НАО «Казахский национальный исследовательский технический университет им К.И. Сатпаева»
Институт кибернетики и телекоммуникационных технологий
Кафедра «Кибербезопасность, обработка и хранение информации»

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

7М06104 - «КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

(научно-педагогическое направление, 2 года)

Магистр технических наук

2-е издание
в соответствии с ГОСО высшего образования 2018 года

Алматы 2020

Программа составлена и подписана сторонами:

От КазНИТУ им К.И. Сатпаева:

Директор Института кибернетики и информационных технологий — Н.А. Сейлова

Заведующий кафедрой «Кибербезопасность, обработка и хранение информации» (КОиХИ) — Н.А. Сейлова

Председатель УМГ кафедры КОиХИ — Е.Ж. Айтхожаева

От работодателей:
Директор департамента ТОО «Казтелепорт» Толеулиев С.

От вуза-партнера:
Национальный авиационный университет (НАУ, Киев, Украина)

Утверждено на заседании Учебно-методического совета Казахского национального исследовательского технического университета им К.И. Сатпаева. Протокол №3 от 15.12.2020 г.

Квалификация:
Уровень 7 Национальной рамки квалификаций:

Профессиональная компетенция: Комплексное обеспечение информационной безопасности, Аудит информационной безопасности, Организация систем информационной безопасности.

1 Краткое описание программы:

Цель образовательной программы:

Целью образовательной программы является обучение магистрантов научно-педагогического направления. Образовательная программа включает базовые и профильные дисциплины с достижением соответствующих компетенций, а также прохождение различных видов практик (исследовательская, экспериментальная, педагогическая и стажировки).

Профессиональная деятельность магистров направлена в область защиты и безопасности информации, а именно на комплексное обеспечение информационной безопасности и инженерно-техническую защиту информации.

Подготовка магистров научно-педагогического направления по информационной безопасности будет осуществляться по новой образовательной программе (ОП) «Комплексное обеспечение информационной безопасности». Программы дисциплин и модулей образовательной программы имеют междисциплинарный и мультидисциплинарный характер, разрабатываются с учетом соответствующих образовательных программ ведущих университетов мира и международного классификатора профессиональной деятельности по направлению информационная безопасность.

Образовательная программа «Комплексное обеспечение информационной безопасности» разработана на базе основных нормативных документов:

- Закон Республики Казахстан «Об образовании» от 27.07.2007 г. №319-III с изменениями и дополнениями от 24.10.2011 г. № 487-VI ЗРК;
- Правила организации учебного процесса по кредитной технологии обучения, утвержденные Приказом Министра МОН РК № 152 от 20.04.2011 г. (последние изменения внесены Приказом Министра МОН РК №90 от 28.01.2016 года);
- Государственный общеобязательный стандарт образования всех уровней образования, приказ №604 от 31.10.2018год и приказ № 182 от 05.05.2020год.
- Национальная рамка квалификаций. Утверждена протоколом от 16 марта 2016 года Республиканской трехсторонней комиссией по социальному партнерству и регулированию социальных и трудовых отношений;
- Отраслевая рамка квалификации (ОРК). Утверждена протоколом от 17 ноября 2016 года №12-03-333 Отраслевой комиссии по социальному партнерству и регулированию социальных и трудовых отношений в сфере электроэнергетики;
- Типовой учебный план 6М100200 - Системы информационной безопасности, утвержденный Приказом Министра МОН РК №425 от 05.07.2016 г.
- Рекомендация международной Ассоциации вычислительной техники (ACM) по учебным программам в области компьютерных наук (серия CC2005).

Магистр образовательной программы «Комплексное обеспечение информационной безопасности» ориентирован на самостоятельное определение цели профессиональной деятельности и выбора адекватных методов и средств их достижения, осуществление научной, инновационной деятельности по получению новых знаний. Кроме того, ориентирован на организацию, проектирование, разработку, управление и аудит систем защиты и безопасности информации прикладного

назначения для всех отраслей экономики, государственных организаций и других областей деятельности.

Программа призвана реализовать принципы демократического характера управления образованием, расширить границы академической свободы и полномочий учебных заведений, что обеспечит подготовку квалифицированных, высоко мотивированных кадров для инновационных и наукоемких отраслей экономики.

Образовательная программа обеспечивает применение индивидуального подхода к обучающимся, трансформацию профессиональных компетенций из профессиональных стандартов и стандартов квалификаций в результаты обучения и пути их достижения.

Образовательная программа разрабатывалась на основе анализа трудовых функций администратора по информационной безопасности, аудитора информационной безопасности, инженера по защите информации, заявленных в профессиональных стандартах.

В разработке образовательной программы участвовали представители казахстанских компаний и ассоциаций, специалисты ведомственных структур в области защиты и безопасности.

Задачи и содержание ОП приведены в разделе 9 «Описание дисциплин».

Основным критерием завершенности обучения по программам магистратуры является освоение всех видов учебной и научной деятельности магистранта.

В случае успешного завершения полного курса магистру присваивается магистр технических наук по образовательной программе «Комплексное обеспечение информационной безопасности».

2 Виды трудовой деятельности

- проектно-конструкторская;
- производственно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая;
- эксплуатационная;
- научная;
- научно-исследовательская.

3 Объекты профессиональной деятельности:

Объектами профессиональной деятельности магистра являются: аудит и мониторинг информационной безопасности; организация и технология защиты информации; обеспечение криптографической защиты информации; реагирование на инциденты информационной безопасности; системы управления информационной безопасности; организационное обеспечение аудита информационной безопасности; планирование аудита информационной безопасности; сопровождение систем защиты информации в ходе ее эксплуатации.

2 ПАСПОРТ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1 Объем и содержание программы

Срок обучения в магистратуре определяется объемом освоенных академических кредитов. При освоении установленного объема академических кредитов и достижении ожидаемых результатов обучения для получения степени магистра, образовательная программа магистратуры считается полностью освоенной. В научно-педагогической магистратуре не менее 120 академических кредитов должно быть освоено за весь период обучения, включая все виды учебной и научной деятельности магистранта.

Планирование содержания образования, способа организации и проведения учебного процесса осуществляется ВУЗом самостоятельно на основе кредитной технологии обучения.

Магистратура по научно-педагогическому направлению реализует образовательные программы послевузовского образования по подготовке научных и научно-педагогических кадров для ВУЗов и научных организаций, обладающих углубленной научно-педагогической и исследовательской подготовкой.

Содержание образовательной программы магистратуры состоит из:

1) теоретического обучения, включающее изучение циклов базовых и профилирующих дисциплин;

2) практической подготовки магистрантов: различные виды практик, научных или профессиональных стажировок;

3) научно-исследовательской работы, включающую выполнение магистерской диссертации.

4) итоговой аттестации.

Наименование: Комплексное обеспечение информационной безопасности

Цель образовательной программы:

- Обеспечить подготовку специалистов научной деятельности и производства в сфере информационной безопасности, умеющих применять различные технологии, знания, навыки и компетенции в организации, управлении и проектировании систем защиты информации.
- Подготовить специалистов научной, педагогической деятельности и производства к производственной деятельности, связанной с процессом аудита, мониторинга, расследования инцидентов информационной безопасности, ориентированных на ожидаемые результаты.
- Подготовить руководителей способных к организационно-управленческой деятельности, связанной с планированием, разработкой, эксплуатацией и сопровождением процессов обеспечения защиты и безопасности информации.
- Создать условия непрерывного профессионального совершенствования, развития социально-личностных компетенций, социальной мобильности и конкурентоспособности на рынке труда.

Задачи образовательной программы:

Подготовка высококвалифицированных специалистов, умеющих решать следующие задачи:

- планирование работы по аудиту информационной безопасности;
- организационное обеспечение аудита информационной безопасности;
- проведение анализа соответствия проектной, эксплуатационной и технической документации по информационной безопасности требованиям в сфере ИКТ и обеспечения ИБ объекта аудита ИБ;
- анализ текущего состояния защищенности объекта аудита ИБ;
- выявление и устранение уязвимостей;
- проведение мониторинга и расследования инцидентов ИБ;
- разработка модели угроз безопасности информации в предприятиях;
- разработка технического задания на создание системы защиты информации.

2 Требования для поступающих

Предшествующий уровень образования абитуриентов - высшее профессиональное образование (бакалавриат). Претендент должен иметь диплом, установленного образца и подтвердить уровень знания английского языка сертификатом или дипломами установленного образца.

