

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Красноярский филиал Финуниверситета

УТВЕРЖДАЮ

Заместитель директора
по учебно – методической работе
Красноярского филиала
Финуниверситета

В.Ч. О.С. Вергейчик
«02» апреля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по профессиональному модулю

**ПМ. 02 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА И АДМИНИСТРИРОВАНИЕ
ИНФОРМАЦИОННЫХ РЕСУРСОВ**

(код, наименование)

09.02.09 Веб-разработка

(код, наименование специальности)

г. Красноярск – 2026

Фонд оценочных средств по профессиональному модулю ПМ. 02 Техническая поддержка и администрирование информационных ресурсов разработан на основании федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.09 Веб-разработка

Составители:

Цирулькевич Алена Викторовна, преподаватель

Фонд оценочных средств по дисциплине рассмотрен и рекомендован к утверждению на заседании предметной (цикловой) комиссии общепрофессиональных дисциплин.

Протокол от «02» апреля 2026 г. № 8

Председатель предметной (цикловой)
комиссии


(подпись)

О.А. Полтавец
(инициалы, фамилия)

**1. Паспорт фонда оценочных средств
по профессиональному модулю ПМ.02 Техническая поддержка и
администрирование информационных ресурсов**

Результаты обучения (знания, умения)	Общие и профессиональные компетенции	Наименование элементов профессионального модуля, раздела, темы	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> - подготовки программной среды для функционирования веб-приложения; - организации и обеспечения функционирования подсистемы резервного копирования и восстановления. <p>Уметь:</p> <ul style="list-style-type: none"> - соблюдать процедуру установки прикладного ПО; - идентифицировать инциденты при установке ПО; - производить настройку параметров веб-сервера; - устанавливать СУБД. <p>Знать:</p> <ul style="list-style-type: none"> - принципы устройства и функционирования информационных ресурсов; - принципы устройства и функционирования программных средств и платформ для разработки веб-ресурсов; - современные стандарты взаимодействия компонентов распределенных приложений. 	<p>ОК 01 – 09 ПК 2.1 ПК 2.2</p>	<p>МДК 02.01 Настройка и сопровождение информационных ресурсов</p> <p>Раздел 1. Настройка и сопровождение информационных ресурсов - Тема 1.1 Установка прикладного программного обеспечения и модулей информационных ресурсов, включая их настройку.</p>	<p>- Защита практических работ №1-6 по теме 1.1. - Выполнение и защита индивидуальных заданий (СР). - Экспертное наблюдение за выполнением заданий.</p>	<p>Дифференцированный зачет по МДК 02.01</p>
<p>Иметь практический</p>	<p>ОК 01 – 09</p>	<p>МДК 02.02 Обеспечение</p>	<p>- Защита практических</p>	<p>Дифференцированный зачет по МДК 02.02</p>

<p>опыт:</p> <ul style="list-style-type: none"> - настройки прав доступа пользователя в существующей системе; - работы с инструментами мониторинга безопасности ИР; - выполнения типовых регламентных процедур по защите ИР. <p>Уметь:</p> <ul style="list-style-type: none"> - идентифицировать права пользователей в зависимости от функционала; - регламентировать уровни прав и ролей; - применять регламентные процедуры управления доступом. <p>Знать:</p> <ul style="list-style-type: none"> - основы информационной безопасности веб-ресурсов; - принципы использования электронно-цифровых подписей; - инструменты и методы коммуникаций. 	<p>ПК 2.3 ПК 2.4 ПК 2.5</p>	<p>безопасности информационных ресурсов</p> <p>Раздел 2. Обеспечение безопасности информационных ресурсов</p> <ul style="list-style-type: none"> - Тема 2.1 Резервное копирование и развертывание резервной копии. - Тема 2.2 Настройка прав пользователей. - Тема 2.3 Применение программных средств обеспечения безопасности. 	<p>работ №1-3 по темам 2.1, 2.2, 2.3.</p> <ul style="list-style-type: none"> - Выполнение и защита индивидуальных заданий (СР). - Экспертное наблюдение за выполнением заданий. 	
<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> - подготовки программной среды; - организации резервного копирования; - настройки прав доступа; - работы с инструментами мониторинга безопасности; - выполнения регламентных процедур по защите ИР. 	<p>ОК 01 – 09 ПК 2.1 – ПК 2.5</p>	<p>Учебная практика Производственная практика</p>	<ul style="list-style-type: none"> - Защита отчетов по практике. - Экспертное наблюдение за выполнением работ. 	<p>Дифференцированный зачет Дифференцированный зачет</p>

