаттайтын оқу нәтижелерін көрсетеді:

1) зерттеу контекстінде идеяларды әзірлеу және (немесе) қолдану кезінде металлургия мен пайдалы қазбаларды байытудың озық білімдеріне негізделген металлургия мен пайдалы қазбаларды байытудың зерделенетін саласында дамып келе жатқан білімі мен түсінігін көрсету;

2) жаңа ортада, неғұрлым кең пәнаралық контексте мәселелерді шешу үшін өз білімін, түсінігін және қабілетін кәсіби деңгейде қолдану;

3) Әлеуметтік, этикалық және ғылыми пайымдауларды ескере отырып, пікірлерді қалыптастыру үшін ақпаратты жинау мен түсіндіруді жүзеге асыру;

4) мамандарға, сондай-ақ маман емес адамдарға ақпаратты, идеяларды, қорытындыларды, мәселелер мен шешімдерді нақты және толық емес хабарлау;

5) оқылатын металлургия және пайдалы қазбаларды байыту саласында одан әрі оқуды өз бетінше жалғастыру үшін қажетті оқыту дағдылары.

6 Оқуды аяқтағандағы құзіреттіліктер

6.1 Профильді магистратура түлектерінің негізгі құзыреттеріне қойылатын талаптар:

1) түсінікке ие болу керек:

- ақпараттық қауіпсіздік және қорғау саласында кәсіби құзіреттілік туралы;
- ресурстар мен платформалар виртуализциясы туралы;
- ДҚ қауіпсіздігінің технологиялары туралы;
- сімсіз желілер мен мобильді қолданбалардың қорғау технологиялары туралы;
- үлкен деректерді талдау туралы;

2) білу керек:

- оқу процесінде магистранттердің танымдық қызметінің психологиясын;
- білім берудің тиімділігі мен сапасын арттырудың психологиялық әдістері мен құралдары;
- ақпаратты криптографиялық қорғаудың алгоритмі туралы;
- АҚ стандарттары және АТ қауіпсіздігін бағалау критерийлері;
- жетекші өндірушілердің виртуалдандыру технологиялары мен виртуалдандыру жүйелерінің ресурстары мен платформалары;
- виртуалдандыру жүйелерінің қатерлері мен тәуекелдері, гипервизаторларды құру принциптері және олардың осалдықтары;

- IP- желілердің ұйымдастырылуын, IP- пакеттер және IP – хаттамалардың құрылымын;
- аутентификацияның әр түрлілігі және принциптері;
- желі аралық экрандар және шабуылдарды анықтау жүйелеріне талаптар;
- ДҚ қоргау технологиялары және қауіпсіз ДҚ жобалау әдістері;
- ДҚ қорғау және қауіпсіздігі жүйелерін ұйымдастыру;
- белсенді аудиттің құралдары және әдістері;

3) қабілетті болу керек:

- заманауй ақпараттық теқнологияларды тарта отырып ақпараттық-талдамалық және ақпараттық-библиографиялық жұмысты жүргізу;
- жаңа проблемаларды және жағдайларды шешу үшін шығармашылық және креативті ойлау;
- жоғары оқу орындарында арнайы пәндерді зерттеу және оқытуды жүзеге асыруға мүмкіндік беретін кәсіби деңгейде шет тілін еркін меңгеру;
- ақпараттың криптографиялық қорғау алгоритмдерін қолдану
- ақпараттық қауіпсіздік стандарттарын қолдану және АТ қауіпсіздігін бағалауды жүргізу;
- жетекші өндірушілерден виртуализация жүйесін қолдануға;
- виртуалдандыру жүйелерінің қауіп-қатерлерін анықтау;
- негізгі ақпаратты және шифрлау әдістерін және құралдарын қолдану
- желі аралық экрандар және шабуылдарды анықтау жүйелеріне талаптар;
- ДҚ қоргау технологиялары және қауіпсіз ДҚ жобалау әдістері;
- ДҚ қорғау және қауіпсіздігі жүйелерін ұйымдастыру;
- белсенді аудиттің құралдары және әдістері;
- ақпараттың инженерлік- техникалық қорғалуы.
- үлкен деректерді талдау құралдарын пайдалануға.

4) дағдылары болу керек:

- кәсіби қарым-қатынас және мәдениетаралық қарым-қатынас;
- шешендік өнер, өз ойын ауызша және жазбаша түрде дұрыс және логикалық рәсімдеу;
- деректер қорының қауіпсіздігін ұйымдастыру және қорғау;
- ақпараттық қауіпсіздік аудитін жүргізу;
- криптографиялық ақпаратты қорғау алгоритмдерін қолдану;
- қауіп-қатерлерді анықтау және оларға қарсы әрекет ету;
- Big Data- мен жұмыс;
- күнделікті кәсіби қызмет үшін қажетті дәрежені кеңейту және тереңдету және докторантурада білімін жалғастыру;

5) құзіретті болу керек:

- ақпараттық қауіпсіздік жүйелерін ұйымдастыруда;
- ақпараттық қауіпсіздік аудитін жүргізуде;
- ұйымның ақпараттық қауіпсіздігін қамтамасыз етуде;
- білімді үнемі жаңартып, кәсіби дағдылар мен қабілеттерін кеңейту жолдарында.

Б- Базалық білімдер, қабілеттер, және дағдылар

Б1- Жобалық менеджмент пәні бойынша білім және қабілеттер.

Б2 - Ақпаратты криптографиялық қорғауды дамытудың заманауи және перспективалық бағыттарын біліп, оны тәжірибеде қолдану;

Б3 - Ресурстар мен платформаларды виртуализациялау технологиясын білу, жетекші өндірушілерден виртуализация жүйесін қолдану;

К- Кәсіби құзіреттілік:

К1 – компьютерлік криминалистика және киберқылмыс сұрақтарында құзіретті болу,қауіптерді анықтау білу және щабуылдардың алдын алу жұмыстарын жүргізу;

К2 – ДҚ қорғау және қауіпсіздік жүйесін ұйымдастыруға қабілетті болу керек және ДҚ қорғау технологияларын қолдану;

К3 – ақпараттық қауіпсіздік жүйелерін ұйымдатыру сұрақтарын білу және тәжірибеде ақпараттық қауіпсіздіктің кешенді қамтамасы бойынша жұмыстар жүргізу;

К4 - сымсыз қауіпсіздік инфрақұрылымын жоспарлау, жобалау, орнату және қолдау мүмкіндігіне ие болу;

К5 – экономикалық жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету сұрақтарында құзіретті болу;

К6 – үлкен деректерді талдай білу;

К7-АҚ стандарттарын және АТ қауіпсіздігін бағалау критерийлерін білу, АҚ тәуекелдерін бағалау құралдары мен әдістерін қолдануға қабілетті болу.

