Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 02.11.2026 10:49:08
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 _23_ _05_ 2025 г. №10

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

«Интернет-программирование»
наименование дисциплины

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

«Информационные системы и технологии»
наименование образовательной программы

09.03.02 «Информационные системы и технологии»
шифр, наименование направления подготовки / специальности

Составители Яницкая Татьяна Сергеевна, к.т.н., доцент, 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
2025

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-6	Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий	ИОПК-6.2. Использует современные языки программирования для разработки алгоритмов и программ ИОПК-6.3. Владеет методами отладки и тестирования программ
ПК-2	Способен к выполнению работ по сопровождению и разработке прототипов ИС	ИПК-2.2. Разрабатывает прототип ИС в соответствии с требованиями
ПК-4	Способен к администрированию процесса управления сетевых устройств и программного обеспечения, настройки политики безопасности на сетевых устройствах	ИПК-4.2. Применяет методы задания базовых параметров и параметров защиты от несанкционированного доступа к операционным системам ИПК-4.5. Осуществляет протоколирование событий, возникающих в процессе функционирования администрируемых сетевых устройств и программного обеспечения

В результате изучения дисциплины обучающийся должен:

владеть навыками: навыками реализации, запуска, отладки и проверки работоспособности веб-приложения.; навыками разработки и документирования прототипа веб-информационной системы.; навыками документирования базовых параметров среды, анализа журнала событий и проверки результата изменения конфигурации.

уметь: разрабатывать клиентские и серверные компоненты веб-приложения, работать с DOM и API, выявлять и устранять программные ошибки, применять тесты.; превращать требования в структуру интерфейса, маршруты, модель данных и API, собирать работающий прототип и демонстрировать соответствие требованиям.; задавать базовые параметры защиты от несанкционированного доступа в пределах учебной среды, настраивать журналирование и использовать логи для диагностики.

знать: основы HTTP, HTML, CSS, JavaScript, клиент-серверного взаимодействия, асинхронного программирования, серверной обработки запросов, отладки и тестирования.; принципы прототипирования веб-ориентированной ИС, структуру пользовательских сценариев и критериев приемки.; базовые параметры среды и контроля доступа веб-приложения, назначение журналирования и состав событий, подлежащих фиксации.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Архитектура Web и протокол HTTP	ОПК-6 ПК-2 ПК-4
2.	HTML: семантическая структура и формы	ОПК-6 ПК-2
3.	CSS и адаптивный интерфейс	ОПК-6 ПК-2
4.	JavaScript, DOM и событийная модель	ОПК-6 ПК-2

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
5.	Асинхронное программирование, JSON и REST API	ОПК-6 ПК-2
6.	Серверная часть, маршрутизация и прототип ИС	ОПК-6 ПК-2
7.	Аутентификация, авторизация и базовая безопасность веб-приложения	ПК-4 ОПК-6
8.	Тестирование, отладка, журналирование и развертывание	ОПК-6 ПК-2 ПК-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 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, опросов).

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

Перечень вопросов и заданий для подготовки к зачету

ОПК-6. Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий

1. Клиент-серверная модель веб-приложения.
2. Основные компоненты клиент-серверного веб-приложения.
3. Принципы взаимодействия клиента и сервера в веб-приложении.
4. Структура HTTP-запроса.
5. Структура HTTP-ответа.
6. Методы HTTP и их назначение.
7. Методы GET, POST, PUT, PATCH и DELETE.
8. Коды состояния HTTP и их классификация.
9. Заголовки HTTP-запросов и HTTP-ответов.
10. DOM и его роль в клиентском веб-программировании.
11. Способы поиска и обращения к элементам DOM.
12. Изменение содержимого и структуры HTML-документа средствами JavaScript.
13. Событийная модель JavaScript.
14. Обработчики событий и распространение событий в DOM.
15. Функции в языке JavaScript.
16. Объекты и работа со свойствами объектов JavaScript.

