Министерство науки и высшего образования Республики Казахстан
НАО «Кызылординский университет имени Коркыт Ата»

УТВЕРЖДАЮ
Председатель комитета
академического качества
Абжалилов Б.Б.
«1» 29.08 2024 г.

МОДЕЛЬ ВЫПУСКНИКА

Бакалавр по образовательной программе

6В06352 – «Системы информационной безопасности»

г. Кызылорда, 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Модель выпускника КУ им. Коркыт Ата представляет собой комплексный образ результата обучения в университете по всем уровням образования. Модель выпускника рекомендуется для использования при разработке образовательных программ.

Разработка компетентностной модели выпускника является важным условием для реализации основных направлений Болонского процесса и требованием современного рынка труда. Компетентностная модель выпускника (бакалавра) призвана отвечать на вопрос о том, какие профессиональные задачи должен уметь решать специалист определенного ранга (должности), того или иного профиля. Формирование современной модели выпускника вуза, отвечающей запросам всех заинтересованных лиц, является главной стратегической целью КУ имени Коркыт Ата и обеспечивается необходимыми ресурсами для образовательного процесса, включающее кадровое, учебно-методическое, информационное и материально-техническое обеспечение. Университет ведет целенаправленную кадровую политику и планомерное улучшение материально-технической базы университета для обеспечения качества подготовки выпускника - бакалавра, востребованного на рынке труда.

1. ОПИСАНИЕ ОП

Образовательная программа предусматривает подготовку специалистов, занимающихся обеспечением безопасности систем и сетевых технологий. В частности, обучается в области методов и средств криптографической защиты информации, компьютерных технологий защиты информации, разработки и проектирования средств криптографической защиты информации, различных методов и средств технической защиты информации, организации и управления службами информационной безопасности, Организации вычислительных систем и сетей, администрирования, обеспечения безопасности облачных технологий.

2. СОСТАВНЫЕ КОМПОНЕНТЫ ПРИ ФОРМИРОВАНИИ МОДЕЛИ ВЫПУСКНИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Ключевые компоненты формирования Модели выпускника образовательной программы включают информацию о целях и задачах образовательной программы, объектах, видах и направлениях профессиональной деятельности, компетентностную модель специалиста (Приложение1), включая дескрипторы, разновидность компетенций в соответствии с образовательной программой, результаты образовательной программы.

2.1 Цели Образовательной программы:

Подготовка высококвалифицированных кадров в области информационной безопасности, способных защищать информацию на объектах информатизации, применять знания и личные навыки и качества в обеспечении информационной безопасности. Обучение обучающихся общеобразовательным, базовым и профильным дисциплинам, ориентированным в области криптографической, технической защиты информации с целью защиты и обеспечения безопасности информации в различных интегрированных компьютерных системах и сетях

2.2 Задачи Образовательной программы:

- подготовка для рынка труда нового поколения технических специалистов в области информационной безопасности, обладающих конкурентоспособными, высокопрофессиональными компетенциями;
- интеграция образовательной и научной деятельности;
- партнерство с ведущими вузами ближнего и дальнего зарубежья в целях улучшения качества образования для поддержки технических и культурных связей;
- формирование практики защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак;
- обеспечение защиты информации и вычислительной техники на основе сетевых стандартов и протоколов;
- проведение мониторинга и анализа эффективности программного оборудования защиты информации в операционных системах и сетях;
- контроль правильности работы программно-аппаратных средств защиты и администрирования системы;
- выявление угроз, уязвимостей и рисков в области безопасности Интернета вещей;
- разработка, проектирование и поддержка средств сетевой безопасности организации;
- оценка уровня безопасности компьютерных систем и сетей организации.

2.3 Общие и профессиональные компетенции

Общие:

- Владеть необходимыми знаниями в области информационной безопасности и понимать возможность их применения в прикладных областях.
- Знать принципов обработки, анализа и представления данных и умение применять их в различных областях.
- Способность быть компетентным в выборе методов ИКТ и математического моделирования для решения конкретных инженерных задач, способность быть готовым к определению естественнонаучной сущности проблем, возникающих в процессе профессиональной деятельности, и умение использовать для ее решения соответствующий математический аппарат.

Профессиональные:

- Понимание архитектуры информационных систем
- Способность применения теоретических и прикладных теорий и методов
- Управление и использование стандартов информационной безопасности на предприятии
- Способность решать профессиональные задачи на основе математических методов и моделей для управления ИТ-инновациями, компьютерными технологиями в области информационной безопасности
- Умение разрабатывать план и программу организации работ по защите информации
- Способность применять математическую теорию и методы для построения качественных и количественных моделей объектов и процессов в естественно-научной сфере
- Способность выбирать и применять соответствующее оборудование, средства и методы исследования для решения задач в области информационной безопасности, умение настраивать и налаживать программно-аппаратные комплексы в контексте безопасности.