Ж- жалпы адамзаттық, әлеуметтік – этикалық құзіреттілік

Ж1 – командада жұмыс істей білу, ұйымдастырушылық қабілеттерге ие болу, басымдықтарды белгілеу, жаңа білім мен дағдыларды тез меңгеру, оларды тәжірибеде қолдану;

Ж2 – нәтижеге қол жеткізуге бағдарланған, өз дамуын тиімді жоспарлау және ұйымдастыру;

Ж3 – іскерлік қарым-қатынас құралы ретінде ағылшын тілін еркін қолдана білу, ақпараттық қауіпсіздікті қамтамасыз ету саласында жаңа білім көзі.

А - Арнайы және басқару құзыреті:

А1 - ұйымның стратегиясы, саясаты мен мақсаттары шеңберінде, проблеманы сыни талқылау, қорытындылар мен ақпараттың құзыретті орындалуы туралы пікірталас шеңберінде еңбек және оқыту іс-әрекеттерінің үдерістерін дербес басқару және бақылау;

А2 - белгілі бір тапсырмаларды шешуге ынталандыру қабілеті, бірліктің немесе кәсіпорынның деңгейінде жұмыстың орындалу нәтижесіне жауапты болуы;

А3 - жұмыс процесін басқаруға арналған дағдылар жиынтығын көрсету, нәтиже алу әдістерін, әдістемелерін және бағалау критерийлерін таңдау, билікті бөлу және өкілеттілік, командаларды қалыптастыру және өндіріс процесінде шешімдер қабылдау мүмкіндігі.

6.2. Профильді магистратурада магистранттың ғылыми – зерттеу жұмысына талаптар:

1) магистрлік диссертация орындалатын және қорғалатын магистратураның білім бағдарламасы профиліне сәйкес келеді;

2) ғылымның, технологияның және өндірістің заманауи жетістіктеріне негізделген және нақты практикалық ұсыныстарды, басқарушылық тапсырмалардың дербес шешімдерін қамтиды;

3) озық ақпараттық технологияларды пайдалана отырып орындалады;

4) негізгі қорғалған ережелер бойынша ғылыми – зерттеу (әдістемелік, тәжірибелік) бөлімдерінен тұрады.

6.3. Тәжірибені ұйымдастыруға талаптар:

Профильді магистратураның білім бағдарламасына КП циклiндегі өндірістік тәжірибе кіреді.

ПД циклiндегі өндірістік тәжірибе оқу процесінде жинақталған теориялық білімдерді нығайту, магистрлік білім беру бағдарламасында тәжірибелік дағдыларды, құзыреттілік пен кәсіптік тәжірибені алу, сондай-ақ озық тәжірибені дамыту мақсатында жүзеге асырылады.

7 ECTS стандарты бойынша дипломға қосымша

Қосымша Европалық Комиссияның, Европа Кеңесінің және ЮНЕСКО / СЕПЕС стандарттарына сәйкес әзірленген. Бұл құжат академиялық тану үшін ғана және білім туралы құжаттың ресми дәлелі болып табылмайды. Жоғары білім туралы дипломсыз жарамсыз. Европалық қосымша толтырудың мақсаты - диплом иегерінің, алған біліктілігі, осы біліктілік деңгейі, оқу бағдарламасының мазмұны, нәтижелері, біліктіліктің функционалды мақсаты, сондай-ақ ұлттық білім беру жүйесі туралы ақпарат. Баға беру үшін қолданылатын қолданбалы модельде еуропалық аудару немесе несие беру жүйесі (ECTS) қолданылады.

Дипломға еуропалық қосымша білім алуды шетелдік университеттерде жалғастыруға мүмкіндік береді, сондай – ақ шетелдік жұмыс берушілер үшін ұлттық жоғарғы білімді растауға мүмкіндік береді. Кәсіби тану үшін шетелге шығу кезінде білім туралы дипломды қосымша заңдастыру қажет.

Европалық диплом қосымшасы жеке сұраныс бойынша ағылшын тілінде толтырылады және тегін беріледі.

8 Модулдер және оқу нәтижелері тізімі

Модуль атауы	**Кәсіби құзірет**	**Модульді қалыптастыратын пәндер**
Гуманитарлық модуль	Пікірталас пен диалог техникасына ие, өздерінің кәсіби қызметінде қарым-қатынас пен шығармашылық дағдыларын иеленеді. Басқару психологиясы және жобаларды басқару мәселелері бойынша құзыретті болу.	Жобалық менеджмент (Басқару психологиясы)
Желілік қауіпсіздікті, бұлтты технологиялар қауіпсіздігін қамтамасыз ету модулі	Қауіпсіздік жүйесін ұйымдастыра білу және қорғау технологияларын қолдану, ақпаратты криптографиялық қорғау дамуының заманауй және перспективті бағыттарын білу Ақпаратты қорғау мен қауіпсіздігінің кешенді қамтамасыз етілуін ұйымдастыра білу. Виртуализацияның заманауй технологияларын қауіпсіз қолдану	ОЖ қорғау әдістері мен құралдары, Стеганографиялық ақпаратты қорғау әдістері Бұлтты технологиялар және виртуализация жүйелер қауіпсіздігі
Деректерді талдау, АҚ-да жасанды интеллектті қолдану және ақпаратты қорғау мен қауіпсіздігін қамтамасыз ету модулі	Ақпараттық қауіпсіздік аудиттерін жүргізу үшін құралдар мен әдістерді білу және қолдану. Киберқылмыс пен компьютерлік криминалистика сараптамасын анықтауға құзыретті болу. Кибершабуылды тану және қарсы алу құралдарын пайдалана білу. Үлкен деректерді талдау, үлкен деректерді талдау әдістерін және құралдарын білу.	Ақпараттық қауіпсіздік менеджмент тәуекелі. Киберқылмыс пен компьютерлік криминалистика, Сімсіз желілер мен мобильді қолданбалардың қорғау технологиялары, Ақпараттық қауіпсіздіктің аудиті Big Data және деректерді талдау, Аналитикалық деректер коймалары және OLAP технологиялары, Ақпараттық қауіпсіздік жүйелерін ұйымдастыру
Тәжірибеге бағытталған модуль	Кәсіби дағдыларды меңгеру. Жаңа идеяларды қалыптастыру мүмкіндігі. Кәсіби салада ғылыми зерттеулер жүргізу, тәжірибені үздіксіз жаңартуды қамтамасыз ету, кәсіби дағдылар мен қабілеттерін кеңейту жолдары. Ақпараттық технологияларды тарту арқылы	Кәсіби тәжірибе