2. Формы промежуточной аттестации по профессиональному модулю

Элементы профессионального модуля	Формы промежуточной аттестации
МДК 02.01 Настройка и сопровождение информационных ресурсов	Дифференцированный зачет
МДК 02.02 Обеспечение безопасности информационных ресурсов	Дифференцированный зачет
Учебная практика	Дифференцированный зачет
Производственная практика (по профилю специальности)	Дифференцированный зачет
ПМ	Экзамен по модулю

3. Комплект оценочных средств

1. Для текущего контроля успеваемости

МДК.02.01 Настройка и сопровождение информационных ресурсов

Тема 1.1 Установка прикладного программного обеспечения и модулей информационных ресурсов, включая их настройку

Практическая работа №1 «Развертывание операционной системы»

– Цель: Получить навыки установки и первичной настройки операционных систем семейства Windows и Linux.

– Задание:

1) Установите ОС Windows 10/11 на виртуальную машину (VirtualBox/VMware) с заданными параметрами (имя компьютера, пароль администратора).

2) Установите дистрибутив Linux (например, Ubuntu Server) на вторую виртуальную машину в режиме минимальной установки.

3) Выполните первичную настройку сетевых интерфейсов (настройка статического IP-адреса).

4) Установите необходимые драйверы и обновления системы (для Windows).

5) Составьте отчет, включающий скриншоты ключевых этапов установки и настройки.

Практическая работа №2 «Установка и настройка WAMP-подобного комплекта» (4 часа)

– Цель: Освоить установку и настройку связки веб-сервера, интерпретатора PHP и СУБД.

– Задание:

- 1) Установите готовый сборщик (WAMP, OpenServer, XAMPP) или выполните ручную установку компонентов (Apache, PHP, MySQL).
- 2) Настройте веб-сервер для работы нескольких сайтов (виртуальные хосты).
- 3) Измените стандартные порты для повышения безопасности.
- 4) Проверьте работоспособность, создав тестовый PHP-скрипт (phpinfo()).
- 5) Оформите отчет с описанием конфигурационных файлов.

Практическая работа №3 «Установка и настройка готовых систем CMS, LMS, CRM» (4 часа)

- Цель: Получить опыт развертывания типовых веб-приложений (CMS).
- Задание:
 - 1) Скачайте дистрибутив одной из CMS (WordPress, Joomla, 1С-Битрикс).
 - 2) Создайте базу данных и пользователя БД для CMS.
 - 3) Выполните установку CMS, следуя инструкциям мастера установки.
 - 4) Настройте базовые параметры системы (название сайта, язык, установка темы оформления).
 - 5) Установите и активируйте один плагин/модуль для расширения функционала.
 - 6) Опишите в отчете возникшие инциденты (если были) и способы их решения.

Практическая работа №4 «Установка систем для функционирования технической поддержки» (4 часа)

- Цель: Ознакомиться с ПО для организации службы технической поддержки (Service Desk, Help Desk).
- Задание:
 - 1) Установите одну из систем helpdesk (например, osTicket, MantisBT, Redmine).
 - 2) Выполните начальную настройку системы: создайте отделы, сотрудников.
 - 3) Создайте тестовую заявку от имени пользователя.
 - 4) Продемонстрируйте процесс обработки заявки: назначение ответственного, изменение статуса, добавление комментария.
 - 5) Подготовьте скриншоты интерфейса системы и опишите ее функционал.

Практическая работа №5 «Установка сред и платформ веб-разработки» (6 часов)

- Цель: Научиться устанавливать и настраивать профессиональные среды разработки.
- Задание:
 - 1) Установите интегрированную среду разработки (IDE) для веб-разработки (VS Code, PhpStorm, WebStorm).
 - 2) Установите и настройте необходимые плагины/расширения для работы с HTML, CSS, JavaScript, PHP.
 - 3) Установите Node.js и менеджер пакетов npm.

