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

БІЛІМ БЕРУ БАҒДАРЛАМАСЫ

7М06104 - «АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ КЕШЕНДІ ҚАМТАМАСЫ»

(ғылыми-педагогиғалық бағыт, 2 жыл)

техника ғылымдарының магистрі

ҚР 2018 жылғы жоғары оқу орнынан кейінгі ББМЖМС сәйкес

2-ші басылым

Алматы 2020

Бағдарлама жасалды және тараптар қол қойды:

Қ.И. Сәтпаев атындағы ҚазҰТЗУ атынан:

Кибернетика және ақпараттық технологиялар институтының директоры — Н.А. Сейлова

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

«Киберкауіпсіздік, ақпаратты өңдеу және сақтау" кафедрасының УМГ төрайымы — Е.Ж.Айтхожаева

Жұмыс беруші атынан:

ЖШС « Казтелепорт» департамент директоры — Толсулиев 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 15.12.2020 ж.

Біліктілік:
7-деңгей: Ұлттық біліктілік шеңбері:

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

1 Бағдарламаның қысқаша сипаттамасы:

1 Білім бағдарламасының мақсаты:

Білім бағдарламасының мақсаты магистранттарды ғылыми – педагогикалық бағытта оқыту. Білім бағдарламасы тиісті құзыреттерге қол жеткізумен қатар, әртүрлі тәжірибе түрлерін (зерттеу, эксперименталдық, 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 ақпараттық-техникалық қорғалуына бағытталған.

Ақпараттық қауіпсіздіктегі ғылыми-педагогикалық 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 толықтырулармен 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 05.05.2020ж. №182 бұйрығы.

- 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 студенттерге 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;
- Эксперименталдік – 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.

2 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. Ғылыми- педагогикалық магистратурада оқудың барлық кезеңінде магистранттың оқу және ғылыми қызметінің барлық түрлерін қосқанда 120-дан кем емес академиялық кредиттер игерілуі тиіс.

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

Ғылыми және педагогикалық бағыттағы магистратура жоғары оқу орнынан кейінгі білім беру бағдарламаларын ғылыми және ғылыми-педагогикалық кадрларды жоғары оқу орындары мен ғылыми ұйымдар үшін терең ғылыми, педагогикалық және ғылыми тағылымдамадан өткізуді 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 диссертацияны орындауды қоса алғанда, ғылыми – 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.

- 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 ұйымдастырушылық 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.

Магистратура бағдарламасын меңгерген түлек магистратура бағдарламасы бағытталған кәсіптік қызмет түрлеріне сәйкес келетін кәсіби біліктілікке ие болуға тиіс:

Ғылыми- зерттеу қызметі:

- магистратураны меңгеру барысында алынған ғылымның іргелі бөлімдерін және мамандандырылған білімін біріктіру арқылы кәсіби проблемаларға диагностикалық шешімдерді қалыптастыру мүмкіндігі;

- өз бетінше кәсіби салада ғылыми эксперименттер және зерттеулер жүргізу,
эксперименттік ақпаратты жинақтап, талдау, қорытындылар жасау, ұсыныстар мен қорытындыларды тұжырымдау;

- ақпаратты қорғау және қауіпсіздік саласындағы терең теориялық және практикалық білімдерді қолдану негізінде зерттелетін объектілердің модельдерін құру және зерттеу мүмкіндігі.

ғылыми- өндірістік қызмет:

- тәжірибелік міндеттерді шешу үшін өз бетінше өндірістік және ғылыми-өндірістік, зертханалық және түсіндірме жұмыстарын жүргізу;

- Магистратураның меңгерген бағдарлама саласында заманауи зертханалық жабдықтар мен аспаптарды кәсіби пайдалану мүмкіндігі;

- өндірістік міндеттерді шешу үшін кешенді ақпаратты өңдеу мен интерпретациялаудың заманауи әдістерін қолдану мүмкіндігі;

жобалық қызмет:

- ақпараттық қауіпсіздік саласында өз бетінше ғылыми- зерттеу және ғылыми- өндірістік жұмыстардың жобаларын жасау және ұсыну;

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

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;

ғылыми- педагогикалық қызмет:

- семинарлық, зертханалық және тәжірибелік сабақтарды жүргізу;
- ақпараттық қауіпсіздікті қамтамасыз ету саласында студенттердің ғылыми –оқу жұмысын басқаруға қатысу мүмкіндігі.

4 Жұмыс оқу жоспары және модульдік білім беру бағдарламасы
4.1. Оқу мерзімі 2 жыл

ЖҰМЫС ОҚУ ЖОСПАРЫ
7М**06104- «Ақпараттық қауіпсіздіктің кешенді қамтамасы»**
білім бағдарламасы

Академиялық дәрежесі: техника ғылымдарының магистрі
Оқу мерзімі:2ж.

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 семестр							**2 семестр**						
	HUM201	Ғылым тарихы мен философиясы	БП ЖК	4	2	1/0/1/2		LNG202	Шет тілі (Кәсіби)	БП ЖК	6	3	0/0/3/3	
	HUM207	Жоғары мектеп педагогикасы	БП ЖК	4	2	1/0/1/2		HUM204	Басқару психологиясы	БП ЖК	4	2	1/0/1/2	
		Электив	ПП ТК	6	3				Электив	ПП ТК	6	3		
		Электив	БП ТК	6	3				Электив	ПП ТК	6	3		
									Электив	БП ТК	6	3		
									Электив	БП ТК	6	3		
1	AAP242	Магистранттың ғылыми-зерттеу жұмысы, оның ішінде тағылымдамадан өту магистрлік диссертацияны орындау	МҒЗЖ	6				AAP244	Педагогикалық тәжірбие	БП ЖК	4			
								AAP242	Магистранттың ғылыми-зерттеу жұмысы, оның ішінде тағылымдамадан өту магистрлік диссертацияны орындау	МҒЗЖ	6			
		Барлығы		**26**							**44**			

	3 семестр							4 семестр						
	SEC204	Ақпараттық қауіпсіздіктің аудиті	ПП ЖК	6	3	2/1/0/3		AAP242	Магистранттың ғылыми-зерттеу жұмысы, оның ішінде тағылымдамадан өту магистрлік диссертацияны орындау	МҒЗЖ	6			
		Электив	ПП ТК	6	3			AAP243	Зерттеу тәжірбиесі	ПП	7			
2		Электив	ПП ТК	6	3			ECA205	Магистрлік диссертацияны рәсімдеу және қорғау (МДРжҚ)	ҚА	12			
		Электив	ПП ТК	6	3									
	AAP242	Магистранттың ғылыми-зерттеу жұмысы, оның ішінде тағылымдамадан өту магистрлік диссертацияны орындау	МҒЗЖ	6										
		Барлығы		**30**					**Барлығы**		**25**			
									Жалпы		**125**			

7М**06104**- «Ақпараттық қауіпсіздіктің кешенді қамтамасы» білім бағдарламасының ЭЛЕКТИВТІ ПӘНДЕР КАТАЛОГІ