	ақпараттық-аналитикалық және ақпараттық-библиографиялық жұмыстарды жүргізу мүмкіндігі. Теориялық білімді IT-саласында өндіріс проблемаларын шешуде өз тұжырымдарын әзірлеу және ұсыну. Кәсіпорынды ұйымдастыру мен басқаруда күрделі және ерекше жағдайларда шешімдер қабылдау мүмкіндігі.	
Қорытынды аттестация модулі	Магистратурада оқу барысында жинақталған білімді кешенді емтиханды сәтті тапсыру үшін жүйелеу және синтездеу. Оқуды тәуелсіз және өз бетінше жалғастыруға мүмкіндік беретін оқу саласындағы қабілет. Ғылыми - зерттеу және аналитикалық жұмыстың нәтижелерін ғылыми мақалалар, есептер, аналитикалық есептер, тезистер түрінде тіркеу. Өздерінің мәліметтерін жеткізе білу және өз білімдерін мамандар мен мамандарға тұжырымдау үшін пайдалану. IT-технологиялар саласындағы ғылыми-техникалық ақпарат, отандық және шетел тәжірибелерін зерттеу, оның шығармашылық түсінігі және олардың ғылыми, техникалық немесе өндірістік проблемаларын дұрыс шешу.	Магистрлік диссертацияны рәсімдеу және қорғау

9. Пән сипаттамасы

Шет тілі (кәсіби)
Professional English for Project Managers
КОД – LNG202
КРЕДИТ – 6
ПРЕРЕКВИЗИТ –Academic English, Business English, IELTS 5.0-5.5

КУРС МАҚСАТТАРЫ ЖӘНЕ МІНДЕТТЕРІ

Курстың мақсаты - магистранттердің ағымдық академиялық зерттеулері үшін ағылшын тілін білуін дамыту және жобаларды басқару саласында жұмысының тиімділігін арттыру.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Курс жобаларды басқару саласында тиімді қарым – қатынас жасау үшін және оқу, жазу, тыңдау мен сөйлесу дағдыларын жақсарту үшін «Intermediate» деңгейінде сөздік қор және грамматиканы дамытуға бағытталған. Магистранттер іскерлік ағылшын тілінде өздерінің сөздік қорын толықтырып, менеджмент контекстінде жиі қолданылатын грамматикалық құрылымдарды меңгереді деп күтіледі. Курс 6 модульден тұрады. 3- ші модуль аралық бақылаумен аяқталады, ал алтыншы модуль курстың соңында тестпен бірге өтеді. Курс қорытынды емтиханмен аяқталады. Сондай – ақ магистранттар өз бетінше білім алу керек(MIS). MIS –мұғалімнің жетекшілігімен магистранттардың өзіндік жұмысы.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Курсты сәтті аяқтағаннан кейін магистранттер бизнес пен басқару контексінде монологтарды, диалогтарды және топтық пікірталастарды тыңдау кезінде негізгі идеяны және негізгі хабарламаны, сондай-ақ нақты мәліметтерді тани алады; менеджментке қатысты тақырыптар бойынша ағылшын тілінде жазбаша және ауызша сөйлеуді түсіну; грамматикалық дәлдіктің жоғары дәрежесі бар және іскери сөздер мен сөз тіркестерін қолданып, әртүрлі іскерлік жағдайлар туралы әңгімелеп, тиісті іскерлік сөздік және грамматикалық құрылымдарды қолдана отырып, жұптар мен топтарда жазылған басқару мәтіндерін (есептер, хаттар, электронды хабарламалар, жиналыс хаттамасы) жазуға қабілетті болады деп күтіледі.

Менеджмент
КОД MNG274
КРЕДИТ 6

ПРЕРЕКВИЗИТ: «Менеджмент» пәні бакалавриат мамандықтары бойынша пәндерді оқудан алынған білімге негізделген

КУРС МАҚСАТТАРЫ ЖӘНЕ МІНДЕТТЕРІ

Пәнді оқытудың мақсаты - әр түрлі қызмет салаларында жоба менеджменті әдіснамасын меңгеру, заманауи жобалық менеджментке және ақпараттық технологияға сай мәдениетті қалыптастыру, жобаны іске асыру саласында жаңа ақпараттық технологияларды енгізу үшін жағдай жасау. Курс жобаларды басқарудың халықаралық жобаларына негізделген (Project Management Body of Knowledge).

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ Пәннің мазмұны жобаларды жоспарлау және орындау мәселелерін шешу үшін маманның болашақ практикалық іс-әрекетіне оларды қолдану мақсатында қазіргі заманғы концепцияларды, әдістерді, жобаларды басқару құралдарын зерттеуге бағытталған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Қабілетті болу:

- жобаның техникалық-экономикалық негіздемесі, жобаның жарғысы және т.б. сияқты инициализациялау кезеңіне құжаттар дайындау.
- жобалық қызметті жоспарлауға қатысты құжаттарды әзірлеу және талдау, шешімдерді қолдаудың әртүрлі әдістерін қолдану;
- жұмыстардың орындалу мерзімін және қадағалау мерзімін дереу қадағалау;
- персоналды таңдау, топ мүшелерінің арасындағы қақтығыстарды шешу;
- жобаларды іске асырудан туындайтын тәуекелдерді басқару.

