МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Колледж информационных и креативных технологий

РАБОЧАЯ ПРОГРАММА

МДК.03.05 Тестирование. Проектирование тестов

ПМ.03 Проектирование и разработка веб-приложений

программы подготовки специалистов среднего звена
специальность
09.02.11 Разработка и управление программным обеспечением

Форма обучения - очная

Владивосток 2026

Рабочая программа МДК.03.05 Тестирование. Проектирование тестов разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением, квалификация программист, утвержденного приказом Министерства просвещения Российской Федерации от 24 февраля 2025 г. № 138

Разработчик(и): Д.А. Трофимов, преподаватель

Рассмотрено и одобрено на заседании цикловой методической комиссии
Протокол № 9 от «20» мая 2026 г.

Председатель ПЦК _____ П.В. Калашников

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

1.1. Цель и место междисциплинарного курса в структуре образовательной программы

Междисциплинарный курс МДК.03.05 Тестирование. Проектирование тестов входит в профессиональный цикл учебного плана образовательной программы в структуру профессионального модуля ПМ.03 «Проектирование и разработка веб-приложений».

Цель: освоение современных методик проектирования тестов (тест-дизайна), проведения ручного и автоматизированного тестирования, аудита информационной безопасности, а также методов технического сопровождения и аварийного восстановления для обеспечения качества, надежности и отказоустойчивости веб-приложений.

1.2. Планируемые результаты освоения междисциплинарного курса

По итогам освоения курса, обучающиеся должны продемонстрировать результаты обучения, соотнесённые с результатами освоения ООП СПО, приведенные в таблице.

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Проектирование и разработка веб-приложений
ПК 3.3	Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием
ПК 3.4	Производить тестирование разработанного веб-приложения
ПК 3.5	Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности

В результате освоения междисциплинарного курса обучающийся должен:

Код ПК	Уметь	Знать	Владеть навыками
ПК 3.3	Выбирать хостинг в соответствии с параметрами веб-приложения. Составлять сравнительную характеристику хостингов и выделенного виртуального сервера. Понимать требования и потребности веб-приложений для выбора наиболее подходящего метода и технологии размещения. Выполнять настройки и конфигурации серверов для обеспечения стабильной работы веб-приложений. Способность мониторить и анализировать производительность веб-приложений для оптимизации и улучшения работы. Подключать и настраивать системы	Характеристики, типы и виды хостингов. Методы и способы передачи информации в сети Интернет. Устройство и работу хостинг-систем. Различные методы и технологии размещения веб-приложений, таких как виртуализация (VMware, Hyper-V), контейнеризация (Docker, Kubernetes), облачные платформы (AWS, Azure) и т.д. Принципы работы веб-серверов, баз данных и других необходимых компонентов для размещения веб-приложений. Методы безопасности и защиты данных при размещении веб-приложений в сети. Основные показатели использования Веб-приложений и способы их анализа. Регламенты работ по резервному копированию и	Установки и настройки веб серверов, СУБД для организации работы веб-приложений. Использования инструментальных средств контроля версий исходного кода и баз данных. Проведения работ по резервному копированию веб-приложений. Выполнения регистрации и обработки запросов заказчика в службе технической поддержки. Настройки и использования средств мониторинга состояния инфраструктуры, таких как Zabbix, Observium, Hakta Heartbeat и других. Создания и настройки мониторинговых шаблонов для отслеживания различных параметров и метрик инфраструктуры. Конфигурации и настройки уведомлений и оповещений для мониторинга состояния инфраструктуры. Анализа и интерпретации данных,

	мониторинга работы Веб-приложений и сбора статистики его использования. Устанавливать и настраивать веб сервера, СУБД для организации работы веб-приложений. Работать с системами Helpdesk. Выяснять из беседы с заказчиком и понимать причины возникших аварийных ситуаций с информационным ресурсом. Анализировать и решать типовые запросы заказчиков. выполнять регламентные процедуры по резервированию данных. Устанавливать прикладное программное обеспечение для резервирования веб приложений. Понимать принципы работы и архитектуры средств мониторинга состояния инфраструктуры. Настраивать мониторинговые параметры и метрики в соответствии с требованиями и потребностями инфраструктуры. Способность анализировать данные мониторинга и принимать действия для устранения	развертыванию резервной копий веб-приложений. способы и средства мониторинга работы веб-приложений. Методы развертывания веб-служб и серверов. Принципы организации работы службы технической поддержки. Общие основы решения практических задач по созданию резервных копий. Основные функциональные возможности и инструменты средств мониторинга, такие как Zabbix, Observium, Hakta Heartbeat и других. Принципы сбора и анализа данных мониторинга для выявления проблем и прогнозирования производительности инфраструктуры. Методы настройки и оптимизации средств мониторинга для достижения максимальной эффективности и точности данных.	собранных с помощью средств мониторинга, для выявления проблем и улучшения производительности. Публикации веб-приложения на базе хостинга или выделенного виртуального сервера в сети Интернет. Размещения веб-приложений в сети с использованием различных методов и технологий, таких как виртуализация, контейнеризация, облачные платформы и т.д. Настройки и конфигурации серверов для хостинга веб-приложений, включая установку необходимого программного обеспечения, настройку сетевых параметров и безопасности. Управления и мониторинга работы веб-приложений, включая отслеживание доступности и производительности, резервное копирование данных и обновление программного обеспечения. Решения проблем, связанных с размещением веб-приложений, таких как неполадки в работе серверов, сбои в сети или проблемы с безопасностью.
ПК 3.4	Выполнять отладку и тестирование программного кода (в том числе с использованием инструментальных средств). Выполнять оптимизацию и рефакторинг программного кода. Кодировать на скриптовых языках программирования.	Сетевые протоколы и основы web-технологий. Современные методики тестирования. Эргономику пользовательских интерфейсов. Основные принципы отладки и тестирования программных продуктов. Методы организации работы при проведении процедур тестирования.	Использования инструментальных средств контроля версий и баз данных, учета дефектов. Тестирования веб-приложений с точки зрения логической целостности. Тестирования интеграции веб-приложения с внешними сервисами и учетными системами