БП Таңдау компонентері - 18 кредит					
	Код	**Пәннің аты**	**Кредит**	**Дәр/зертх/прак/СӨЖ**	**Семестр**
	SEC221	Желілік ОЖ-дің қауіпсіздік құралдары	6	2/0/1/3	1
	CSE249	Model-Driven Software Engineering	6	2/0/1/3	
	SEC201	Ақпаратты криптологиялық қорғау алгоритмдері	6	2/0/1/3	2
	SEC 238	Стеганографиялық ақпаратты қорғау әдістері	6	1/1/1/3	
	SEC244	Виртуализация және бұлт жүйелерінің қауіпсіздіг	6	2/1/0/3	2
	SEC 208	Ақпаратты инженерлік-техникалық қорғау	6	1/1/1/3	
		Барлығы	**18**		
ПП Таңдау компонентері - 42 кредит					

	SEC215	Ақпараттық қауіпсіздік жүйелерін ұйымдастыру	6	1/1/1/3	1
	GEN200	Инженерия саласындағы сандық әдістер	6	1/1/1/3	2
	SEC214	ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру	6	2/0/1/3	2
	CSE746	Machine Learning & Deep Learning	6	2/0/1/3	3
	CSE720	Киберқылмыс пен компьютерлік сот сараптамасы	6	2/1/0/3	3
	SEC218	Шағын контроллерді бағдарламалау	6	2/1/0/3	3
	SEC245	Киберқауіпсіздікте рисктерді басқару	6	2/0/1/3	3
	SEC206	Электрондық бизнес жүйелерінің қауіпсіздігі	6	2/1/0/3	3
	SEC246	Big Data және деректер анализы	6	2/1/0/3	3
		Барлығы	**36**		

МОДУЛДІК БІЛІМ БЕРУ БАҒДАРЛАМАСЫ

Білім беру бағдарламасы: 7М**06104 - Ақпараттық қауіпсіздіктің кешенді қамтамасы**

Оқу түрі: Күндізгі
Оқу мерзімі:2ж.
Академиялық дәрежесі: техника ғылымдарының магистрі

Пәннің циклі	Пәннің коды	Пәннің аты	Семестр	акад. кредитте	Дәр	зерт	прак.	ОӨЖ	Бақылау түрі	Каф
Профиль бойынша оқыту модулі										
Базалық пәндер (БП) (40 кредит)										
ЖОО компоненті (18 кредит)										
БД 1.1.1	HUM201	Ғылым тарихы мен философиясы	1	4	1	0	1	2	Емтихан	ҚП
БД 1.2.1	HUM207	Жоғары мектеп педагогикасы	1	4	1	0	1	2	Емтихан	ҚП
БД 1.3.1	LNG202	Шет тілі (Кәсіби)	2	6	0	0	3	3	Емтихан	АТ
БД 1.4.1	HUM204	Басқару психологиясы	2	4	1	0	1	2	Емтихан	ЖБҒББО
Практикалық-бағдарланған модуль										
	AAP244	Педагогикалық практика	2	4					Есеп	
Таңдауы бойынша компонент (18 кредит)										
Желілік қауіпсіздікті және бұлтты технологияларды және ақпаратты криптографиялық қорғауды қамтамасыз ету модулі										
БД	SEC221	Желілік ОЖ-дің қауіпсіздік құралдары	1	6	2	0	1	3	Емтихан	КАӨжС
БД	CSE249	Model-Driven Software Engineering			2	0	1	3	Емтихан	КАӨжС
БД	SEC201	Ақпаратты криптологиялық қорғау алгоритмдері	2	6	2	0	1	3	Емтихан	КАӨжС
БД	SEC 238	Стеганографиялық ақпаратты қорғау әдістері			1	1	1	3	Емтихан	КАӨжС
БД	SEC244	Виртуализация және бұлт жүйелерінің қауіпсіздіг	2	6	2	1	0	3	Емтихан	КАӨжС
БД	SEC 208	Ақпаратты инженерлік-техникалық қорғау			1	1	1	3	Емтихан	КАӨжС
Профильді пәндер (ПП)(49 кредит)										
Ғылыми зерттеулер, ақпараттық қауіпсіздік жүйесін ұйымдастыру және ақпаратты қорғауды қамтамасыз ету модулі										
ЖОО компоненті (6 кредит)										
ПД	SEC204	Ақпараттық қауіпсіздіктің аудиті	3	6	2	1	0	3	Емтихан	КАӨжС
Таңдауы бойынша компонент (36 кредит)										
ПД	SEC215	Ақпараттық қауіпсіздік жүйелерін ұйымдастыру	1	6	1	1	1	3	Емтихан	КАӨжС
ПД	GEN200	Инженерия саласындағы сандық әдістер	2	6	1	1	1	3	Емтихан	ҚМжИГ
ПД	SEC214	ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру	2	6	2	0	1	3	Емтихан	КАӨжС
ПД	CSE746	Machine Learning & Deep Learning	3	6	2	0	1	3	Емтихан	БЖ
ПД	CSE720	Киберқылмыс пен компьютерлік сот			2	1	0	3	Емтихан	КАӨжС

		сараптамасы	3	6						
ПД	SEC218	Шағын контроллерді бағдарламалау	3	6	2	1	0	3	Емтихан	КАӨжС
ПД	SEC245	Киберқауіпсіздікте рисктерді басқару	3	6	2	0	1	3	Емтихан	КАӨжС
ПД	SEC206	Электрондық бизнес жүйелерінің қауіпсіздігі	3	6	2	1	0	3	Емтихан	КАӨжС
ПД	SEC246	Big Data және деректер анализы	3	6	2	0	1	3	Емтихан	КАӨжС
Практикалық-бағдарланған модуль										
ПД	AAP236	Зерттеу практикасы	4	7					Есеп	
Ғылыми-зерттеу модулі (24 кредит)										
МҒЗЖ	AAP242	Магистранттың ғылыми-зерттеу жұмысы	1	6					Есеп	
МҒЗЖ	AAP242	Магистранттың ғылыми-зерттеу жұмысы	2	6					Есеп	
МҒЗЖ	AAP242	Магистранттың ғылыми-зерттеу жұмысы	3	6					Есеп	
МҒЗЖ	AAP242	Магистранттың ғылыми-зерттеу жұмысы	4	6					Есеп	
Қорытынды аттестациялау модулі (12 кредит)										
ИА	ECA205	Магистрлік диссертацияны рәсімдеу және қорғау	4	12					Диссертация қорғау	
		Барлығы		**125**						

5 Білімі, дағдысы мен құзыреттілігінің деңгейі мен көлемі туралы дескрипторлар

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) зерттеліп отырған ақпараттық технологиялар мен ақпараттық қауіпсіздік саласындағы білім мен түсініктің дамуын көрсетуге;

2) кәсіби деңгейде өзінің білімін, түсінігін және жаңа ортадағы мәселелерді шешу қабілеттерін, пәнаралық тұрғыдан кеңірек қолдануға;

3) әлеуметтік, этикалық және ғылыми ойларды ескере отырып, пікірлер қалыптастыру үшін ақпаратты жинауға және түсіндіруге;

4) ақпаратты, идеяларды, тұжырымдарды, мәселелер мен шешімдерді мамандарға да, маман емес адамдарға да айқын және біржақты жеткізуге;

5) оқылатын ақпараттық технологиялар мен ақпараттық қауіпсіздік саласындағы қосымша білім беруді өз бетінше жалғастыру үшін қажетті оқу дағдылары.