17. Модули JavaScript и организация программного кода.
18. Асинхронное программирование в веб-приложениях.
19. Объект Promise и состояния асинхронной операции.
20. Цепочки Promise и обработка ошибок.
21. Конструкция async/await и особенности ее применения.
22. Fetch API для выполнения HTTP-запросов.
23. Обработка сетевых ошибок при использовании Fetch API.
24. JSON как формат обмена данными между клиентом и сервером.
25. Сериализация и десериализация данных JSON.
26. Отладка клиентского кода веб-приложения.
27. Отладка серверного кода веб-приложения.
28. Модульное тестирование компонентов веб-приложения.
29. Интеграционное тестирование клиентской и серверной частей веб-приложения.
30. Диагностика программных ошибок по наблюдаемому поведению, сообщениям об ошибках и журналам приложения.

ПК-2. Способен к выполнению работ по сопровождению и разработке прототипов ИС

1. Понятие прототипа информационной системы.
2. Назначение прототипирования при разработке информационных систем.
3. Виды прототипов информационных систем.
4. Требования к учебному веб-прототипу информационной системы.
5. Связь требований к системе и пользовательских сценариев.
6. Формирование пользовательских сценариев для веб-приложения.
7. Определение функциональности прототипа на основе требований.
8. Проектирование структуры страниц веб-прототипа.
9. Организация навигации между страницами веб-приложения.
10. Семантическая структура HTML-документа.
11. HTML-форма как средство реализации пользовательского ввода.
12. Основные элементы HTML-форм.
13. Клиентская валидация данных HTML-форм.
14. Обработка данных формы средствами JavaScript.
15. Принципы разработки адаптивного пользовательского интерфейса.
16. Использование медиазапросов при разработке адаптивных веб-интерфейсов.
17. Применение Flexbox и Grid при построении интерфейса веб-прототипа.
18. Понятие REST и основные принципы REST-архитектуры.
19. Проектирование REST API для прототипа информационной системы.
20. Определение ресурсов, маршрутов и HTTP-методов REST API.
21. Маршрутизация в серверном веб-приложении.
22. Обработка параметров маршрута и строки запроса.
23. Валидация пользовательских входных данных.
24. Валидация программных данных на серверной стороне.
25. Разделение клиентского, серверного и информационного слоев веб-приложения.
26. Организация взаимодействия клиентской и серверной частей прототипа.
27. Обработка ошибок и исключительных ситуаций в веб-приложении.
28. Документирование функциональных возможностей и ограничений учебного прототипа.
29. Проверка работоспособности прототипа по пользовательским сценариям.
30. Демонстрация соответствия разработанного прототипа заданным требованиям и критериям приемки.

ПК-4. Способен к администрированию процесса управления сетевых устройств и программного обеспечения, настройки политики безопасности на сетевых устройствах

1. Основные угрозы безопасности веб-приложений.
2. Понятие аутентификации пользователя в веб-приложении.
3. Понятие авторизации и ее отличие от аутентификации.
4. Основные способы аутентификации в веб-приложениях.
5. Сеансовая аутентификация и механизм пользовательских сессий.
6. Токенная аутентификация в веб-приложениях.
7. Управление правами и ролями пользователей веб-приложения.
8. Принцип наименьших привилегий при организации доступа.
9. Базовые параметры контроля доступа к ресурсам веб-приложения.
10. Проверка прав доступа на клиентской и серверной сторонах.
11. Назначение протокола HTTPS.
12. Принципы защиты сетевого взаимодействия с помощью TLS.
13. Отличия HTTP и HTTPS.
14. Сертификаты и их назначение при защищенном сетевом взаимодействии.
15. Понятие конфигурации среды веб-приложения.
16. Переменные окружения и их использование при настройке приложения.
17. Правила хранения конфигурационных параметров и секретов.
18. Риски хранения паролей, токенов и ключей непосредственно в программном коде.
19. Назначение журналирования событий веб-приложения.
20. Основные уровни журналирования.
21. Состав контекста события в журнале веб-приложения.
22. Журналирование ошибок клиентской и серверной частей приложения.
23. Использование журналов для диагностики программных и конфигурационных ошибок.
24. Журналирование неуспешных попыток аутентификации.
25. Журналирование ошибок авторизации и нарушений контроля доступа.
26. Документирование базовой конфигурации среды веб-приложения.
27. Документирование сетевых параметров и точек подключения веб-приложения.
28. Анализ последовательности событий по журналам приложения.
29. Проверка работоспособности веб-приложения после изменения конфигурации.

Проверка безопасности и корректности контроля доступа после изменения конфигурации среды приложения.