Министерство науки и высшего образования Республики Казахстан

НАО «Кызылординский университет имени Коркыт Ата»

«УТВЕРЖДАЮ»
Председатель комитета
Академического качества
_____ Абжалелов Б.Б.
«_28_» _9_ _08_ 2026г.

Модель выпускника

по образовательной программе 7М06303- «Кибербезопасность» (магистратура)

Кызылорда, 2026г.

СОДЕРЖАНИЕ

Введение

1 Описание ОП

2 Составные компоненты при формировании модели выпускника образовательной программы

2.1 Цели Образовательной программы

2.2 Задачи Образовательной программы

2.3 Общие и профессиональные компетенции

2.4 Матрица соотнесения результатов обучения образовательной программы с формируемыми компетенциями

2.5 Личные качества специалиста по информационной безопасности

Выводы

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.

2.4 Матрица соотнесения результатов обучения образовательной программы с формируемыми компетенциями

Құзыреттілік	ON1	ON2	ON3	ON4	ON5	ON6	ON7	ON8	ON9	0N10
ЖҚ1/ОК1/GC1	+									
ЖҚ2/ОК2/GC2	+									
ЖҚ3/ОК3/GC3	+									
ЖҚ4/ОК4/GC4	+									
КҚ1/ПК1/РС1			+							
КҚ2/ПК2/РС2		+								
КҚ3/ПК3/РС3										+
КҚ4/ ПК4/РС4					+					
КҚ5/ ПК5/РС5		+								
КҚ6/ ПК6/РС6						+				
КҚ7/ ПК7/РС7								+		+
КҚ8/ ПК8/РС8						+		+		
КҚ9/ ПК9/РС9										+
КҚ10/ПК10/РС10							+			
КҚ11/ПК11/РС11						+				
КҚ12/ПК12/РС12				+					+	
КҚ13/ПК13/РС13				+						+
КҚ14/ПК14/РС14			+	+						
КҚ15/ПК15/РС15										+

RO1	Знает современные теории истории науки, методологию педагогики высшей школы, достижения психологической науки и профессиональный иностранный язык. Применяет современные достижения науки и образовательные технологии при решении профессиональных задач и в образовательном процессе.
RO2	Анализирует криптографические и стеганографические системы, оценивает криптостойкость алгоритмов защиты информации, применяет современные криптографические методы, включая постквантовые криптографические алгоритмы, и использует результаты анализа в образовательной и научно-исследовательской деятельности.
RO3	Проектирует архитектуру защищённых информационных систем, компьютерных сетей и программных комплексов, осуществляет анализ угроз и обосновывает выбор методов и средств защиты информации для обеспечения конфиденциальности, целостности и доступности данных в научно-исследовательской и образовательной деятельности.
RO4	Проектирует, разрабатывает и сопровождает защищённые клиент-серверные, облачные и распределённые информационные системы, включая масштабируемые и отказоустойчивые облачные архитектуры, применяет технологии контейнеризации, оркестрации, микросервисного взаимодействия и DevSecOps для обеспечения безопасности программных решений в научной и образовательной деятельности.
RO5	Применяет современные методы обеспечения информационной безопасности в среде Интернета вещей (IoT), киберфизических систем и интеллектуальных инфраструктур, использует технологии искусственного интеллекта для выявления угроз, анализа событий безопасности, оценки рисков и повышения устойчивости информационных систем в образовательной и научно-

	исследовательской деятельности.
RO6	Осуществляет мониторинг событий информационной безопасности, выявляет, анализирует и расследует инциденты с применением SIEM-систем, технологий Big Data и методов интеллектуального анализа данных (Data Mining, машинное обучение) для обнаружения аномалий, выявления киберугроз, корреляции событий безопасности и поддержки процессов цифровой криминалистики в образовательной и научно-исследовательской деятельности.
RO7	Осуществляет аудит информационной безопасности, оценивает риски и уровень защищённости информационных систем, планирует и организует аудиторские проверки, применяет международные стандарты и методологии аудита, разрабатывает рекомендации по совершенствованию систем управления информационной безопасностью в научной и образовательной деятельности.
RO8	Проектирует и внедряет механизмы идентификации, аутентификации, авторизации и управления доступом, применяет современные модели контроля доступа и технологии управления цифровой идентичностью для обеспечения защищённости информационных систем в научно-исследовательской и образовательной деятельности.
RO9	Применяет технологии распределённых реестров (блокчейн) для обеспечения целостности, достоверности и доверия при обработке информации, анализирует возможности их использования для повышения защищённости цифровых сервисов и информационных систем в образовательной и научно-исследовательской деятельности.
RO10	Применяет современные методы обнаружения, анализа и противодействия вредоносному программному обеспечению, использует методы статического и динамического анализа кода, технологии искусственного интеллекта, машинного обучения и моделирования для выявления, классификации, оценки и прогнозирования киберугроз в профессиональной, научно-исследовательской и образовательной деятельности.