Пәнді өту кезінде алынған білім:

- жобаларды басқару саласындағы қазіргі заманғы стандарттар және олардың сипаттамалары;
- PMI-нің жобаны басқаруға көзқарасы;
- Инвестициялық жоспарлау;
- жобалық тәуекелдерді есепке алу;
- қолда бар ресурстарды пайдалануды оңтайландыру әдістері;
- жанжалды жағдайларды шешу жолдары;
- прогресті уақтылы реттеу үшін нақты көрсеткіштерді талдау.

Біліктілігі:

- Жобаны басқарудың заманауи талаптарына сәйкес жоба менеджменті;
- MS Project бағдарламалық қамтама жобаларын басқару процесінде қолдану.

БАСҚАРУ ПСИХОЛОГИЯСЫ

КОД - HUM204

Кредит – 4

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

Курстың мақсаты - жеке тұлғалар мен ұйымдардағы адамдардың топтарының мінез-құлқын зерттеу; қызметкерлердің мінез-құлқына әсер ететін психологиялық және әлеуметтік факторларды анықтау. Сондай-ақ, адамдардың ішкі және сыртқы мотивацияларына көп көңіл бөлінеді.
Курстың басты мақсаты - ұйымның тиімділігін арттыру үшін осы білімді қолдану.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Курс пәнді қамтитын барлық негізгі элементтерді теңгерімді сипаттауды қамтамасыз етеді. Онда қысқаша ұйымдық мінез-құлық теориясы мен практикасының туындауы мен дауму мәселелерін талқылайды, сонымен қатар басқарудың тиімділігіне назар аударумен басқару функциясы мен машықтануына, басты рольдер қарастырылады, олар нақты өмір тақырыптық зерттеулер мысалдармен және тақырыптық зерттеулермен көркемделген.

Курсты оқығаннан кейінгі күтілетін нәтижелер:

Курсты бітіргеннен кейін магистранттер жеке және топтық мінез-құлық негіздерін; мотивацияның негізгі теориясы; негізгі көшбасшылық теориялар; ұйымдағы қарым-қатынас, жанжалдарды басқару және стресстерді біледі. Ұйымдардағы менеджерлердің әртүрлі рөлін анықтауға мүмкіндік береді; ұйымдарға менеджерлер тұрғысынан қарау; тиімді басқару тиімді ұйымдастыруға қалай ықпал ететінін түсіну.

Желілік операциялық жүйелер қауіпсіздігінің құралдары

КОД – SEC 221
КРЕДИТ – 6
ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

IP-желілерін ұйымдастыру негіздерінде магистранттердің теориялық және практикалық дайындығы, маршруттау, IP-хаттамаларының жұмыс істеу ерекшеліктері, желі операциялық жүйесінің сорттары және олардың ақпараттық қауіпсіздігін қамтамасыз ету, сондай-ақ ОС-ның құрамдас бөліктерінің (бағдарламалық жасақтаманың) тұтастығын бақылау және өзгертуге қарсы әдістер. Курстың мақсаты: желілік операциялық жүйелердің қауіпсіздігін жалпы түсінуді қалыптастыру; IP-ге негізделген желілерді ұйымдастыру, ОЖ-дағы ақпараттық сақтауды ішкі ұйымдастыруымен танысу, желілік ОЖ қауіпсіздігін қамтамасыз ету әдістерімен танысу; ОЖ жүйесінде қорғанысты ұйымдастыру мен қауіп-қатерлерді анықтауда тәжірибелік дағдыларды игеру.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Желілік операциялық жүйелер қауіпсіздігінің құралдары курсы IP-желілерді ұйымдастырудың негіздерін, IP- адрестерді тарату, IP-хаттамалардың ауқымы мен жұмыс істеуі және желілік операциялық жүйелердің түрлерін оқытады. Өзгерістен қорғау және бағдарламалық қамтаманың тұтастығын бақылау. Негізгі ақпаратты сақтау әдістері мен құралдары. Көпфакторлы аутентификация қағидалары. Сәйкестендіру және аутентификациялау техникалық құрылғылары. Сәйкестендіру және аутентификацияның парольдік шағын жүйелері. Биометриялық құрылғыларды көмегімен пайдаланушыларды сәйкестендіру және түпнұсқаландыру. Шифрлаудың бағдарлама – аппараттық құралдары. Windows, Unix жүйелерінде қауіпсіздікті қамтамасыз ету, ақпаратты тасымалдаушылардың ішкі ұйымдастыруымен танысу. Шабуылдарды анықтау жүйелері. Желі аралық экрандар архитектурасының негізгі компоненттері. Желі аралық экрандарға заманауй талаптар.

Қауіптілік көздерін анықтау үшін желілік трафикті ұстап алу мен талдауда практикалық дағдыларды береді. Жүйе ішінде вирустарды таратудан қорғауды ұйымдастыру үшін файлдық жүйелер құрылымын қарап шығу және талдау. Бағдарламалық жасақтама әзірлеу дағдылары (әзірлеу ортаны тыңдаушы таңдайды): 1) жергілікті желідегі компьютерлер арасында IP пакеттерін қалыптастыру арқылы қысқа хабарламаларды алмасу үшін; 2) желі аралық экран орнату кезінде желілік шабуылдар әдістерін егжей-тегжейлі ұсыну үшін, бұрынғы бағдарламамен құрылған IP-пакеттерін талдау және DoS-шабуылының пакеттерін қалыптастыру.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді оқу нәтижесінде магистрант білу керек:

- IP- желілердің ұйымдастырылуын, IP- пакеттердің құрылымын және IP-хаттамаларды;
- ОЖ ақпаратын тасымалдаушылардың ішкі ұйымдастырылуын;
- Шифрлау мен негізгі ақпаратты сақтау құралдары мен әдістері;
- Аутентификация принциптері және түрлілігі;
- Шабуылдарды анықтау жүйелеріне және желі аралық экрандарға талаптар.

