ПРИЛОЖЕНИЕ А
ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ «Особенности защиты информации объектов критической информационной инфраструктуры»

1. Перечень оценочных средств для компетенций, формируемых в результате освоения дисциплины

Код контролируемой компетенции	Способ оценивания	Оценочное средство
ПК-4: Способен участвовать в исследованиях защищенности объектов и средств защиты	Экзамен	Комплект контролирующих материалов для экзамена

2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Оцениваемые компетенции представлены в разделе «Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций» рабочей программы дисциплины «Особенности защиты информации объектов критической информационной инфраструктуры».

При оценивании сформированности компетенций по дисциплине «Особенности защиты информации объектов критической информационной инфраструктуры» используется 100-балльная шкала.

Критерий	Оценка по 100-балльной шкале	Оценка по традиционной шкале
Студент освоил изучаемый материал (основной и дополнительный), системно и грамотно излагает его, осуществляет полное и правильное выполнение заданий в соответствии с индикаторами достижения компетенций, способен ответить на дополнительные вопросы.	75-100	*Отлично*
Студент освоил изучаемый материал, осуществляет выполнение заданий в соответствии с индикаторами достижения компетенций с непринципиальными ошибками.	50-74	*Хорошо*
Студент демонстрирует освоение только основного материала, при выполнении заданий в соответствии с индикаторами достижения компетенций допускает отдельные ошибки, не способен систематизировать материал и делать выводы.	25-49	*Удовлетворительно*
Студент не освоил основное содержание изучаемого материала, задания в соответствии с	<25	*Неудовлетворительно*

индикаторами достижения компетенций не выполнены или выполнены неверно.		

3. Типовые контрольные задания или иные материалы, необходимые для оценки уровня достижения компетенций в соответствии с индикаторами

1.Пример заданий на обеспечение безопасности объекта КИИ

Компетенция	Индикатор достижения компетенции
ПК-4 Способен участвовать в исследованиях защищенности объектов и средств защиты	ПК-4.1 Демонстрирует знание методов исследования защищенности объектов и средств защиты
	ПК-4.2 Предлагает методы исследования объектов информатизации с учетом их особенностей

Задания на обеспечение безопасности объекта КИИ.

Для обеспечения безопасности типового объекта критической информационной инфраструктуры ИС или ИТКС или АСУ, согласно предлагаемого варианта, выберите необходимые методы исследования защищенности объекта информатизации и средств защиты, и представьте решение задачи профессиональной деятельности для задания представленного ниже:

1. Осуществите сбор и проведите анализ нормативно-методической базы объектов КИИ организации для обеспечения их безопасности. Определите и сформируйте необходимый состав нормативно-методической документации защищаемого объекта КИИ организации.
2. Проведите ревизию систем (ИС, ИТКС, АСУ), имеющихся в организации. Оцените задействованность ИС, ИТКС, АСУ в бизнес-процессах. Составьте Реестр бизнес-процессов. Оцените критичность бизнес-процессов. Сформируйте Перечень потенциально значимых объектов КИИ.
3. Определите состав процессов, осуществляемых при категорировании объектов КИИ организации. Определите бизнес-процессы организации. Определите и сформулируйте Перечень объектов КИИ организации. Сформируйте Реестр бизнес-процессов организации. Оформите сведения о результатах категорирования.
4. Определите сценарий реализации компьютерных атак на объекты КИИ и сформируйте состава возможных событий (инцидентов), которые могут возникнуть в результате реализации наихудшего сценария целенаправленных компьютерных атак на ИС, ИТКС, АСУ
5. Проведите расчет показателей критериев значимости объектов КИИ. Определите порядок подготовки заключения о присвоении объекту КИИ организации одной из категорий значимости. Оформите Акт категорирования объекта КИИ и при необходимости пересмотрите категории значимости объектов КИИ.
6. Обеспечьте безопасность предложенных Вам значимых объектов КИИ. Обеспечьте создание системы безопасности значимых объектов КИИ. Выполните мероприятия по организации взаимодействия с центрами ГосСОПКА.
7. Проведите тестирование системы безопасности объектов КИИ организации на отказоустойчивость и реагирование на компьютерные инциденты. Оцените реагирование системы безопасности субъекта КИИ на сценарий проведения компьютерных атак.

Примечание: Конкретная организация и её специфика приведены в билетах.

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