4) Разверните локально проект с использованием системы сборки (например, Gulp или Webpack) или установите фреймворк (Laravel, Vue CLI).

5) Опишите процесс настройки окружения.

Практическая работа №6 «Публикация веб-приложения на хостингах разного типа» (6 часов)

– Цель: Получить практический опыт размещения веб-приложений на реальных хостинг-площадках.

– Задание:

1) Зарегистрируйтесь на бесплатном хостинге (например, на хостинге для статических сайтов) и загрузите простой статический сайт (HTML, CSS).

2) Настройте подключение по FTP/SSH.

3) Для созданного ранее сайта на CMS настройте перенос на хостинг с поддержкой PHP и MySQL (можно использовать локальный сервер или облачный сервис).

4) Настройте привязку доменного имени (или использование поддомена хостинга).

5) Сравните различные типы хостинга (виртуальный, VPS, выделенный сервер) в отчете.

Тема 1.2 Обработка запросов заказчика в службе технической поддержки в соответствии с трудовым заданием

Практическая работа №1 «Составление блок-схемы работы оператора технической поддержки» (6 часов)

– Цель: Систематизировать знания о процессе обработки инцидентов.

– Задание:

1) Изучить типовой процесс работы службы поддержки (на примере ITIL).

2) Составить блок-схему алгоритма действий оператора первой линии при поступлении заявки от пользователя.

3) В схеме должны быть отражены этапы: регистрация, категоризация, приоритизация, диагностика, решение, эскалация, закрытие заявки.

4) Защитить разработанную блок-схему.

Практическая работа №2 «Выполнение обработки запросов в специализированной информационной системе» (6 часов)

– Цель: Научиться работать в системе Service Desk (Help Desk).

– Задание:

1) Используя установленную в ПР №4 (Тема 1.1) систему, смоделировать рабочий день оператора техподдержки.

2) Получить несколько тестовых заявок (от преподавателя).

3) Обработать заявки согласно их типу и приоритету: связаться с "клиентом" (уточнить детали), дать рекомендации по решению, назначить исполнителя, закрыть заявку.

4) Вести переписку внутри тикет-системы.

5) Предоставить скриншоты обработанных заявок.

Практическая работа №3 «Решение и разбор примеров критических ситуаций в службе поддержки» (6 часов)

- Цель: Развить навыки решения конфликтных ситуаций и коммуникации.
- Задание: Преподаватель раздает карточки с описанием критических инцидентов

- 1) Проанализировать ситуацию.
- 2) Предложить алгоритм действий оператора.
- 3) Составить текст ответа (письменного или устного) для клиента/руководства.
- 4) Провести ролевую игру, где один студент — оператор, другой — недовольный клиент.

МДК.02.02 Обеспечение безопасности информационных ресурсов

Тема 2.1 Резервное копирование и развертывание резервной копии

Практическая работа №1 «Резервное копирование и восстановление файловой системы веб-браузера» (2 часа)

- Цель: Научиться сохранять и восстанавливать пользовательские данные (закладки, пароли, настройки).

- Задание:

- 1) Создайте в браузере несколько закладок и сохраните пароль от какого-либо сайта.
- 2) Найдите папку с профилем пользователя браузера на диске.
- 3) Выполните резервное копирование этой папки.
- 4) Удалите (переместите) исходную папку, чтобы имитировать сбой.
- 5) Восстановите данные из резервной копии и убедитесь, что закладки и пароли сохранились.
- 6) Опишите процесс в отчете.

Практическая работа №2 «Резервное копирование и восстановление базы данных веб-приложения» (2 часа)

- Цель: Освоить резервирование и восстановление БД MySQL/MariaDB.

- Задание:

- 1) Используя ранее установленную CMS (например, WordPress), наполните её тестовым контентом (пара статей, рубрик).
- 2) С помощью утилиты командной строки `mysqldump` создайте дамп базы данных.
- 3) Удалите (или переименуйте) существующую базу данных и создайте новую пустую.

- 4) Восстановите базу данных из дампа.
- 5) Проверьте работоспособность сайта. Сохранился ли контент?
- 6) Оформите отчет с командами.

Практическая работа №3 «Использование сценариев и скриптов для организации процесса резервирования и восстановления данных» (2 часа)

- Цель: Научиться автоматизировать процесс резервного копирования с помощью скриптов.