Порядок приема граждан в магистратуру устанавливается в соответствии с «Типовыми правилами приема на обучение в организации образования, реализующие образовательные программы послевузовского образования».

Формирование контингента магистрантов, осуществляется посредством размещения государственного образовательного заказа на подготовку научных и педагогических кадров, а также оплаты обучения за счет собственных средств граждан и иных источников. Гражданам Республики Казахстан государство обеспечивает предоставление права на получение на конкурсной основе в соответствии с государственным образовательным заказом бесплатного послевузовского образования, если образование этого уровня они получают впервые.

На «входе» магистрант должен иметь все пререквизиты, необходимые для освоения соответствующей образовательной программы магистратуры. Перечень необходимых пререквизитов определяется высшим учебным заведением самостоятельно.

При отсутствии необходимых пререквизитов магистранту разрешается их освоить на платной основе.

3 Требования для завершения обучения и получение диплома

Присуждаемая степень/квалификация: Выпускнику данной образовательной программы присваивается степень магистра технических наук по образовательной программе «Комплексное обеспечение информационной безопасности».

Выпускник, освоивший программы магистратуры, должен обладать следующими общепрофессиональными компетенциями:

– способностью самостоятельно приобретать, осмысливать, структурировать и использовать в профессиональной деятельности новые знания и умения, развивать свои инновационные способности;

– способностью самостоятельно формулировать цели исследований, устанавливать последовательность решения профессиональных задач;

– способностью применять на практике знания фундаментальных и прикладных разделов дисциплин, определяющих направленность (профиль) программы магистратуры;

– способностью профессионально выбирать и творчески использовать современное научное и техническое оборудование для решения научных и практических задач;

– способностью критически анализировать, представлять, защищать, обсуждать и распространять результаты своей профессиональной деятельности;

– владением навыками составления и оформления научно-технической документации, научных отчетов, обзоров, докладов и статей;

– готовностью руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия;

– готовностью к коммуникации в устной и письменной формах на иностранном языке для решения задач профессиональной деятельности.

Выпускник, освоивший программу магистратуры, должен обладать профессиональными компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа магистратуры:

научно-исследовательская деятельность:

– способностью формировать диагностические решения профессиональных задач путем интеграции фундаментальных разделов наук и специализированных знаний, полученных при освоении программы магистратуры;

– способностью самостоятельно проводить научные эксперименты и исследования в профессиональной области, обобщать и анализировать экспериментальную информацию, делать выводы, формулировать заключения и рекомендации;

– способностью создавать и исследовать модели изучаемых объектов на основе использования углубленных теоретических и практических знаний в области защиты и безопасности информации;

– *научно-производственная деятельность:*

– способностью самостоятельно проводить производственные и научно-производственные, лабораторные и интерпретационные работы при решении практических задач;

– способностью к профессиональной эксплуатации современного лабораторного оборудования и приборов в области освоенной программы магистратуры;

– способностью использовать современные методы обработки и интерпретации комплексной информации для решения производственных задач;

– *проектная деятельность:*

– способностью самостоятельно составлять и представлять проекты научно-исследовательских и научно-производственных работ в области информационной безопасности;

– готовностью к проектированию комплексных научно-исследовательских и научно-производственных работ при решении профессиональных задач;

– *организационно-управленческая деятельность:*

– готовностью к использованию практических навыков организации и управления научно-исследовательскими и научно-производственными работами при решении профессиональных задач;

– готовностью к практическому использованию нормативных документов при планировании и организации научно-производственных работ в области информационной безопасности;

– *научно-педагогическая деятельность:*

– способностью проводить семинарские, лабораторные и практические занятия;

– способностью участвовать в руководстве научно-учебной работой обучающихся в области информационной безопасности.

4 Рабочий учебный план и модульная образовательная программа

4.1. Срок обучения 2 года

РАБОЧИЙ УЧЕБНЫЙ ПЛАН
образовательной программы
7М**06104- «Комплексное обеспечение информационной безопасности»**

Академическая степень: магистр технических наук
Срок обучения: 2 года

Год обучения	Код	Наименование дисциплины	Компонент	Кредиты		Лк/лб/пр/СРО	Пререквизиты	Код	Наименование дисциплины	Компонент	Кредиты		Лк/лб/пр/СРО	Пререквизиты
				ECTS	РК						ECTS	РК		
1	**1 семестр**							**2 семестр**						
	HUM201	История и философия науки	БД ВК	4	2	1/0/1/2		LNG202	Иностранный язык (профессиональный)	БД ВК	6	3	0/0/3/3	
	HUM207	Педагогика высшей школы	БД ВК	4	2	1/0/1/2		HUM204	Психология управления	БД ВК	4	2	1/0/1/2	
		Электив	ПД КВ	6	3				Электив	ПД КВ	6	3		
		Электив	БД КВ	6	3				Электив	ПД КВ	6	3		
	AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	6					Электив	БД КВ	6	3		
									Электив	БД КВ	6	3		
								AAP244	Педагогическая практика	БД ВК	4			
								AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	6			
		Всего		**26**					**Всего**		**44**			
2	**3 семестр**							**4 семестр**						
		Электив	ПД КВ	6	3			AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	6			

	SEC204	Аудит информационной безопасности	ПД ВК	6	3	2/1/0		AAP236	Исследовательская практика	ПД	7			
		Электив	ПД КВ	6	3			ECA205	Оформление и защита магистерской диссертации (ОиЗМД)	ИА	12			
		Электив	ПД КВ	6	3									
	AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	6										
		Всего		**30**					**Всего**		**25**			
									Итого		**125**			

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН
Образовательной программы
7М**06104- «Комплексное обеспечение информационной безопасности»**

БД Компоненты по выбору - 18 кредитов					
	Код	**Наименование дисциплин**	**Кредиты**	**Лк/лб/пр/СРО**	**Семестр**
	SEC221	Средства безопасности сетевых ОС	6	2/0/1/3	1
	CSE249	Model-Driven Software Engineering	6	2/0/1/3	1
	SEC201	Алгоритмы криптографической защиты информации	6	2/0/1/3	2
	SEC 238	Стеганографические методы защиты информации	6	1/1/1/3	2
	SEC244	Безопасность систем виртуализация и облачных технологий	6	2/1/0/3	2
	SEC 208	Инженерно-техническая защита информации	6	1/1/1/3	2
		Всего	**18**		
ПД Компоненты по выбору - 42 кредита					
	SEC215	Организация систем информационной безопасности	6	1/1/1/3	1
	GEN200	Численные методы в инженерии	6	1/1/1/3	2
	SEC214	Организация защиты и безопасности БД	6	2/0/1/3	2
	CSE746	Machine Learning & Deep Learning	6	2/0/1/3	3
	CSE720	Киберпреступность и компьютерная криминалистика	6	2/1/0/3	3
	SEC218	Программирование микроконтроллеров	6	2/1/0/3	3
	SEC245	Риск менеджмент информационной безопасности	6	2/0/1/3	3
	SEC206	Безопасность систем электронного бизнеса	6	2/1/0/3	3
	SEC246	Big Data и анализ данных	6	2/1/0/3	3
		Всего	**36**		

МОДУЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

Образовательная программа: 7М**06104- «Комплексное обеспечение информационной безопасности»**

Форма обучения: *дневная*
Срок обучения: 2 *г.*
Академическая степень: магистр технических наук

