ПРИЛОЖЕНИЕ А
ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО ДИСЦИПЛИНЕ «Основы управления информационной безопасностью»

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

Код контролируемой компетенции	Способ оценивания	Оценочное средство
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-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Экзамен	Комплект контролирующих материалов для экзамена
ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	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 «Основы управления информационной безопасностью» с декомпозицией: знать, уметь, владеть.

При оценивании сформированности компетенций по дисциплине «Основы управления информационной безопасностью» 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	Назначение, структура и содержание управления информационной безопасностью. Современные модели управления информационной безопасностью предприятия.	ОПК-4, ПК-13, ПК-14
2	Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности. Методология управления рисками в области информационной безопасности. Менеджмент инцидентов информационной безопасности в организации. Структура, задачи и функции подразделений обеспечивающих информационную безопасность предприятия. В том числе принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации). А также основные понятия и методы в области управленческой деятельности; содержание управленческой работы руководителя подразделения.	ПК-13, ПК-14
3	Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государства. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ	ОПК-4, ПК-13, ПК-14
4	Практическое задание. Кейс 1. Описание ситуации В одной из компаний был зафиксирован следующий инцидент: при увольнении с работы системный администратор украл разрабатываемый в компании	ПК-13, ПК-14

№ пп	Вопрос/Задача	Проверяемые компетенции
	программный продукт и передал его конкурентам, которые выпустили программу на рынок под своим товарным знаком. Кроме этого, он внес изменения в информационную систему, в результате которых после его ухода функционирование определенных ее компонентов было нарушено. Привлечь администратора к ответственности в данном случае оказалось невозможно, так как, во-первых, не выполнялась регистрация его действий, во-вторых, администратор мог удалить все доказательства своих неправомерных действий и, в-третьих, не была налажена процедура сбора улик об инциденте. Задание. 1. Определите возможные причины инцидента и степень ответственности сотрудника. 2. Определите меры, направленные на предотвращение повторных инцидентов. 3. Какие документы должны быть подготовлены?	

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