6 Оқуды аяқтағандағы құзіреттіліктер

6.1 Ғылыми және педагогикалық магистратура түлектерінің негізгі құзыреттеріне қойылатын талаптар:

1) түсінікке ие болу керек:

- қоғамдық өмірдегі ғылым мен білімнің рөлі туралы;
- ғылыми танымды дамытудағы заманауй тенденциялары туралы;
- жаратылыстану (әлеуметтік, гуманитарлық, экономикалық) ғылымдарының өзекті әдістемелік және философиялық мәселелері туралы;
- жоғары оқу орнының оқытушысының кәсіби біліктілігі туралы;
- жаһандану процестерінің әлеуметтік – экономикалық салдары мен қайшылықтары туралы;
- ақпараттық қауіпсіздік және қорғау саласындағы кәсіби біліктілік туралы;
- ресурстар мен платформалардың технологиялық виртуализациясы туралы;
- ақпараттық қауіпсіздік құралдарын интеллектуализациялау туралы;
- ДҚ қорғау технологиясы туралы;
- ақпаратты криптографиялық қорғаудың алгоритмдері туралы;
- үлкен деректерді талдау туралы.

2) білу керек:

- ғылыми танымның әдістемесін;
- ғылыми қызметті ұйымдастырудың құрылымы мен принциптері;
- оқу процесінде студенттердің 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;
- ОЖ ақпаратын тасымалдаушылардың ішкі ұйымдастырылуы;
- Негізгі ақпаратты сақтау және шифрлау әдістері мен құралдары;
- 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;
- ақпараттың инженерлік- техникалық қорғалуы.

3) қабілетті болу керек:

- алынған білім ғылыми зерттеулер контексінде идеяларды түпнұсқа әзірлеу және қолдану үшін пайдалану;
- үрдістер мен құбылыстарды талдау үшін қолданыстағы ұғымдарды, теориялар мен тәсілдерді сыни талдау;
- жаңа таныс емес жағдайлардағы зерттеу мәселелерін шешу үшін әртүрлі пәндерден алынған білімді интеграциялау;
- білімді интеграциялау, шешімдер қабылдау және толық емес немесе шектеулі ақпарат негізінде шешімдер қабылдау;
- педагогикалық және психология білімдерін өздерінің педагогикалық қызметінде қолдануға;
- оқытудың интерактивті әдістерін қолдануға;
- заманауи ақпараттық технологияларды тарту арқылы ақпараттық-талдамалық және ақпараттық-библиографиялық жұмысты жүргізу;
- жаңа проблемаларды және жағдайларды шешу үшін шығармашылық және шығармашылық ойлау;
- жоғары оқу орындарында арнайы пәндерді зерттеу және оқытуды жүзеге асыруға мүмкіндік беретін кәсіби деңгейде шет тілін еркін меңгеру;
- диссертация, ғылыми мақала, баяндама, аналитикалық жазба және т.б. түрінде ғылыми-зерттеу және аналитикалық жұмыстардың нәтижелерін қорытындылайды;

- ақпараттың криптографиялық қорғау алгоритмдерін қолдану
- ақпараттық қауіпсіздік стандарттарын қолданады және АТ қауіпсіздігін бағалауды жүргізеді;
- 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.

4) дағдылары болу керек:

- ғылыми- зерттеу қызмет, стандартты ғылыми міндеттерді шешу;
- кредиттік технология оқу бойынша білімдік және педагогикалық қызметті жүзеге асыру;
- кәсіптік пәндерді оқыту әдістемесі
- оқу үрдісінде заманауи ақпараттық технологияларды пайдалану
- кәсіби қарым-қатынас және мәдениетаралық қарым-қатынас
- ауызша және жазбаша түрде өз ойларының шешендік, дұрыс және логикалық дизайны;
- 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 қызметте және докторантурада үздіксіз білім алуға қажетті білімді кеңейту және тереңдету.

5) құзіретті болу керек:

- ғылыми зерттеу методология саласында;
- жоғары оқу орындарында ғылыми-педагогикалық қызмет саласында;
- қазіргі заманғы білім беру технологиялары мәселелерінде;
- ғылыми жобалар мен кәсіби салада зерттеулер жүргізу;
- ақпараттық қауіпсіздік жүйелерін ұйымдастыруда;
- ақпараттық қауіпсіздік аудитін жүргізуде;
- ұйымның ақпараттық қауіпсіздігін қамтамасыз етуде;
- білімді үнемі жаңартып, кәсіби дағдылар мен қабілеттерін кеңейту жолдары.

Б- Базалық білімдер, қабілеттер, және дағдылар

Б1- Желілік операциялық жүйелердің қауіпсіздігін бағалай білу.

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 кибер қылмыстар мәселелерінде құзіретті болу, қатерлерді анықтауға қабілетті болу және шабуылдардың алдын алу жұмыстарын жүргізу;

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

К3 - ақпараттық қауіпсіздік жүйелерін ұйымдастыруды біледі және интеграцияланған ақпараттық қауіпсіздікті қамтамасыз етуде жұмыс істей алады.

К4 - ақпараттарды инженерлік және техникалық қорғау мәселелерінде құзыретті болуға тиіс.

К5 – сымсыз қауіпсіздік инфрақұрылымын жоспарлау, жобалау, орнату және қолдау мүмкіндігіне ие болу.

К6 – кибер шабуылдарға қарсы әрекет және интеллектуалды тану құралдарын пайдалануда құзіретті болу.

К7-АҚ стандарттарын және АТ қауіпсіздігін бағалау критерийлерін білу, белсенді аудит құралдарын және 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.

Р - кәсіби құзыреттіліктер:

Р1 - ақпараттық қауіпсіздік жүйелерін ұйымдастыру мәселелерін біледі және іс жүзінде интеграцияланған ақпараттық қауіпсіздік бойынша жұмыстар жүргізе алады.

Р2 - қолданбалы есептерді техникада сандық әдістерді қолдана отырып шеше білу

Р3 - дерекқорды қорғау және қауіпсіздік жүйесін ұйымдастыра білу және мәліметтер қорын қорғау технологияларын қолдану.

Р4 - машиналық оқыту және тереңдетіп оқыту модельдерінде құзыретті болыңыз

Р5- киберқылмыс пен компьютерлік криминалистикаға құзыретті, қауіп-қатерлерді анықтай алады және кірудің алдын алу шараларын жүргізе алады.