2.1 Матрица соотнесения результатов обучения образовательной программы с формируемыми компетенциями

Құзыреттілік	ON1	ON 2	ON 3	ON 4	ON 5	ON 6	ON 7	ON 8
ЖБК1/ОК1/G1	+							
ЖБК2/ОК2/G2	+							
ЖБК3/ОК3/G3	+							
ЖБК4/ОК4/G4	+							
ЖБК5/ОК5/G5		+	+					
ЖБК6/ОК6/G6	+							
ЖБК7/ОК7/G7	+							
ЖБК8/ОК8/G8	+							
АҚ1/СК1/SC1	+	+						
АҚ2/СК2/SC2	+	+						
АҚ3/СК3/SC3			+		+			
АҚ4/СК4/SC4		+						
АҚ5/СК5/SC5			+		+			
АҚ6/СК6/SC6			+					
АҚ7/СК7/SC7	+							
АҚ8/СК8/SC8		+		+				
АҚ9/СК9/SC9			+					
АҚ10/СК10/SC10				+				
АҚ11/СК11/SC11			+					
АҚ12/СК12/SC12	+	+						
АҚ13/СК13/SC13			+					
АҚ14/СК14/SC14				+				
АҚ15/СК15/SC15		+						
АҚ16/СК16/SC16			+					
АҚ17/СК17/SC17				+				
АҚ18/СК18/SC18 Minor					+			
АҚ19/СК19/SC19 Minor			+	+				
АҚ20/СК20/SC20				+		+	+	
АҚ21/СК21/SC21								+
АҚ22/СК22/SC22	+							
БҚ1/ ПК1/ РС1				+				
БҚ2/ ПК2/ РС2			+					
БҚ3/ ПК3/ РС3							+	+
БҚ4/ ПК4/ РС4				+				
БҚ5/ ПК5/ РС5						+		+
БҚ6/ ПК6/ РС6					+			+
БҚ7/ ПК7/ РС7							+	+
БҚ8/ ПК8/ РС8	+							
БҚ9/ ПК9/ РС9 Minor			+					+

RO1	Демонстрировать способности и готовности применять знания в естественно-научной, гуманитарной, социально-экономической, предпринимательской сферах. Знание базовых требований международных и национальных законодательных, организационных и процедурных актов, регулирующих деятельность в области информационной безопасности
RO2	Применять теоретические и практические знания в области естественных наук и математики для решения профессиональных задач и моделирования процессов области информационной безопасности. Знать принципов теории электрических цепей и цифровой обработки сигналов
RO3	Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов
RO4	Демонстрировать знания в области теории информации и кодирования и криптологии, знание математических принципов работы алгоритмов криптографии и других методов сокрытия информации. Умение выбора и применения программных и технических средств обеспечения информационной безопасности
RO5	Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
RO6	Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и обнаружении компьютерных инцидентов
RO7	Применять теоретические знания и практические навыки для функционирования систем мониторинга уязвимостей, систем управления событиями ИБ и систем предотвращения утечек информации
RO8	Применять знания в области проектирования и безопасной разработки программного обеспечения для верификации, статического анализа и выявления уязвимостей программного кода. Применять знания принципов безопасного использования и защиты облачных технологий, демонстрация знаний и навыков в области безопасности больших данных

2.4 Личные качества специалиста по информационной безопасности

- Аналитические навыки: проведение системный анализ информации; систематизация информации; сравнение данных; абстрагирование информации; проектирование результата.
- Диагностические навыки: умение структурировать полученную информацию; осуществлять инновационные и комбинационные процессы, связанные со способностью к прогнозированию; определять стратегические, тактические и оперативные цели; формулировать и решать профессиональные задачи; использовать положительный опыт; принимать управленческие решения; диагностировать возможные варианты решений.

- Вербальные и невербальные навыки: налаживание деловых отношений с коллегами; сотрудничество с партнерами; формулирование профессиональных задач; овладение устной и письменной речью; решение нестандартных задач с помощью методов и средств; определение значимости в экстремальных ситуациях.
- Навыки прогнозирования: уверенность в своих действиях в соответствии с оценкой всего происходящего; целеустремленность, управление, информационное моделирование, мобилизация энергии, настойчивость, активность, умение нести нагрузку, как условие настойчивости при выполнении сложных задач.
- Коррекционные навыки: самоанализ, самокоррекция; определение траекторий саморазвития и самообразования; понимание своих профессиональных и личностных возможностей.