2.5 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	ОК1			РО1 Знает современные теории истории науки, методологию педагогики высшей школы, достижения психологической науки и профессиональный иностранный язык. Применяет современные достижения науки и образовательные технологии при решении профессиональных задач и в образовательном процессе.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5	ОК2			РО1 Знает современные теории истории науки, методологию педагогики высшей школы, достижения психологической науки и профессиональный иностранный язык. Применяет современные достижения науки и образовательные технологии при решении профессиональных задач и в образовательном процессе.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5	ОК3			РО1 Знает современные теории истории науки, методологию педагогики высшей школы, достижения психологической науки и профессиональный иностранный язык. Применяет современные достижения науки и образовательные технологии при решении профессиональных задач и в образовательном процессе.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5	ОК4			РО1 Знает современные теории истории науки, методологию педагогики высшей школы, достижения психологической науки и профессиональный иностранный язык. Применяет современные достижения науки и образовательные технологии при решении профессиональных задач и в образовательном процессе.

М1	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК 1	РО3 Проектирует архитектуру защищённых информационных систем, компьютерных сетей и программных комплексов, осуществляет анализ угроз и обосновывает выбор методов и средств защиты информации для обеспечения конфиденциальности, целостности и доступности данных в научно-исследовательской и образовательной деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК2	РО2 Анализирует криптографические и стеганографические системы, оценивает криптостойкость алгоритмов защиты информации, применяет современные криптографические методы, включая постквантовые криптографические алгоритмы, и использует результаты анализа в образовательной и научно-исследовательской деятельности.
М2	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК4	РО5 Применяет современные методы обеспечения информационной безопасности в среде Интернета вещей (IoT), киберфизических систем и интеллектуальных инфраструктур, использует технологии искусственного интеллекта для выявления угроз, анализа событий безопасности, оценки рисков и повышения устойчивости информационных систем в образовательной и научно-исследовательской деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК5	РО2 Анализирует криптографические и стеганографические системы, оценивает криптостойкость алгоритмов защиты информации, применяет современные криптографические методы, включая постквантовые криптографические алгоритмы, и использует результаты анализа в образовательной и научно-исследовательской деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК6	РО6 Осуществляет мониторинг событий информационной безопасности, выявляет, анализирует и расследует инциденты с применением SIEM-систем, технологий Big Data и методов интеллектуального анализа данных (Data Mining, машинное обучение) для обнаружения аномалий, выявления киберугроз, корреляции событий безопасности и поддержки процессов цифровой криминалистики в образовательной и научно-исследовательской деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК7	РО8 Проектирует и внедряет механизмы идентификации, аутентификации, авторизации и управления доступом, применяет современные модели контроля доступа и технологии управления цифровой идентичностью для обеспечения защищённости информационных систем в научно-исследовательской и образовательной деятельности. РО10 Применяет современные методы обнаружения, анализа и противодействия вредоносному программному обеспечению, использует методы статического и динамического анализа кода, технологии искусственного интеллекта, машинного обучения и моделирования для выявления, классификации, оценки и прогнозирования киберугроз в профессиональной, научно-исследовательской и образовательной деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4			ПК8	РО6 Осуществляет мониторинг событий информационной безопасности, выявляет, анализирует и расследует инциденты с применением SIEM-систем, технологий Big Data и методов интеллектуального анализа данных (Data Mining, машинное