Цикл дисц.	Код дисц.	Наименование дисциплин	Семестр	Академ кред.	лек.	лаб	практика	СРО	Вид контроля	Кафедра
Модуль профильной подготовки										
Базовые дисциплины (БД) (40 кредитов)										
Вузовский компонент (ВК) (18 кредитов)										
БД 1.1.1	LNG202	Иностранный язык (профессиональный)	2	6	0	0	3	3	Экзамен	АЯ
БД 1.2.1	HUM201	История и философия науки	1	4	1	0	1	2	Экзамен	ОД
БД 1.3.1	HUM207	Педагогика высшей школы	1	4	1	0	1	2	Экзамен	ОД
БД 1.4.1	HUM204	Психология управления	2	4	1	0	1	2	Экзамен	НОЦ УП
Практико – ориентированный модуль										
	AAP244	Педагогическая практика	2	4	0	0	2	2	Отчет	
Компонент по выбору (КВ) (18 кредитов)										
Модуль обеспечения сетевой безопасности и облачных технологий и криптографической защиты информации										
БД	SEC221	Средства безопасности сетевых ОС	1	6	2	0	1	3	Экзамен	КОиХИ
БД	CSE249	Model-Driven Software Engineering	1	6	2	0	1	3	Экзамен	КОиХИ
БД	SEC201	Алгоритмы криптографической защиты информации	2	6	2	0	1	3	Экзамен	КОиХИ
БД	SEC 238	Стеганографические методы защиты информации	2	6	1	1	1	3	Экзамен	КОиХИ
БД	SEC244	Безопасность систем виртуализация и облачных технологий	2	6	2	1	0	3	Экзамен	КОиХИ
БД	SEC 208	Инженерно-техническая защита информации	2	6	1	1	1	3	Экзамен	КОиХИ
Профилирующие дисциплины (ПД) (49 кредитов)										
Вузовский компонент (ВК) (6 кредитов)										
Модуль научных исследований, организации системы информационной безопасности и обеспечения защиты информации										
ПД	SEC204	Аудит информационной безопасности	3	6	2	1	0	3	Экзамен	КОиХИ
Компонент по выбору (КВ) (36 кредитов)										
ПД	SEC215	Организация систем информационной безопасности	1	6	1	1	1	3	Экзамен	КОиХИ
ПД	GEN200	Численные методы в инженерии	2	6	1	1	1	3	Экзамен	ПМиИГ

ПД	SEC214	Организация защиты и безопасности БД	2	6	2	0	1	3	Экзамен	КОиХИ
ПД	CSE746	Machine Learning & Deep Learning	3	6	2	0	1	3	Экзамен	ПИ
ПД	CSE720	Киберпреступность и компьютерная криминалистика	3	6	2	1	0	3	Экзамен	КОиХИ
ПД	SEC218	Программирование микроконтроллеров	3	6	2	1	0	3	Экзамен	КОиХИ
ПД	SEC245	Риск менеджмент информационной безопасности		6	2	0	1	3	Экзамен	КОиХИ
ПД	SEC206	Безопасность систем электронного бизнеса	3	6	2	1	0	3	Экзамен	КОиХИ
ПД	SEC246	Big Data и анализ данных		6	2	1	0	3	Экзамен	КОиХИ
Практико – ориентированный модуль										
ПД	AAP236	Исследовательская практика	4	7					Отчет	
Научно-исследовательский модуль (24 кредита)										
НИРМ	AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	1	6					Отчет	
НИРМ	AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	2	6					Отчет	
НИРМ	AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	3	6					Отчет	
НИРМ	AAP242	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	4	6					Отчет	
Модуль итоговой аттестации (12 кредитов)										
ИА	ECA205	Оформление и защита магистерской диссертации	4	12					Защита диссертаций	
Всего кредитов				**125**						

5 Дескрипторы уровня и объема знаний, умений, навыков и компетенций

Требования к уровню подготовки магистранта определяются на основе Дублинских дескрипторов второго уровня высшего образования (магистратура) и отражают освоенные компетенции, выраженные в достигнутых результатах обучения.

Результаты обучения формулируются как на уровне всей образовательной программы магистратуры, так и на уровне отдельных модулей или учебной дисциплины.

Дескрипторы отражают результаты обучения, характеризующие способности обучающегося:

1) демонстрировать развивающиеся знания и понимание в изучаемой области информационных технологий и информационной безопасности;

2) применять на профессиональном уровне свои знания, понимание и способности для решения проблем в новой среде, в более широком междисциплинарном контексте;

3) осуществлять сбор и интерпретацию информации для формирования суждений с учетом социальных, этических и научных соображений;

4) четко и недвусмысленно сообщать информацию, идеи, выводы, проблемы и решения, как специалистам, так и неспециалистам;

5) навыки обучения, необходимые для самостоятельного продолжения дальнейшего обучения в изучаемой области информационных технологий и информационной безопасности.

6 Компетенции по завершению обучения

6.1 Требования к ключевым компетенциям выпускников *научно-педагогической магистратуры*, должен:

1) иметь представление:

– о роли науки и образования в общественной жизни;

– о современных тенденциях в развитии научного познания;

– об актуальных методологических и философских проблемах естественных (социальных, гуманитарных, экономических) наук;

– о профессиональной компетентности преподавателя высшей школы;

– о противоречиях и социально-экономических последствиях процессов глобализации;

– о профессиональной компетентности в области защиты и безопасности информации;

– о технологии виртуализации ресурсов и платформ;

– об интеллектуализации средств обеспечения информационной безопасности;

- о технологиях защиты БД;

– об алгоритмах криптографической защиты информации;

– об анализе больших данных.

2) знать:

– методологию научного познания;

– принципы и структуру организации научной деятельности;

– психологию познавательной деятельности студентов в процессе обучения;

– психологические методы и средства повышения эффективности и качества обучения;

– алгоритмы криптографической защиты информации;

– стандарты ИБ и критерии оценки безопасности ИТ;

- технологии виртуализации ресурсов и платформ и системы виртуализации от ведущих производителей;

- угрозы и риски систем виртуализации, принципы построения гипервизоров и их уязвимости;

– организацию IP-сетей, структуру IP-пакетов и IP-протоколов;

– внутреннюю организацию носителей информации ОС;

– методы и средства хранения ключевой информации и шифрования;

– разновидности и принципы аутентификации;

– требования к межсетевым экранам и системам обнаружения вторжений;

- технологии защиты БД и методы проектирования безопасных БД;

- организацию системы защиты и безопасности БД;

– методы и инструменты активного аудита;

– инженерно-техническую защиту информации.

3) уметь:

– использовать полученные знания для оригинального развития и применения идей в контексте научных исследований;

– критически анализировать существующие концепции, теории и подходы к анализу процессов и явлений;

– интегрировать знания, полученные в рамках разных дисциплин для решения исследовательских задач в новых незнакомых условиях;

– путем интеграции знаний выносить суждения и принимать решения на основе неполной или ограниченной информации;

– применять знания педагогики и психологии высшей школы в своей педагогической деятельности;

– применять интерактивные методы обучения;

– проводить информационно-аналитическую и информационно-библиографическую работу с привлечением современных информационных технологий;

– креативно мыслить и творчески подходить к решению новых проблем и ситуаций;

– свободно владеть иностранным языком на профессиональном уровне, позволяющим проводить научные исследования и осуществлять преподавание специальных дисциплин в вузах;

– обобщать результаты научно-исследовательской и аналитической работы в виде диссертации, научной статьи, отчета, аналитической записки и др.;

– применять алгоритмы криптографической защиты информации;

- применять стандарты ИБ и проводить оценку безопасности ИТ;

- применять системы виртуализации от ведущих производителей;

- выявлять угрозы и риски систем виртуализации;

– применять методы и средства хранения ключевой информации и шифрования;

– работать с межсетевыми экранами и системами обнаружения вторжений;
– применять технологии защиты БД и методы проектирования безопасных БД;
– организовать систему защиты и безопасности БД;
– применять методы и инструменты активного аудита;
– применять инструменты анализа больших данных.

4) иметь навыки:

– научно-исследовательской деятельности, решения стандартных научных задач;
– осуществления образовательной и педагогической деятельности по кредитной технологии обучения;
– методики преподавания профессиональных дисциплин;
– использования современных информационных технологий в образовательном процессе;
– профессионального общения и межкультурной коммуникации;
– ораторского искусства, правильного и логичного оформления своих мыслей в устной и письменной форме;
– организации и защиты безопасности БД;
– проведения аудита информационной безопасности;
– применения алгоритмов криптографической защиты информации;
– выявления угроз и противодействия им;
– работы с Big Data;
– расширения и углубления знаний, необходимых для повседневной профессиональной деятельности и продолжения образования в докторантуре.

5) быть компетентным:

– в области методологии научных исследований;
– в области научной и научно-педагогической деятельности в высших учебных заведениях;
– в вопросах современных образовательных технологий;
– в выполнении научных проектов и исследований в профессиональной области;
– в организации систем информационной безопасности;
– в проведении аудита информационной безопасности;
– в обеспечении информационной безопасности организации;
– в способах обеспечения постоянного обновления знаний, расширения профессиональных навыков и умений.

Б – Базовые знания, умения и навыки

Б1- Уметь проводить оценку защищенности сетевых операционных систем и изучение принципов и методов разработки программного обеспечения информационных систем.

Б2 - Знать современные и перспективные направления развития криптографической защиты информации и применять ее на практике.