Р6 - әмбебап тілдерде бағдарламаларды жоспарлау, жобалау, бағдарламалау және күйін келтіруді білу.

Р7 - АЖ стандарттарын және АТ қауіпсіздігін бағалау критерийлерін білу, белсенді аудиттің әдістері мен құралдарын қолдана білу.

Р8 - Электрондық бизнестегі қауіпсіздік қатерлерінің қолданыстағы түрлері бойынша сауатты болу. Автоматтандырылған банктік жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету мүмкіндігі.

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

6.2. Ғылыми – педагогикалық магистратурада магистранттың ғылыми – зерттеу жұмысына талаптар:

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

2) өзекті, ғылыми жаңалығы мен тәжірибелік маңызы бар;

3) ғылым және тәжірибенің заманауй теориялық, әдістемелік және технологиялық жетістіктеріне негізделген;

4) ғылыми зерттеулердің заманауй әдістерін қолданумен орындалады;

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

6) тиісті білім саласындағы халықаралық озық тәжірибелерге негізделген.

6.3. Тәжірибені ұйымдастыруға талаптар:

Ғылыми – педагогикалық магистратураның білім бағдарламасы теориялық оқумен қатар жеке кезеңдерде де өткізілетін тәжірибенің екі түрін қамтиды:

1) БД циклінде педпгогикалық – ЖОО-да;
2) КД циклінде зерттеу – диссертацияны орындау орнында;

Педагогикалық тәжірибе оқу және оқыту әдістемесінің тәжірибелік дағдыларын қалыптастыру мақсатында жүргізіледі. Бұл жағдайда магистранттар университеттің қалауы бойынша бакалавриатта сабақ жүргізуге тартылады.

Магистранттың ғылыми тәжірибесі отандық және шетелдік ғылымның соңғы теориялық, әдістемелік және технологиялық жетістіктерімен, ғылыми зерттеулердің қазіргі заманғы әдістерімен, эксперименталды деректерді өңдеу мен интерпретациялаумен танысу мақсатында жүргізіледі.

7 ECTS стандарты бойынша дипломға қосымша

Қосымша Еуропалық Комиссияның, Еуропа 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. Еуропалық 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.

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

8 Модулдер және оқу нәтижелері тізімі

Модуль атауы	**Кәсіби құзірет**	**Модульді қалыптастыратын пәндер**
Бейіндік оқыту модулі	Ғылымның философиялық сұрақтарын, ғылым дамуының негізгі тарихи этаптарын түсіну, ғылыми - философиялық мәселелердә сыни бағалау және талдау, инженерлік ғылымның ерекшеліктерін түсіну, аналитикалық ойлау және философиялық ойлау дағдыларына ие болу, өздерінің ұстанымдарын ақтауға және қорғауға, талқылау мен диалогқа қатысуға, өздерінің кәсіби қызметінде қарым-қатынас пен шығармашылық дағдыларына ие болу. Психология және педагогика мәселелері бойынша білікті болу.	Ғылым философиясы тарихы, жоғары мектеп педагогикасы, басқару психологиясы
Желілік қауіпсіздікті және бұлтты технологияларды және ақпаратты криптографиялық қорғауды қамтамасыз ету модулі	ДҚ қауіпсіздігі мен қорғау жүйесін ұйымдастыра білу және ДҚ қорғау технологияларын қолдану, ақпаратты криптографиялық қорғау дамуының перспективті және заманауй бағыттарын білу және оларды тәжірибеде қолдану. Ақпараттың қауіпсіздігі және қорғалуы кешенді қамтамасын ұйымдастыра білу. Мәліметтер қорын қорғау және қауіпсіздік жүйесін ұйымдастыра білу және мәліметтер қорын қорғау технологияларын қолдана білу, ақпаратты криптографиялық қорғаудың қазіргі заманғы және перспективалық бағыттарын білу және оны практикада қолдана білу. Ақпаратты кешенді қорғауды және қауіпсіздікті ұйымдастыра білу.	ДҚ қауіпсіздігі және қорғалуын ұйымдастыру, Ақпаратты криптографиялық қорғаудың алгоритмдері, Ақпараттық қауіпсіздік жүйелерін ұйымдастыру. Желілік операциялық жүйелерге арналған қауіпсіздік құралдары, виртуалдандыру жүйелері мен бұлтты технологиялардың қауіпсіздігі, криптографиялық ақпаратты қорғау алгоритмдері, инженерлік және техникалық ақпарат қауіпсіздігі, модельді басқаратын бағдарламалық қамтамасыз ету, стеганографиялық ақпараттық қауіпсіздік әдістері.

Ғылыми зерттеулер, ақпараттық қауіпсіздік жүйесін ұйымдастыру және ақпаратты қорғауды қамтамасыз ету модулі	Мәліметтер қорын қорғау және қауіпсіздік жүйесін ұйымдастыра білу және мәліметтер қорын қорғау технологияларын қолдана білу, ақпаратты криптографиялық қорғаудың қазіргі заманғы және перспективалық бағыттарын білу және оны практикада қолдана білу. Ақпаратты кешенді қорғауды және қауіпсіздікті ұйымдастыра білу. Компьютерлік криминалистика және киберқылмыстарды анықтау мәселелерінде құзіретті болу. Кибершабуылдарды тану және қарсы тұру құралдарын қолдана білу. Ақпаратты техникалық қорғаудың техникалық құралдары мен әдістерін білу, ақпаратты инженерлік – техникалық қорғауды ұйымдастыруда құзіретті болу.Үлкен деректерді талдай білу, үлкен деректерді талдау құралдары мен әдістерін білу. Киберқылмысты анықтау және компьютерлік криминалистика бойынша білікті болу. Кибер шабуылдарды тану және оларға қарсы тұру құралдарын қолдана білу. Ақпараттың техникалық құралдары мен әдістерін білу, ақпаратты инженерлік-техникалық қорғауды ұйымдастыруда құзыретті болу. Үлкен деректерді талдай білу, үлкен деректерді талдау әдістері мен құралдарын білу. Ақпараттық қауіпсіздік аудитін жүргізудің әдістері мен құралдарын білу және қолдану	Мәліметтер базаларын қорғауды және қауіпсіздікті ұйымдастыру, ақпараттық қауіпсіздік жүйелерін ұйымдастыру, инженериядағы сандық әдістер, машиналық оқыту және терең оқыту. Компьютерлік криминалистика және киберқылмыс, Кибершабуылдарды тану және қарсы тұру зияткерлік құралдары, Ақпаратты инженерлік – техникалық қорғау, Big Data және деректерді қорғау. Киберқылмыс және компьютерлік криминалистика, микроконтроллерді бағдарламалау, үлкен мәліметтер және деректерді талдау Ақпараттық қауіпсіздік аудиті, Ақпараттық қауіпсіздік тәуекелдерін басқару, киберқылмыс және компьютерлік криминалистика, Үлкен мәліметтер мен деректерді талдау, Электрондық бизнес жүйелерінің қауіпсіздігі.