дағдылары болу керек:

- желілік трафикті ұстап қалу және талдау, сондай-ақ осалдықтарды анықтау;
- FAT32, NTFS, EXT4 файлдық жүйелерінің құрылымын талдау және физикалық деңгейде ақпаратты (он алтылық форматта) іздеу, оқу және өзгерту;
- әртүрлі желілік хаттамаларды қолданатын компьютерлер арасындағы қауіпсіз деректермен алмасуды қамтамасыз ететін бағдарламалар әзірлеу;

келесі құзыреттерге иеболу керек:

- желілік операциялық жүйелердің қауіпсіздігін қамтамасыз ету үшін анықтамалық және ақпараттық материалдарды пайдалану;
- қауіпсіздікті қамтамасыз етудің бағдарлама – техникалық құралдарын таңдауды жүзеге асыру;
- төмен және жоғарғы деңгей тілдерінде бағдарламалар және алгоритмдер әзірлеу;
- желілік ОЖ қауіпсіздігін бағалау.

ОЖ қорғау әдістері мен құралдары

КОД –CSE749
КРЕДИТ – 6
ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Опреациялық жүйелердегі ақпаратты қорғаудың нұсқаулары мен негізгі түсіктері. Ақпаратты-есептеу жүйелеріндегі ақпараттың қауіпсіздік қатерлері. ОЖ қауіпсіздік қатерлері. ОЖ қауіпсіздікке қойылатын талаптары. Заманауи операциялық жүйелердің қауіпсіздігін талдау. Windows, Unix, Mac OS құрамдасқан қауіпсіздік құралдары. Заманауи ОЖ шабуылдар негізінде жатқан әдістердің статистикасы. ОЖ қатынауды шектеу. ОЖ пайдаланушылардың идентификациясы мен аутентификациясы. Windws, Unix, Mac OS ОЖ қорларға қатынауға шектеулер орнату. ОЖ аудиті. Бағдарламалық қамтаманы қорғау жүйелері.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді оқу нәтижесінде магистрант білу керек:

- Шифрлау мен негізгі ақпаратты сақтау құралдары мен әдістері;
- Аутентификация принциптері және түрлілігі;

- қауіпсіздікті қамтамасыз етудің бағдарлама – техникалық құралдарын таңдауды жүзеге асыру;
- төмен және жоғарғы деңгей тілдерінде бағдарламалар және алгоритмдер әзірлеу;
- желілік ОЖ қауіпсіздігін бағалау.

Ақпаратты қорғаудың стеганографиялық әдістері

КОД - SEC 238

КРЕДИТ – 4

ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ - ашық арналар арқылы берілетін басқа деректерге көзге көрінбейтін етіп енгізу арқылы құпия деректердің жасырын берілуін және сақталуын қамтамасыз етуден тұратын стеганографияның негізгі принциптерін игеру.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Пәннің мазмұны стеганографиялық алгоритмдер мен авторлық құқықты қорғау алгоритмдерін қолдана отырып, математикалық түрлендірулер арқылы ақпаратты қорғауға қатысты бірқатар мәселелерді қамтиды.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді игеру нәтижесінде магистрант білуі керек:

- дамудың перспективалық бағыттары
- стеганографиялық жүйелердің жіктелуі
- деректерді беру үшін цифрлық стеганожүйелерді, су белгілері мен стеганожүйелерді құру принциптері.
- Steganography компьютерлік жүйелерінде аудио және графикалық ақпаратты ұсыну форматтары

Жүйелердің стеганографиялық қарсылығын анықтай білу, стеганографияда бағдарламалық өнімдерді қолдану және стеганожүйелерге визуалды шабуылдар ұйымдастыру.

Виртуализация және бұлт жүйелерінің қауіпсіздігі

КОД – SEC244

КРЕДИТ – 4

ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Бұлтты технологиялар және виртуализация жүйелерінің қауіпсіздігі» пәнінің мақсаты бұлтты технологиялар және виртуализация саласында магистранттерге кәсіби құзіреттілік беру.

«Бұлтты технологиялар және виртуализация жүйелерінің қауіпсіздігі» пәнінің міндеті бұлтты технологиялар және виртуализация жүйелерін қауіпсіз қолдануды ұйымдастырудың базалық принциптерін меңгеру болып табылады.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

«Бұлтты технологиялар және виртуализация жүйелерінің қауіпсіздігі» оқу курсының бағдарламасы бұлттық есептеулердің технологиялық негіздерін - виртуалдандыру және виртуалдандыру жүйелерінің тұжырымдамаларын, бұлтты технологиялар қызметтерін зерттеуге және олардың қауіпсіздігін және қорғалуын қамтамасыз етуге бағытталған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді меңгеру нәтижесінде магистрант білуі керек:

- Ресурстар мен платформаларды виртуалдандыру технологияларын;
- Жетекші өндірушілерден виртуалдандыру жүйелерін;
- гипервизорларды құру принциптері және олардың осалдығы;
- виртуалдандыру жүйелерінің қатерлері мен тәуекелдері;
- IaaS, PaaS и SaaS бұлтты технологиялардың негізгі сервистері;
- Бұлтқа кең таралған шабуылдар;

Қабілетті болу:

- виртуалдандыру жүйелерін орнату;
- бұлтты сервистермен жұмыс істеу;
- виртуалды машиналарды осалдыққа тестілеу;
- виртуалды шифрланған дискі жасау;

дағдыларға ие болу:

- виртуалды машиналарды жасау;
- виртуалды машинада қосымшалармен жұмыс;
- бұлтдағы деректерді криптографиялық қорғауды қолдану;
- бұлтты есептеулердің қауіпсіздігін қамтамасыз ету үшін Cloud Security Alliance ұсынымдарын пайдалану.

Жасанды зияткерлік модельдері мен әдістері

КОД – CSE 210
КРЕДИТ – 6
ПРЕРЕКВИЗИТ – жоқ.

«Жасанды интеллекттің модельдері мен әдістері» пәнін оқытудың мақсаты жасанды интеллекттің технологиялары мен білімді көрсетудің модельдерінде математикалық әдістерді оқыту, жасанды интеллект жүйесін құру принциптерін оқыту.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді оқытудың нәтижесінде білім алушылар жасанды интеллект жүйесін құру принциптерін, жасанды интеллект технологиясында және білімді көрсету модельдерінде қолданылатын математикалық әдістерді білулері керек.

Big Data және деректерді талдау

КОД – SEC246
КРЕДИТ – 6
ПРЕРЕКВИЗИТ – жоқ.

