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

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

7М06110 - «КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Профильное обучение (1,5)

Магистр техники и технологий по образовательной программе «7М06110 Комплексное обеспечение информационной безопасности»

1-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 Института информационных и телекоммуникационных технологий Т.Ф. Умаров

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 19.12.2018 г.

Квалификация:
Уровень 7 Национальной рамки квалификаций:

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

Краткое описание программы:

1 Цель образовательной программы:

Целью образовательной программы является обучение магистрантов профильного 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 профильного 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 техники и технологий образовательной программы «7М06110 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 техники и технологии 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.

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..

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

Магистратура по профильному направлению реализует образовательные программы послевузовского образования по подготовке управленческих кадров, обладающих углубленной профессиональной 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) экспериментально-исследовательской работы включающую выполнение магистерского проекта;

4) итоговой аттестации.

Наименование: Комплексное обеспечение информационной безопасности

Цель образовательной программы:

- Обеспечить подготовку специалистов для профессиональной деятельности в сфере информационной безопасности, умеющих применять различные технологии, знания, навыки и компетенции в организации, управлении и проектировании систем защиты информации.

- Подготовить специалистов 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:

1. 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 «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/ квалификации: Выпускнику данной образовательной программы присваивается степень магистра техники и технологий по образовательной программе «7М06110 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:

– *производственная деятельность:*

– способностью самостоятельно проводить 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;

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

При разработке программы магистратуры все общекультурные и общепрофессиональные компетенции, а также профессиональные компетенции, отнесенные к тем видам профессиональной деятельности, на которые ориентирована программа магистратуры, включаются в набор требуемых результатов освоения программы магистратуры.

4 Рабочий учебный план образовательной программы

4.1. Срок обучения 1,5 года

РАБОЧИЙ УЧЕБНЫЙ ПЛАН
образовательной программы

Образовательная программа: 7М**06110- «Комплексное обеспечение информационной безопасности»**

Форма обучения: *дневная* Срок обучения: 1,5 *г.*.

Академическая степень: магистр техники и технологий по образовательной программе «7М06110 Комплексное обеспечение информационной безопасности»

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						
	LNG202	Иностранный язык (профессиональный)	БД ВК	6	3	0/0/3/3			Электив	БД КВ	4	3		
	HUM204	Психология управления	БД ВК	4	2	1/0/1/2			Электив	ПД КВ	6	3		
	MNG274	Менеджемнт	БД ВК	6	3	2/0/1/3			Электив	ПД КВ	6	3		
		Электив	ПД КВ	6	3				Электив	ПД КВ	6	3		
		Электив	БД КВ	6	3				Электив	ПД КВ	6	3		
									Электив	ПД КВ	6	3		
								AAP221	Экспериментально-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерского проекта	ЭИРМ	4			
		Всего		**28**					**Всего**		**38**			
2	3 семестр							4 семестр						
	AAP246	Производственная практика	ПД	9										
	AAP220	Экспериментально-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерского проекта	ЭИРМ	14										

	ECA205	Оформление и защита магистерской диссертации (ОиЗМД)	ИА	12										
		Всего		**35**										
									Итого			**101**		

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН
Образовательной программы:
7М**06110- «Комплексное обеспечение информационной безопасности»**

БД Компоненты по выбору - 10 кредитов					
	Код	**Наименование дисциплин**	**Кредиты**	**Лк/лб/пр/СРО**	**Семестр**
	SEC221	Средства безопасности сетевых ОС	6	2/0/1/3	1
	CSE749	Методы и средства защиты в ОС	6	1/1/1/3	1
	SEC 238	Стеганографические методы защиты информации	4	1/0/1/2	2
	SEC244	Безопасность систем виртуализация и облачных технологий	4	1/1/0/2	2
		Всего	**18**		
ПД Компоненты по выбору - 36 кредитов					
	CSE210	Модели и методы искусственного интеллекта	6	2/1/0/3	1
	SEC246	Big Data и анализ данных	6	2/1/0/3	1
	SEC222	Технологии защиты безпроводных сетей и мобильных приложений	6	2/1/0/3	2
	SEC 215	Организация систем информационной безопасности	6	1/1/1/3	2
	SEC204	Аудит информационной безопасности	6	2/1/0/3	3
	SEC245	Риск менеджмент информационной безопасности	6	2/0/1/3	3
	SEC247	Интеллектуализированные средства распознавания и противодействия кибератакам	6	1/1/1/3	3
	SEC239	Хранилища аналитических данных и OLAP технологии	6	1/1/1/3	3
	SEC218	Программирование микроконтроллеров	6	2/1/0/3	3
	CSE720	Киберпреступность и компьютерная криминалистика	6	2/1/0/3	3
		Всего	**36**		

МОДУЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

Образовательная программа: 7М**06110- «Комплексное обеспечение информационной безопасности»**

Форма обучения: *дневная* Срок обучения: 1,5 *г.*. Академическая степень: магистр техники и технологий

Цикл дисц.	Код дисц.	Наименование дисциплин	Семестр	Академ кред.	лек.	лаб.	практика	СРО	Вид контроля	Кафедра
Модуль профильной подготовки										
Базовые дисциплины (БД)										
Вузовский компонент (ВК)										
БД 1.1.1	LNG202	Иностранный язык (профессиональный)	1	6	0	0	3	3	Экзамен	АЯ
БД 1.2.1	MNG274	Менеджмент	1	6	2	0	1	3	Экзамен	НОЦ УП
БД 1.3.1	HUM204	Психология управления	1	4	1	0	1	2	Экзамен	НОЦ УП
Компонент по выбору (КВ) (10 кредитов)										
Модуль обеспечения сетевой безопасности, безопасности облачных технологий										
БД	CSE749	Методы и средства защиты в ОС	1	6	1	1	1	3	Экзамен	КОиХИ
БД	SEC221	Средства безопасности сетевых ОС	1	6	2	0	1	3	Экзамен	КОиХИ
БД	SEC 238	Стеганографические методы защиты информации	2	4	1	0	1	2	Экзамен	КОиХИ
БД	SEC205	Безопасность и защита облачных вычислений и телекоммуникаций	2	4	1	1	0	2	Экзамен	КОиХИ
Профилирующие дисциплины (ПД)										
Компонент по выбору (КВ) (36 кредитов)										
Модуль анализа данных, применения искусственного интеллекта в ИБ и обеспечения защиты и безопасности информации										
ПД	CSE210	Модели и методы искусственного интеллекта	1	6	2	1	0	3	Экзамен	КОиХИ
ПД	SEC246	Big Data и анализ данных	1	6	2	1	0	3	Экзамен	КОиХИ
ПД	SEC222	Технологии защиты безпроводных сетей и мобильных приложений	2	6	2	1	0	3	Экзамен	КОиХИ
ПД	SEC 215	Организация систем информационной безопасности	2	6	1	1	1	3	Экзамен	КОиХИ
ПД	SEC204	Аудит информационной безопасности	2	6	2	1	0	3	Экзамен	КОиХИ
ПД	SEC245	Риск менеджмент информационной безопасности	2	6	2	0	1	3	Экзамен	КОиХИ
ПД	SEC247	Интеллектуализированные средства распознавания и противодействия кибератакам	2	6	1	1	1	3	Экзамен	КОиХИ
ПД	SEC239	Хранилища аналитических данных и OLAP технологии	2	6	1	1	1	3	Экзамен	КОиХИ
ПД	SEC240	Киберпреступность и компьютрная криминалистика	2	6	2	1	0	3	Экзамен	КОиХИ

ПД	SEC218	Программирование микроконтроллеров	2	6	2	1	0	3	Экзамен	КОиХИ
Практико – ориентированный модуль										
ПД	AAP246	Производственная практика	3	9					Отчет	
Научно-исследовательский модуль										
ЭИРМ	AAP221	Экспериментально-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерского проекта	2	4					Отчет	
ЭИРМ	AAP220	Экспериментально-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерского проекта	3	14					Отчет	
Модуль итоговой аттестации (12 кредитов)										
ИА	ECA205	Оформление и защита магистерского проекта	3	12					Защита диссертаций	
Всего кредитов				101						

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 металлургии и обогащения полезных ископаемых, основанные на передовых знаниях металлургии и обогащения полезных ископаемых, при разработке и (или) применении идей в контексте исследования;

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 металлургии и обогащения полезных ископаемых.

6 Компетенции по завершению обучения

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

1) иметь представление:

– о профессиональной компетентности в области защиты и безопасности информации;

– о технологии виртуализации ресурсов и платформ;

- о технологиях защиты БД;

– о технологии защиты безпроводных сетей и мобильных приложений;

– об анализе больших данных.

2) знать:

– психологию познавательной деятельности магистрантов в процессе обучения;

– психологические методы и средства повышения эффективности и качества обучения;

– технологию защиты безпроводных сетей и мобильных приложений;

– 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;
– 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.