Б3 - Знать технологии виртуализации ресурсов и платформ, уметь применять системы виртуализации от ведущих производителей и быть компетентным в вопросах инженерно-технической защиты информации.

П – Профессиональные компетенции:

П1 – знать вопросы организации систем информационной безопасности и уметь на практике проводить работы по комплексному обеспечению информационной безопасности.

П2 – Умение решать прикладные задачи с применением численных методов в инженерии

П3 – уметь организовать систему защиты и безопасности БД и применять технологии защиты БД.

П4 – быть компетентным в вопросах машинного обучения и моделях глубокого обучения

П5 - быть компетентным в вопросах киберпреступлений и компьютерной криминалистики, уметь выявлять угрозы и проводить работы по предотвращению вторжений.

П6 - уметь планировать, проектировать, программировать и проводить отладку программ на универсальных языках.

П7 - знать стандарты ИБ и критерии оценки безопасности ИТ, уметь применять методы и инструменты активного аудита.

П8 – быть компетентным в вопросах о существующих видах угроз безопасности в электронном бизнесе. Умение обеспечивать информационную безопасность автоматизированных банковских систем.

О - Общечеловеческие, социально-этические компетенции

О1- способность работать в команде, обладать организационными навыками, расставлять приоритеты, быстро осваивать новые знания и навыки, применять их на практике;

О2 - быть ориентированным на достижение результата, эффективно планировать и упорядочивать свое развитие;

О3 - способность свободно пользоваться английским языком как средством делового общения, источника новых знаний в области информационной безопасности.

С – Специальные и управленческие компетенции:

С1 - самостоятельное управление и контроль процессами трудовой и учебной деятельности в рамках стратегии, политики и целей организации, критическое обсуждение проблемы, аргументирование выводов и грамотное оперирование информацией;

С2 - способность к мотивации для решения определенных задач, способность нести ответственность за результат выполнения работ на уровне подразделения или предприятия;

С3 - способность демонстрировать набор навыков управления процессом работы, умение выбирать методы, методики и критерии оценки для получения результатов, распределять и делегировать полномочия, формировать команды, а также принимать решения по ходу производственного процесса.

6.2 Требования к научно-исследовательской работе магистранта в научно-педагогической магистратуре:

1) соответствует профилю образовательной программы магистратуры, по которой выполняется и защищается магистерская диссертация;

2) актуальна и содержит научную новизну и практическую значимость;

3) основывается на современных теоретических, методических и технологических достижениях науки и практики;

4) выполняется с использованием современных методов научных исследований;

5) содержит научно-исследовательские (методические, практические) разделы по основным защищаемым положениям;

6) базируется на передовом международном опыте в соответствующей области знания.

6.3 Требования к организации практик:

Образовательная программа научно-педагогической магистратуры включает два вида практик, которые проводятся параллельно с теоретическим обучением или в отдельный период:

1) педагогическую в цикле БД – в ВУЗе;

2) исследовательскую в цикле ПД – по месту выполнения диссертации.

Педагогическая практика проводится с целью формирования практических навыков методики преподавания и обучения. При этом магистранты привлекаются к проведению занятий в бакалавриате по усмотрению ВУЗа.

Исследовательская практика магистранта проводится с целью ознакомления с новейшими теоретическими, методологическими и технологическими достижениями отечественной и зарубежной науки, современными методами научных исследований, обработки и интерпретации экспериментальных данных.

7 Приложение к диплому по стандарту ECTS

Приложение разработано по стандартам Европейской комиссии, Совета Европы и ЮНЕСКО/СЕПЕС. Данный документ служит только для академического признания и не является официальным подтверждением документа об образовании. Без диплома о высшем образовании не действителен. Цель заполнения Европейского приложения – предоставление достаточных данных о владельце диплома, полученной им квалификации, уровне этой квалификации, содержании программы обучения, результатах, о функциональном назначении квалификации, а также информации о национальной системе образования. В модели приложения, по которой будет выполняться перевод оценок, используется европейская система трансфертов или перезачёта кредитов (ECTS).

Европейское приложение к диплому даёт возможность продолжить образование в зарубежных университетах, а также подтвердить национальное высшее образование для зарубежных работодателей. При выезде за рубеж для профессионального признания потребуется дополнительная легализация диплома об образовании. Европейское приложение к диплому заполняется на английском языке по индивидуальному запросу и выдается бесплатно.

8 Перечень модулей и результатов обучения

ОП – Комплексное обеспечение информационной безопасности
Квалификация: магистр технических наук

Наименование модуля	Профессиональные компетенции	Дисциплины, формирующие модуль
Модуль профильной подготовки	Понимать философские вопросы науки, основные исторические этапы развития науки, уметь критически оценивать и анализировать научно-философские проблемы, понимать специфику инженерной науки, владеть навыками аналитического мышления и философской рефлексии, уметь обосновывать и отстаивать свою позицию, владеть приемами ведения дискуссии и диалога, владеть навыками коммукативности и креативности в своей профессиональной деятельности. Быть компетентным в вопросах психологии и педагогики.	История философия науки, Педагогика высшей школы, Психология управления
Модуль обеспечения сетевой безопасности и облачных технологий, и криптографической защиты информации	Уметь проводить оценку защищенности сетевых операционных систем. Безопасно применять современные технологии виртуализации.	Средства безопасности сетевых ОС, Безопасность систем виртуализации и облачных технологий, Алгоритмы криптографической защиты информации, Инженерно-техническая защита информации, Model-Driven Software Engineering, Стеганографические методы защиты информации

Модуль научных исследований, организации системы информационной безопасности и обеспечения защиты информации	Уметь организовать систему защиты и безопасности БД и применять технологии защиты БД, знать современные и перспективные направления развития криптографической защиты информации и применять ее на практике. Уметь организовать комплексное обеспечение защиты и безопасности информации. Быть компетентным в вопросах выявления киберпреступлении и компьютерной криминалистики. Уметь использовать средства распознавания и противодействия кибератакам. Знать технические средства и методы технической защиты информации, быть компетентным в организации инженерно-технической защиты информации. Уметь анализировать большие данные, знать методы и средства анализа больших данных. Знать и применять методы и средства для проведения аудита информационной безопасности.	Организация защиты и безопасности БД, Организация систем информационной безопасности, Численные методы в инженерии, Machine Learning & Deep Learning Киберпреступность и компьютерная криминалистика, Программирование микроконтроллеров, Big Data и анализ данных Аудит информационной безопасности, Риск менеджмент кибербезопасности, Киберпреступность и компьютерная криминалистика, Big Data и анализ данных, Безопасность систем электронного бизнеса
Научно-исследовательский модуль	Представление о современных тенденциях в развитии научного познания. Знание методологии научного познания. Способность формулировать проблемы, задачи и методы научного исследования, получать новые достоверные факты на основе наблюдений, опытов, научного анализа эмпирических данных, реферировать научные труды, составлять аналитические обзоры накопленных сведений в мировой науке и производственной деятельности, обобщать полученные результаты в контексте ранее накопленных в науке знаний, формулировать выводы и практические рекомендации на	Научно-исследовательская работа магистранта

	основе репрезентативных и оригинальных результатов исследований. Получение компетенций, необходимых для выполнения научных проектов и исследований в области IT-технологий.	
Практико-ориентированный модуль	Получение навыков самостоятельной научно-исследовательской работы и работы в научном коллективе. Способность порождать новые идеи. Практика в выполнении научных проектов и исследований в профессиональной области, в способах обеспечения постоянного обновления знаний, расширения профессиональных навыков и умений. Умение проводить информационно-аналитическую и информационно-библиографическую работу с привлечением информационных технологий. Применение теоретических знаний для выработки и представления собственных заключений при решении производственных задач в сфере IT. Умение принимать решения в сложных и нестандартных ситуациях в области организации и управления деятельностью предприятия.	Педагогическая практика, исследовательская практика
Модуль итоговой аттестации	Систематизация и обобщение знаний, полученных во время обучения в магистратуре, для успешной сдачи комплексного экзамена. Умение в области обучения, позволяющее продолжать обучение в значительной мере самостоятельно и автономно. Оформление результатов научно-исследовательской и аналитической работы в виде научных статей, отчетов, аналитических отчетов, диссертации. Умение сообщать свои	Оформление и защита магистерской диссертации

	выводы и используемые для их формулировки знания специалистам и неспециалистам. Изучение научно-технической информации, отечественного и зарубежного опыта в области IT-технологий для творческого его осмысления и выработки правильного решения своей научно-технической или производственной задачи.	