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Big Data және деректерді талдау» пәнінің мақсаты үлкен деректерді талдау саласында магистранттерге кәсіби құзіреттілік беру.

Пәннің міндеті магистранттардың үлкен деректерді талдау, арнайы әдістер мен талдау құралдарын пайдалану туралы теориялық және практикалық білімдерін алу болып табылады.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Пән жоғары технологиялық деректерге, құралдарға, архитектураларға және жоғары өнімді желілерде үлкен деректермен шешілетін есептеу жүйелеріне негізделген үлкен деректерді жасау, сақтау, басқару, беру, іздеу, талдауды зерттеуге бағытталған. BigData шешімдерінің кең ауқымын әзірлеуді, енгізуді және іске асыруды көрсететін нақты BigData қосымшалары мен түрлі салалардағы (әсіресе ғылым саласындағы) жұмыс үрдістері ұсынылған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді меңгеру нәтижесінде магистрант білуі керек:

- үлкен деректерді талдау үшін жаңа технологиялар, құралдар, архитектураны және жүйелерді;
- үлкен деректер саласындағы шешімдер;
- деректерді талдау, сақтау және жинау әдістері.

Қабілетті болу:

- үлкен деректерді талдау үшін соңғы технологиялар, құралдар мен жүйелерді қолдану;
- ірі деректер саласында практикалық шешімдерді пайдалану;
- деректерді жинау, сақтау және талдауды жүзеге асыру.

дағдылары болу керек:

- үлкен деректерді талдау;
- үлкен деректермен жұмыс істеу әдістері мен құралдарын қолдану.

Мобильді қосымшаларды және сымсыз желілерді қорғау технологилары

КОД – SEC222

КРЕДИТ -6

ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

Курстың мақсаты мобильді қосымшалар және сымсыз желілер қауіпсіздігі инфрақұрылымын қолдау, орнату,жобалау және жоспарлау. Алаяқтардың, сондай-ақ жеке кәсіпкерлердің қарсы шараларына ерекше көңіл бөлінеді.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Бұл курста сіз ұялы пайдаланушылар үшін сымсыз қатынау желілерінде түпнұсқалықты растауды, кілттерді таратуды, тұтастығын, құпиялылығын және анонимділігін іске асыру үшін функциялар, протоколдар және конфигурациялармен танысасыз. Курс WPAN, WLAN, UMTS, IMS сияқты қолданыстағы жүйелерде қолданылатын қауіпсіздік әдістерін ұсынады. Арнайы желілердің әртүрлі типтері сияқты жаңа желілік технологияларға ұсынылатын шешімдер. Сымсыз жүйелерде сандық кримрналистика.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді аяқтағандағы білім:

- сымсыз қатынау желілерінің мобильді пайдаланушыларына қызмет көрсететін байланыс жүйелерінің ақпараттық қорғау технологиялары мен әдістерін білу;
- WEE IEEE 802.11, WAN 802.16, GSM / UMTS / LTE, Ad-hoc және сенсорлық желілер сияқты қазіргі заманғы технологиялар сияқты сымсыз байланыс жүйелеріндегі қауіпсіздік механизмдері мен хаттамаларын білу және түсіну.
- аутентификация және негізгі қатынас хаттамалары үшін сымсыз желі қауіпсіздігінде қолданылатын кейбір модельдерді, жобалау принциптерін, механизмдерін және шешімдерін білу.

Дағдылар:

- сымсыз қатынау желілерінің мобильді пайдаланушыларына қызмет көрсететін әдістер мен технологиялардың ақпараттық қауіпсіздігін бағалауда байланыс жүйелері үшін практикалық және аналитикалық дағдыларды игеру.
- Сымсыз желілер мен ұялы қосымшаларды қорғаудағы тәжірибелік дағдылар.

Ақпараттық қауіпсіздік жүйелерін ұйымдастыру

КОД – SEC215
КРЕДИТ – 6 (1/1/1/3)
ПРЕРЕКВИЗИТ – жоқ.

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Ақпараттық қауіпсіздік жүйелерін ұйымдастыру» пәнінің мақсаты мекемедегі ақпараттық қауіпсіздік жүйелерін ұйымдастыру саласындағы кәсіби білімді қалыптастыру болып табылады.

Пәннің міндеттері болып: ақпараттық қауіпсіздікті қамтамасыз ету саласындағы халықаралық, отандық стандарттардағы ағымдық үрдістерді зерттеу, ұйымның ақпараттық қауіпсіздік жүйесін құру, қорғау объектілеріне, құпиялылық дәрежесіне, заманауи әдістерді, құралдарды және қауіпсіздік техникасын пайдалануды ескере отырып, тиімді қауіпсіздік саясаты мен бағдарламаларын әзірлеу.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

«Ақпараттық қауіпсіздік жүйелерін ұйымдастыру» оқу курсының бағдарламасы магистранттерді қорғауды ұйымдастыру, құру, ақпараттық қауіпсіздік жүйелерін құру, қауіпсіздік және қорғау бағдарламаларын әзірлеу, қорғау объектілерін анықтау, қылмыскердің моделін қалыптастыру, ақпараттық қауіпсіздіктің процедуралық деңгейлерінде қорғауды ұйымдастыру, тәуекелдерді талдау және оларды бағалау, қорғау әдістерін, құралдарын және технологияларын таңдау қорғау объектілерінің тәуелділіктері, құпиялылық дәрежесі және бизнестің бағытымен таныстыру болып табылады.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді меңгеру нәтижесінде магистрант түсінікке ие болуы керек:

- басқару принциптері және өндірістік қатынастардың негіздері туралы;
- қауіпсіздікті қамтамасыз ету саласындағы зерттеудің заманауй әдістері туралы;

Пәнді меңгеру нәтижесінде магистрант білуі керек:

- ақпаратты қорғау саласындағы заманауй технологиялар, бағдарламалық қамтама және есептеу техникасының құралдары мен әдістері;
- ақпаратты қорғау саласындағы заманауй технологиялар;
- ақпараттық қауіпсіздікті қамтамасыз ету бойынша халықаралық стандарт;
- Қазақстан Республикасының ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнамалық актілері;
- Қазақстан Республикасында келісілген ақпаратты қорғау және ақпараттық қауіпсіздік стандарттары мен ерекшеліктер.