	ДДБ5				обучение) для обнаружения аномалий, выявления киберугроз, корреляции событий безопасности и поддержки процессов цифровой криминалистики в образовательной и научно-исследовательской деятельности. РПроектирует и внедряет механизмы идентификации, аутентификации, авторизации и управления доступом, применяет современные модели контроля доступа и технологии управления цифровой идентичностью для обеспечения защищённости информационных систем в научно-исследовательской и образовательной деятельности.О8
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК10	РО7 Осуществляет аудит информационной безопасности, оценивает риски и уровень защищённости информационных систем, планирует и организует аудиторские проверки, применяет международные стандарты и методологии аудита, разрабатывает рекомендации по совершенствованию систем управления информационной безопасностью в научной и образовательной деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК11	РО6 Осуществляет мониторинг событий информационной безопасности, выявляет, анализирует и расследует инциденты с применением SIEM-систем, технологий Big Data и методов интеллектуального анализа данных (Data Mining, машинное обучение) для обнаружения аномалий, выявления киберугроз, корреляции событий безопасности и поддержки процессов цифровой криминалистики в образовательной и научно-исследовательской деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК12	РО4 Проектирует, разрабатывает и сопровождает защищённые клиент-серверные, облачные и распределённые информационные системы, включая масштабируемые и отказоустойчивые облачные архитектуры, применяет технологии контейнеризации, оркестрации, микросервисного взаимодействия и DevSecOps для обеспечения безопасности программных решений в научной и образовательной деятельности. РО9 Применяет технологии распределённых реестров (блокчейн) для обеспечения целостности, достоверности и доверия при обработке информации, анализирует возможности их использования для повышения защищённости цифровых сервисов и информационных систем в образовательной и научно-исследовательской деятельности.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК13	РО4 Проектирует, разрабатывает и сопровождает защищённые клиент-серверные, облачные и распределённые информационные системы, включая масштабируемые и отказоустойчивые облачные архитектуры, применяет технологии контейнеризации, оркестрации, микросервисного взаимодействия и DevSecOps для обеспечения безопасности программных решений в научной и образовательной деятельности. РО10 Применяет современные методы обнаружения, анализа и противодействия вредоносному программному обеспечению, использует методы статического и динамического анализа кода, технологии искусственного интеллекта, машинного обучения и моделирования для выявления, классификации, оценки и прогнозирования киберугроз в профессиональной, научно-исследовательской и образовательной деятельности.

	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК14	РО3 Проектирует архитектуру защищённых информационных систем, компьютерных сетей и программных комплексов, осуществляет анализ угроз и обосновывает выбор методов и средств защиты информации для обеспечения конфиденциальности, целостности и доступности данных в научно-исследовательской и образовательной деятельности. РО4 Проектирует, разрабатывает и сопровождает защищённые клиент-серверные, облачные и распределённые информационные системы, включая масштабируемые и отказоустойчивые облачные архитектуры, применяет технологии контейнеризации, оркестрации, микросервисного взаимодействия и DevSecOps для обеспечения безопасности программных решений в научной и образовательной деятельности.
М3	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК3	RO10 Знает современные методы и технологии обеспечения информационной безопасности, принципы защиты информационных систем и компьютерных сетей. Владеет методами анализа киберугроз, оценки рисков и выявления уязвимостей. Применяет современные технологии киберзащиты и результаты научных исследований для решения профессиональных задач.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК9	RO10 Знает современные методы научных исследований в области информационной безопасности, принципы выявления кибератак и оценки защищённости информационных систем. Владеет методами экспериментального исследования, анализа сетевого трафика и обработки данных. Применяет алгоритмы машинного обучения, нейронные сети и современные средства киберзащиты для обнаружения угроз, прогнозирования атак и повышения безопасности информационных систем.
	ДДБ1 ДДБ2 ДДБ3 ДДБ4 ДДБ5			ПК15	RO10 Знает современные методы и технологии защиты информации, принципы функционирования защищённых компьютерных систем и сетей, методы оценки их надёжности и безопасности. Владеет навыками проведения научных экспериментов, анализа уязвимостей и исследования сетевых угроз. Применяет методы искусственного интеллекта, машинного обучения и анализа данных для выявления кибератак, обнаружения аномалий и разработки эффективных механизмов защиты информации.

М1 - Научные знания
М2 - Наука (по отраслям) и инновации
М3 - Итоговая аттестация