Виды профессиональной деятельности бакалавра в области информационно–коммуникационных технологий по образовательной программе 6В06352-«Системы информационной безопасности»:

- Аудитор информационной безопасности
- Инженер по защите информации
- Администратор информационной безопасности
- Системный администратор
- Специалист службы информационной безопасности
- Аналитик баз данных
- Научный сотрудник
- Руководители служб и подразделений в сфере информационно-коммуникационных технологий и информационной безопасности.

ВЫВОДЫ

В рыночных условиях вузы начинают уделять больше внимания качеству выпускников: выпускник – это результат университетского образования, поступающего на рынок труда. И он должен быть конкурентоспособным. Для подготовки востребованных на рынке выпускников необходимо сформировать его комплексный портрет, определенную матрицу характеристик. Формирование образовательных программ с пониманием основных преимуществ, характеристик, компетенций выпускников, необходимых работодателям, создание инфраструктуры, переход к созданию эффективного современного университета, основанного на использовании новых форматов обучения.

ПРИЛОЖЕНИЕ 1

Компетентностная модель выпускника

Модуль	ДДБ (Дублинские дескрипторы бакалавриата)	Формируемые компетенции			Планируемые результаты обучения
		общеобразовательные компетенции	базовые компетенции	профилирующие компетенции	
1	2	3	4	5	6
М1	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5	ОК 1, ОК 2, ОК3, ОК 4, ОК 5			РО1 Демонстрировать способности и готовности применять знания в естественно-научной, гуманитарной, социально-экономической, предпринимательской сферах. Знание базовых требований международных и национальных законодательных, организационных и процедурных актов, регулирующих деятельность в области информационной безопасности.
М1	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5	ОК 6			РО2 Применять теоретические и практические знания в области естественных наук и математики для решения профессиональных задач и моделирования процессов области информационной безопасности. Знать принципов теории электрических цепей и цифровой обработки сигналов РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5	ОК7, ОК 8			РО1 Демонстрировать способности и готовности применять знания в естественно-научной, гуманитарной, социально-экономической, предпринимательской сферах. Знание базовых требований международных и национальных законодательных, организационных и процедурных актов, регулирующих деятельность в области информационной безопасности.
М3	ДДБ1 ДДБ2		СК1, СК2,		РО1 Демонстрировать способности и готовности применять знания в естественно-научной, гуманитарной, социально-

	ДДБ3 ДДБ4 ДДБ5		СК4, СК10		экономической, предпринимательской сферах. Знание базовых требований международных и национальных законодательных, организационных и процедурных актов, регулирующих деятельность в области информационной безопасности. РО2 Применять теоретические и практические знания в области естественных наук и математики для решения профессиональных задач и моделирования процессов области информационной безопасности. Знать принципов теории электрических цепей и цифровой обработки сигналов
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК3, СК7		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов. РО4 Демонстрировать знания в области теории информации и кодирования и криптологии, знание математических принципов работы алгоритмов криптографии и других методов сокрытия информации. Умение выбора и применения программных и технических средств обеспечения информационной безопасности РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
М2	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК5		РО1 Демонстрировать способности и готовности применять знания в естественно-научной, гуманитарной, социально-экономической, предпринимательской сферах. Знание базовых требований международных и национальных законодательных, организационных и процедурных актов, регулирующих деятельность в области информационной безопасности. РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК6		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов.
М3	ДДБ1 ДДБ2 ДДБ3 ДДБ4		СК8 СК12		РО2 Применять теоретические и практические знания в области естественных наук и математики для решения профессиональных задач и моделирования процессов области информационной безопасности. Знать принципов теории электрических цепей и цифровой обработки сигналов

	ДДБ5				
М5	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК9		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов. РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
М4	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК11 СК13		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов.
М5	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК14		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов. РО4 Демонстрировать знания в области теории информации и кодирования и криптологии, знание математических принципов работы алгоритмов криптографии и других методов сокрытия информации. Умение выбора и применения программных и технических средств обеспечения информационной безопасности РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
М4	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК15 СК17		РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
	ДДБ1 ДДБ2 ДДБ3		СК16 СК18		РО2 Применять теоретические и практические знания в области естественных наук и математики для решения профессиональных задач и моделирования процессов области информационной безопасности. Знать принципов теории электрических цепей и