Ғылыми – зерттеу модулі	Ғылыми таным дамуындағы заманауй үрдістер туралы түсінік. Ғылыми таным әдістемесін білу. Ғылыми зерттеулердің мәселелерін, міндеттерін және әдістерін қалыптастыру, байқау, эксперимент, эмпирикалық деректерді ғылыми талдау, ғылыми мақалаларды қайта қарау, әлемдік ғылым мен өндірістегі жинақталған ақпараттарға аналитикалық шолулар жасай отырып, жаңадан алынған сенімді фактілерді алу, ғылымда бұрын жинақталған нәтижелерді жинақтау. білімі, тұжырымдары мен практикалық ұсыныстарды тұжырымдай отырып, өкілдік және түпнұсқа зерттеулердің нәтижелері. IT-технология саласында ғылыми жобалар мен зерттеулерді орындау үшін қажет құзіреттерді алу.	Магистранттың ғылыми – зерттеу жұмысы, Зерттеу тәжірибесі.
Тәжірибеге бағытталған модуль	Өз бетінше ғылыми – зерттеу жұмыс және ғылыми ұжымда жұмыс дағдыларын алу. Жаңа идеяларды қалыптастыру қабілеті. Кәсіби салада ғылыми жобалар мен зерттеулерді жүзеге асыруда, білімді үнемі жаңартып, кәсіби дағдылар мен қабілеттерін кеңейту жолында тәжірибе. Ақпараттық технологияларды тарту арқылы ақпараттық-аналитикалық және ақпараттық-библиографиялық жұмыстарды жүргізу қабілеті. Теориялық білімді IT-саласында өндіріс проблемаларын шешуде өз тұжырымдарын әзірлеу және ұсыну. Кәсіпкерлікті ұйымдастыру және басқару саласында қиын және ерекше жағдайларда шешімдер қабылдау мүмкіндігі.	Педагогикалық тәжірибе, зерттеу тәжірибесі
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 Пәндер сипаттамасы

Шет тілі (кәсіби)
КОД – LNG202
КРЕДИТ – 6 (0/0/3/3)
ПРЕРЕКВИЗИТ –Academic English, Business English, IELTS 5.0-5.5

КУРС МАҚСАТТАРЫ ЖӘНЕ МІНДЕТТЕРІ

Курстың мақсаты - студенттердің 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. Студенттер 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 студенттер 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.

Ғылым тарихы және философиясы
КОД – HUM201
КРЕДИТ – 4 (1/0/1/2)
ПРЕРЕКВИЗИТ - HUM124

КУРС МАҚСАТТАРЫ ЖӘНЕ МІНДЕТТЕРІ – ғылым мен философия байланысын ашып көрсету, ғылым мен ғылыми білімдердің философиялық мәселелерін, ғылым тарихының негізгі кезеңдерін, ғылым философиясының жетекші тұжырымдамаларын, ғылыми-техникалық шындықты дамытудың заманауи мәселелерін айқындау.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ - ғылымның философиясы, ғылымның динамикасы, ғылымның ерекшелігі, антикалық және теориялық ғылымның қалыптасуы, ғылымның тарихи дамуының негізгі кезеңдері, классикалық ғылымның классикалық емес ғылымдары, математика, физика, инженерия және технология философиясы, ғылым, этика, ғалым мен инженердің әлеуметтік және моральдық жауапкершілігі.

БАСҚАРУ ПСИХОЛОГИЯСЫ

КОД - HUM204

Кредит – 4 (1/0/1/2)

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 студенттер 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.

Жоғары мектеп педагогикасы

КОД – HUM207

КРЕДИТ – 4 (1/0/1/2)

ПРЕРЕКВИЗИТ

Курстың мақсаты мен міндеттері курс жоғары мектептің білім беру үрдісінің психологиялық-педагогикалық мәнін меңгеруге; қазіргі кезеңдегі жоғары мектептің дамуының негізгі тенденциялары туралы түсініктерді қалыптастыруға, жоғары мектепте оқу үрдісінің әдістемелік негіздерін, сонымен қатар оқытудың табыстылығына, өзара әрекеттесуіне, оқу үрдісінің субъектілерін басқаруына әсер ететін психологиялық механизмдерді қарастыруға бағытталған. Магистранттардың психологиялық-педагогикалық ойлауын дамыту.

Курстың қысқаша сипаттамасы курсты оқу барысында магистранттар жоғары мектеп дидактикасымен, жоғары мектепте оқытуды ұйымдастыру формалары мен әдістерімен, табысты оқытудың психологиялық факторларымен, психологиялық әсер ету ерекшеліктерімен, тәрбиелік ықпал ету механизмдерімен, педагогикалық технологиялармен, педагогикалық қарым-қатынас сипаттамаларымен, оқыту процесін басқару механизмдерімен танысады. Ұйымдастырушылық жанжалдар мен оларды шешу тәсілдерін, педагог тұлғасының психологиялық деструкциялары мен деформацияларын талдайды.

Курсты аяқтағаннан кейінгі білім, білік, дағды – курсты аяқтағаннан кейін магистрант қазіргі заманғы жоғары кәсіптік білім беру жүйесінің ерекшеліктерін, педагогикалық зерттеуді ұйымдастыруды, білім беру үдерісі субъектілерінің сипаттамаларын, жоғары мектепте оқу үдерісін ұйымдастырудың дидактикалық негіздерін, педагогикалық технологияларды, педагогикалық қарым-қатынастың заңдылықтарын, студенттерге тәрбиелік Ықпал етудің ерекшеліктерін, сондай-ақ педагогикалық іс-әрекет мәселелерін білуі тиіс.

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 студенттерді 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 студент түсінікке ие болуы керек:

- басқару принциптері және өндірістік қатынастардың негіздері туралы;

- қауіпсіздікті қамтамасыз ету саласындағы зерттеудің заманауй әдістері туралы;

Пәнді меңгеру нәтижесінде студент 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 студент 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.

Дерекқорларды қорғауды және қауіпсіздікті ұйымдастыру

КОД – SEC214

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ – Ақпараттық қауіпсіздік жүйелерін ұйымдастыру

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Дерекқорларды қорғауды және қауіпсіздікті ұйымдастыру» пәнінің мақсаты Дерекқорларды қорғауды және қауіпсіздікті кешенді ұйымдастыру саласында студенттерге кәсіби құзіреттілік беру.