	Тестировать веб-приложения с использованием тест-планов. Применять инструменты подготовки тестовых данных. Выбирать и комбинировать техники тестирования веб-приложений. Работать с системами контроля версий в соответствии с регламентом использования системы контроля версий. Выполнять проверку веб-приложения по техническому заданию	Возможности используемой системы. Контроль версий и вспомогательных инструментальных программных средств для обработки исходного текста программного кода. Регламент использования системы контроля версий. Предметную область проекта для составления тест-планов	
ПК 3.5	Осуществлять аудит безопасности веб приложений. Модифицировать веб-приложение с целью внедрения программного кода по обеспечению безопасности его работы. Способность проводить аудит безопасности веб-приложений, используя различные инструменты и методы, такие как сканирование уязвимостей, тестирование на проникновение и анализ кода. Анализировать полученные результаты аудита и тестирования на проникновение для определения уязвимостей и рисков безопасности. Предоставлять отчеты и рекомендации по улучшению безопасности веб-приложений на основе проведенного аудита.	Источники угроз информационной безопасности и меры по их предотвращению. Регламенты и методы разработки безопасных веб-приложений. Различные инструменты и методы для проведения аудита безопасности веб-приложений, такие как сканеры уязвимостей (Nessus, OpenVAS), инструменты тестирования на проникновение (Metasploit, Burp Suite) и анализ кода (SonarQube). Основные уязвимости и риски безопасности веб-приложений, такие как инъекции, межсайтовый скриптинг, подделка запросов между сайтами и т.д. Знание методов и рекомендаций по устранению уязвимостей и повышению безопасности веб-приложений на основе результатов аудита.	Обеспечения безопасной и бесперебойной работы. Осуществления аудита безопасности веб-приложения в соответствии с регламентом по безопасности. Идентификации потенциальных уязвимостей и рисков безопасности веб-приложения. Проведения тестирования на проникновение для проверки уровня защиты веб-приложения. Анализ полученных результатов аудита и тестирования на проникновение для определения слабых мест и рекомендаций по их устранению

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

2.1 Объем МДК и виды учебной работы

Вид учебной работы	Объем в часах	В т.ч. в форме практ. подготовки

Учебные занятия	42	28
Самостоятельная работа	20	
Консультации	2	
Промежуточная аттестация	4	
Всего	**68**	**28**

2.2. Тематический план и содержание МДК

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Проектирование тестов и разработка тестовой документации		**22**	**ПК 3.4**
Тема 1.1. Основы обеспечения качества и техники проектирования тестов (Тест-дизайн)	**Содержание учебных материалов**	**3**	
	Жизненный цикл тестирования ПО (STLC), принципы тестирования, верификация и валидация веб-приложения на соответствие ТЗ.	1	ПК 3.4
	Классификация тестирования по уровням и видам: модульное (Unit), интеграционное, системное, сквозное (E2E), регрессионное и приёмочное.	1	ПК 3.4
	Техники проектирования тестов (тест-дизайна): эквивалентное разделение, анализ граничных значений, таблицы принятия решений, диаграммы переходов состояний и попарное тестирование (Pairwise).	1	ПК 3.4
	В том числе практических занятий	**4**	
	Анализ требований технического задания на тестируемость и выделение объектов проверки.	2	ПК 3.4
	Проектирование тестовых наборов данных с использованием техник классов эквивалентности, граничных значений и таблиц решений.	2	ПК 3.4
Тема 1.2. Разработка тестовой документации и управление жизненным циклом дефектов	**Содержание учебных материалов**	**3**	
	Структура и правила разработки плана тестирования (Test Plan), матрицы трассируемости требований (RTM) и чек-листов проверки.	1	ПК 3.4
	Проектирование и оформление тестовых сценариев (Test Cases) и тестовых наборов (Test Suites) в системах управления тестированием (TMS).	1	ПК 3.4
	Жизненный цикл дефекта, классификация ошибок по критичности (Severity) и приоритету (Priority), правила составления отчётов об ошибках (Bug Reports).	1	ПК 3.4