- Задание:

1) Напишите скрипт для командной строки (bash для Linux, .bat или PowerShell для Windows), который выполняет следующие действия:

- Создает дамп базы данных.
- Архивирует папку с файлами сайта.
- Сохраняет архив и дамп в папку с датой в имени (например, backup_2026-03-01).

2) Удаляет резервные копии старше 7 дней.

3) Добавьте скрипт в планировщик задач для автоматического выполнения раз в сутки.

4) Продемонстрируйте работу скрипта.

Тема 2.2 Настройка прав пользователей в соответствии с функциональными задачами (ролями)

Практическая работа №1 «Настройка прав доступа к файловой системе и базе данных» (2 часа)

– Цель: Освоить управление доступом на уровне ОС и СУБД.

– Задание:

1) В ОС Linux создайте нескольких пользователей и группу web-developers.

2) Настройте права доступа к папке с проектом так, чтобы:

– Владелец (root) имел полный доступ.

– Группа web-developers имела права на чтение и запись.

– Остальные пользователи не имели доступа.

3) В СУБД MySQL создайте двух пользователей: admin_db (с полными правами на БД) и user_app (только с правами SELECT, INSERT, UPDATE на определенную таблицу).

4) Продемонстрируйте разницу в доступе.

Практическая работа №2 «Настройка ролей доступа пользователей в CMS, LMS или CRM» (4 часа)

– Цель: Научиться управлять ролями и правами в типовых веб-приложениях.

– Задание:

1) В ранее установленной CMS (WordPress) создайте несколько пользователей с разными ролями: Администратор, Редактор, Автор, Подписчик.

2) Войдите в систему под каждым из пользователей и проверьте, какие возможности у них есть (создание записей, редактирование, удаление, доступ к настройкам).

3) Создайте пользовательскую роль (например, "Модератор комментариев") с помощью плагина или вручную (если есть опыт).

4) Опишите в отчете, какие права имеет каждая роль.

Тема 2.3 Применение программных средств обеспечения безопасности информации веб-приложений

Практическая работа №1 «Анализ безопасности веб-сервиса на предмет наличия уязвимостей» (6 часов)

– Цель: Освоить базовые методы аудита безопасности веб-приложений.

– Задание (выполняется на специально подготовленном учебном стенде или локальном сайте):

1) Проверьте сайт на наличие уязвимостей:

– SQL-инъекции (попробуйте ввести ' OR '1'='1 в поля форм).

– XSS (межсайтовый скриптинг) — введите `<script>alert('test')</script>`.

– Открытые директории (попробуйте перейти по адресам типа `site.ru/images/`).

2) Проверьте HTTP-заголовки безопасности с помощью инструментов разработчика.

3) Используйте онлайн-сканеры (например, Qualys SSL Labs для проверки SSL).

4) Составьте отчет с описанием найденных уязвимостей и рекомендациями по их устранению.

Практическая работа №2 «Настройка веб-сервера с использованием протокола HTTPS» (4 часа)

– Цель: Научиться настраивать SSL/TLS-шифрование для веб-сайта.

– Задание:

1) Сгенерируйте самоподписанный SSL-сертификат с помощью OpenSSL.

2) Настройте веб-сервер Apache или Nginx для работы по HTTPS, используя созданный сертификат.

3) Настройте автоматическое перенаправление (редирект) с HTTP на HTTPS.

4) Для хостинга с реальным доменом изучите процесс получения бесплатного сертификата Let's Encrypt (Certbot).

5) Проверьте работоспособность и уровень защиты (например, на сайте ssllabs.com).

Практическая работа №3 «Настройка программного файрволла для веб-приложения» (4 часа)

– Цель: Освоить настройку межсетевого экрана (брандмауэра) для защиты веб-сервера.

– Задание:

1) Для Linux: Настройте iptables или ufw так, чтобы:

– был открыт только 22 (SSH), 80 (HTTP) и 443 (HTTPS) порты.

– все остальные входящие соединения были заблокированы.

– разрешите исходящие соединения для обновлений.

2) Для Windows: Настройте брандмауэр Windows в режиме повышенной безопасности, создав правила для блокировки входящего трафика на неиспользуемые порты.

3) Настройте WAF (Web Application Firewall), например, модуль `mod_security` для Apache, и включите базовые правила.