3) уметь:

– 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;
– 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;
– 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:

– 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.

5) быть компетентным:

– 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- знания и умения по дисциплине Проектный менеджмент.

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.

П – Профессиональные компетенции:

П1 – быть компетентным в вопросах киберпреступлений и компьютерной криминалистики, уметь выявлять угрозы и проводить работы по предотвращению вторжений.

П2 – уметь организовать систему защиты и безопасности БД и применять технологии защиты БД.

П3 – знать вопросы организации систем информационной безопасности и уметь на практике проводить работы по комплексному обеспечению информационной безопасности.

П4 – уметь планировать, проектировать, устанавливать и обслуживать инфраструктуры безопасности беспроводных сетей.

П5 – быть компетентным вопросах обеспечения информационной безопасности экономических систем.

П6 – уметь анализировать большие данные.

П7 - знать стандарты ИБ и критерии оценки безопасности ИТ, уметь проводить оценку рисков ИБ.

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 экспериментально-исследовательской работе магистранта в профильной магистратуре:

1) соответствует профилю образовательной программы магистратуры, по которой выполняется и защищается магистерский проект;

2) основывается на современных достижениях науки, техники и производства и содержит конкретные практические рекомендации, самостоятельные решения управленческих задач;

3) выполняется с применением передовых информационных технологий;

4) содержит экспериментально-исследовательские (методические, практические) разделы по основным защищаемым положениям.

6.3 Требования к организации практик:

Образовательная программа профильной магистратуры включает производственную практику в цикле ПД.

Производственная практика в цикле ПД проводится с целью закрепления теоретических знаний, полученных в процессе обучения, приобретения практических навыков, компетенций и опыта профессиональной деятельности по обучаемой образовательной программе магистратуры, а также освоения передового опыта.

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
Гуманитарный модуль	владеть приемами ведения дискуссии и диалога, владеть навыками коммукативности и креативности в своей профессиональной деятельности. Быть компетентным в вопросах психологии управления и проектного менеджмента.	Проектный менеджмент (Психология управления)
Модуль обеспечения сетевой безопасности, безопасности облачных технологий	Уметь организовать систему защиты и безопасности информации, знать современные и перспективные направления развития криптографической защиты информации и применять ее на практике. Уметь организовать комплексное обеспечение защиты и безопасности информации. Безопасно применять современные технологии виртуализации.	Безопасность систем виртуализации и облачных технологий, Методы и средства защиты в ОС, Стеганографические методы защиты информации, Безопасность и защита облачных вычислений и телекоммуникаций
Модуль анализа данных, применения искусственного интеллекта в ИБ и обеспечения защиты и безопасности информации	Знать и применять методы и средства для проведения аудита информационной безопасности. Быть компетентным в вопросах выявления киберпреступлении и компьютерной криминалистики. Уметь использовать средства распознавания и противодействия кибератакам. Уметь анализировать большие данные, знать методы и средства анализа больших данных.	Модели и методы искусственного интеллекта, Риск менеджмент информационной безопасности., Киберпреступность и компьютерная криминалистика, Организация систем информационной безопасности, Big Data и анализ данных, Технологии защиты безпроводных сетей и мобильных приложений, Архитектура микросервисов и распределенных

		вычислительных систем, Риск менеджмент информационной безопасности, OLAP и хранилище данных, Программирование микроконтроллеров
Практико-ориентированный модуль	Получение навыков профессиональной деятельности. Способность порождать новые идеи. Практика в выполнении 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.	Профессиональная 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 выводы и используемые для их формулировки знания специалистам и неспециалистам. Изучение научно-технической информации, отечественного и зарубежного опыта в области IT-	Оформление и защита магистерской диссертации

	технологий для творческого его осмысления и выработки правильного решения своей научно-технической или производственной задачи.	

9. Описание дисциплин

Иностранный язык (профессиональный)
Professional English for Project Managers

КОД – LNG205
КРЕДИТ – 6
ПРЕРЕКВИЗИТ –Academic English, Business English, IELTS 5.0-5.5

ЦЕЛЬ И ЗАДАЧИ КУРСА

Цель курса состоит в том, чтобы развить у магистрантов 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 магистранты 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 магистранты 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.

