Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:54
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42ba...

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса»
(ФГБОУ ВО «ПВГУС»)

УТВЕРЖДЕНО

на заседании Высшей школы интеллектуальных систем и кибертехнологий

Протокол от 10.11.2023 № 3

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств)
для проведения промежуточной аттестации по дисциплине

Б1.В.ДВ.05.1 «Управление рисками информационной безопасности»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриат**

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»
наименование образовательной программы

10.03.01 «Информационная безопасность»
шифр, наименование направления подготовки / специальности

Составители Коновалова Анжелика Денисовна, старший преподаватель, Высшая школа интеллектуальных систем и кибертехнологий
ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2023

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
ПК-7	Способен организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации	ИПК-7.1. Принимает участие в организации, поддержании в актуальном состоянии процесса защиты информации автоматизированных систем и совершенствовании системы управления защиты информации автоматизированных систем ИПК-7.2. Организует работу (содержание и порядок) деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации. ИПК-7.3. Осуществляет управление процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации по защите информации ИПК-7.4. Осуществляет разработку, внедрение и контроль реализации правил и процедур управления системой защиты информации, работы с угрозами, инцидентами, автоматизированными системами и системами защиты информации

В результате изучения дисциплины обучающийся должен:

владеть: навыками ведения реестра активов и рисков, построения сценариев угроз и модели нарушителя, документирования экспертных оценок и расчетов ожидаемых потерь; подготовки матрицы ответственности, плана обработки, обоснования принятия остаточного риска, показателей контроля и отчета для владельца процесса защиты информации

уметь: определять границы и критерии оценки, выявлять сценарии нарушения безопасности и оценивать ущерб; выбирать и применять методику анализа рисков, обосновывать вероятность и последствия; сопоставлять варианты обработки, распределять задачи персонала, разрабатывать план и процедуры управления рисками с учетом применимых требований; проверять остаточный риск и основания пересмотра

знать: понятия и этапы управления рисками информационной безопасности, способы установления контекста, идентификации активов, угроз, уязвимостей и последствий; качественные и количественные методы оценки, ограничения исходных данных; порядок распределения ответственности, обработки и принятия риска, документирования и пересмотра решений

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1	Основы управления рисками и установление контекста	ПК-7
2	Информационные активы и анализ последствий	ПК-7
3	Идентификация угроз, уязвимостей и сценариев риска	ПК-7
4	Качественная оценка и ранжирование рисков	ПК-7
5	Количественная оценка и анализ неопределенности	ПК-7
6	Выбор мер и планирование обработки рисков	ПК-7
7	Экономическое обоснование и документирование решений	ПК-7
8	Контроль, коммуникация и пересмотр рисков	ПК-7

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – экзамен.

Уровень сформированности	100-балльная шкала, %	Шкала освоения, %	5-балльная дифференцированная оценка/балл
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2
пороговый	61–85,9	61–69,9	«удовлетворительно» / 3
пороговый	61–85,9	70–85,9	«хорошо» / 4
повышенный	86–100	86–100	«отлично» / 5

2. Перечень оценочных материалов для проведения промежуточной аттестации

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

Перечень вопросов и заданий для подготовки к экзамену

ПК-7. Способен организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации

1. Понятие риска информационной безопасности и его отличие от угрозы, уязвимости и инцидента.
2. Этапы управления рисками и их связь с процессом защиты информации автоматизированной системы.
3. Установление контекста: цели, границы, временной горизонт и заинтересованные стороны.
4. Назначение ГОСТ Р ИСО 31000-2019, ГОСТ Р 58771-2019 и ISO/IEC 27005:2022.
5. Критерии последствий, вероятности и принятия риска. Порядок их согласования.
6. Начальная, текущая и остаточная оценка: как отражаются существующие и планируемые меры?
7. Информационные активы, их владельцы и связь с процессами организации.
8. Состав реестра активов и проверка полноты инвентаризации.
9. Анализ зависимостей и общих точек отказа информационной системы.
10. Оценка последствий нарушения конфиденциальности, целостности и доступности.

11. Расчет прямого ущерба от простоя и восстановления; исключение двойного учета.
12. Сбор сведений у владельцев процессов и учет неденежных последствий.
13. Структура сценария риска и требования к его формулировке.
14. Модель нарушителя: возможности, доступ, ресурсы и ограничения.
15. Использование банка данных угроз и обследования при идентификации риска.
16. Техническая тяжесть уязвимости и риск для конкретного процесса: различие оценок.
17. Существующие защитные меры и доказательства их работоспособности.
18. Объединение дублирующих сценариев и документирование общих причин.
19. Выбор качественного метода оценки при ограниченных исходных данных.
20. Шкалы вероятности и последствий: признаки категорий и временной горизонт.
21. Матрица риска, правила ранжирования и ограничения произведения порядковых баллов.
22. Организация экспертного оценивания и разрешение расхождений.
23. Ранжирование рисков с одинаковым баллом и различными последствиями.
24. Анализ чувствительности качественной оценки и учет неопределенности.
25. Вероятность одного события и частота повторяющихся событий: различие и единицы.
26. Модели ожидаемых потерь для единичного и повторяющегося события.
27. Источники количественных параметров и проверка сопоставимости статистики.
28. Сценарный анализ и расчет чувствительности к частоте и величине потерь.
29. Зависимость событий, пересечение ущерба и ограничения агрегирования рисков.
30. Проверка расчетной таблицы, граничные значения и документирование допущений.
31. Варианты обработки риска и ограничения его переноса третьей стороне.
32. Подбор превентивных, обнаруживающих и восстанавливающих мер по сценарию.
33. Состав плана обработки риска и распределение ответственности персонала.
34. Проверка внедрения и эффективности мер: критерии приемки и свидетельства.
35. Прогнозный и подтвержденный остаточный риск. Порядок принятия решения.
36. Обязательные требования, компенсирующие меры и эскалация отклонений.
37. Состав затрат на защиту и сопоставимый временной горизонт вариантов.
38. Ожидаемое снижение потерь и чистый расчетный эффект защитной меры.
39. Выбор решения при бюджетном ограничении и заданном критерии принятия.
40. Совместимость мер, пересечение эффектов и недопустимость двойного учета.
41. Анализ устойчивости экономического обоснования и неденежные критерии.
42. Документирование решения руководства: расчетное приложение и протокол.
43. Плановый и событийный пересмотр рисков: основания и порядок действий.
44. Показатели факторов риска, выполнения мероприятий и эффективности защиты.
45. Регламент контроля: источники, периодичность, пороги и ответственность.
46. Пересмотр оценки после инцидента, отказа меры или изменения поставщика.
47. Коммуникация рисков, эскалация превышений и отчет руководству.
48. Проверка согласованности реестра рисков, плана обработки и решений о принятии.