4) Проверьте эффективность настройки, попытавшись подключиться к заблокированному порту.

2. Вопросы для промежуточной аттестации

Вопросы к дифференцированному зачету по МДК 02.01

1. Перечислите основные этапы установки операционной системы Windows Server/Linux.
2. Опишите процесс настройки сетевых интерфейсов в ОС (настройка статического IP).
3. Что такое LAMP/WAMP? Опишите назначение каждого компонента.
4. Как создать виртуальный хост в Apache/Nginx?
5. Перечислите основные этапы установки CMS (на примере WordPress).
6. Какие инциденты могут возникнуть при установке программного обеспечения? Приведите примеры и способы их решения.
7. Что такое хостинг? Сравните различные типы хостинга (виртуальный, VPS, выделенный).
8. Опишите процесс публикации веб-приложения на удаленном сервере (по FTP/SSH).
9. Что такое служба технической поддержки (Service Desk)? Ее основные функции.
10. Опишите жизненный цикл заявки (тикета) в службе поддержки.
11. Какие существуют уровни (линии) технической поддержки?
12. Что такое ITIL? Какие процессы ITIL относятся к управлению инцидентами?
13. Назовите основные правила коммуникации с пользователем при возникновении конфликтной ситуации.
14. Какие инструменты автоматизации службы поддержки вы знаете?
15. Что такое база знаний (knowledge base) и как она используется в техподдержке?
16. Опишите структуру ответа пользователю на технический запрос.
17. Какие метрики используются для оценки качества работы службы поддержки?
18. Что такое эскалация инцидента? Когда она применяется?
19. Какие способы резервного копирования данных вы знаете (полное, инкрементное, дифференциальное)?
20. В чем разница между резервным копированием файлов сайта и базы данных?

Вопросы к дифференцированному зачету по МДК 02.02

21. Дайте определение понятию «информационная безопасность». Назовите три ее основные составляющие (конфиденциальность, целостность, доступность).
22. Перечислите основные угрозы для веб-приложений.
23. Что такое резервное копирование? Какие стратегии резервирования существуют?
24. Опишите процесс восстановления данных из резервной копии.
25. Что такое модель управления доступом? Какие модели вы знаете (дискреционная, мандатная, ролевая)?

26. Что такое RBAC (Role-Based Access Control)? Приведите примеры ролей в CMS.
27. Как настроить права доступа к файлам и папкам в ОС Linux (chmod, chown)?
28. Как создать пользователя в СУБД MySQL и назначить ему привилегии?
29. Что такое SQL-инъекция? Как защититься от нее?
30. Что такое XSS (межсайтовый скриптинг)? Типы XSS и методы защиты.
31. Что такое SSL/TLS-сертификат? Для чего он нужен?
32. Опишите процесс получения и установки SSL-сертификата.
33. Что такое файрволл (межсетевой экран)? Какие задачи он решает?
34. Настройка простых правил для брандмауэра Windows/Linux.
35. Что такое электронно-цифровая подпись (ЭЦП)? Принципы ее работы.
36. Какие программные средства обеспечения безопасности веб-приложений вы знаете (антивирусы, WAF, сканеры уязвимостей)?
37. Что такое DDoS-атака? Методы защиты.
38. Какие стандарты и регламенты в области информационной безопасности вы знаете?
39. Что такое двухфакторная аутентификация (2FA)? Приведите примеры.
40. Какие правила безопасной разработки (Secure Coding Practices) необходимо соблюдать?

3. К экзамену по модулю

Теоретические вопросы:

1. Перечислите основные этапы установки операционной системы (Windows Server / Linux). На что следует обратить особое внимание?
2. Охарактеризуйте процесс настройки сетевых параметров в ОС (статический и динамический IP-адрес).
3. Что такое LAMP/WAMP? Опишите назначение и взаимодействие каждого компонента стека.
4. Какие существуют способы установки веб-сервера (Apache, Nginx)? Опишите процесс установки и первичной настройки.
5. Что такое виртуальные хосты (Virtual Hosts) в веб-сервере? Для чего они нужны и как настраиваются?
6. Опишите процесс установки и настройки системы управления базами данных (MySQL/MariaDB).
7. Какие инциденты могут возникнуть при установке программного обеспечения? Приведите примеры и алгоритмы их решения.
8. Что такое хостинг? Проведите сравнительный анализ типов хостинга (виртуальный, VPS, выделенный сервер, облачный).
9. Опишите процесс публикации веб-приложения на удаленном сервере (с использованием FTP/SFTP/SSH).
10. Какие существуют способы автоматизации развертывания веб-приложений?

