Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 08:25:20
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»)

Колледж креативных индустрий и предпринимательства

УТВЕРЖДЕНО
на заседании ПЦК

по образовательной программе 09.02.07 Информационные системы и программирование

Протокол от 24.10.2025 г. № 2

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств) для проведения промежуточной аттестации

по междисциплинарному курсу
учебному предмету, дисциплине, междисциплинарному курсу, профессиональному модулю

«Проектирование и дизайн информационных систем»
наименование учебного предмета, дисциплины, междисциплинарного курса, профессионального модуля

по образовательной программе среднего профессионального образования –

программе подготовки специалистов среднего звена
программе подготовки специалистов среднего звена / программе подготовки квалифицированных рабочих, служащих

Информационные системы и программирование
наименование образовательной программы

09.02.07 Информационные системы и программирование
шифр, наименование специальности / профессии

Составитель Абсалямов М.А., преподаватель Колледжа креативных индустрий и предпринимательства
ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2025

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ (ДАЛЕЕ – ФОС)

1.1. Планируемые результаты обучения по междисциплинарному курсу

Код компетенции	Наименование компетенции
ПК 5.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.
ПК 5.6	Разрабатывать техническую документацию на эксплуатацию информационной системы.
ПК 5.7	Производить оценку информационной системы для выявления возможности ее модернизации.

В результате освоения МДК обучающийся должен:

иметь практический опыт:

- управлении процессом разработки приложений с использованием инструментальных
- средств;
- обеспечении сбора данных для анализа использования и функционирования
- информационной системы;
- программировании в соответствии с требованиями технического задания;
- использовании критериев оценки качества и надежности функционирования
- информационной системы;
- применении методики тестирования разрабатываемых приложений;
- определении состава оборудования и программных средств разработки информационной
- системы;
- разработке документации по эксплуатации информационной системы;
- проведении оценки качества и экономической эффективности информационной системы
- в рамках своей компетенции;
- модификации отдельных модулей информационной системы

уметь:

- осуществлять постановку задач по обработке информации;
- проводить анализ предметной области;
- осуществлять выбор модели и средства построения информационной системы и
- программных средств;
- использовать алгоритмы обработки информации для различных приложений;
- решать прикладные вопросы программирования и языка сценариев для создания
- программ;
- разрабатывать графический интерфейс приложения;
- создавать и управлять проектом по разработке приложения;
- проектировать и разрабатывать систему по заданным требованиям и спецификациям

знать:

- основные виды и процедуры обработки информации, модели и методы решения задач
- обработки информации;
- основные платформы для создания, исполнения и управления информационной

- системой;
- основные процессы управления проектом разработки;
- основные модели построения информационных систем, их структуру, особенности и
- области применения;
- методы и средства проектирования, разработки и тестирования информационных
- систем;
- систему стандартизации, сертификации и систему обеспечения качества продукции

1.2. Содержание междисциплинарного курса

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
6 семестр		
1	Основы проектирования информационных систем.	ПК 5.3 ПК 5.7 ПК 5.7
7 семестр		
2	Система обеспечения качества информационных систем.	ПК 5.3 ПК 5.6 ПК 5.7
8 семестр		
3	Разработка документации информационных систем.	ПК 5.3 ПК 5.6 ПК 5.7

1.3. Система оценивания по междисциплинарному курсу

Междисциплинарный курс изучается в течение трёх семестров. Форма промежуточной аттестации по междисциплинарному курсу в 6,7 семестре – контрольная работа, в 8 семестре – дифференцированный зачет

6, 7 семестр:

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины	
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	недифференцированная оценка
допороговый	ниже 61	ниже 61	не зачтено
пороговый	61-85,9	61-69,9	зачтено
		70-85,9	
повышенный	86-100	86-100	

8 семестр:

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины	
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	дифференцированная оценка
допороговый	ниже 61	ниже 61	неудовлетворительно
пороговый	61-85,9	61-69,9	удовлетворительно
		70-85,9	хорошо
повышенный	86-100	86-100	отлично

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Вопросы для подготовки к контрольной работе (6 семестр)