	В том числе практических занятий	**6**	
	Разработка чек-листов и детализированных тест-кейсов для ключевых модулей веб-приложения на основе технического задания.	4	ПК 3.4
	Локализация дефектов в веб-приложении и оформление баг-репортов в системе баг-трекинга.	2	ПК 3.4
	В том числе самостоятельная работа обучающихся Разработка плана тестирования (Test Plan) и матрицы покрытия требований для заданного веб-приложения.	**5**	**ПК 3.4**
Раздел 2. Проведение тестирования, аудит безопасности и техническое сопровождение веб-приложений		**40**	**ПК 3.3, ПК 3.4, ПК 3.5**
Тема 2.1. Функциональное, интеграционное и автоматизированное тестирование веб-приложений	**Содержание учебных материалов**	**2**	
	Методика функционального (UI/UX), интеграционного (REST API, GraphQL в Postman) и нагрузочного тестирования веб-приложений (JMeter, Lighthouse).	1	ПК 3.4
	Архитектура автоматизированного тестирования: модульные и компонентные тесты (Jest, Mocks) и сквозные E2E-автотесты в браузере (Cypress / Playwright / Selenium).	1	ПК 3.4
	В том числе практических занятий	**6**	
	Проведение функционального тестирования интерфейса и тестирования REST API веб-приложения с использованием коллекций и автотестов в Postman.	2	ПК 3.4
	Разработка и запуск модульных (Unit) и сквозных (E2E) автоматизированных тестов для проверки ключевых сценариев веб-приложения.	4	ПК 3.4
	В том числе самостоятельная работа обучающихся Проведение нагрузочного и кроссбраузерного тестирования веб-приложения и составление сводного отчёта о качестве.	**5**	**ПК 3.4**
Тема 2.2. Аудит безопасности и тестирование защищённости веб-приложений	**Содержание учебных материалов**	**3**	
	Регламенты безопасности веб-приложений и методика тестирования уязвимостей из перечня OWASP Top 10 (XSS, CSRF, SQL-инъекции, небезопасная десериализация).	1	ПК 3.5
	Проектирование тестов безопасности для проверки механизмов аутентификации, управления сессиями (JWT, Cookies), ролевого доступа, политик CORS и заголовков CSP.	1	ПК 3.5
	Инструменты автоматизированного аудита безопасности: статический и	1	ПК 3.5

	динамический анализ (SAST/DAST, OWASP ZAP) и аудит уязвимостей сторонних пакетов (npm audit).		
	В том числе практических занятий	**6**	
	Проведение аудита безопасности и тестирования форм ввода и API веб-приложения на наличие уязвимостей (XSS, SQLi, CSRF, обход авторизации).	4	ПК 3.5
	Выполнение автоматизированного сканирования зависимостей и конфигурации веб-приложения на соответствие регламенту по безопасности.	2	ПК 3.5
	В том числе самостоятельная работа обучающихся Составление регламентного отчёта по результатам аудита безопасности веб-приложения и плана устранения выявленных уязвимостей.	**5**	**ПК 3.5**
Тема 2.3. Техническое сопровождение, мониторинг и восстановление веб-приложений	**Содержание учебных материалов**	**3**	
	Организация технического сопровождения веб-приложений по ТЗ: регламенты поддержки (SLA), мониторинг доступности (Health Checks), сбор метрик и логирование ошибок.	1	ПК 3.3
	Диагностика сбоев в промышленной эксплуатации, анализ логов сервера и клиента, порядок выпуска патчей и отката неисправных обновлений (Rollback).	1	ПК 3.3
	Стратегии резервного копирования (полное, инкрементальное, дифференциальное) и процедуры аварийного восстановления (Disaster Recovery) кода, конфигураций и БД веб-приложения.	1	ПК 3.3
	В том числе практических занятий	**6**	
	Настройка системы логирования и мониторинга работоспособности веб-приложения, диагностика причин искусственно вызванного сбоя.	2	ПК 3.3
	Выполнение резервного копирования и полного восстановления веб-приложения и его базы данных после сбоя с проведением пост-аварийного дымового тестирования (Smoke Test).	4	ПК 3.3
	В том числе самостоятельная работа обучающихся Разработка регламента технического сопровождения и плана аварийного восстановления (Disaster Recovery Plan) веб-приложения по ТЗ.	**5**	**ПК 3.3**
Консультации		**2**	**ПК 3.3, ПК 3.4, ПК 3.5**
Промежуточная аттестация		**4**	**ПК 3.3, ПК 3.4, ПК 3.5**

Всего		**68**	**ПК 3.3, ПК 3.4, ПК 3.5**

3. УСЛОВИЯ РЕАЛИЗАЦИИ МЕЖДИСЦИПЛИНАРНОГО КУРСА

3.1. Материально-техническое обеспечение

Для реализации программы МДК.03.05 «Тестирование. Проектирование тестов» предусмотрено наличие следующих помещений:

Лаборатория организации и принципов построения информационных систем.