9. Описание дисциплин

Иностранный язык (профессиональный)
КОД – LNG202
КРЕДИТ – 6 (0/0/3/3)
ПРЕРЕКВИЗИТ –Academic English, Business English, IELTS 5.0-5.5

ЦЕЛЬ И ЗАДАЧИ КУРСА

Цель курса состоит в том, чтобы развить у студентов знания английского языка для их текущих академических исследований и повышения эффективности их работы в области управления проектами.

КРАТКОЕ ОПИСАНИЕ КУРСА

Курс направлен на формирование словарного запаса и грамматики для эффективного общения в области управления проектами и на улучшение навыков чтения, письма, аудирования и разговорной речи на уровне «Intermediate». Ожидается, что студенты приобретут пополнят свой словарный запас делового английского языка и изучат грамматические структуры, которые часто используются в контексте менеджмента. Курс состоит из 6 модулей. 3-й модуль курса завершается промежуточным тестом, а 6-й модуль сопровождается тестом по окончании курса. Курс завершается итоговым экзаменом. Магистрантам также необходимо заниматься самостоятельно (MIS). MIS - самостоятельная работа магистрантов под руководством преподавателя.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

После успешного завершения курса ожидается, что студенты будут уметь распознавать основную идею и главный посыл, а также конкретные детали при прослушивании монологов, диалогов и групповых обсуждений в контексте бизнеса и управления; понимать письменную и устную речь на английском языке по темам, связанным с управлением; писать управленческие тексты (отчеты, письма, электронные письма, протоколы заседаний), следуя общепринятой структуре с более высокой степенью грамматической точности и используя деловые слова и фразы, говорить о различных деловых ситуациях, используя соответствующий деловой словарный запас и

грамматические структуры - в парных и групповых дискуссиях, на встречах и переговорах.

История и философия науки

КОД – HUM201

КРЕДИТ – 4 (1/0/1/2)

ПРЕРЕКВИЗИТ - HUM124

ЦЕЛИ И ЗАДАЧИ КУРСА - раскрыть связь философии и науки, выделить философские проблемы науки и научного познания, основные этапы истории науки, ведущие концепции философии науки, современные проблемы развития научно-технической реальности

КРАТКОЕ ОПИСАНИЕ КУРСА - предмет философии науки, динамика науки, специфика науки, наука и преднаука, античность и становление теоретической науки, основные этапы исторического развития науки, особенности классической науки, неклассическакя и постнеклассическая наука, философия математики, физики, техники и технологий, специфика инженерных наук, этика науки, социально-нравственная ответственность ученого и инженера

ЗНАНИЯ,УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА - знать и понимать философские вопросы науки, основные исторические этапы развития науки, ведущие концепции философии науки, уметь критически оценивать и анализировать научно-философские проблемы, понимать специфику инженерной науки, владеть навыками аналитического мышления и философской рефлексии, уметь обосновывать и отстаивать свою позицию, владеть приемами ведения дискуссии и диалога, владеть навыками коммукативности и креативности в своей профессиональной деятельности

ПСИХОЛОГИЯ УПРАВЛЕНИЯ

КОД - HUM204

КРЕДИТ – 4 (1/0/1/2)

ЦЕЛЬ И ЗАДАЧИ КУРСА

Основная цель курса направлена на изучение особенностей поведения индивидуумов и групп людей в рамках организаций; определяющие психологические и социальные факторы влияния на поведение работников. Также большое внимание будет уделено вопросам внутренней и внешней мотивации людей

Главная цель курса - применение этих знаний для повышения эффективности организации.

КРАТКОЕ ОПИСАНИЕ КУРСА

Курс разработан так, чтобы обеспечить сбалансированное освещение всех ключевых элементов, составляющих дисциплину. В нем кратко будет рассмотрено происхождение и развитие теории и практики организационного поведения, а затем будут рассмотрены основные роли, навыки и функции управления с акцентом на эффективность управления, проиллюстрированные примерами из реальной жизни и тематическими исследованиями.

ЗНАНИЯ,УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

По окончании курса студенты будут знать: основы индивидуального и группового поведения; основные теории мотивации; основные теории лидерства; концепции коммуникаций, управления конфликтами и стрессом в организации.

Будут способны определять различные роли руководителей в организациях; смотреть на организации с точки зрения менеджеров; понимать, как эффективный менеджмент способствует эффективной организации.

Педагогика высшей школы

КОД – HUM207

КРЕДИТ – 4 (0/0/2/2)

ПРЕРЕКВИЗИТ

ЦЕЛЬ И ЗАДАЧИ КУРСА

Курс направлен на изучение психолого-педагогической сущности образовательного процесса высшей школы; формирования представлений об основных тенденциях развития высшей школы на современном этапе, рассмотрение методических основ процесса обучения в высшей школе, а также психологических механизмов, влияющих на успешность обучения, взаимодействия, управления субъектов учебного процесса. Развитие психолого-педагогического мышления магистрантов.

КРАТКОЕ ОПИСАНИЕ КУРСА

В ходе изучения курса магистранты знакомятся с дидактикой высшей школы, формами и методами организации обучения в высшей школе, психологическими факторами успешного обучения, особенностями психологического воздействия, механизмами воспитательного влияния, педагогическими технологиями, характеристиками педагогического общения, механизмами управления процессом обучения. Анализируют организационные конфликты и способы их разрешения, психологические деструкции и деформации личности педагога.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА – по окончанию курса магистрант должен знать особенности современной системы высшего профессионального образования, организацию педагогического исследования, характеристики субъектов образовательного процесса, дидактические основы организации процесса обучения в высшей школе, педагогические технологии, закономерности педагогического общения, особенности воспитательных воздействий на студентов, а также проблемы педагогической деятельности.

Организация систем информационной безопасности

КОД – SEC215

КРЕДИТ – 6 (1/1/1/3)

ПРЕРЕКВИЗИТ – нет.

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Организация систем информационной безопасности» (ОСИБ) является формирование профессиональных знаний в области организации систем информационной безопасности на объекте.

Задачами дисциплины являются: изучение современных тенденций международных, отечественных стандартов в области информационной безопасности, построения систем информационной безопасности организации, разработке эффективной политики и программы безопасности в зависимости от объектов защиты, степени ее конфиденциальности, применения современных методов, средств и технологий обеспечения безопасности.

КРАТКОЕ ОПИСАНИЕ КУРСА

Программа учебного курса «Организация систем информационной безопасности» направлена на ознакомление магистрантов с основами организации, построения, системы информационной безопасности, разработки программы и политики безопасности, определения объектов защиты, формирования модели нарушителя, организации защиты на административном, процедурном уровнях информационной безопасности, проведение анализа рисков и их оценку, осуществлять выбор методов, средств и технологий защиты в зависимости объектов защиты, степени ее конфиденциальности и направлению бизнеса

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен иметь представление:

- об основах производственных отношений и принципах управления;
- о современных методах исследований в области обеспечения безопасности;

В результате освоения дисциплины обучающийся должен знать:

- современные технологии в области защиты информации, методы и средства вычислительной техники и программного обеспечения;
- современные технологии в области защиты информации;
- международный стандарт по обеспечению информационной безопасности;
- законодательные акты Республики Казахстан в области информационной безопасности;
- гармонизированные в Республике Казахстан стандарты и спецификации информационной безопасности и защиты информации.

В результате освоения дисциплины обучающийся должен уметь:

- создавать и применять современные технологии в области защиты информации;
- применять современные технологии защиты информации в системах информационной безопасности;
- управлять информационной безопасностью систем и сетей.

Иметь навыки:

- выявления угроз и уязвимостей в системе информационной безопасности организации;
- разработки политики и программы безопасности организации;
- обеспечения управления и контроля на административном и процедурном уровнях информационной безопасности организации;
- анализа и выбора методов защиты информации;
- обеспечения и оценки безопасности объекта.

Организация защиты и безопасности баз данных

КОД – SEC214

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ – Организация систем информационной безопасности

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Организация защиты и безопасности баз данных» (ОЗиББД) является приобретение обучающимися профессиональных компетенций в области организации комплексной защиты и безопасности баз данных (БД).

Задачей изучения дисциплины “Организация защиты и безопасности баз данных” является усвоение базовых принципов организации систем защиты и безопасности серверов баз данных и их применение.

