

Документ подписан простой электронной подписью
Информация о документе
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 28.07.2026 09:33:11
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

«Интеграция систем обработки и защиты информации»

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-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
ПК-4.	Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных	ИПК-4.3. Разрабатывает архитектуру системы защиты информации автоматизированных систем, а также интеллектуальных и информационно-аналитических систем в частности

В результате изучения дисциплины обучающийся должен:

владеть: Умением проводить анализ рисков безопасности и разрабатывать соответствующие стратегии защиты..Навыками применения технических мер безопасности в разработке информационных систем; Методиками анализа угроз и рисков информационной безопасности.

уметь: Разрабатывать архитектуру системы защиты информации с учетом специфики деятельности организации. Проводить анализ уязвимостей информационных систем и разрабатывать меры по их устранению. Разрабатывать технический проект системы обеспечения информационной безопасности; Проектировать компоненты и подсистемы защищенных информационных систем

знать: Принципы построения архитектуры систем защиты информации. Основные угрозы и уязвимости, с которыми сталкиваются информационные системы. Принципы построения защищенных информационных систем; Технические меры обеспечения информационной безопасности;

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Тема 1. Разработка и реализация комплексных систем защиты информации, включающих в себя технические, организационные и правовые меры	ОПК-2 ПК-4
2.	Тема 2. Исследование методов и технологий интеграции различных систем обработки и защиты информации, в том числе с использованием облачных технологий	
3.	Тема 3. Анализ рисков информационной безопасности и разработка стратегий их минимизации	
4.	Тема 4. Оценка эффективности систем обработки и защиты информации и разработка рекомендаций по их оптимизации	
5.	Тема 5. Исследование вопросов международного сотрудничества в области информационной безопасности и интеграции систем обработки и защиты информации	

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-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

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии с набранными за семестр баллами

2. Перечень оценочных материалов для проведения промежуточной аттестации

Перечень вопросов и заданий для подготовки к зачету

ОПК -2:ИОПК-2.2, ИОПК-2.3. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

1. Понятие интегрированной корпоративной информационной системы.
2. Основные типы интеграционных задач
3. Методология «открытых систем» и проблема интеграции.
4. Базовые модели интеграции (передача файлов, обмен сообщениями, удаленный вызов процедуры, использование общей базы данных) и их сильные и слабые стороны.
5. Уровни интеграции корпоративных приложений
6. Проблема стандартизации. Основные организации, занимающиеся утверждением стандартов.
7. Сценарии интеграции данных. Получение данных для хранилищ данных и систем бизнес-аналитики (технология ETL).
8. Платформы для интеграции корпоративной информации (Oracle Data Integrator, Informatica power center, IBM Information Server).
9. Технологии Big Data и проблема интеграции.
10. Опишите самый современный подход интеграции бизнес процессов
11. Чего помогает добиться Композитное (составное) приложение
12. Как называется система позволяющая наращивать и записывать в себя информацию и выстраивающая интеграционную систему
13. Управления рисками информационной безопасности
14. Основные источники угроз и виды нарушений в области информационной безопасности.
15. Процесс управления непрерывностью. Преимущества и проблемы процесса.
16. Процесс управления безопасностью. Цели и преимущества процесса
17. Основные положения стандарта BS7799
18. Основные положения стандарта ISO 17799.
19. Система информационной безопасности предприятия (задачи системы, объекты защиты) Основные источники угроз и виды нарушений в области информационной безопасности.
20. Цели и задачи интеграции систем обработки и защиты информации
21. Что такое ИСОЗИ и какие принципы лежат в её основе?

22. Какие методы и технологии используются для защиты информации в интегрированных системах?
23. Как обеспечить совместимость между различными системами обработки и защиты информации?
24. Какие роли и обязанности возлагаются на интегратора систем обработки и защиты информации?
25. Какие технологии шифрования применяются для защиты информации в интегрированных системах обработки и защиты?
26. Как происходит интеграция систем мониторинга и аудита в информационной безопасности?
27. Как происходит проектирование и настройка интегрированных систем обработки и защиты информации?
28. Какие меры предпринимаются для обеспечения защиты от DDoS-атак в интегрированных системах обработки и защиты информации?

ПК-4:ИПК-4.3. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных.

29. Как обеспечить безопасность при передаче данных между различными подсистемами в интегрированных системах?
30. Какие методы аутентификации и авторизации используются в интегрированных системах обработки и защиты информации?
31. Каким образом осуществляется интеграция различных уровней защиты в информационных системах?
32. Какие протоколы и стандарты используются при интеграции систем обработки и защиты информации?
33. Какие меры предпринимаются для обеспечения безопасности в случае вывода из эксплуатации информационных систем или оборудования?
34. Какие методы и технологии используются для обнаружения и предотвращения утечек конфиденциальной информации в интегрированных системах обработки и защиты информации?
35. Какие методы обеспечения целостности данных используются в интегрированных системах обработки и защиты информации?
36. Каким образом осуществляется резервное копирование и восстановление данных в интегрированных системах обработки и защиты информации?
37. Какие методы используются для защиты от атак на прикладные уровни в интегрированных системах обработки и защиты информации?
38. Как осуществляется мониторинг и анализ сетевого трафика в интегрированных системах обработки и защиты информации?
39. Каким образом осуществляется контроль и защита информации при передаче
40. Понятие интегрированной корпоративной информационной системы. Концепция ERP (Enterprise Resource Planning)
41. Типовая архитектура ERP-систем. ERP-система как центр интеграционного решения.
42. Как оценить уровень риска при использовании интегрированных систем?
43. Принципы построения архитектуры систем защиты информации.