Основное оборудование: Компьютеризированные рабочие места обучающихся с выходом в сеть "Интернет" - 20 шт., стулья - 20 шт., комплект мебели (стол и стул) для преподавателя - 1 шт., графические станции ПК №2 WorkStation WS 917 20 шт., автоматизированное рабочее место преподавателя ПК №2 WorkStation WS 917, графический планшет Wacom - 20 шт., мультимедийное оборудование - 1 шт., телевизор, экран, многофункциональное устройство (МФУ) формат А3 -1 шт., доска маркерная - 1 шт.

Программное обеспечение: PyCharm, Visual Studio Code, IntelliJ IDEA, JetBrains Rider, Python (Anaconda3) с TensorFlow/PyTorch, Microsoft Visio, Draw.io, Figma, Figma, Adobe Illustrator, MySQL Workbench, HeidiSQL, MySQL, PostgreSQL, Git, Docker Desktop, Microsoft Project, Draw.io, Microsoft SQL Server Management Studio, Microsoft Office.

Основное оборудование: Рабочие места на базе компьютерной техники с возможностью подключения к информационно-телекоммуникационной сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ВВГУ: комплекты учебной мебели (столы и стулья) – 19 шт., персональные компьютеры (облачные мониторы) - 19 шт; доска маркерная - 1шт., лазерный копир-принтер-сканер с 2 лотками Xerox WorkCentre 3345 DNI.

Программное обеспечение: Microsoft Windows 7 Professional; Microsoft Office ProPlus 2010 Russian Acdmc; СПС КонсультантЮрист: Версия Проф; Adobe Acrobat Reader; Google Chrome; Adobe Flash Player; 7-Zip 18.01 (x64).

3.2. Учебно-методическое обеспечение

Для реализации программы учебной дисциплины библиотечный фонд ВВГУ укомплектован печатными и электронными изданиями.

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Основные источники

1. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 273 с. — (Профессиональное образование). — ISBN 978-5-534-20362-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562355

2. Грекул, В. И. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 404 с. — (Профессиональное образование).
— ISBN 978-5-534-19506-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/566739

3. Соколова, В. В. Разработка мобильных приложений : учебное пособие для среднего профессионального образования / В. В. Соколова. — Москва : Издательство Юрайт, 2024. —160 с. — (Профессиональное образование). — ISBN 978-5-534-16868-6. —

Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542342

Дополнительные источники

1. Черпаков, И. В. Основы программирования : учебник и практикум для среднего профессионального образования / И. В. Черпаков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 196 с. — (Профессиональное образование). — ISBN 978-5-534- 18760-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561922

2. Зыков, С. В. Объектно-ориентированное программирование : учебник и практикум для вузов / С. В. Зыков. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 151 с. — (Высшее образование). — ISBN 978-5-534-16941-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537385

3. Станкевич, Л. А. Интеллектуальные системы и технологии : учебник и практикум для среднего профессионального образования / Л. А. Станкевич. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 478 с. — (Профессиональное образование). — ISBN 978-5-534-20364-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/566524

Электронные ресурсы

1. Информационно-справочная система «Консультант Плюс» – http://www.consultant.ru/
2. Профессиональная база данных: "Открытая база ГОСТов"/ Режим доступа: http://standartgost.ru/, доступ свободный
3. Электронная библиотечная система «РУКОНТ» - Режим доступа: https://lib.rucont.ru/
4. Электронная библиотечная система ZNANIUM.COM - Режим доступа: https://znanium.com/
5. Электронно-библиотечная система издательства "Юрайт" - Режим доступа: https://urait.ru/
6. Электронно-библиотечная система издательства "Лань" - Режим доступа: https://e.lanbook.com/
7. Президентская библиотека им. Б.Н. Ельцина (база данных различных профессиональных областей) Режим доступа: https://www.prlib.ru/, доступ свободный

4 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ИЗУЧЕНИЮ И РЕАЛИЗАЦИИ МЕЖДИСЦИПЛИНАРНОГО КУРСА

Начиная изучение дисциплины, студенту необходимо:

- ознакомиться с программой, изучить список рекомендуемой литературы;
- внимательно разобраться в структуре курса, в системе распределения учебного материала по видам занятий, формам контроля, чтобы иметь представление о курсе в целом.

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. Кроме того, для расширения и углубления знаний по дисциплине целесообразно использовать: публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза. Успешное освоение дисциплины предполагает активную

работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу.

4.1 Методические рекомендации обучающимся по обеспечению самостоятельной работы

Самостоятельная работа проводится с целью: систематизации, закрепления, углубления и расширения теоретических знаний и практических умений, приобретаемых студентами в ходе аудиторных занятий; формирования умений использовать специальную литературу; развития познавательных способностей и активности обучающихся; формирования самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации; развития исследовательских умений.

Для лучшего освоения материала и систематизации знаний по дисциплине необходимо отвечать на вопросы для самоконтроля. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. В случае необходимости обращаться к преподавателю за консультацией. Студент должен четко уяснить, что именно с лекции начинается его подготовка к практическому занятию. Вместе с тем, лекция лишь организует мыслительную деятельность, но не обеспечивает глубину усвоения программного материала.

При подготовке к практическому занятию особое внимание необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. В процессе подготовки рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь.