КРАТКОЕ ОПИСАНИЕ КУРСА

Программа учебного курса «Организация защиты и безопасности баз данных» направлена на изучение технологий обеспечения безопасности баз данных (БД). Курс посвящен применению методов и средств для решения практических задач защиты и безопасности БД.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:

- организацию системы защиты и безопасности БД;
- технологии защиты БД и методы проектирования безопасных БД;
- встроенные механизмы обеспечения безопасности БД в серверах БД;
- уметь:
- применять на практике технологии обеспечения безопасности и защиты БД;
- применять на практике встроенные механизмы серверов БД для защиты и безопасности БД;

иметь навыки:

- проектирования безопасных БД в CASE-средствах;

использования языка SQL для создания, работы и обеспечения защиты и безопасности БД;

- использования криптографических встроенных средств защиты.

Численные методы в инженерии

КОД - GEN200

КРЕДИТ – 6 (1/1/1/3)

ПРЕРЕКВИЗИТ – нет

ЦЕЛЬ И ЗАДАЧИ КУРСА

Этот курс направлен на предоставление необходимых теоретических знаний численных методов и навыков применения процедур для численного решения различных проблем, возникающих в инженерных приложениях.

КРАТКОЕ ОПИСАНИЕ КУРСА

Данная дисциплина будет охватывать численные методы, связанные с решением систем линейных алгебраических уравнений, нелинейных уравнений, полиномиальной

аппроксимации и интерполяции, численного интегрирования и дифференцирования обыкновенных и дифференциальных уравнений в частных производных.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

Студенты будут иметь четкое представление о возможностях и теоретических основах численных методов и смогут продемонстрировать применение этих методов для решения проблем, связанных с инженерными приложениями.

Machine Learning & Deep Learning

КОД - CSE746

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ – нет

ЦЕЛЬ И ЗАДАЧИ КУРСА

Цель курса - освоение базовой теории и практики методов машинного обучения на базе широко используемых библиотек открытого доступа. Научить применять модели машинного обучения в практических задачах разработки программного обеспечения. Основные задачи курса:

- Рассмотреть основные модели машинного обучения и решаемые ими задачи Получить понимание и опыт работы нейронных сетей
- Рассмотреть современные методы классификации и кластеризации данных
- Изучение актуальных направлений исследования моделей глубокого обучения

КРАТКОЕ ОПИСАНИЕ КУРСА Курс посвящен моделям глубокого обучения. Являясь областью в рамках машинного обучения, модели глубокого обучения иллюстрируют количественно-качественный переход. Новые модели и их свойства требуют отдельного изучения и практики настройки метапараметров таких моделей.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА По завершении курса студенты будут:

Понимать

- Особенности моделей глубокого обучения
- Актуальные направления исследований в области AI

Знать

- Задачи и области применения моделей глубокого обучения

Уметь

- Использовать модели машинного обучения

Безопасность систем виртуализации и облачных технологий

КОД – SEC244

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – нет

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Безопасность систем виртуализации и облачных технологий» (БСВиОТ) является приобретение обучающимися профессиональных компетенций в области виртуализации и облачных технологий.

Задачей изучения дисциплины «Безопасность систем виртуализации и облачных технологий» является усвоение базовых принципов организации безопасного использования систем виртуализации и облачных технологий.

КРАТКОЕ ОПИСАНИЕ КУРСА

Программа учебного курса «Безопасность систем виртуализации и облачных технологий» направлена на изучение технологических основ облачных вычислений - концепций виртуализации и систем виртуализации, сервисов облачных технологий и обеспечения их безопасности и защиты.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:
- технологии виртуализации ресурсов и платформ;
- системы виртуализации от ведущих производителей;
- принципы построения гипервизоров и их уязвимости;
- угрозы и риски систем виртуализации;
- основные сервисы облачных технологий IaaS, PaaS и SaaS;
- распространенные атаки на облака;

уметь:
- устанавливать системы виртуализации;
- работать с облачными сервисами;
- тестировать виртуальные машины на уязвимость;
- создавать виртуальный зашифрованный диск;

иметь навыки:
- создания виртуальных машин;
- работы с приложениями в виртуальной машине;
- использования криптографической защиты данных в облаках;
- использования рекомендаций от Cloud Security Alliance по обеспечению безопасности облачных вычислений.

Алгоритмы криптографической защиты информации

КОД – SEC201

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ – Организация систем информационной безопасности

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Алгоритмы криптографической защиты информации» является формирование системы профессиональных знаний о правилах, регламентирующих применение криптографических преобразований и алгоритмов целях защиты информации, развитие навыков решения задач, связанных с преобразованием и передачей информации.

Задачами дисциплины являются: изучение криптографических протоколов, используемых при исследовании и построении современных алгоритмов, методов и моделей преобразования и защиты информации; овладение методами анализа и реализации криптографических протоколов; приобретение навыков решения теоретических и практических задач.

КРАТКОЕ ОПИСАНИЕ КУРСА

Программа учебного курса «Алгоритмы криптографической защиты информации» направлена на ознакомление магистрантов с криптографическими протоколами, основными характеристиками, свойствами, характеризующими безопасность протоколов; видами криптографических протоколов, атаки на безопасность протоколов, формальные методы анализа протоколов обеспечения безопасности; протоколы распределения ключей; квантовая криптография и квантовые протоколы распределения ключей, схемы разделения секрета, протоколы с нулевым разглашением, протоколы решения математических задач; протокол привязки к биту; игровые протоколы подбрасывания монеты по телефону, игра в покер по телефону; протокол подписания контракта.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:

- математические модели криптографических протоколов;
- современные технологии в области защиты информации;
- формулировки научных проблем в области создания и исследования правил, регламентирующих использование криптографических преобразований и алгоритмов;
- виды криптографических протоколов и области защиты информации, в которых они используются;
- математические основы криптографических протоколов.

В результате освоения дисциплины обучающийся должен уметь:

- - решать математические задачи, возникающие при создании криптографических протоколов;
- применять языки и методы программирования для реализации криптографических алгоритмов;
- работать с научными публикациями, посвященным вопросам регламентации криптографических преобразований информации, и находить практическое применение изложенным в работах результатов исследований;
- выполнять выбор и оценку криптографических протоколов при решении прикладных задач криптографии
- создавать необходимые для конкретных объектов защиты информации необходимые модификации правил, регламентирующих использование криптографических преобразований и алгоритмов.

Иметь навыки:

- анализа математическими методами криптографических протоколов;
- навыками реализации основных алгоритмов, реализующих криптографические протоколы на основе современных информационных технологий и сетевых ресурсов;
- обладать знаниями математического аппарата криптографии, необходимые для научно-исследовательской работы.
- навыками построения криптографических конструкций, в которых присутствуют криптографические протоколы.

Стеганографические методы защиты информации

КОД – SEC 238

КРЕДИТ –6 (1/1/1/3)

ПРЕРЕКВИЗИТ –нет

ЦЕЛЬ И ЗАДАЧИ КУРСА является освоение основополагающих принципов стеганографии, состоящих в обеспечении скрытной передачи и хранения конфиденциальных данных путем незаметного встраивания их в другие данные, передаваемые по открытым каналам.

КРАТКОЕ ОПИСАНИЕ КУРСА

Содержание дисциплины охватывает круг вопросов, связанных с защитой информации путем математических преобразований с помощью стеганографических алгоритмов и алгоритмов защиты авторских прав.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:

- перспективные направления развития
- классификацию стеганографических систем
- принципы построения стеганосистем цифровых, водяных знаков и стеганосистем передачи данных.
- форматы представления аудио и графической информации в компьютерных системах Стеганографии

Уметь определять стеганографическую стойкость систем, применять программные продукты в стеганографии и организовывать визуальные атаки на стеганосистемы.

Средства безопасности сетевых Операционных систем

КОД – SEC 221

КРЕДИТ – 6 (2/0/1/3)

ПРЕРЕКВИЗИТ – Организация систем информационной безопасности

ЦЕЛЬ И ЗАДАЧИ КУРСА

Теоретическое и практическое обучение слушателей основам организации IP-сетей, маршрутизации, особенностям работы IP-протоколов, разновидностей сетевых ОС и обеспечение их информационной безопасности, а также методам защиты от изменения и контроля целостности компонентов ОС (программного обеспечения). Задачи курса: сформировать общие представления по обеспечению безопасности сетевых ОС; ознакомить с организацией IP-сетей, с внутренней организацией хранения информации в ОС;ознакомить с методами и средствами обеспечения безопасности сетевых ОС; получить практические навыки по определению очагов угрозы и организации защиты в ОС.

