

Документ подписан простой электронной подписью
Информация о документе:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 28.07.2026 09:55:10
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

«Защищенные информационные системы»

наименование дисциплины

по образовательной программе высшего образования – программе **магистратуры**

бакалавриата,
специалитета,
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

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	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем
ОПК-4	Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок».	ИОПК-4.3. Формирует планы и проекты технических разработок защищённых информационных систем

В результате изучения дисциплины обучающийся должен:

Владеть: навыками управления проектами систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты; навыками разработки проектов и комплексов управления информационной безопасностью с учетом особенностей объектов защиты;

навыками сбора и обработки информации, разработки планов и программ научных исследований; навыками использования результатов обзора научно-технической литературы при решении вопросов информационной безопасности телекоммуникационных систем и сетей.

Уметь: организовывать и осуществлять контроль за разработкой технических проектов систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты; находить ведомственные документы в части проектирования подсистем и применения средств обеспечения информационной безопасности;

выбирать методы и средства решения задачи в рамках проводимого исследования, вырабатывать планы и программы проведения научных исследований и технических разработок.

Знать: методы разработки систем и комплексы управления информационной безопасностью с учетом особенностей объектов защиты; основные компоненты технического проекта; перечень необходимых исходных данных для проектирования подсистем либо компонентов системы;

методы сбора, обработки, анализа и систематизации научно-технической информации; современную научно-техническую литературу, нормативные и методические документы по вопросам информационной безопасности.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Введение в предмет «защищённые информационные системы»	ОПК-2, ОПК-4.
2.	Интегральная безопасность информационных систем	ОПК-2, ОПК-4.
3.	Безопасность хранения и передачи информации	ОПК-2, ОПК-4.
4.	Методы проектирования и анализа информационных систем	ОПК-2, ОПК-4.
5.	Определение степени защищённости информационной системы	ОПК-2, ОПК-4
6.	Реализация программ информационной защиты и защиты информации	ОПК-2, ОПК-4.

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 балльная шкала, %	100 балльная 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 для подготовки к зачету

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

1. Общие определения и характеристики информационных систем. Структура и классификация систем.
2. Понятие сложности, критерии и свойства. Критерии и свойства для информационной системы.
3. Вероятностная модель системы и пример пограничных состояний. Базовые информационные процессы в системах.
4. Основные принципы обеспечения информационной безопасности для информационных систем.
5. Методическая и нормативная база для построения защищенных систем.
6. Виды защищенных информационных систем в соответствии с требованиями ГОСТ.
7. Принципы защиты информации в автоматизированных системах в соответствии с требованиями ГОСТ.
8. Понятие о задаче интегральной безопасности информационных систем.
9. Примеры задач интегральной безопасности.
10. Физическая безопасность информационных систем.
11. Безопасность сетей и телекоммуникационных устройств.
12. Безопасность ПО.
13. Обеспечение конфиденциальности, целостности и доступности данных.
14. Постановка задачи, её структура.
15. Частный, комплексный и интегральных подходы к решению проблемы передачи и хранения данных.
16. Постановка задачи проектирования и анализа информационной системы.
17. Модель системы с общим перекрытием.
17. Концептуальные требования направленные на обеспечение безопасности функционирования информационной системы.
18. Важнейшие принципы построения архитектуры ИС.

ОПК-4: Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок,

19. Анализ безопасности ИС.
20. Постановка задачи защищённости ИС.
21. Наличие и полнота политики безопасности.
22. Гарантированность безопасности.
23. Трёхуровневая модель параметров оценки защищенности ИС.
24. Аудит сетей связи. Мониторинг функционирования, обнаружение атак и принятие адекватных мер противодействия.
25. Средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (File Encryption System – FES).
26. Средства авторизации и разграничения доступа к информационным ресурсам, а также защита от несанкционированного доступа к информации с использованием технологии токенов (смарт-карты, touch-memory, ключи для USB-портов и т.п.).

27. Средства защиты от внешних угроз при подключении к общедоступным сетям связи, а также средства управления доступом Интернета с использованием технологии межсетевых экранов (FireWall) и содержательной фильтрации (Content Inspection).
28. Политика реализации межсетевых экранов и их функциональные возможности. Классификация межсетевых экранов. Недостатки фильтрующего маршрутизатора (Filter Router - FR).
29. Шлюз сеансового уровня (Session Level Gateway - SLG). Шлюз уровня приложений (Application Layer Gateway - ALG). Преимущества ALG.
30. Что такое Антивирусы?
31. Средства обеспечения активного исследования защищенности информационных ресурсов с использованием технологии обнаружения атак (Intrusion Detection).
32. Инфраструктура открытых ключей (Public Key Infrastructure - PKI).
33. Средства обеспечения конфиденциальности, целостности, доступности и подлинности информации, передаваемой по открытым каналам связи с использованием технологии защищенных виртуальных частных сетей (VPN).
34. Четыре вида архитектуры организации защиты информации на базе применения технологии VPN. Классификация VPN.
35. Средства обеспечения централизованного управления системой ИБ в соответствии с согласованной и утвержденной политикой безопасности.
36. Информация и данные. Свойства информации. Функции информации.
37. Информационная безопасность и защита информации. Задачи информационной безопасности.
38. Направления информационной безопасности.
39. Составляющие информационной безопасности.
40. Нормативно-правовое обеспечение информационной безопасности. Основные документы.
41. Государственная тайна и ее защита.
42. Ответственность за нарушения в сфере информационной безопасности.
43. Защита персональных данных. Понятия и основные документы.
44. Регуляторы в области защиты персональных данных. Их функции и требования.
45. Ответственность за несоблюдение требований законодательства в сфере защиты персональных данных.
46. Угрозы и риски информационной безопасности. Источники угроз. Виды угроз.
47. Риски нарушения информационной безопасности. Систематизация рисков. Измерение рисков, шкалы рисков.
48. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь.
49. Экономические проблемы информационных ресурсов. Основные подходы к определению затрат на защиту информации.