При необходимости следует обращаться за консультацией к преподавателю. Перед консультацией, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса. Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций.

4.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КУРСА

Код ПК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки

ПК.3.3	Оценка «отлично»: техническое сопровождение, настройка мониторинга, резервное копирование и восстановление веб-приложения после сбоя выполнены в полном соответствии с ТЗ и в нормативные сроки. Оценка «хорошо»: процедуры сопровождения и восстановления веб-приложения выполнены в соответствии с ТЗ, но имеются незначительные неточности в настройке логирования или скриптах резервного копирования. Оценка «удовлетворительно»: техническое сопровождение и восстановление веб-приложения выполнены частично, устранены только базовые сбои с нарушением регламента.	Проверка выполнения практических работ по диагностике сбоев, резервному копированию и восстановлению веб-приложения, защита регламента сопровождения.
ПК.3.4	Оценка «отлично»: проектирование тестов с применением техник тест-дизайна, разработка тестовой документации (тест-кейсов, баг-репортов) и проведение ручного и автоматизированного тестирования веб-приложения выполнены в полном объёме и без ошибок. Оценка «хорошо»: тестовая документация и тестирование веб-приложения выполнены в соответствии с методикой, но допускаются мелкие недочёты в тестовом покрытии или оформлении автотестов. Оценка «удовлетворительно»: проектирование тестов и тестирование веб-приложения выполнены частично, проверены только базовые позитивные сценарии.	Защита отчётов по практическим работам, экспертная оценка разработанных тест-планов, тест-кейсов, баг-репортов и работающих автотестов.
ПК.3.5	Оценка «отлично»: аудит безопасности и тестирование защищённости веб-приложения проведены в полном соответствии с регламентом по безопасности, все уязвимости выявлены и задокументированы корректно. Оценка «хорошо»: аудит безопасности выполнен в соответствии с регламентом, но имеются мелкие неточности в классификации угроз или оформлении отчёта об уязвимостях. Оценка «удовлетворительно»: аудит безопасности веб-приложения проведён поверхностно, выявлены только базовые несоответствия регламенту.	Проверка практических заданий по проведению аудита безопасности, защита отчёта о выявленных уязвимостях и контроль на зачёте / экзамене.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Колледж информационных и креативных технологий

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации

по **МДК 03.05 Тестирование. Проектирование тестов**

ПМ.03 Проектирование и разработка веб-приложений

программы подготовки специалистов среднего звена
09.02.11 Разработка и управление программным обеспечением

Форма обучения: очная

Владивосток 2026

1. Общие сведения

Фонд оценочных средств (далее – ФОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу МДК.03.05 «Тестирование. Проектирование тестов» в соответствии с техническим заданием и оценка их качества

ФОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта (с использованием оценочного средства - устный опрос в форме ответов на вопросы билетов, устный опрос в форме собеседования, выполнение письменных заданий, тестирование и т.д.).

2. Планируемые результаты обучения, обеспечивающие результаты освоения образовательной программы

Код ПК	Код результата обучения	Наименование результата обучения
ПК 3.3	З1	Регламенты технического сопровождения, мониторинга работоспособности и поддержки жизненного цикла веб-приложений в соответствии с техническим заданием.
	З2	Методы анализа журналов событий (логов), диагностики сбоев, стратегии резервного копирования (Backup) и аварийного восстановления (Disaster Recovery) веб-приложений.
	З3	Порядок выпуска и установки обновлений (патчей, хотфиксов), управления конфигурацией и отката версий (Rollback) при сбоях в работе веб-приложения.
	У1	Осуществлять мониторинг доступности и производительности веб-приложения, анализировать логи ошибок и выявлять причины технических сбоев.
	У2	Выполнять резервное копирование и полное восстановление работоспособности веб-приложения и его баз данных после нештатных ситуаций в соответствии с ТЗ.
	У3	Проводить плановое техническое обслуживание, обновление компонентов и послеаварийную проверку веб-приложения.
	П1	Технического сопровождения, мониторинга работоспособности и диагностики сбоев веб-приложений в соответствии с техническим заданием.
	П2	Резервного копирования, восстановления работоспособности и обновления веб-приложений после технических сбоев.
ПК 3.4	З1	Методологии обеспечения качества (QA), виды и уровни тестирования веб-приложений (модульное, интеграционное, системное, сквозное E2E, регрессионное и нагрузочное).
	З2	Техники проектирования тестов / тест-дизайна (классы эквивалентности, граничные значения, таблицы решений, попарное тестирование) и стандарты оформления тестовой документации.
	З3	Инструменты функционального, API, нагрузочного и автоматизированного тестирования веб-приложений (Jest, Cypress/Playwright, Postman, JMeter).
	У1	Применять техники тест-дизайна для проектирования тестовых сценариев, разрабатывать планы тестирования (Test Plan), тест-кейсы и чек-листы на основе ТЗ.
	У2	Производить ручное и автоматизированное тестирование пользовательского интерфейса, клиент-серверного взаимодействия (API) и производительности веб-приложения.