Менеджмент

КОД MNG274

КРЕДИТ 6

ПРЕРЕКВИЗИТ: Дисциплина «Проектный менеджмент» базируется на знаниях, полученных в результате изучения дисциплин по курсам бакалавриата

ЦЕЛЬ И ЗАДАЧИ КУРСА Целью преподавания дисциплины "Проектный менеджмент" является освоение методологии управления проектами в различных сферах деятельности, воспитание культуры, адекватной современному проектному менеджменту и информационным технологиям, создание условий для внедрения новых информационных технологий в сферу выполнения проектов. Курс основывается на международных рекомендациях по управлению проектами (Project Management Body of Knowledge).

КРАТКОЕ ОПИСАНИЕ КУРСА Содержание дисциплины направлено на изучение современных концепций, методов, инструментов проектного менеджмента с целью применения их в дальнейшей практической деятельности специалиста для решения задач планирования и исполнения проектов.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

Уметь:

- подготавливать документы этапа инициализации проекта, такие как технико-экономическое обоснование, устав проекта и др.
- разработать и анализировать документы, относящиеся к планированию проектной деятельности, применять различные методы поддержки принятия решения;
- оперативно контролироватьисполнение работ и отслеживать сроки;
- подбирать кадры, разрешать противоречия между членами команды;
- управлять рисками, возникающими при реализации проектов.

Знания, полученные при прохождении дисциплины:

- Современные стандарты в облатси управления проектамии их характеристики;
- Подход PMI к управлению проектами;
- Планирование инвестиционной деятельности;
- Учет проектных рисков;
- Методы оптимизации использования имеющихся ресурсов;
- Способы урегулирования конфликтных ситуаций;
- Анализ фактических показателей для своевременной корректировки хода работ.

Навыки:

- ведения проектов в соответствии с современными требованиями проектного менеджмента- применять в процессе управления проектами программными обеспечением MS Project

ПСИХОЛОГИЯ УПРАВЛЕНИЯ

КОД - HUM204

КРЕДИТ – 4

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 магистранты 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.

Средства безопасности сетевых Операционных систем

КОД – SEC 221

КРЕДИТ – 6

ПРЕРЕКВИЗИТ - нет

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.

Методы и средства защиты в ОС

КОД – SEC 221

КРЕДИТ – 6

ПРЕРЕКВИЗИТ – нет

КРАТКОЕ ОПИСАНИЕ КУРСА

Основные понятия и положения защиты информации в операционных системах. Угрозы безопасности информации в информационно-вычислительных системах. Угрозы безопасности ОС. Требования к защите ОС. Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix, Mac OS. Статистика методов, лежащих в основе атак на современные ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Разграничение доступа к ресурсам в ОС Windws, Unix, Mac OS. Аудит в ОС. Системы защиты программного обеспечения.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате изучения дисциплины обучающийся должен знать:

- методы и средства хранения ключевой информации и шифрования;
- разновидности и принципы аутентификации;
- осуществлять выбор программно-технических средств обеспечение безопасности;
- разрабатывать алгоритмы и программы на языках низкого и высокого уровней;
- оценивать защищенность сетевых ОС.

Стеганографические методы защиты информации

КОД – SEC 238

КРЕДИТ – 4

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.

Безопасность систем виртуализации и облачных технологий

КОД – SEC244

КРЕДИТ – 4

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.

Модели и методы искусственного интеллекта

КОД – CSE 210

КРЕДИТ –6

ПРЕРЕКВИЗИТ –нет

Целью курса «Модели и методы искусственного интеллекта» является обучение математическим методам в технологиях искусственного интеллекта и моделях

представления знаний, изучение принципов создания системы искусственного интеллекта.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

В результате изучения дисциплины магистранты должны знать принципы системы искусственного интеллекта, математические методы, используемые в технологии искусственного интеллекта, и модели представления знаний.

Big Data и анализ данных

КОД – SEC246

КРЕДИТ – 6

ПРЕРЕКВИЗИТ – нет

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.

Технологии защиты беспроводных сетей и мобильных приложений

КОД – SEC222

КРЕДИТ -6

ПРЕРЕКВИЗИТ –нет

ЦЕЛЬ И ЗАДАЧИ КУРСА

Целью данного курсе является планирование, проектирование, установка и облуживание инфраструктур безопасности беспроводных сетей и мобильных приложений. Особое внимание уделяется контрмерам и в отношении мошенников, а так же частных предпринимателей.