КРАТКОЕ ОПИСАНИЕ КУРСА

Курс «Средства безопасности сетевых операционных систем» обучает основам организации IP-сетей, распределению IP-адресов, области применения и особенностям работы IP-протоколов, разновидностям сетевых ОС. Защита от изменения и контроль целостности программного обеспечения. Методы и средства хранения ключевой

информации. Принципы многофакторной аутентификации. Технические устройства идентификации и аутентификации. Парольные подсистемы идентификации и аутентификации. Идентификация и аутентификация пользователей с помощью биометрических устройств. Программно-аппаратные средства шифрования. Обеспечение безопасности в системах Windows, Unix, ознакомление с внутренней организацией носителей информации. Системы обнаружения вторжений. Основные компоненты архитектуры межсетевых экранов. Современные требования к межсетевым экранам.

Дает практические навыки по перехвату и анализу сетевого трафика в целях определения очагов угрозы. Просмотр и анализ структуры файловых систем в целях организации защиты от распространения вирусов внутри системы. Навыки по разработке программ *(среду разработки выбирает слушатель)*: 1) по обмену короткими сообщениями с формированием IP-пакетов между компьютерами в локальной сети; 2) проводящая анализ IP-пакетов формируемой предыдущей программой и формирования пакетов точечной DoS-атаки в целях детального представления методов сетевых атак при настройке межсетевых экранов.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате изучения дисциплины обучающийся должен знать:

- организацию IP-сетей, структуру IP-пакетов и IP-протоколов;
- внутреннюю организацию носителей информации ОС;
- методы и средства хранения ключевой информации и шифрования;
- разновидности и принципы аутентификации;
- требования к межсетевым экранам и системам обнаружения вторжений;

иметь навыки:

- перехвата и анализа сетевого трафика, а также выявление уязвимостей;
- анализа структуры файловых систем FAT32, NTFS, EXT4 и поиска, чтение и изменение информации (в шестнадцатеричном формате) на физическом уровне;
- по разработке программ обеспечивающее обмен данными в защищенном формате между компьютерами с применением различных сетевых протоколов;

обладать следующими компетенциями:

- пользоваться справочными и информационными материалами по обеспечению безопасности сетевых ОС;
- осуществлять выбор программно-технических средств обеспечение безопасности;
- разрабатывать алгоритмы и программы на языках низкого и высокого уровней;
- оценивать защищенность сетевых ОС.

Model-Driven Software Engineering
КОД - CSE249
КРЕДИТ – 6 (2/0/1/3)
ПРЕРЕКВИЗИТ – нет

ЦЕЛЬ И ЗАДАЧИ КУРСА
КРАТКОЕ ОПИСАНИЕ КУРСА

Целью курса является изучение принципов и методов разработки программного обеспечения информационных систем. Принципы разработки, управляемой моделями. Модели, спецификации и их роль в создании программных систем. Моделе-ориентированная программная инженерия. Общие сведения об унифицированном языке моделирования№ Общие сведения об унифицированном языке моделирования и объектном языке ограничений. Предметно-ориентированные языки моделирования

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В процессе изучения дисциплины магистранты должны:

- знать современные методы проектирования, анализа и применения информационных систем; уметь применять различные пакеты инструментального программного обеспечения при исследовании методов разработки информационных систем.

Иметь навыки организации построения моделей и алгоритмов функционирования информационных систем и управления процессом разработки программного продукта в команде.

Инженерно-техническая защита информации
КОД – SEC208
КРЕДИТ – 6 (1/1/1/3)
ПРЕРЕКВИЗИТ – Организация систем информационной безопасности

ЦЕЛЬ И ЗАДАЧИ КУРСА. Целью дисциплины «Инженерно-техническая защита информации» является ознакомление магистрантов с техническими каналами утечки информации, техническими средствами и методами несанкционированного доступа к конфиденциальной информации и защиты ее безопасности от утечки по различным техническим каналам связи, а также с принципами построения и работы схем технических средства акустической разведки и защиты безопасности информации от утечки по радиоканалу, телефонным линиям связи, оптическому каналу и т. д.

Задачами изучения дисциплины являются получение знаний по: техническим каналам утечки информации; техническим средствам несанкционированного доступа к конфиденциальной информации; техническим средствам прослушивания телефонных каналов связи и защиты информации от утечки по этим каналам; методам и средствам защиты информации от утечки по радиоканалу; техническим средствам защиты информации от утечки по оптическому каналу связи; по фильтрации информационных сигналов, по помехоподавляющим фильтрам и по вопросам зашумления.

КРАТКОЕ ОПИСАНИЕ КУРСА

Секретная, конфиденциальная и открытая информация. Технические каналы утечки информации. Технические средства акустической разведки. Технические

средства несанкционированного доступа к конфиденциальной информации. Технические средства прослушивания телефонных каналов связи и защиты информации от утечки по ним. Технические средства для поиска и обнаружения закладных устройств. Технические средства защиты информации от утечки по оптическому каналу связи. Цифровой генератор шума. Генераторы белого шума и их особенности.. Фильтрация информационных сигналов для подавления кондуктивных помех. Технические каналы утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН).

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

По окончании курса «Инженерно-техническая защита информации» магистрант должен **знать:**

- виды конфиденциальной информации, перечни сведений конфиденциального характера;
- технические каналы утечки информации и угрозы безопасности информации в результате несанкционированного доступа;
- принципы построения и работы схем электронных устройств, применяемых в технических средствах защиты информации;
- принципы действия и особенности функционирования технических средств нелегального съема и защиты информации от утечки по радиоканалу, телефонному и оптическому каналам связи;
- вопросы фильтрация информационных сигналов, помехоподавляющие фильтры и вопросы зашумления.

уметь и иметь навыки:

- различать виды защищаемой информации, идентифицировать её источники и носители;
- выявлять основные угрозы безопасности информации и оценивать их степень;
- уметь применять технические средства защиты акустической информации от утечки по различным техническим каналам;
- владеть навыками работы с основными узлами аппаратных средств инженерно-технической защиты информации;
- применять полученные знания в своей дальнейшей профессиональной деятельности.

Аудит информационной безопасности

КОД – SEC204

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – Организация систем информационной безопасности

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Аудит информационной безопасности» (АИБ) является приобретение обучающимися профессиональных компетенций в области аудита информационной безопасности.

Задачей дисциплины является приобретение магистрантами теоретических и практических знаний по аудиту информационной безопасности (ИБ) предприятия.

КРАТКОЕ ОПИСАНИЕ КУРСА

Программа учебного курса «Аудит информационной безопасности» направлена на изучение стандартов ИБ, организации и методов проведения аудита, их практического применения.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:

- стандарты ИБ и критерии оценки безопасности ИТ;
- типы аудита и этапы аудита;
- методы и инструменты активного аудита;
- систему оценки уязвимостей CVSS;
- методы анализа данных при аудите ИБ;

уметь:

- составлять план проведения внутреннего аудита;
- проводить внутренний аудит;
- пользоваться системой оценки уязвимостей CVSS;
- пользоваться инструментами анализа рисков;

иметь навыки:

- проведения тестирования на проникновение;
- анализа рисков.

Киберпреступность и компьютерная криминалистика

КОД – SEC240

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – Организация систем информационной безопасности**,** Средства безопасности сетевых ОС

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Киберпреступность и компьютерная криминалистика» является приобретение обучающимися профессиональных компетенций в области киберпреступности и расследования киберпреступлений.

Задачей изучения дисциплины « Киберпреступность и компьютерная криминалистика» является усвоение принципов использования систем и средств раскрытия преступлений, связанных с компьютерной информацией.

КРАТКОЕ ОПИСАНИЕ КУРСА

Основы Форензики (компьютерная криминалистика, расследование киберпреступлений) - прикладная наука о раскрытии преступлений, связанных с компьютерной информацией. Изучаются средства проведения исследований цифровых доказательств и методы поиска, получения и закрепления доказательств.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать: основы Форензики, вопросы и решения компьютерной криминалистики; средства для исследования цифровых доказательств.

уметь:

- проводить расследования;

- исследовать цифровые доказательства;
- применять современные методы и средства для обнаружения киберпреступлений.

Иметь навыки:

- использования современных методов и средств расследования киберпреступлений;
- обнаружения киберпреступлений;
- проведения анализа цифровых доказательств.

