ПРИЛОЖЕНИЕ А
ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО ДИСЦИПЛИНЕ «Криптографические методы защиты информации»

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код контролируемой компетенции	Способ оценивания	Оценочное средство
ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач	Экзамен	Комплект контролирующих материалов для экзамена
ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Экзамен	Комплект контролирующих материалов для экзамена
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Экзамен	Комплект контролирующих материалов для экзамена

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Показатели оценивания компетенций представлены в разделе «Требования к результатам освоения дисциплины» рабочей программы дисциплины «Криптографические методы защиты информации» с декомпозицией: знать, уметь, владеть.

При оценивании сформированности компетенций по дисциплине «Криптографические методы защиты информации» используется 100-балльная шкала.

Критерий	Оценка по 100-балльной шкале	Оценка по традиционной шкале
Студент твёрдо знает программный материал, системно и грамотно излагает его, демонстрирует необходимый уровень компетенций, чёткие, сжатые ответы на дополнительные вопросы, свободно владеет понятийным аппаратом.	75-100	*Отлично*
Студент проявил полное знание программного материала, демонстрирует сформированные на достаточном уровне умения и навыки, указанные в программе компетенции, допускает непринципиальные неточности при изложении ответа на вопросы.	50-74	*Хорошо*

Студент обнаруживает знания только основного материала, но не усвоил детали, допускает ошибки, демонстрирует не до конца сформированные компетенции, умения систематизировать материал и делать выводы.	25-49	*Удовлетворительно*
Студент не усвоил основное содержание материала, не умеет систематизировать информацию, делать необходимые выводы, чётко и грамотно отвечать на заданные вопросы, демонстрирует низкий уровень овладения необходимыми компетенциями.	<25	*Неудовлетворительно*

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности.

№ пп	Вопрос/Задача	Проверяемые компетенции
1	Определение основных понятий: "криптография", "стеганография", "шифрование", "ключ", "режим шифрования", "криптосистема", "шифртехника", "криптостойкость", "криптоанализ", "аутентификация", "цифровая подпись".	ОПК-4
2	Обзор традиционных криптосистем. Атаки на традиционные криптосистемы. Становление и развитие криптографии. Цели криптографии. Обзор применения информационных технологии для криптографической обработки информации.	ОПК-4
3	Современные симметричные шифры. Обзор и основные правила построения. Режимы использования шифров. Атаки на симметричные шифры.	ОПК-4
4	Потоковые шифры. Шифрование методом гаммирования. Регистры сдвига с линейной обратной связью. Методы генерации псевдослучайных последовательностей чисел.	ОПК-2, ОПК-4
5	Элементы теории чисел. Однонаправленные функции. Построение больших простых чисел. Тесты проверки на простоту. Хеш-функции. Программная реализация методов генерации псевдослучайных последовательностей чисел, методов построения больших простых чисел, хеш-функций.	ОПК-2
6	Концепция криптосистемы с открытым ключом. Решаемые задачи. Требования к алгоритмам. Система распределения ключей Диффи-Хеллмана. Шифры Шамира, Эль-Гамаля, RSA. Гибридные криптосистемы. Электронная подпись. Применение соответствующего математического аппарата для решения профессиональных задач с использованием	ОПК-2, ОПК-4

№ пп	Вопрос/Задача	Проверяемые компетенции
	ассиметричной криптографии.	
7	Криптографические протоколы. Виды криптографических протоколов. Основные определения. Методы аутентификации информации. Управление ключами.	ОПК-2, ОПК-4
8	Программная реализация симметричного шифра ГОСТ 28147-89, системы распределения ключей Диффи-Хеллмана, шифра Эль-Гамаля, алгоритма RSA, криптографических протоколов (по заданию).	ОПК-2, ОПК-4
9	Работа с популярными средствами криптографической защиты информации. Выполнение работ по установке, настройке и обслуживанию программных криптографических средств защиты информации: КриптоПро CSP, КриптоАРМ, ViPNet. Функционал систем. Приобретение практических навыков шифрования данных и подписания информации.	ПК-1

4. Файл и/или БТЗ с полным комплектом оценочных материалов прилагается.