11. Дайте определение понятию «резервное копирование». Назовите основные цели резервирования.
12. Охарактеризуйте типы резервного копирования: полное, инкрементное, дифференциальное. В чем их преимущества и недостатки?
13. Опишите стратегии резервного копирования (например, "дед-отец-сын"). Какую стратегию вы выберете для небольшого интернет-магазина и почему?
14. Какие существуют методы резервного копирования файловой системы (копирование, архивация, использование snapshots)?
15. Как выполнить резервное копирование и восстановление базы данных MySQL/MariaDB с помощью утилиты mysqldump?
16. Какие инструменты и программные средства для резервного копирования вы знаете?
17. Как автоматизировать процесс резервного копирования с помощью скриптов и планировщика задач (cron, Task Scheduler)?
18. Что такое политика хранения резервных копий (retention policy)? Как определить оптимальный срок хранения?
19. Опишите пошаговый процесс восстановления сайта (файлы + БД) из резервной копии после сбоя.
20. Какие риски связаны с резервным копированием и как их минимизировать?
21. Что такое управление доступом? Назовите основные модели управления доступом (дискреционная, мандатная, ролевая).
22. Раскройте понятие RBAC (Role-Based Access Control). Приведите примеры реализации ролей в веб-приложениях (CMS, CRM).
23. Как настроить права доступа к файлам и каталогам в ОС Linux (команды chmod, chown)? Что означают права 755, 644, 777?
24. Как управлять пользователями и группами в ОС Linux (команды useradd, usermod, groupadd)?
25. Как создать пользователя в СУБД MySQL/MariaDB и назначить ему привилегии (GRANT, REVOKE)?
26. Что такое аутентификация, авторизация и аудит? В чем различие между этими понятиями?
27. Какие существуют способы аутентификации пользователей в веб-приложениях (парольная, двухфакторная, через социальные сети)?
28. Как организовать разграничение прав доступа в CMS (на примере WordPress: роли администратор, редактор, автор)?
29. Что такое принцип минимальных привилегий (Principle of Least Privilege)? Как его применять на практике?
30. Как вести учет и аудит действий пользователей в системе?
31. Дайте определение понятию «информационная безопасность». Назовите триаду CIA (конфиденциальность, целостность, доступность).
32. Перечислите основные угрозы безопасности веб-приложений (OWASP Top 10).
33. Что такое SQL-инъекция (SQL Injection)? Опишите механизм атаки и методы защиты.

34. Что такое межсайтовый скриптинг (XSS)? Какие типы XSS существуют и как защититься?
35. Что такое межсайтовая подделка запроса (CSRF)? Принцип атаки и способы предотвращения.
36. Что такое SSL/TLS-сертификат? Для чего он нужен и как работает? Опишите процесс установки сертификата на веб-сервер.
37. Какие программные средства обеспечения безопасности веб-приложений вы знаете (антивирусы, файрволлы, WAF, сканеры уязвимостей)?
38. Что такое файрволл (межсетевой экран)? Какие задачи он решает? Приведите примеры настройки простых правил.
39. Что такое DDoS-атака? Какие существуют методы защиты от DDoS?
40. Какие правила безопасной разработки (Secure Coding Practices) необходимо соблюдать программистам?
41. Что такое служба технической поддержки (Service Desk / Help Desk)? Каковы ее основные функции и задачи?
42. Опишите жизненный цикл заявки (тикета) от поступления до закрытия.
43. Что такое SLA (Service Level Agreement)? Какие параметры качества обслуживания в нем фиксируются?
44. Какие существуют уровни (линии) технической поддержки и в чем их различие?
45. Какие инструменты и системы автоматизации работы службы поддержки вы знаете (osTicket, Redmine, Jira Service Management)?
46. Что такое эскалация инцидента? Когда и почему она применяется?
47. Назовите основные правила эффективной коммуникации с пользователем при возникновении конфликтной ситуации.
48. Что такое база знаний (knowledge base)? Как она используется в работе технической поддержки?
49. Какие метрики используются для оценки качества работы службы поддержки (время реакции, время решения, удовлетворенность клиента)?
50. Опишите процесс обработки критического инцидента (например, недоступность сайта интернет-магазина).