Код ПК	Код результата обучения	Наименование результата обучения
	У3	Выявлять, локализовывать и документировать дефекты в баг-трекинговых системах (баг-репорты), выполнять повторное (Re-test) и регрессионное тестирование.
	П1	Проектирования тестов с применением формальных техник тест-дизайна и разработки тестовой документации по техническому заданию.
	П2	Проведения комплексного (ручного и автоматизированного) тестирования разработанного веб-приложения и управления дефектами.
ПК 3.5	З1	Регламенты обеспечения безопасности веб-приложений и классификацию основных уязвимостей (OWASP Top 10: XSS, CSRF, SQL-инъекции, ошибки авторизации и конфигурации).
	З2	Методики проектирования тестов безопасности (Security Testing), проведения статического и динамического анализа (SAST/DAST) и аудита сторонних зависимостей.
	У1	Проводить аудит безопасности веб-приложения, его API и серверной конфигурации в соответствии с регламентом по безопасности.
	У2	Проектировать и выполнять тесты на проникновение (проверку форм ввода, сессий, токенов доступа и политик CORS/CSP) и составлять отчёт по результатам аудита.
	П1	Проведения аудита безопасности и тестирования защищённости веб-приложений в соответствии с регламентом по безопасности.
	П2	Выявления уязвимостей, проверки надежности механизмов защиты и составления регламентной отчётности по безопасности веб-приложения.

3. Описание процедуры оценивания

Результаты обучения по модулю, уровень сформированности компетенций оцениваются по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» (по бальной системе. Максимальная сумма баллов по дисциплине равна 100 баллов.)

Текущая аттестация по модулю проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по модулю результатов обучения, обеспечивающих результаты освоения образовательной программы в целом. Оценка на зачете / экзамене выставляется с учетом оценок, полученных при прохождении текущей аттестации.

Критерии оценивания устного ответа

(оценочные средства: контрольная работа, собеседование, устное сообщение.)

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры;

свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

(оценочные средства: реферат, конспект, контрольная работа, письменный отчет по практической работе, портфолио, доклад (сообщение), в том числе выполненный в форме презентации, творческое задание, курсовая работа).

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно

Количество правильных ответов	91 % и ≥	от 81% до 90,9 %	не менее 70%	менее 70%

Критерии выставления оценки студенту на зачете/ экзамене

(оценочные средства: устный опрос в форме ответов на вопросы билетов, устный опрос в форме собеседования, выполнение письменных разноуровневых задач и заданий, комплексная расчетно-графическая работа, творческое задание, кейс-задача, портфолио, проект и т.п.)

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

4. Примеры оценочных средств для проведения промежуточной аттестации

Вопросы для дифференцированного зачета

1. Что такое обеспечение качества (QA), контроль качества (QC) и тестирование ПО? В чём разница между верификацией и валидацией?
2. Из каких этапов состоит жизненный цикл тестирования программного обеспечения (STLC)?
3. Перечислите и раскройте 7 базовых принципов тестирования ПО (ISTQB).
4. Как классифицируется тестирование по знанию внутренней структуры системы (методы «чёрного», «белого» и «серого» ящика)?
5. Что такое «пирамида тестирования»? Опишите назначение модульного (Unit), интеграционного и сквозного (E2E) уровней тестирования.
6. В чём разница между дымовым (Smoke), санитарным (Sanity) и регрессионным (Regression) тестированием?

7. Что такое тест-дизайн и зачем применяются формальные техники проектирования тестов?
8. В чём заключается суть техник тест-дизайна «Классы эквивалентности» (Equivalence Partitioning) и «Анализ граничных значений» (Boundary Value Analysis)?
9. Как проектируются тесты с использованием таблицы принятия решений (Decision Table) и диаграммы переходов состояний (State Transition)?
10. В чём суть комбинаторной техники попарного тестирования (Pairwise Testing) и когда она применяется?
11. Что такое план тестирования (Test Plan) и какие обязательные разделы в него входят по стандарту IEEE 829 / ISO 29119?
12. Что такое матрица трассируемости требований (RTM) и как она помогает оценить тестовое покрытие ТЗ?
13. Из каких атрибутов состоит тест-кейс (Test Case) и в каких случаях выгоднее использовать чек-листы?
14. Каков жизненный цикл дефекта (Bug Life Cycle) в баг-трекинговой системе?
15. Правила оформления баг-репорта: чем отличается серьёзность (Severity) дефекта от его приоритета (Priority)? Приведите примеры.
16. Какие особенности включает в себя тестирование пользовательского интерфейса (UI/UX), адаптивности и кроссбраузерности веб-приложений?
17. Как проводится тестирование REST API (проверка HTTP-методов, кодов ответа, структуры JSON, граничных параметров и времени отклика)?
18. В чём разница между нагрузочным (Load), стрессовым (Stress), объёмным (Volume) тестированием и тестированием стабильности (Soak)?
19. Как устроено модульное тестирование (Unit Testing) на примере Jest? Зачем используются заглушки, стабы и моки (Mocks / Stubs)?
20. Как проектируются и запускаются сквозные (E2E) автоматизированные тесты веб-интерфейсов (на примере Cypress / Playwright)? Что такое паттерн Page Object Model?
21. Что представляет собой регламент по безопасности веб-приложения и каковы этапы проведения аудита безопасности?
22. Что такое стандарт OWASP Top 10? Назовите основные категории уязвимостей современных веб-приложений.
23. Как проектируются тесты для выявления уязвимости межсайтового скриптинга (XSS: отражённый, хранимый, DOM-based)?
24. Как возникают SQL-инъекции (SQLi) и какими тестовыми векторами проверяется защищённость форм ввода и параметров URL?
25. В чём суть уязвимости межсайтовой подделки запросов (CSRF) и как проверить наличие и корректность CSRF-защиты?
26. Что такое уязвимости нарушения контроля доступа (Broken Access Control / IDOR) и как они выявляются при тестировании API?
27. Как проводится аудит безопасности механизмов аутентификации, восстановления пароля и защиты от перебора (Brute-force)?
28. На какие уязвимости проверяются JWT-токены и сессионные куки (флаги HttpOnly, Secure, SameSite, время жизни токена)?
29. Как проверить правильность настройки политик безопасности браузера CORS и заголовков защиты контента (CSP, X-Frame-Options, HSTS)?
30. В чём разница между статическим (SAST) и динамическим (DAST) анализом защищённости веб-приложения?
31. Как проводится аудит безопасности сторонних библиотек и зависимостей проекта (SCA, npm audit) на наличие известных CVE-уязвимостей?

