Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:53
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 06.09.2024 г. № 2

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

«Аудит информационной безопасности»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриата**

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

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

Составители Дробот Олеся Алексеевна, 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 2024

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-2.4	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ИОПК-2.4.1. Знает требования, предъявляемые к защищенным объектам информатизации. ИОПК-2.4.2. Проводит аудит защищенности объекта информатизации.
ПК-3	Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИПК-3.1.Оценивает работоспособность применяемых средств защиты информации с использованием штатных средств и методик. ИПК-3.2.Оценивает эффективность применяемых средств защиты информации с использованием штатных средств и методик. ИПК-3.3. Определяет уровень защищенности и доверия средств защиты информации.

В результате изучения дисциплины обучающийся должен:

владеть навыками: навыками планирования и проведения аудита защищенности объекта информатизации, фиксации несоответствий, подготовки обоснованных выводов и оформления отчета по результатам аудита.; навыками подготовки исходных данных и сценариев контрольной проверки, регистрации результатов, интерпретации полученных показателей и подготовки заключения о работоспособности и эффективности применяемых средств защиты информации.

уметь: определять область и критерии аудита, формировать программу и чек-листы проверки, собирать и анализировать аудиторские свидетельства, сопоставлять фактическое состояние объекта информатизации с установленными требованиями.; проводить контрольные проверки работоспособности и эффективности средств защиты информации по заданной методике, анализировать результаты испытаний и журналов, выявлять отклонения и определять уровень защищенности и доверия.

знать: требования, предъявляемые к защищенным объектам информатизации; цели, принципы, этапы и критерии аудита защищенности; виды аудиторских свидетельств и правила документирования результатов проверки.; порядок организации контрольных проверок средств защиты информации; штатные средства и методики проверки работоспособности и эффективности; показатели, критерии и документируемые результаты оценки уровня защищенности и доверия.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
	Основы аудита информационной безопасности и требования к защищенным объектам информатизации	ОПК-2.4 ПК-3
	Планирование аудита и формирование программы проверки	ОПК-2.4 ПК-3
	Аудит организационных мер и управления доступом	ОПК-2.4 ПК-3
	Технический аудит защищенности автоматизированной системы	ОПК-2.4 ПК-3
	Контроль работоспособности и эффективности средств защиты информации	ОПК-2.4 ПК-3
	Оценка уровня защищенности, оформление результатов и завершение аудита	ОПК-2.4 ПК-3

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, проверки самостоятельной работы).

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

Перечень вопросов и заданий для подготовки к зачету

ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

1. Понятие и назначение аудита информационной безопасности.
2. Цели и задачи аудита защищенности объекта информатизации.
3. Объект, предмет и область аудита информационной безопасности.
4. Критерии аудита и источники требований к защищенному объекту информатизации.
5. Основные требования, предъявляемые к защищенным объектам информатизации.
6. Принципы объективности, независимости и доказательности аудита.
7. Этапы жизненного цикла аудита информационной безопасности.
8. Инициирование аудита и определение его целей и ограничений.
9. Программа аудита: назначение, состав и правила разработки.
10. План аудита и распределение ответственности участников проверки.
11. Аудиторский чек-лист: структура и правила применения.
12. Виды аудиторских свидетельств и требования к их достаточности.
13. Методы получения свидетельств: анализ документов, интервью, наблюдение.
14. Выборочный контроль и ограничения выборки при проведении аудита.
15. Документарный аудит организационных мер защиты информации.
16. Аудит распределения ролей, полномочий и ответственности.
17. Аудит управления учетными записями и правами доступа.
18. Аудит процедур управления изменениями и конфигурациями.
19. Аудит журналирования и регистрации событий безопасности.
20. Аудит резервного копирования и восстановления информации.
21. Аудит мер реагирования на инциденты информационной безопасности.
22. Содержание технического аудита защищенности автоматизированной системы.
23. Проверка конфигурационных параметров безопасности как метод аудита.
24. Ограничения инструментальных методов при аудите действующего объекта.
25. Фиксация фактов и обеспечение прослеживаемости аудиторских выводов.
26. Классификация выявленных несоответствий при аудите.
27. Формирование аудиторского вывода на основе собранных свидетельств.
28. Структура и содержание отчета по аудиту информационной безопасности.
29. Рекомендации по результатам аудита и требования к их обоснованности.
30. Повторная проверка и подтверждение устранения выявленных несоответствий.

ПК-3 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

1. Назначение контрольных проверок средств защиты информации.
2. Различие проверки наличия, работоспособности и эффективности средства защиты информации.
3. Организация контрольной проверки работоспособности средства защиты.
4. Организация контрольной проверки эффективности средства защиты.

5. Штатные средства диагностики и их роль в контрольной проверке.
6. Требования к методике проверки средства защиты информации.
7. Исходные данные для подготовки программы контрольной проверки.
8. Критерии работоспособности программного средства защиты информации.
9. Критерии работоспособности программно-аппаратного средства защиты информации.
10. Критерии работоспособности технического средства защиты информации.
11. Понятие эффективности применяемых мер и средств защиты информации.
12. Формирование безопасного тестового сценария контрольной проверки.
13. Ожидаемый результат и критерии приемки при проведении проверки.
14. Использование журналов событий при оценке работоспособности средства защиты.
15. Использование диагностических сообщений и штатной телеметрии при проверке.
16. Анализ ложных срабатываний и пропусков событий при оценке эффективности.
17. Проверка устойчивости настроек средства защиты после изменения конфигурации.
18. Контроль корректности функционирования механизмов идентификации и аутентификации.
19. Контроль корректности функционирования механизмов разграничения доступа.
20. Контроль корректности регистрации событий информационной безопасности.
21. Проверка работоспособности сетевых средств защиты информации.
22. Проверка работоспособности средств антивирусной и иной защитной обработки.
23. Проверка работоспособности криптографических механизмов штатными средствами.
24. Сопоставление фактических результатов проверки с установленными критериями.
25. Определение уровня защищенности по результатам контрольных проверок.
26. Понятие уровня доверия к средству защиты информации.
27. Связь результатов проверок с оценкой уровня защищенности и доверия.
28. Оформление протокола контрольной проверки.
29. Формулирование заключения о работоспособности и эффективности средства защиты.
30. Документирование ограничений, допущений и повторных проверок.