Пәнді меңгеру нәтижесінде магистрант қабілетті болуы керек:

- ақпаратты қорғау саласында заманауй технологияларды құру және қолдану;
- ақпаратты қорғау заманауй технологияларын ақпараттық қауіпсіздік жүйелерінде қолдану;
- желілер мен жүйелердің ақпараттық қауіпсіздігін басқару.

Дағдылары болу керек:

- ұйымның ақпараттық қауіпсіздік жүйесінде қатерлер мен осалдықтарды анықтау;
- ұйымның қауіпсіздік бағдарламалары мен саясаттарын әзірлеу;
- ұйымның ақпараттық қауіпсіздігінің әкімшілік және іс жүргізу деңгейлерінде басқаруды және бақылауды қамтамасыз ету;
- ақпаратты қорғау әдістерін таңдау және талдау;
- объект қауіпсіздігін бағалау және қамтамасыз ету.

Ақпараттық қауіпсіздіктің аудиті

КОД – SEC204

КРЕДИТ – 6

ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Ақпараттық қауіпсіздік аудиті» пәнінің мақсаты ақпараттық қауіпсіздік аудиті саласында магистранттерге кәсіби құзіреттілік беру.

Пәннің міндеті магистранттарға кәсіпорынның ақпараттық қауіпсіздік аудитінің теориялық және практикалық білімдерін беру.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

«Ақпараттық қауіпсіздік аудиті» курсының бағдарламасы ақпараттық қауіпсіздік стандарттарын, аудиттерді ұйымдастыру мен өткізу әдістерін және олардың практикалық қолданылуын зерделеуге бағытталған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді меңгеру нәтижесінде магистрант білуі керек:

- АҚ стандарттары және АТ қауіпсіздігін бағалау критерийлері ;
- аудит типтері және этаптары;
- белсенді аудит құралдары мен әдістері;
- CVSS осалдығын бағалау жүйесі;
- АҚ аудитінде деректерді талдау әдістері.

Қабілетті:

- ішкі аудитті жүргізу жоспарын құру;
- ішкі аудитті жүргізу;
- CVSS осалдығын бағалау жүйесін қолдану;
- Тәуекелдерді талдау құралдарын қолдану.

Дағдыларға ие болу керек:

- енуге тестілеу жүргізу;
- тәуекелдерді талдау.

Киберқауіпсіздікте тәуекелдерді басқару

КОД – SEC 245
КРЕДИТ – 6
ПРЕРЕКВИЗИТ – жоқ

КУРС МАҚСАТТАРЫ ЖӘНЕ МІНДЕТТЕРІ

«Киберқауіпсіздіктегі тәуекелдерді басқару» пәнінің мақсаты - киберқауіпсіздіктегі тәуекелдерді басқару саласында магистранттерге кәсіби құзіреттілік беру.

Пәннің мақсаты - магистранттердің ақпараттық қауіпсіздік тәуекелдерін басқарудың теориялық және практикалық білімдерін меңгеруі.

«Киберқауіпсіздіктегі тәуекелдерді басқару» оқу курсының бағдарламасы тәуекелдерді басқару стандарттарын, тәуекелдерді бағалау құралдарын және олардың практикалық қолданылуын зерттеуге бағытталған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәндерді меңгеру нәтижесінде магистрант білуі керек:

- Ақпараттық қауіпсіздіктегі (АҚ) тәуекелдердің негізгі түсініктері;
- тәуекелдерді басқару стандарттары;
- ақпараттық қауіпсіздікті талдау және тәуекелдерді басқарудың негізгі мәселелері;
- компанияның ақпараттық тәуекелдерін бағалау әдісі;
- сандық және сапалық тәуекелділік шаралары;
- автоматты тәуекелдерді бағалау әдісі (АОР);
- ақпараттық қауіпсіздікті қамтамасыз ететін қарсы шаралар;

Қабілетті болу:

- тәуекелдерді бағалау;
- тәуекелді азайту үшін қарсы шаралар таңдау;
- тәуекелдерді алдаудың қарсы шараларын таңдау;
- тәуекел сипатын өзгерту үшін қарсы шаралар таңдау;
- АОР құралдарын пайдалану;

дағдылары бар:
- тәуекелдерді талдау;
- АОР көмегімен тәуекелдерді бағалау;
- тәуекелді қабылдау.

Аналитикалық деректер қоймалары және OLAP технологиялары

КОД – SEC 239
КРЕДИТ – 6
ПРЕРЕКВИЗИТ – жоқ

КУРС МАҚСАТТАРЫ ЖӘНЕ МІНДЕТТЕРІ

Деректерді өңдеу технологиясының принциптерін зерттеу.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

OLAP (ағылшын аналитикалық өңдеу) - деректерді өңдеу технологиясы, көп өлшемді принципке сәйкес құрылымдалған үлкен деректер жиынтығы негізінде біріктірілген ақпаратты дайындаудан тұрады. OLAP технологиясын енгізу Business Intelligence сыныбының бағдарламалық шешімдерінің құрамдас бөлігі болып табылады

Тану зияткерлік құралдары және кибершабуылдарға қарсы әрекет

КОД – SEC247
КРЕДИТ – 3
ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

Тану зияткерлік құралдары және кибершабуылдарға қарсы әрекет жұмысының принциптерімен танысу. Тану және кибершабуылдарға қарсы әрекет құралдары мен әдістерін тәжірибеде қолдану.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Ақпараттың ағып кету каналдары мен тәуекелдері. APT (Advanced Persistent Threat) шабуылдар. Деректерді ағып кетуден қорғау технологиялары. Кибершабуылдарға қарсы әрекет және тану жүйелері. DLP жүйелерінің жіктелуі, құпия ақпаратты тану әдістері. DLP жүйелерінің жұмыс кезеңдері. Жүйенің кибер-шабуылына қарсы тану және оған қарсы әрекет етудің зияткерлік құралдарын дамыту. Оқиғаларды тергеу және талдау үшін аналитикалық құралдар.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Білу:

- кибершабуылдарға қарсы іс-қимыл мен интеллектуалды құралдарды ақпараттық қорғау технологиялары мен әдістері туралы;
- кибер-шабуылдарды тану және қарсы тұрудың интеллектуалды құралдарының қауіпсіздік механизмдері туралы;
- кибершабуылға қарсы тану және қарсы тұру құралдарында қолданылатын модельдер, жобалау принциптері, механизмдері мен шешімдері туралы.