№	Содержание вопроса
ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.	
1.	Что такое подсистема безопасности информационной системы?
2.	Какие ключевые задачи стоят перед специалистом при разработке подсистем безопасности?
3.	Какие основные этапы разработки подсистемы безопасности информационной системы?
4.	Как техническое задание влияет на проектирование подсистемы безопасности?
5.	Какие требования безопасности должны быть учтены при разработке подсистемы?
6.	Какие нормативные документы и стандарты безопасности необходимо учитывать при разработке?
7.	Что такое модель угроз, и как она используется при проектировании подсистемы безопасности?
8.	Какие методы защиты данных должны быть реализованы в подсистеме безопасности?
9.	Какое влияние на подсистему безопасности оказывают особенности архитектуры информационной системы?
10.	Какие средства аутентификации и авторизации должны быть предусмотрены в подсистеме безопасности?
11.	Как осуществляется мониторинг и управление безопасностью в рамках подсистемы?
12.	Как осуществляется тестирование и проверка эффективности работы подсистемы безопасности?
13.	Как осуществляется взаимодействие подсистемы безопасности с другими подсистемами информационной системы?
14.	Какие критерии успешности разработки подсистемы безопасности можно выделить?
15.	Какие риски могут возникнуть при разработке подсистемы безопасности, и как их минимизировать?
ПК 5.6. Разрабатывать техническую документацию на эксплуатацию информационной системы.	
16.	Как проводить аудит документации по эксплуатации информационной системы?
17.	Какие данные необходимо собирать для составления технической документации?
18.	Как разработать документацию для системы с высокой степенью безопасности?
19.	Каковы этапы разработки документации по эксплуатации информационной системы?
20.	Какие требования предъявляются к оформлению технических рисков в документации?
21.	Как определить приоритетность элементов документации при ее разработке?
22.	Как описать процессы установки и настройки системы в документации?
23.	Какие разделы документации наиболее важны для администраторов системы?
24.	Какую информацию необходимо указать в разделе "Обслуживание системы"?
25.	Как описывать процедуры аварийного восстановления в документации?
26.	Как описывать способы и процедуры мониторинга системы?
27.	Какие сведения о безопасности и защите данных необходимо включать в документацию?
28.	Какие рекомендации по эксплуатации системы должны быть включены в документацию?
29.	Как следует представлять информацию о совместимости с другими системами?
30.	Каковы особенности написания документации для масштабируемых систем?
ПК 5.7. Производить оценку информационной системы для выявления возможности ее модернизации.	

31.	Какие основные цели и задачи стоят перед процессом оценки информационной системы?
32.	Как определить, что информационная система нуждается в модернизации?
33.	Какие ключевые показатели эффективности системы нужно учитывать при оценке?
34.	Какую информацию необходимо собрать для проведения оценки информационной системы?
35.	Как проводится анализ производительности информационной системы?
36.	Какие метрики используются для оценки текущей архитектуры системы?
37.	Как оценить соответствие системы современным требованиям безопасности?
38.	Как анализировать уровень совместимости системы с другими компонентами?
39.	Какие проблемы могут возникать из-за устаревших технологий в информационной системе?
40.	Как анализировать влияние текущей системы на бизнес-процессы организации?
41.	Как выявить узкие места в работе информационной системы?
42.	Как оценить степень масштабируемости информационной системы?
43.	Какие критерии следует учитывать при оценке возможностей для интеграции новых технологий?
44.	Как анализировать возможности для автоматизации процессов в информационной системе?
45.	Какие инструменты и методы используются для мониторинга и оценки работы системы?

Вопросы для подготовки к промежуточной аттестации (контрольная работа)

7 семестр

№	Содержание вопроса
ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.	
1.	Как вы определяете требования к безопасности при анализе технического задания?
2.	Какие типы угроз могут быть актуальными для разработки подсистемы безопасности?
3.	Какие методы шифрования должны быть использованы для защиты данных в подсистеме?
4.	Какие меры по защите от несанкционированного доступа должны быть предусмотрены в подсистеме безопасности?
5.	Как обеспечивается защита от атак типа "отказ в обслуживании" (DoS) в информационной системе?
6.	Каковы основные принципы безопасной архитектуры информационных систем?
7.	Какие средства контроля целостности данных должны быть внедрены в подсистему безопасности?
8.	Что такое инцидент безопасности, и как подсистема должна реагировать на такие инциденты?
9.	Как осуществляется управление доступом к данным и ресурсам в подсистеме безопасности?
10.	Как обеспечивается безопасность при передаче данных по сети в рамках подсистемы?
11.	Как производится аудит безопасности информационной системы и какие инструменты для этого используются?
12.	Как подсистема безопасности должна обеспечивать соответствие законодательства о защите данных (например, GDPR)?
13.	Как учитывать риски, связанные с внешними и внутренними угрозами при проектировании подсистемы безопасности?
14.	Как выполняется интеграция подсистемы безопасности с системами управления инцидентами безопасности (SIEM)?
15.	Какие подходы используются для защиты от вредоносного программного обеспечения (malware) в подсистемах безопасности?
ПК 5.6. Разрабатывать техническую документацию на эксплуатацию информационной	