32. Что такое фаззинг-тестирование (Fuzzing) и как оно применяется при аудите безопасности API?
33. Какова структура итогового отчёта по результатам аудита безопасности веб-приложения и как оценивается риск уязвимостей (шкала CVSS)?
34. Что включает в себя техническое сопровождение веб-приложения после ввода в эксплуатацию и какие виды сопровождения существуют?
35. Что такое соглашение об уровне обслуживания (SLA) и какие показатели надёжности (Uptime, MTBF, MTTR) в нём фиксируются?
36. Как организуется система мониторинга работоспособности веб-приложения (Health Checks, мониторинг ресурсов сервера, доступности эндпоинтов)?
37. Зачем нужно централизованное логирование событий в веб-приложении и какие уровни логов (DEBUG, INFO, WARN, ERROR, FATAL) используются для диагностики?
38. Каков порядок действий инженера сопровождения при возникновении критического инцидента (сбоя) в работе веб-приложения?
39. Что такое показатели RPO (Recovery Point Objective) и RTO (Recovery Time Objective) при планировании восстановления после сбоев?
40. Сравните основные виды резервного копирования: полное (Full), инкрементальное (Incremental) и дифференциальное (Differential).
41. В чём заключается правило резервного копирования «3-2-1» и как проверяется целостность созданных бэкапов?
42. Каков алгоритм полного восстановления веб-приложения и его базы данных из резервной копии после аварийного сбоя?
43. Как безопасно устанавливать обновления и хотфиксы (Hotfixes) на работающее веб-приложение и как выполнить быстрый откат версии (Rollback)?
44. Какие стратегии развёртывания (Blue-Green Deployment, Canary Release) позволяют минимизировать риски простоя при сопровождении веб-приложения?
45. Зачем после проведения аварийного восстановления или обновления обязательно выполняется дымовое (Smoke) и регрессионное тестирование?

Экзаменационные билеты

Билет 1

1. Жизненный цикл тестирования ПО (STLC), базовые принципы тестирования и отличие верификации от валидации.
2. Проанализируйте фрагмент технического задания на модуль «Оформление доставки», выявите в требованиях неоднозначности и противоречия и сформулируйте вопросы к аналитику/заказчику.

Билет 2

1. Техники тест-дизайна: эквивалентное разделение (EP) и анализ граничных значений (BVA).
2. Спроектируйте минимально достаточный набор тестовых значений (позитивных и негативных) для поля ввода «Возраст заёмщика» (по ТЗ кредит выдаётся лицам от 21 до 65 лет включительно, при сумме от 10 000 до 500 000 руб.).

Билет 3

1. Техники тест-дизайна: таблицы принятия решений (Decision Table) и диаграммы переходов состояний (State Transition).

2. Составьте таблицу принятия решений и тест-кейсы для модуля расчёта скидки интернет-магазина (условия: наличие клубной карты, сумма заказа свыше 5000 руб., промокод первого заказа).

Билет 4

1. Комбинаторные техники проектирования тестов: попарное тестирование (Pairwise Testing).
2. Спроектируйте проверочную таблицу методом попарного тестирования для проверки кроссбраузерной совместимости веб-приложения (3 ОС, 3 браузера, 2 разрешения экрана, 2 темы оформления).

Билет 5

1. Структура и правила разработки тестовой документации: план тестирования (Test Plan), чек-листы и тест-кейсы (Test Cases).
2. Разработайте чек-лист из 10 проверок и 3 детализированных тест-кейса (с предусловиями, шагами, тестовыми данными и ожидаемым результатом) для модуля «Восстановление пароля по Email».