Big Data и анализ данных

КОД – SEC245

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – Организация защиты и безопасности БД, Безопасность систем виртуализации и облачных технологий.

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Big Data и анализ данных» является приобретение обучающимися профессиональных компетенций в области анализа больших данных.

Задачей дисциплины является приобретение магистрантами теоретических и практических знаний по анализу больших данных, применения специальных методов и средств анализа.

КРАТКОЕ ОПИСАНИЕ КУРСА

Дисциплина направлена на изучение создания, хранения, управления, передачи, поиска, анализ больших данных с акцентом на новейшие технологии, инструменты, архитектуры и системы, которые являются вычислительными решениями с большими данными в высокопроизводительных сетях. Реальные приложения BigData и рабочие процессы в различных областях (особенно в области науки) представлены в качестве примеров использования для иллюстрации разработки, развертывания и реализации широкого спектра новых решений в области BigData.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:

- новейшие технологий, инструменты, архитектуру и системы для анализа больших данных;
- решения в области больших данных;
- методы сбора данных, хранения данных и анализа данных.

уметь:

- применять новейшие технологии, инструменты и системы для анализа больших данных;
- использовать на практике решения в области больших данных;
- осуществлять сбор, хранение и анализ данных.

иметь навыки:

- проведения анализа больших данных
- применения методов и средств для работы с большими данными.

Безопасность систем электронного бизнеса

КОД – SEC206

КРЕДИТ – 6 (2/1/0/3)

ПРЕРЕКВИЗИТ – Организация систем информационной безопасности, Организация защиты и безопасности БД.

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины “Безопасность систем электронного бизнеса” является приобретение обучающимися профессиональных компетенций в области информационной безопасности экономических систем (ЭС).

Задачей дисциплины “Безопасность систем электронного бизнеса” является усвоение базовых принципов обеспечения безопасной работы экономических систем.

КРАТКОЕ ОПИСАНИЕ КУРСА

Программа учебного курса “Безопасность систем электронного бизнеса” направлена на изучение теоретических и практических вопросов обеспечения информационной безопасности организаций различных форм собственности.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:

- стандарты РК по защите служебной информации;
- принципы организации экономической деятельности в Интернет;
- модели ведения электронного бизнеса;
- угрозы безопасности экономических систем;
- методы и средства защиты информации в ЭС;
- технологии обеспечения информационной безопасности ЭС;
- особенности защиты баз данных в ЭС;
- организацию систем информационной безопасности ЭС.

уметь:

- работать с Web-сайтами разных моделей ведения электронного бизнеса;
- устанавливать и конфигурировать межсетевые экраны;
- устанавливать и настраивать системы обнаружения вторжений;
- устанавливать и настраивать системы предотвращения вторжений;
- устанавливать и настраивать системы резервного копирования и восстановления данных;

иметь навыки:

- обнаружения вторжений;
- предотвращения вторжений;
- резервного копирования и восстановления данных.

Риск менеджмент в кибербезопасности
КОД – SEC 245
КРЕДИТ – 6 (2/0/1/3)
ПРЕРЕКВИЗИТ – Организация систем информационной безопасности

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью дисциплины «Риск менеджмент в кибербезопасности» (РМвКБ) является приобретение обучающимися профессиональных компетенций в области управления рисками в кибербезопасности.

Задачей дисциплины является приобретение студентами теоретических и практических знаний по управлению рисками информационной безопасности.

КРАТКОЕ ОПИСАНИЕ КУРСА

Программа учебного курса «Риск менеджмент в кибербезопасности» направлена на изучение стандартов управления рисками, инструментальных средств оценивания рисков и их практическое применение.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:
- базовые понятия риска в информационной безопасности (ИБ);
- стандарты управления рисками;
- ключевые вопросы анализа и управления рисками ИБ;
- методики оценки информационных рисков компании;
- количественные и качественные меры риска;
- средства автоматической оценки риска (АОР);
- контрмеры, обеспечивающие режим ИБ;

уметь:
- оценивать риски;
- выбирать контрмеры для уменьшения риска;
- выбирать контрмеры для уклонения от риска;
- выбирать контрмеры для изменения характера риска;
- пользоваться инструментами АОР;

иметь навыки:
- анализа рисков;
- оценки рисков с использованием АОР;
- принятия риска.

Программирование микроконтроллеров
КОД – SEC 218
КРЕДИТ –6 (2/1/0/3)
ПРЕРЕКВИЗИТ – Организация систем информационной безопасности

ЦЕЛЬ И ЗАДАЧИ КУРСА Изучение принципов построения микропроцессоров и микроконтроллеров, программирование микроконтроллеров, а также проектирование, разработка и изготовление электронных узлов криптографических систем с применением микроконтроллеров.

КРАТКОЕ ОПИСАНИЕ КУРСА

Технические характеристики и программно-доступные средства микроконтроллера. Основные определения, характеристики, область применения и особенности работы микропроцессоров. Разновидности и архитектура микроконтроллеров. Проектирование криптографических систем с применением микроконтроллеров. Режимы работы микроконтроллеров. Организация подсистемы памяти и интерфейсов. Система прерываний и исключений, а также энергосберегающие режимы. Типы и характеристики интерфейсов, сопроцессоры прямого доступа к памяти (DMA). Тенденция развития микроконтроллеров.

Проектирование и разработка схемных решений на базе САПР «Altium Designer». Программирование работы отдельных блоков микроконтроллерных систем в среде разработки CooCox.

Формирование навыков программирование на языке Си микроконтроллеров для решения различных задач в криптографических системах с применением технических возможностей микроконтроллеров.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате освоения дисциплины обучающийся должен знать:

- формат представления данных в микропроцессорных системах и их обработка;
- устройства электроники (фотоэлектронные приборы, транзистор, т.д.);
- микросхемы (операционные усилители, стабилизаторы, т.д.) и их условное обозначение (SMD компоненты), назначение, типоразмеры, характеристики.

Уметь:

- проектировать и разрабатывать электрические схемы электронных узлов с применением САПР;
- проводить монтаж электрических компонентов устройств;
- применять на практике измерительные приборы.

Образовательная программа научной и педагогической магистратуры включает два вида практик:

- педагогическую;
- исследовательскую.

Педагогическая практика проводится с целью формирования практических навыков и методики преподавания. Педагогическая практика может проводиться в период теоретического обучения без отрыва от учебного процесса.

Исследовательская практика магистранта проводится с целью ознакомления с новейшими теоретическими, методологическими и технологическими достижениями отечественной и зарубежной науки, с современными методами научных исследований, обработки и интерпретации экспериментальных данных. Научно-исследовательская работа магистранта

Научно-исследовательская работа в научной и педагогической магистратуре должна:

- соответствовать основной проблематике специальности, по которой защищается магистерская диссертация;
- быть актуальной, содержать научную новизну и практическую значимость; - основываться на современных теоретических, методических и технологических достижениях науки и практики;
- выполняться с использованием современных методов научных исследований;
- содержать научно-исследовательские (методические, практические) разделы по основным защищаемым положениям;
- базироваться на передовом международном опыте в соответствующей области знания.
- выполняться с применением передовых информационных технологий;
- содержать экспериментально-исследовательские (методические, практические) разделы по основным защищаемым положениям.

Защита магистерской диссертации

КОД – ECA2013

КРЕДИТ –12

Целью выполнения магистерской диссертации является:

демонстрация уровня научной/исследовательской квалификации магистранта, умения самостоятельно вести научный поиск, проверка способности к решению конкретных научных и практических задач, знания наиболее общих методов и приемов их решения.

КРАТКОЕ ОПИСАНИЕ

Магистерская диссертация – выпускная квалификационная научная работа, представляющая собой обобщение результатов самостоятельного исследования магистрантом одной из актуальных проблем конкретной специальности соответствующей отрасли науки, имеющая внутреннее единство и отражающая ход и результаты разработки выбранной темы.

Магистерская диссертация – итог научно-исследовательской /экспериментально-исследовательской работы магистранта, проводившейся в течение всего периода обучения магистранта.

Защита магистерской диссертации является заключительным этапом подготовки магистра. Магистерская диссертация должна соответствовать следующим требованиям:

– в работе должны проводиться исследования или решаться актуальные проблемы в области защиты и безопасности информации;

– работа должна основываться в определении важных научных проблем и их решении;

– решения должны быть научно-обоснованными и достоверными, иметь внутреннее единство;

– диссертационная работа должна быть написана единолично.

Содержание