КРАТКОЕ ОПИСАНИЕ КУРСА

В данном курсе вы ознакомитесь с функциями, протоколами и конфигурациями для реализации аутентификации, распределения ключей, целостности, конфиденциальности и анонимности в сетях беспроводного доступа для мобильных пользователей. Курс представляет методы безопасности, используемые в существующих системах, таких как WPAN, WLAN, UMTS, IMS. Предлагаемые решения для новых сетевых технологий, таких как различные типы специальных сетей. Цифровая криминалистика в беспроводных системах.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

Знания по окончанию дисциплины:

- знания о технологиях и методах защиты информации для систем связи, которые предоставляют услуги для мобильных пользователей сетями беспроводного доступа;
- знание и понимание механизмов безопасности и протоколов в системах беспроводной связи, таких как актуальные технологии WLAN IEEE 802.11, WAN 802.16, GSM / UMTS / LTE, Ad-hoc и сенсорных сетей.
- знание некоторых моделей, принципов проектирования, механизмов и решений, используемых в безопасности беспроводной сети для получения аутентификации и ключевых транспортных протоколов.

Навыки:

- приобретение практических и аналитических навыков в оценке информационной безопасности технологий и методов для систем связи, которые предоставляют услуги для мобильных пользователей сетями беспроводного доступа.
- практические навыки по технологиям защиты беспроводных сетей и мобильных приложений.

Организация систем информационной безопасности

КОД – SEC215

КРЕДИТ – 6

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.

Аудит информационной безопасности

КОД – SEC204

КРЕДИТ – 6

ПРЕРЕКВИЗИТ – нет

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.

Риск менеджмент в кибербезопасности

КОД – SEC 245

КРЕДИТ –6

ПРЕРЕКВИЗИТ –нет

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 магистрантами 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.

Хранилища аналитических данных и OLAP технологии

КОД – SEC 239

КРЕДИТ – 6

ПРЕРЕКВИЗИТ – нет

ЦЕЛЬ И ЗАДАЧИ КУРСА Изучение принципов технологий обработки данных.

КРАТКОЕ ОПИСАНИЕ КУРСА

OLAP (англ. online analytical processing, интерактивная аналитическая обработка) — технология обработки данных, заключающаяся в подготовке суммарной (агрегированной) информации на основе больших массивов данных, структурированных по многомерному принципу. Реализации технологии OLAP являются компонентами программных решений класса Business Intelligence.

Интеллектуализированные средства распознавания и противодействия кибератакам

КОД – SEC 247

КРЕДИТ –6

ПРЕРЕКВИЗИТ – нет

ЦЕЛЬ И ЗАДАЧИ КУРСА

Ознакомится с принципом работы интеллектуализированных средств распознавания и противодействия кибератакам. Применять на практике методы и средства распознавания и противодействия кибератакам.

КРАТКОЕ ОПИСАНИЕ КУРСА

Риски и каналы утечки информации, классификация нарушителей. APT (Advanced Persistent Threat) атаки. Технологии защиты от утечки данных. Системы распознавания и противодействия кибератакам. Классификация DLP систем, методы распознавания

конфиденциальной информации. Этапы работы DLP систем. Развитие интеллектуализированных средств распознавания и противодействия кибератакам систем. Аналитические инструменты расследования и анализа инцидентов.

ЗНАНИЯ, УМЕНИЯ, НАВЫКИ ПО ЗАВЕРШЕНИЮ КУРСА

Знать:

- о технологиях и методах защиты информации интеллектуализированных средств распознавания и противодействия кибератакам
- о механизмах безопасности интеллектуализированных средств распознавания и противодействия кибератакам.
- о моделях, принципах проектирования, механизмах и решениях, используемых в интеллектуализированных средствах распознавания и противодействия кибератакам.

Навыки:

- применения технологий и методов защиты информации для распознавания и противодействия кибератакам
- применения механизмов безопасности интеллектуализированных средств распознавания и противодействия кибератакам.
- применения моделей, принципов построения, механизмов и решения, используемых в интеллектуализированных средствах распознавания и противодействия кибератакам.

Программирование микроконтроллеров

КОД – SEC 218

КРЕДИТ –6

ПРЕРЕКВИЗИТ – нет

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.

Киберпреступность и компьютерная криминалистика

КОД – SEC240

КРЕДИТ – 6

ПРЕРЕКВИЗИТ – нет

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.

Защита магистерского проекта
КОД – ECA2013
КРЕДИТ –12

Целью выполнения магистерской диссертации/проекта 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/проект – 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/проект – итог научно-исследовательской /экспериментально-исследовательской работы магистранта, проводившейся в течение всего периода обучения магистранта.

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

– в работе должны проводиться исследования или решаться актуальные проблемы в области информационной безопасности;

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

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

– диссертационная работа/проект должна быть написана единолично;

Содержание