

Документ подписан простой электронной подписью
Информация о документе:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 28.07.2026 09:53:10
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 02.12.2022г. № 4

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

«Технологии обеспечения информационной безопасности»

наименование дисциплины

по образовательной программе высшего образования – программе магистратуры

**«Информационная безопасность интеллектуальных и информационно-аналитических
систем»**

наименование образовательной программы

10.04.01 «Информационная безопасность»

шифр, наименование направления подготовки / специальности

Составитель Мунирова Юлия Сергеевна, старший
преподаватель, Высшая школа
интеллектуальных систем и кибертехнологий

ФИО, должность, структурное подразделение,
ученая степень, ученое звание

Тольятти
2022

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-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемы ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем

В результате изучения дисциплины обучающийся должен:

владеть: инструментарием формирования требований к системе обеспечения информационной безопасности, навыками проектирования подсистемы обеспечения информационной безопасности

уметь: разрабатывать проект технического задания на создание системы обеспечения информационной безопасности, разрабатывать технический проект системы (подсистемы, либо компонента системы) обеспечения информационной безопасности

знать: требования к системе обеспечения информационной безопасности; методы концептуального проектирования технологий систем обеспечения информационной безопасности

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Тема 1. Понятие системы, технологии функционирования. Сложные системы. Технология обеспечения информационной безопасности.	ОПК-1 ОПК-2
2.	Тема 2. Проектирование и совершенствование технологии обеспечения информационной безопасности. Этапы. Цели и задачи. Требования. Методы и способы. проектирования	
3.	Тема 3. Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем	
4.	Тема 4. Технология создания защищенных систем. Анализ требований, угроз, уязвимостей объекта защиты.	
5.	Тема 5. Особенности построения защищенных информационных систем	
6.	Тема 6. Вычисление структурно-топологических характеристик систем управления	

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – экзамен.

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-бальная 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 для подготовки к экзамену

ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

1. Что такое информация, субъекты информационных отношений?
2. Дайте определение Информационной технологии.
3. Компьютерная система-это...
4. Элементы и подсистемы, управление и информация, самоорганизация.
5. Раскройте терм информация безопасность
6. Определение автоматизированной системы
7. Свойства информации
8. Что такое уязвимость?
9. Основные принципы системного подхода при создании сложных систем.
10. Технология функционирования сложной системы.
11. Перечислите основные объекты информационной безопасности. Дайте их определения.
12. Понятия ущерба, риска и угрозы.
13. Основные угрозы безопасности информации АС и их классификация.
14. Каково назначение Политики информационной безопасности?
15. Для чего нужна стандартизация в сфере информационной безопасности?
16. Какую информацию относят к секретной, конфиденциальной?
17. Цели и задачи проектирования ИБ
18. Что такое система физической защиты объекта?
19. Перечислите основные риски ИБ. Дайте их определения.

ОПК-2: Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

20. Какие требования предъявляются к комплексной системе безопасности объекта?
21. В чем суть гарантированного уничтожения данных?
22. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
23. Охарактеризуйте понятие большие данные.
24. Какую информацию относят к секретной, конфиденциальной?
25. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
26. Какие применяются методы защиты информации от промышленного шпионажа?
27. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
28. Какие организационные меры обеспечения безопасности Вы знаете?
29. Какие технические меры обеспечения безопасности Вы знаете?
30. Основные принципы обеспечения ИБ

31. Основные функции системы безопасности.
32. Основные принципы политики ИБ.
33. Какое свойство информации является наиболее актуальным при обеспечении ИБ? Дайте его определение.
34. Свойство информации при котором невозможно ее искажение...
35. Охарактеризуйте ИБ поиска информации.
36. Охарактеризуйте ИБ обработки данных.
37. Охарактеризуйте эмерджентные технологии.
38. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?
39. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?
40. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?
41. Укажите модель управления доступом, к которой относится основная теорема безопасности.
42. Какие виды информации существуют в зависимости от категории доступа к ней?
43. Защищаемая информация – это..
44. Правовые методы обеспечения ИБ
45. Способы представления информации о правах доступа.
46. Характеристика качества
47. Показатели и критерии эффективности
48. Методические вопросы оценки эффективности сложных систем.
49. Дайте определение понятию «ядро безопасности»
50. Кратко опишите архитектуру защищенной системы.