Дағдылар:

- кибер-шабуылдарды тану және қарсы тұрудың ақпараттық технологияларын және әдістерін қолдану;
- кибершабуылға қарсы іс-қимылдарды тану және оған қарсы әрекет етудің зияткерлік құралдарын қорғау тетіктерін қолдану;
- кибершабуылға қарсы тану және қарсы тұру әдістерінде қолданылатын модельдерді, құрылыстың принциптерін, механизмдерін және шешімдерін қолдану.

Шағын контроллерді бағдарламалау

КОД - SEC 218

КРЕДИТ – 6

ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

Микропроцессорлар мен микроконтроллерлерді құру, микроконтроллерлерді бағдарламалау, сонымен қатар микроконтроллерлерді қолданып криптографиялық жүйелердің электрондық компоненттерін құру, жасау принциптерін оқып үйрену.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Микроконтроллердің техникалық сипаттамалары және бағдарламалық жасақтамасы. Микропроцессорлық жұмыстың негізгі анықтамалары, сипаттамалары, қолдану аясы және ерекшеліктері. Микроконтроллерлердің түрлері және архитектурасы. Микроконтроллерлерді қолданатын криптографиялық жүйелерді жобалау. Микроконтроллерлердің жұмыс режимдері. Жадының ішкі жүйесін және интерфейстерді ұйымдастыру. Үзілістер мен ерекшеліктер жүйесі, сондай-ақ энергияны үнемдеу режимдері. Интерфейстердің типтері мен сипаттамалары, тікелей жадыға қол жеткізу (DMA) сопроцессорлары. Микроконтроллерлердің даму тенденциясы.

«Altium Designer» АЖЖ негізінде схемалық шешімдерді жобалау және әзірлеу. CooCox даму ортасында микроконтроллер жүйелерінің жеке блоктарының жұмысын бағдарламалау.

Микроконтроллерлердің техникалық мүмкіндіктерін қолдана отырып криптографиялық жүйелердегі әр түрлі мәселелерді шешуге арналған микроконтроллерлердің Си тілінде бағдарламалау дағдыларын қалыптастыру.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді игеру нәтижесінде магистрант білуі керек:

- микропроцессорлық жүйелердегі мәліметтерді ұсыну форматы және оларды өңдеу;
- электрондық құрылғылар (фотоэлектрондық құрылғылар, транзисторлар және т.б.);
- микросхемалар (жұмыс күшейткіштері, тұрақтандырғыштар және т.б.) және олардың белгісі (SMD компоненттері), тағайындалуы, өлшемдері, сипаттамалары.

Білу:

- АЖЖ жүйелерін қолдана отырып, электронды компоненттердің электр тізбектерін жобалау және әзірлеу;
- құрылғылардың электрлік компоненттерін монтаждауды жүзеге асыруға;

- өлшеу құралдарын тәжірибеде қолдану.

Киберқылмыс және компьютерлік криминалистика

КОД – SEC240
КРЕДИТ – 6
ПРЕРЕКВИЗИТ – жоқ
КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Киберқылмыс және компьютерлік криминалистика» пәнінің мақсаты магистранттерге киберқылмыстарды тергеу және киберқылмыс саласында кәсіби құзіреттілік беру.

«Киберқылмыс және компьютерлік криминалистика» пәнін оқудың міндеті компьютерлік ақпаратпен байланысты қылмысты ашу құралдары мен жүйелерді қолдану принциптерін меңгеру.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Форензика негіздері(компьютерлік криминалистика, киберқылмыстарды тергеу) - компьютерлік ақпаратпен байланысты қылмысты ашу туралы қолданбалы ғылым. Сандық дәлелдер мен іздеу әдістері, дәлелдерді алу мен бекітуге зерттеу жүргізу құралдары зерттеледі.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді меңгеру нәтижесінде магистрант білуі керек: Форензика негіздері, компьютерлік криминалистиканың сұрақтары мен шешімдері; сандық дәлелдерді зерттеу құралдары.

Қабілетті болу:

- тергеу жүргізу;
- сандық дәлелдерді зерттеу;
- киберқылмысты анықтаудың заманауи әдістері мен құралдарын қолдану.

Дағдыларға ие болу:

- киберқылмысты тергеудің заманауи әдістері мен құралдарын қолдану.
- киберқылмысты анықтау;
- сандық дәлелдерге талдау жүргізу.

Магистерлік диссертацияны қорғау
КОД – ECA2013
КРЕДИТ –12

Магистрлік диссертацияның мақсаты: Магистранттың ғылыми-зерттеу біліктілігінің деңгейін көрсету, өзіндік ғылыми ізденіс жүргізу қабілеті, белгілі бір ғылыми және практикалық мәселелерді шешу қабілеттілігін тексеру, оларды шешудің кең таралған әдістері мен әдістерін білу.

ҚЫСҚАША СИПАТТАМАСЫ

Магистрлік диссертация - магистранттың ішкі бірлікке ие және таңдап алынған тақырыпты дамытудың прогресі мен нәтижелерін көрсететін нақты саладағы нақты мамандықтың өзекті мәселелерінің бірін тәуелсіз зерттеу нәтижелерін синтездейтін соңғы біліктілік ғылыми жұмыс

Магистрлік диссертация – магистранттың магистранттың барлық оқу кезеңінде өткізілген ғылыми – зерттеу/ экспериментальды – зерттеу жұмысының қорытындысы.

Магистрлік диссертация қорғау магистрлік дайындықтың соңғы кезеңі болып табылады. Магистрлік диссертация келесі талаптарға сай болуы керек:

- жұмыс ақпараттық қауіпсіздік және қауіпсіздік саласындағы өзекті мәселелерді зерттеуге немесе шешуге тиіс;
- жұмыс маңызды ғылыми проблемаларды анықтауға және оларды шешуге негізделуі тиіс;
- шешімдер ғылыми негізделген және сенімді болуға, ішкі бірлікке ие болуы тиіс;
- диссертациялық жұмыс / жоба дербес жазылуға тиіс.

Мазмұны