«Дерекқорларды қорғауды және қауіпсіздікті ұйымдастыру» пәнін оқудың міндеті дерекқор серверлерін қорғау және қауіпсіздік жүйелерін ұйымдастырудың негізгі қағидаларын игеру және оларды қолдану.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

«Дерекқорларды қорғауды және қауіпсіздікті ұйымдастыру» оқу курсының бағдарламасы дерекқорлардың қауіпсіздігін қамтамасыз ету технологияларын зерттеуге бағытталған. Курс ДҚ қорғау мен қауіпсіздіктің тәжірибелік мәселелерін шешудің әдістері мен құралдарын пайдалануға арналған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді меңгеру нәтижесінде студент білуі керек:

- дерекқорларды қорғау және қауіпсіздік жүйелерін ұйымдастыру;
- ДҚ қорғау технологиялары және қауіпсіз ДҚ жобалау әдістері;
- ДҚ серверлеріндегі ДҚ қауіпсіздігін қамтамасыз етудің ендірілген механизмдері.

Қабілетті болу:

- дерекқордың қауіпсіздігін және қорғалуын қамтамасыз ету технологияларын тәжірибеде қолдану;
- дерекқордың қорғауы мен қауіпсіздігі үшін деректер базасы серверлерінің енгізілген механизмдерін тәжірибеде қолдану;

дағдылары болуы керек:

- CASE-құралдарында қауіпсіз ДҚ жобалау;
- SQL тілін дерекқордың қорғанысы мен қауіпсіздігін қамтамасыз етуді және жұмыс істеуді құру үшін пайдалану;
- Қорғаныстың криптографиялық кірістірілген құралдарын пайдалану.

Инженерия саласындағы сандық әдістер

КОД - GEN200

КРЕДИТ – 6 (1/1/1/3)

ПРЕРЕКВИЗИТ – нет

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

Бұл курс сандық әдістер туралы қажетті теориялық білімді және инженерлік қосымшаларда кездесетін әр түрлі есептерді сандық шешу процедураларын қолдану дағдыларын беруге бағытталған.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Бұл пән сызықтық және сызықтық емес алгебралық теңдеулер жүйелерін шешуге, полиномдық жуықтауға және интерполяциялауға, қарапайым және дербес дифференциалдық теңдеулерді сандық интегралдауға бағытталған есептеу әдістерін қарастырады.

КУРСТЫ АЯҚТАУ БОЙЫНША БІЛІМ, БІЛІК, ДАҒДЫ

Студенттер сандық әдістердің мүмкіндіктері мен теориялық негіздері туралы нақты түсінікке ие болады және инженерлік қосымшаларға қатысты есептерді шешу үшін осы әдістері қалай қолданылатынын көрсете алады.

Machine Learning & Deep Learning
КОД - CSE746
КРЕДИТ – 6 (2/0/1/3)
ПРЕРЕКВИЗИТ –жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

Курстың мақсаты-кең қолданылатын ашық қатынау кітапханалары негізінде Машиналық оқыту әдістерінің базалық теориясы мен практикасын меңгеру. Бағдарламалық қамтамасыз етуді әзірлеудің практикалық есептерінде Машиналық оқыту моделін қолдануды үйрету. Курстың негізгі міндеттері: - Машиналық оқытудың негізгі модельдерін және олардың шешетін міндеттерін қарастыру - Нейрондық желілердің түсінігін және жұмыс тәжірибесін алу - Деректерді классификациялау мен кластерлеудің қазіргі заманғы әдістерін қарастыру - Терең оқыту модельдерін зерттеудің өзекті бағыттарын зерттеу.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

Курс терең оқыту модельдеріне арналған. Машиналық оқыту аясында сала бола отырып, терең оқыту модельдері сандық-сапалық көшуді бейнелейді. Жаңа модельдер және олардың қасиеттері осындай модельдердің метапараметрларын баптау тәжірибесін және бөлек оқытуды талап етеді.

КУРСТЫ АЯҚТАУ БОЙЫНША БІЛІМ, БІЛІК, ДАҒДЫ

Курс соңында студенттер: Түсіну - Терең оқыту үлгілерінің ерекшеліктері - AI саласындағы зерттеулердің өзекті бағыттары Білуге - Терең оқыту модельдерін қолдану міндеттері мен салалары Білу - Машиналық оқыту моделін пайдалану

Бұлтты технологиялар және виртуализация жүйелерінің қауіпсіздігі
КОД – SEC244
КРЕДИТ – 6 (2/1/0/3)
ПРЕРЕКВИЗИТ – жоқ

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Бұлтты технологиялар және виртуализация жүйелерінің қауіпсіздігі» пәнінің мақсаты бұлтты технологиялар және виртуализация саласында студенттерге 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 студент 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.

Ақпаратты криптографиялық қорғау алгоритмдері

КОД – SEC201

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ – Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, Киберқылмыс және компьютерлік криминалистика

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Ақпаратты криптографиялық қорғау алгоритмдері» пәнінің мақсаты ақпараттың трансформациялануы мен берілуіне байланысты мәселелерді шешу дағдыларын дамыту үшін криптографиялық өзгерістер мен алгоритмдерді пайдалануды реттейтін ережелерді кәсіби білімдер жүйесін қалыптастыру болып табылады.

Пәннің міндеттері болып табылады: қазіргі заманғы алгоритмдерді зерттеу мен құруда қолданылатын криптографиялық хаттамаларды, ақпаратты конверсиялау мен қорғаудың әдістері мен модельдерін зерттеу;

криптографиялық хаттамаларды талдау және енгізу әдістерін игеру; теориялық және практикалық мәселелерді шешу дағдыларын меңгеру.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

«Ақпаратты криптографиялық қорғау алгоритмдері» оқу курсының бағдарламасы студенттерді хаттамалардың қауіпсіздігін сипаттайтын негізгі сипаттамалар, қасиеттер; криптографиялық хаттамалардың түрлері, хаттамалардағы қауіпсіздік шабуылдары, қауіпсіздік хаттамаларын талдаудың формалды әдістері; негізгі тарату хаттамалары; кванттық криптография және кванттық кілттер тарату хаттамалары, жасырын ортақ схемалар, нөлдік ашылу хаттамалары, математикалық есептерді шешу хаттамалары; бит байланыстыру

хаттамасы; монетаны телефон арқылы лақтыру, телефондағы покер ойыны ойын хаттамалары ; шартқа қол қою хаттамасымен таныстыруға бағытталған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді оқу нәтижесінде студент білу керек:

- криптографиялық хаттамалардың математикалық модельдері;
- ақпараттық қауіпсіздік саласындағы заманауй технологиялар;
- криптографиялық түрлендірулер мен алгоритмдерді пайдалануды реттейтін ережелер құру және зерттеу саласындағы ғылыми мәселелерді қалыптастыру;
- криптографиялық хаттамалардың түрлері және олар пайдаланылатын ақпаратты қорғау аймақтары;
- криптографиялық хаттамалардың математикалық негіздері.