	ДДБ4 ДДБ5				цифровой обработки сигналов
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК19		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов. РО4 Демонстрировать знания в области теории информации и кодирования и криптологии, знание математических принципов работы алгоритмов криптографии и других методов сокрытия информации. Умение выбора и применения программных и технических средств обеспечения информационной безопасности РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
М6	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК20		РО1 Демонстрировать способности и готовности применять знания в естественно-научной, гуманитарной, социально-экономической, предпринимательской сферах. Знание базовых требований международных и национальных законодательных, организационных и процедурных актов, регулирующих деятельность в области информационной безопасности.. РО8 Применять знания в области проектирования и безопасной разработки программного обеспечения для верификации, статического анализа и выявления уязвимостей программного кода. Применять знания принципов безопасного использования и защиты облачных технологий, демонстрация знаний и навыков в области безопасности больших данных
М5	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК21		РО2 Применять теоретические и практические знания в области естественных наук и математики для решения профессиональных задач и моделирования процессов области информационной безопасности. Знать принципов теории электрических цепей и цифровой обработки сигналов РО8 Применять знания в области проектирования и безопасной разработки программного обеспечения для верификации, статического анализа и выявления уязвимостей программного кода. Применять знания принципов безопасного использования и защиты облачных технологий, демонстрация знаний и навыков в области безопасности больших данных
М6	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК22		РО1 Демонстрировать способности и готовности применять знания в естественно-научной, гуманитарной, социально-экономической, предпринимательской сферах. Знание базовых требований международных и национальных законодательных, организационных и процедурных актов, регулирующих деятельность в области информационной безопасности.

М5	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК23		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов. РО4 Демонстрировать знания в области теории информации и кодирования и криптологии, знание математических принципов работы алгоритмов криптографии и других методов сокрытия информации. Умение выбора и применения программных и технических средств обеспечения информационной безопасности РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК24		РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта. РО6 Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и обнаружении компьютерных инцидентов
М3	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК25		РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
М5	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5		СК26		РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов. РО6 Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и обнаружении компьютерных инцидентов
М6	ДДБ1 ДДБ2 ДДБ3		СК27		РО6 Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и обнаружении компьютерных инцидентов

	ДДБ4 ДДБ5				
М4	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 1	РО6 Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и обнаружении компьютерных инцидентов
М5	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК2	РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов.
М6	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 3 ПК11	РО7 Применять теоретические знания и практические навыки для функционирования систем мониторинга уязвимостей, систем управления событиями ИБ и систем предотвращения утечек информации РО8 Применять знания в области проектирования и безопасной разработки программного обеспечения для верификации, статического анализа и выявления уязвимостей программного кода. Применять знания принципов безопасного использования и защиты облачных технологий, демонстрация знаний и навыков в области безопасности больших данных
М5	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 4	РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта. РО7 Применять теоретические знания и практические навыки для функционирования систем мониторинга уязвимостей, систем управления событиями ИБ и систем предотвращения утечек информации РО8 Применять знания в области проектирования и безопасной разработки программного обеспечения для верификации, статического анализа и выявления уязвимостей программного кода. Применять знания принципов безопасного использования и защиты облачных технологий, демонстрация знаний и навыков в области безопасности больших данных
М6	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 5	РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов.
М7	ДДБ1 ДДБ2			ПК 6	РО6 Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и

	ДДБ3 ДДБ4 ДДБ5				обнаружении компьютерных инцидентов РО8 Применять знания в области проектирования и безопасной разработки программного обеспечения для верификации, статического анализа и выявления уязвимостей программного кода. Применять знания принципов безопасного использования и защиты облачных технологий, демонстрация знаний и навыков в области безопасности больших данных
М6	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 7	РО3 Демонстрировать знания об архитектуре операционных систем, компьютерных систем и сетей и их администрировании и обеспечении безопасности, настройке политики безопасности СУБД, технологиях и методах программирования для защиты информации и информационных процессов. РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта.
М6	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 8	РО6 Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и обнаружении компьютерных инцидентов РО7 Применять теоретические знания и практические навыки для функционирования систем мониторинга уязвимостей, систем управления событиями ИБ и систем предотвращения утечек информации
М7	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 9	РО4 Демонстрировать знания в области теории информации и кодирования и криптологии, знание математических принципов работы алгоритмов криптографии и других методов сокрытия информации. Умение выбора и применения программных и технических средств обеспечения информационной безопасности
М7	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК10	РО4 Демонстрировать знания в области теории информации и кодирования и криптологии, знание математических принципов работы алгоритмов криптографии и других методов сокрытия информации. Умение выбора и применения программных и технических средств обеспечения информационной безопасности РО5 Применяет принципы построения и виды архитектуры систем искусственного интеллекта. Взаимодействует с подразделениями организации в рамках процесса проектирования приложений, структуры базы данных, программных интерфейсов. Знает основные инструментальные средства искусственного интеллекта, а также методы и средства проверки работоспособности систем искусственного интеллекта. РО6 Применять знания, понимания фактов и зависимостей при обнаружении вредоносных программ, практическом пентестинге и обнаружении компьютерных инцидентов