Билет 6

1. Жизненный цикл дефекта. Правила оформления баг-репортов и классификация ошибок по серьёзности (Severity) и приоритету (Priority).
2. По описанию найденных в веб-приложении 4 различных дефектов определите для каждого связку Severity / Priority, обоснуйте выбор и оформите один полный баг-репорт по стандарту.

Билет 7

1. Методика тестирования клиент-серверного взаимодействия и REST API веб-приложений.
2. Спроектируйте набор тестов (проверка статус-кодов, JSON-схемы, позитивных и негативных сценариев) для тестирования эндпоинта POST /api/v1/users (создание пользователя).

Билет 8

1. Архитектура модульного (Unit) и интеграционного тестирования кода веб-приложения. Использование заглушек (Mocks / Stubs).
2. Напишите модульные тесты (на базе Jest) для функции расчёта стоимости корзины с учётом промокода, налогов и граничных случаев (пустая корзина, некорректный промокод, отрицательная цена).

Билет 9

1. Автоматизация сквозного (E2E) тестирования веб-интерфейсов и паттерн проектирования Page Object Model (POM).
2. Спроектируйте структуру Page Object класса и напишите сценарий E2E-теста (на базе Cypress / Playwright) для проверки авторизации пользователя и перехода в личный кабинет.

Билет 10

1. Нефункциональное тестирование веб-приложений: нагрузочное, стрессовое и тестирование стабильности. Основные метрики производительности (RPS, Response Time, Error Rate).
2. Разработайте профиль нагрузки и план проведения нагрузочного тестирования веб-сервиса продажи билетов перед стартом крупной распродажи.

Билет 11

1. Регламент по безопасности веб-приложений и методика проведения аудита безопасности по стандарту OWASP Top 10.
2. Составьте чек-лист аудита безопасности для модуля «Форма обратной связи с загрузкой файлов» и укажите, какие типы атак возможны при отсутствии фильтрации.

Билет 12

1. Методика проектирования тестов безопасности для выявления межсайтового скриптинга (XSS) и инъекций (SQLi).
2. Проанализируйте предложенный уязвимый код обработчика поискового запроса веб-приложения, составьте тестовые векторы (Payloads) для демонстрации уязвимостей XSS и SQLi и опишите способ их закрытия.

Билет 13

1. Уязвимости контроля доступа (IDOR, Broken Access Control) и межсайтовая подделка запросов (CSRF): методы тестирования и защиты.
2. Спроектируйте сценарий тестирования безопасности API личного кабинета на уязвимость IDOR (попытка чтения и изменения чужого профиля путём подмены ID в запросе) и предложите архитектурное исправление.

Билет 14

1. Аудит безопасности механизмов аутентификации, управления сессиями (JWT, Cookies) и политик браузера (CORS, CSP).
2. Проведите аудит HTTP-заголовков ответа и настроек Cookie предложенного веб-приложения, выявите нарушения регламента безопасности и составьте корректную конфигурацию заголовков (Content-Security-Policy, Strict-Transport-Security, Set-Cookie).

Билет 15

1. Инструменты автоматизированного аудита безопасности: статический и динамический анализ (SAST/DAST) и проверка зависимостей (npm audit).
2. Проанализируйте лог проверки уязвимостей сторонних пакетов веб-проекта, классифицируйте угрозы по шкале критичности и составьте отчёт по результатам аудита с планом обновления и патчинга.

Билет 16

1. Организация технического сопровождения веб-приложений в соответствии с ТЗ: соглашение SLA, метрики надёжности (MTBF, MTTR) и регламент обработки инцидентов.
2. Разработайте регламент классификации и эскалации технических инцидентов (3 уровня критичности) с указанием времени реакции и восстановления работоспособности веб-приложения.

Билет 17

1. Мониторинг работоспособности и анализ журналов событий (логов) веб-приложения для диагностики технических сбоев.
2. Проанализируйте фрагмент лог-файла веб-сервера и приложения в момент отказа системы (ошибки 502/504, переполнение пула соединений БД), определите первопричину сбоя и составьте алгоритм устранения.

Билет 18

1. Стратегии резервного копирования веб-приложений и баз данных (полное, инкрементальное, дифференциальное). Показатели RPO и RTO.
2. Спроектируйте расписание и схему резервного копирования для высоконагруженного интернет-магазина с требованиями ТЗ: допустимая потеря данных (RPO) — не более 15 минут, время восстановления (RTO) — не более 1 часа.

Билет 19

1. Процедура аварийного восстановления (Disaster Recovery) веб-приложения после критического сбоя сервера или повреждения данных.
2. Составьте пошаговый технический план (Disaster Recovery Plan) развёртывания резервной копии веб-приложения и восстановления базы данных с проверкой целостности данных.

Билет 20

1. Управление обновлениями при техническом сопровождении веб-приложений: выпуск патчей, стратегии безопасного развёртывания (Blue-Green, Canary) и откат версий (Rollback).
2. Разработайте алгоритм действий инженера сопровождения при неудачном обновлении веб-приложения на продуктивном сервере: порядок отката релиза (Rollback) и чек-лист пост-аварийного дымового тестирования (Smoke Test).