Пәнді оқу нәтижесінде студент қабілетті болу керек:

- криптографиялық хаттамаларды құру кезінде пайда болатын математикалық есептерді шешуге;
- криптографиялық алгоритмдерді жүзеге асыру үшін бағдарламалау әдістері мен тілдерін қолдану;
- ақпараттың криптографиялық түрленулері сұрақтарына арналған ғылыми басылымдармен жұмыс істеу және зерттеу нәтижелерінде көрсетілген тәжірибелік қолдануды табу;
- ақпаратты қорғаудың нақты объектілері үшін криптографиялық түрлендірулерді және алгоритмдерді пайдалануды реттейтін ережелерді қажетті түрлендіруді қажет етеді.

Дағдыларға ие болу керек:

- криптографиялық хаттамаларды математикалық әдістермен талдау;
- заманауи ақпараттық технологиялар мен желілік ресурстарға негізделген криптографиялық хаттамаларды іске асыратын негізгі алгоритмдерді енгізу дағдылары;
- ғылыми зерттеу жұмысына қажет криптографияның математикалық аппаратын білу;
- криптографиялық хаттамалар бар криптографиялық құрылыстарды құру
- дағдылары.

Ақпаратты қорғаудың стеганографиялық әдістері

КОД - SEC 238

КРЕДИТ – 6 (1/1/1/3)

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 студент 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.

Желілік операциялық жүйелер қауіпсіздігінің құралдары

КОД – SEC 221

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ – Ақпараттық қауіпсіздік жүйелерін ұйымдастыру

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

IP-желілерін ұйымдастыру негіздерінде студенттердің 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 студент 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.

Бағдарламалық жасақтаманы модельдеу

КОД - CSE249

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ У - жоқ

КУРС МАҚСАТЫ МЕН МІНДЕТТЕРІ

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ Курстың мақсаты - ақпараттық жүйелер үшін бағдарламалық қамтамасыз етуді құру принциптері мен

әдістерін зерттеу. Модельді дамыту принциптері. Бағдарламалық жүйелерді құрудағы модельдер, техникалық шарттар және олардың рөлі. Бағдарламалық жасақтама моделі негізінде. Бірыңғай модельдеу тілі туралы жалпы ақпарат # Бірыңғай модельдеу тілі және объектілік шектеу тілі туралы жалпы ақпарат. Доменге тән модельдеу тілдері

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді оқу барысында магистранттар:

- ақпараттық жүйелерді жобалау, талдау және қолданудың заманауи әдістерін білу; ақпараттық жүйелерді құру әдістерін оқып үйренуде әртүрлі бағдарламалық пакеттерді қолдана білу.

Ақпараттық жүйелер жұмысының модельдері мен алгоритмдерін құруды ұйымдастыру және командалық бағдарламалық өнімді жасау процесін басқару дағдыларына ие болу.

Ақпаратты инженерлік – техникалық қорғау

КОД – SEC208

КРЕДИТ – 6 (1/1/1/3)

ПРЕРЕКВИЗИТ – Ақпараттық қауіпсіздік жүйелерін ұйымдастыру

КУРС МАҚСАТЫ МЕН МІНДЕТТЕРІ. «Ақпаратты инженерлік – техникалық қорғау» пәнін оқытудың мақсаты магистранттарды ақпараттық ақпараттардың техникалық арналарымен, техникалық құралдармен және құпия ақпаратқа рұқсатсыз қол жеткізу әдістерімен таныстыру және оның қауіпсіздігін түрлі техникалық байланыс арналары арқылы ағып кетуден, акустикалық іздестіру және ақпараттық қауіпсіздікті радиохабарлардан, телефон желілерінен, оптикалық каналдан және т.б. ағып кетуден қорғау болып табылады.

Пәндерді оқудың міндеттері: ақпараттың ағып кетуінің техникалық арналары; құпия ақпаратқа рұқсатсыз кірудің техникалық құралдары; телефон байланыс арналарын тыңдаудың техникалық құралдары мен ақпаратты осы каналдар арқылы ағып кетуден қорғау; ақпаратты аэромадан ағып кетуден қорғаудың әдістері мен құралдары; ақпараттарды оптикалық байланыс арнасы арқылы ағып кетуден қорғаудың техникалық құралдары; ақпараттық сигналдарды сүзу, шуды басу сүзгілері және шу шығару туралы білім алу болып табылады.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Ақпаратты инженерлік – техникалық қорғау курсын аяқтағанда магистрант білуі керек:

- құпия ақпараттың түрлері, құпия сипаттағы мәліметтер тізімі;
- рұқсатсыз кіру нәтижесінде ақпараттың қауіпсіздік қатерлері және ақпараттардың ағып кетуінің техникалық арналары;
- ақпаратты қорғаудың техникалық құралдарында қолданылатын электрондық құрылғылардың сұлбаларын құру және пайдалану принциптері;

- радио, телефон және оптикалық байланыс арналары арқылы ақпаратты заңсыз алып тастау және қорғаудың техникалық құралдарының жұмыс істеу әрекеттері мен ерекшеліктері;
- ақпарат сүзу сұрақтары, шуды басу сүзгілері және шу шығару туралы мәселелер.

Қабілеті және дағдылары болу керек:

- қорғалатын ақпарат түрлерін ажырата білу, оның көздерін және тасымалдаушысын айқындау;
- ақпарат қауіпсіздігінің негізгі қауіптерін анықтау және олардың дәрежесін бағалау;
- әртүрлі техникалық арналар арқылы акустикалық ақпаратты қорғаудың техникалық құралдарын қолдануға;
- инженерлік және техникалық ақпаратты қорғаудың негізгі аппараттық түйіндерімен жұмыс істеу дағдысын иеленеді;
- болашақ кәсіби қызметінде алынған білімдерді қолдануға.

Ақпараттық қауіпсіздіктің аудиті

КОД – SEC204

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – Ақпараттық қауіпсіздік жүйелерін ұйымдастыру

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Ақпараттық қауіпсіздік аудиті» пәнінің мақсаты ақпараттық қауіпсіздік аудиті саласында студенттерге 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 студент 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.

Киберқылмыс және компьютерлік криминалистика

КОД – SEC240

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – Ақпараттық қауіпсіздік жүйелерін ұйымдастыру

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Киберқылмыс және компьютерлік криминалистика» пәнінің мақсаты студенттерге 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 студент 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.

Big Data және деректерді талдау

КОД – SEC245

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – Дерекқорларды қорғауды және қауіпсіздікті ұйымдастыру, Бұлтты технологиялар және виртуализация жүйелерінің қауіпсіздігі.

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Big Data және деректерді талдау» пәнінің мақсаты үлкен деректерді талдау саласында студенттерге 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 студент 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.

Электрондық бизнес жүйелерінің қауіпсіздігі

КОД - SEC206

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ - Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, Деректер қорын қорғауды және қорғауды ұйымдастыру.

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Электрондық бизнес жүйелерінің қауіпсіздігі» пәнінің мақсаты - студенттердің экономикалық жүйелердің ақпараттық қауіпсіздігі (ЕС) саласындағы кәсіби құзыреттіліктерге ие болуы.