№	Содержание вопроса
системы.	
16.	Как проводить аудит документации по эксплуатации информационной системы?
17.	Какие данные необходимо собирать для составления технической документации?
18.	Как разработать документацию для системы с высокой степенью безопасности?
19.	Каковы этапы разработки документации по эксплуатации информационной системы?
20.	Какие требования предъявляются к оформлению технических рисков в документации?
21.	Как определить приоритетность элементов документации при ее разработке?
22.	Как описать процессы установки и настройки системы в документации?
23.	Какие разделы документации наиболее важны для администраторов системы?
24.	Какую информацию необходимо указать в разделе "Обслуживание системы"?
25.	Как описывать процедуры аварийного восстановления в документации?
26.	Как описывать способы и процедуры мониторинга системы?
27.	Какие сведения о безопасности и защите данных необходимо включать в документацию?
28.	Какие рекомендации по эксплуатации системы должны быть включены в документацию?
29.	Как следует представлять информацию о совместимости с другими системами?
30.	Каковы особенности написания документации для масштабируемых систем?
ПК 5.7. Производить оценку информационной системы для выявления возможности ее модернизации.	
31.	Как оценить возможности системы для работы с большими данными (Big Data)?
32.	Какой вклад в процесс модернизации может внести использование облачных технологий?
33.	Как учитывать потребности пользователей при оценке возможности модернизации?
34.	Как выявить и оценить риски, связанные с текущим состоянием информационной системы?
35.	Как проводить анализ затрат на модернизацию системы?
36.	Как оценить совместимость системы с новыми версиями операционных систем и программного обеспечения?
37.	Как учитывать требования к производительности при модернизации системы?
38.	Какие методы оценки текущего состояния информационной системы существуют?
39.	Как анализировать текущее состояние аппаратного обеспечения системы?
40.	Как определить, какие части системы нуждаются в модернизации, а какие могут оставаться без изменений?
41.	Как проводить оценку на соответствие законодательным и нормативным требованиям?
42.	Как учитывать возможности системы для работы с мобильными устройствами и приложениями?
43.	Как оценить текущую документацию и процесс ее обновления в контексте модернизации системы?
44.	Как оценивается уровень поддержки системы в текущей версии (поставщик, сервис, обновления)?
45.	Какие методики используются для анализа потенциальных улучшений в области безопасности системы?

Вопросы для подготовки к промежуточной аттестации (дифференцированный зачет) 8 семестр

№	Содержание вопроса
ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.	
1.	Как внедрять политику безопасности в организацию в процессе разработки

№	Содержание вопроса
	подсистемы?
2.	Какие средства защиты от внешних атак (например, межсетевые экраны, системы предотвращения вторжений) должны быть интегрированы в подсистему безопасности?
3.	Каковы требования к защите личных данных пользователей в рамках подсистемы безопасности?
4.	Какие меры должны быть приняты для защиты от социальных атак (например, social engineering)?
5.	Как осуществлять защиту информации в мобильных приложениях и на устройствах в рамках подсистемы безопасности?
6.	Как осуществлять управление уязвимостями в подсистемах безопасности?
7.	Каковы особенности разработки подсистем безопасности для распределённых информационных систем?
8.	Как разработка подсистемы безопасности зависит от особенностей работы с данными в реальном времени?
9.	Как обеспечить поддержку и обновление подсистемы безопасности после её внедрения?
10.	Какие подходы используются для обеспечения безопасности на уровне операционной системы и приложений?
11.	Как нужно работать с криптографическими средствами при разработке подсистем безопасности?
12.	Как учитывать угрозы, связанные с использованием несанкционированных мобильных устройств в сети организации?
13.	Как обеспечить безопасное управление паролями и другими конфиденциальными данными в подсистемах безопасности?
14.	Какую роль играет обучение персонала в обеспечении безопасности информационной системы?
15.	Какие методы аутентификации пользователей должны быть использованы в подсистемах безопасности?
ПК 5.6. Разрабатывать техническую документацию на эксплуатацию информационной системы.	
16.	Как проводить аудит документации по эксплуатации информационной системы?
17.	Какие данные необходимо собирать для составления технической документации?
18.	Как разработать документацию для системы с высокой степенью безопасности?
19.	Каковы этапы разработки документации по эксплуатации информационной системы?
20.	Какие требования предъявляются к оформлению технических рисков в документации?
21.	Как определить приоритетность элементов документации при ее разработке?
22.	Как описать процессы установки и настройки системы в документации?
23.	Какие разделы документации наиболее важны для администраторов системы?
24.	Какую информацию необходимо указать в разделе "Обслуживание системы"?
25.	Как описывать процедуры аварийного восстановления в документации?
26.	Как описывать способы и процедуры мониторинга системы?
27.	Какие сведения о безопасности и защите данных необходимо включать в документацию?
28.	Какие рекомендации по эксплуатации системы должны быть включены в документацию?
29.	Как следует представлять информацию о совместимости с другими системами?
30.	Каковы особенности написания документации для масштабируемых систем?
ПК 5.7. Производить оценку информационной системы для выявления возможности ее модернизации.	
31.	Какие основные цели и задачи стоят перед процессом оценки информационной системы?
32.	Как определить, что информационная система нуждается в модернизации?
33.	Какие ключевые показатели эффективности системы нужно учитывать при оценке?

34.	Какую информацию необходимо собрать для проведения оценки информационной системы?
35.	Как проводится анализ производительности информационной системы?
36.	Какие метрики используются для оценки текущей архитектуры системы?
37.	Как оценить соответствие системы современным требованиям безопасности?
38.	Как анализировать уровень совместимости системы с другими компонентами?
39.	Какие проблемы могут возникать из-за устаревших технологий в информационной системе?
40.	Как анализировать влияние текущей системы на бизнес-процессы организации?
41.	Как выявить узкие места в работе информационной системы?
42.	Как оценить степень масштабируемости информационной системы?
43.	Какие критерии следует учитывать при оценке возможностей для интеграции новых технологий?
44.	Как анализировать возможности для автоматизации процессов в информационной системе?
45.	Какие инструменты и методы используются для мониторинга и оценки работы системы?