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:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

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 г. № 3

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

Б.1.В.03.05 «Методы оценки надежности систем защиты информации»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриата**
«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 Мунирова Юлия Сергеевна, старший преподаватель, Высшая школа интеллектуальных систем и кибертехнологий
Курцев Евгений Александрович, ассистент, 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
ОПК-2.1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ИОПК-2.1.2. Выявляет потенциальные угрозы объекта защиты, их возможные цели.
ПК-5	Способен выявлять уязвимости в системах защиты информации автоматизированных систем, разрабатывать методики, предложения и процедуры совершенствования процесса защиты информации, оптимизировать параметры программных, программно-аппаратных и технических средств защиты информации автоматизированных систем	ИПК-5.1. Осуществляет сбор и анализ исходных данных, необходимых для проектирования систем защиты информации автоматизированных систем. ИПК-5.2. Осуществляет поиск уязвимостей в параметрах автоматизированных систем.

В результате изучения дисциплины обучающийся должен:

владеть навыками: навыками построения моделей отказов и определения критичных элементов объекта защиты; навыками анализа деревьев отказов, применения FMEA и разработки предложений по повышению надежности.

уметь: выявлять потенциальные угрозы и сценарии нарушения работоспособности системы защиты; собирать исходные данные, рассчитывать показатели надежности, выявлять уязвимые параметры и сравнивать варианты построения защиты.

знать: угрозы и отказы, влияющие на надежность систем защиты информации, показатели надежности и условия их применения; вероятностные, статистические и структурные методы оценки надежности систем защиты информации.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Основные понятия и показатели надежности	ОПК-2.1 ПК-5
2.	Вероятностные модели отказов и восстановления	ОПК-2.1 ПК-5
3.	Структурная надежность систем защиты	ОПК-2.1 ПК-5
4.	Готовность и марковские модели	ОПК-2.1 ПК-5
5.	Статистическая оценка надежности	ОПК-2.1 ПК-5
6.	Анализ видов и последствий отказов	ОПК-2.1 ПК-5
7.	Надежность многоуровневой системы защиты	ОПК-2.1 ПК-5
8.	Испытания, мониторинг и повышение надежности	ОПК-2.1 ПК-5

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – зачет.

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
		70-85,9	«хорошо» / 4	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

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 зачету

ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба

1. Понятие надежности системы защиты информации.
2. Свойства надежности: безотказность, ремонтопригодность, долговечность и сохраняемость.
3. Отказ, повреждение и сбой в системе защиты информации.
4. Классификация отказов элементов системы защиты.
5. Угрозы, приводящие к нарушению работоспособности средств защиты.
6. Единичная точка отказа и ее влияние на защищенность объекта.
7. Наработка до отказа как показатель надежности.
8. Вероятность безотказной работы и вероятность отказа.
9. Интенсивность отказов и условия ее применения.
10. Среднее время восстановления средства защиты.
11. Коэффициент готовности и коэффициент простоя.
12. Связь надежности и эффективности системы защиты информации.
13. Исходные данные для анализа надежности объекта защиты.
14. Функциональная декомпозиция системы защиты.
15. Выявление критичных функций системы защиты информации.
16. Сценарии отказов средств идентификации и аутентификации.
17. Сценарии отказов системы контроля доступа.
18. Сценарии отказов средств регистрации и мониторинга.
19. Сценарии отказов сетевых средств защиты.
20. Сценарии отказов антивирусных средств.
21. Зависимые и общие отказы элементов системы.
22. Ошибки персонала как причина отказов системы защиты.
23. Влияние отказов электропитания и связи на функции защиты.

24. Деградация функций многоуровневой системы защиты.
25. Оценка возможных целей реализации угроз надежности.
26. Оценка последствий отказа критичного элемента.
27. Определение допустимого времени простоя защитной функции.
28. Учет восстановительных мероприятий в модели угроз.
29. Критерии приоритизации угроз нарушения надежности.
30. Документирование результатов анализа угроз и отказов.

ПК-5. Способен выявлять уязвимости в системах защиты информации автоматизированных систем, разрабатывать методики, предложения и процедуры совершенствования процесса защиты информации, оптимизировать параметры программных, программно-аппаратных и технических средств защиты информации автоматизированных систем

1. Экспоненциальная модель времени до отказа.
2. Функция распределения и плотность распределения времени до отказа.
3. Допущения простейшего потока отказов.
4. Оценка параметров модели по эксплуатационным данным.
5. Расчет надежности последовательной структуры.
6. Расчет надежности параллельной структуры.
7. Структурные схемы надежности систем защиты информации.
8. Влияние резервирования на вероятность безотказной работы.
9. Нагруженное и ненагруженное резервирование.
10. Ограничения структурных моделей при зависимых отказах.
11. Состояния и переходы в марковской модели надежности.
12. Марковская модель восстанавливаемой системы.
13. Расчет коэффициента готовности по интенсивностям отказа и восстановления.
14. Влияние времени обнаружения отказа на готовность системы.
15. Сбор и очистка данных об отказах средств защиты.
16. Полные и цензурированные наблюдения при оценке надежности.
17. Точечная оценка интенсивности отказов.
18. Доверительный интервал для показателя надежности.
19. Проверка применимости вероятностной модели к наблюдаемым данным.
20. Назначение и этапы метода FMEA.
21. Оценка тяжести последствий, частоты и обнаруживаемости отказов.
22. Приоритетное число риска и его интерпретация.
23. Построение дерева отказов для критического события.
24. Минимальные сечения дерева отказов.
25. Выявление уязвимостей в параметрах системы защиты.
26. Сравнение вариантов архитектуры по показателям надежности.
27. Планирование испытаний системы защиты на надежность.
28. Мониторинг эксплуатационных показателей надежности.
29. Разработка корректирующих мер по результатам оценки.
30. Оптимизация параметров средств защиты с учетом требований надежности.