«Электрондық бизнес жүйелерінің қауіпсіздігі» пәнінің міндеті экономикалық жүйелердің қауіпсіз жұмысын қамтамасыз етудің негізгі принциптерін игеру болып табылады.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

«Электрондық бизнес жүйелерінің қауіпсіздігі» оқу курсының бағдарламасы әртүрлі меншік формасындағы ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етудің теориялық және практикалық мәселелерін зерттеуге бағытталған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді игеру нәтижесінде студент білуі керек:
- меншікті ақпаратты қорғаудың ҚР стандарттары;
- Интернеттегі экономикалық қызметті ұйымдастыру принциптері;
- электрондық бизнес модельдері;
- экономикалық жүйелердің қауіпсіздігіне төнетін қатерлер;
- ақпаратты қорғаудың әдістері мен құралдары;
- ЭС ақпараттық қауіпсіздігін қамтамасыз ету технологиялары;
- ЭҚ-да мәліметтер қорын қорғау ерекшеліктері;
- ES ақпараттық қауіпсіздік жүйелерін ұйымдастыру.

істей алады:
- электрондық бизнестің әр түрлі модельдерінің веб-сайттарымен жұмыс;
- брандмауэрлерді орнату және баптау;
- кіруді анықтау жүйелерін орнату және баптау;
- кірудің алдын алу жүйелерін орнату және баптау;
- сақтық көшірме жасау және деректерді қалпына келтіру жүйелерін орнату және конфигурациялау;

дағдыларға ие болу:
- кіруді анықтау;
- кірудің алдын алу;
- деректердің сақтық көшірмесін жасау және қалпына келтіру.

Киберқауіпсіздікте рисктерді басқару

КОД - SEC 245

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ - Ақпараттық қауіпсіздік жүйелерін ұйымдастыру

КУРСТЫҢ МАҚСАТЫ МЕН МІНДЕТТЕРІ

«Киберқауіпсіздік жағдайындағы тәуекелдерді басқару» (RMSB) пәнінің мақсаты студенттерге киберқауіпсіздік жағдайында тәуекелдерді басқару саласындағы кәсіби құзыреттіліктерді қалыптастыру болып табылады.

Пәннің мақсаты студенттердің ақпараттық қауіпсіздік тәуекелдерін басқару бойынша теориялық және практикалық білімдерді меңгеруі болып табылады.

КУРСТЫҢ ҚЫСҚАША СИПАТТАМАСЫ

«Киберқауіпсіздік жағдайындағы тәуекелдерді басқару» оқу курсының бағдарламасы тәуекелдерді басқару стандарттарын, тәуекелдерді бағалау құралдарын және оларды тәжірибеде қолдануға бағытталған.

КУРСТЫ АЯҚТАҒАНДАҒЫ БІЛІМ, БІЛІК, ДАҒДЫ

Пәнді игеру нәтижесінде студент білуі керек:
- ақпараттық қауіпсіздік (АЖ) тәуекелінің негізгі түсініктері;
- тәуекелдерді басқару стандарттары;
- ақпараттық қауіпсіздік тәуекелдерін талдау мен басқарудың негізгі мәселелері;
- компанияның ақпараттық тәуекелдерін бағалау әдістері;

- сандық және сапалық тәуекел шаралары;
- тәуекелді автоматты бағалау құралдары (АРА);
- АЖ режимін қамтамасыз етуге қарсы шаралар;

істей алады:

- тәуекелдерді бағалау;
- тәуекелді азайту үшін қарсы шараларды таңдау;
- тәуекелді болдырмау үшін қарсы шараларды таңдау;
- тәуекел сипатын өзгертуге қарсы шараларды таңдау;
- АОР құралдарын қолдану;

дағдыларға ие болу:

- тәуекелді талдау;
- АОР қолдану арқылы тәуекелді бағалау;
- тәуекелге бару.

Шағын контроллерді бағдарламалау

КОД - SEC 218

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ - Ақпараттық қауіпсіздік жүйелерін ұйымдастыру.

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 студент 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.

Ғылыми және педагогикалық магистратураның білім беру бағдарламасы практиканың екі түрін қамтиды:

- педагогикалық;
- зерттеу.

Педагогикалық тәжірибе практикалық дағдыларды және оқыту әдістемесін қалыптастыру мақсатында жүргізіледі. Педагогикалық тәжірибе Теориялық оқыту кезеңінде оқу процесінен қол үзбей жүргізілуі мүмкін.

Магистранттың зерттеу практикасы отандық және шетелдік ғылымның жаңа теориялық, әдіснамалық және технологиялық жетістіктерімен, ғылыми зерттеулердің заманауи әдістерімен, тәжірибелік деректерді өңдеу және интерпретациялаумен танысу мақсатында жүргізіледі.

Магистранттың ғылыми-зерттеу жұмысы Ғылыми және педагогикалық магистратурадағы ғылыми-зерттеу жұмысы:

- магистрлік диссертация қорғалатын мамандықтың негізгі проблематикасына сәйкес келу;
- өзекті болу, ғылыми жаңалықты және практикалық маңыздылығын қамтамасыз ету;
- ғылым мен тәжірибенің заманауи теориялық, әдістемелік және технологиялық жетістіктеріне негізделу;
- ғылыми зерттеулердің заманауи әдістерін қолдану арқылы орындалады;
- негізгі қорғалатын ережелер бойынша ғылыми-зерттеу (әдістемелік, практикалық) бөлімдерді ұстау;
- тиісті білім саласындағы озық халықаралық тәжірибеге сүйену.
- озық ақпараттық технологияларды қолдану арқылы орындалады;
- негізгі қорғалатын ережелер бойынша Эксперименталды-зерттеу (әдістемелік, практикалық) бөлімдерді ұстау.

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/ эксперименталды – зерттеу жұмысының қорытындысы.

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

- жұмыс ақпараттық қауіпсіздікті және қауіпсіздік саласындағы өзекті мәселелерді зерттеуге немесе шешуге тиіс;
- жұмыс маңызды ғылыми проблемаларды анықтауға және оларды шешуге негізделуі тиіс;
- жұмыс ақпараттық қорғау және қауіпсіздік саласындағы өзекті мәселелерді зерттеуге немесе шешуге тиіс;
- жұмыс маңызды ғылыми проблемаларды анықтауға және оларды шешуге негізделуі тиіс.

Мазмұны

Бағдарламаныі қысқаша сипаттамасы	3
Білім бағдарламасының паспорты	5
Бағдарламаның мазмұны мен көлемі	5
Оқуға түсушіге қойылатын талаптар	6
Оқуды аятау және дипломды алуға талаптар	6
Жұмыс оқу жоспары және модульдік білім беру бағдарламасы	9
Білімі, дағдысы, қабілеті және құзыреттілігінің деңгейлері мен көлемі дескрипторлары	14
Оқуды аяқтау бойынша құзіреттіліктер	14
ECTS стандарты бойынша дипломға қосымша	18
Модульдер мен оқу нәтижелерінің тізімі	19
Пәннің сипаттамасы	22