Практико-ориентированные задания:

1. Установите на виртуальную машину (VirtualBox/VMware) операционную систему Ubuntu Server. Выполните первичную настройку: задайте имя хоста, настройте статический IP-адрес, установите необходимые обновления. Составьте отчет с описанием всех выполненных шагов и скриншотами.
2. Произведите установку и первичную настройку веб-сервера Apache и интерпретатора PHP. Проверьте работоспособность, создав тестовый файл `info.php` с функцией `phpinfo()`. Обеспечьте доступ к этому файлу из браузера хостовой машины.
3. Установите и настройте систему управления базами данных MySQL (MariaDB). Установите пароль для root, удалите анонимных пользователей, создайте тестовую базу данных и пользователя с полными правами на эту базу.
4. Разверните локально (OpenServer/XAMPP/WAMP) или на виртуальном сервере сайт на базе CMS WordPress (или любой другой CMS). Выполните все этапы:

создание БД, подключение к CMS, настройка основных параметров сайта. Установите и активируйте один плагин.

5. Настройте веб-сервер Apache для работы двух сайтов (виртуальные хосты): `site1.local` и `site2.local`. Создайте для каждого простую HTML-страницу-заглушку. Проверьте доступность обоих сайтов.

6. Осуществите публикацию ранее созданного сайта на бесплатном хостинге (или на учебном сервере). Перенесите файлы сайта и базу данных. Проверьте работоспособность сайта на удаленном сервере.

7. Установите и настройте FTP-сервер (например, `vsftpd`) для удаленного доступа к файлам сайта. Создайте отдельного пользователя для загрузки файлов, ограничьте его домашним каталогом.

8. Для установленного сайта на WordPress создайте резервную копию вручную:

- Выполните дамп базы данных с помощью `mysqldump`.
- Архивируйте папку с файлами сайта.
- Сохраните обе копии в отдельную папку с текущей датой.

9. Напишите `bash`-скрипт (или `.bat` для Windows), который автоматически создает резервную копию базы данных и файлов сайта, сохраняет их в папку `/backups/дата/` и удаляет копии старше 7 дней. Добавьте скрипт в планировщик задач (`cron`).

10. Сымитируйте сбой: удалите (переместите) папку с файлами сайта и удалите базу данных. Выполните полное восстановление сайта из ранее созданной резервной копии. Убедитесь в работоспособности сайта после восстановления.

11. Настройте резервное копирование профиля пользователя браузера (закладки, пароли) с помощью ручного копирования папки профиля. Затем удалите оригинальную папку и восстановите данные из копии.

12. В ОС Linux создайте двух пользователей: `webmaster` и `content-manager`. Создайте группу `webteam`. Настройте права доступа к папке `/var/www/site` так, чтобы:

- Владелец (`root`) имел полные права.
- Группа `webteam` имела права на чтение и запись.
- Остальные пользователи не имели доступа.
- Пользователь `content-manager` НЕ должен иметь доступа к этой папке (вывести его из группы).

13. В СУБД MySQL создайте двух пользователей:

- `db_admin` — с полными привилегиями на базу данных `mydb`.
- `db_user` — только с правами `SELECT`, `INSERT`, `UPDATE` на все таблицы базы `mydb`.

Продемонстрируйте разницу в их возможностях, подключившись к СУБД под каждым из них.

14. В установленной CMS (WordPress) создайте трех пользователей с ролями: Администратор, Редактор, Подписчик. Войдите в систему под каждым и опишите в отчете, какие действия (создание записей, редактирование, доступ к настройкам) доступны каждой роли.

15. Проведите базовый аудит безопасности вашего локального сайта (например, на WordPress). Проверьте:

- Наличие уязвимостей (SQLi, XSS) в формах (можно использовать тестовые строки).
- Права доступа к файлам (не должно быть 777).
- Версию CMS и плагинов (нет ли известных уязвимостей).

Составьте отчет с рекомендациями по усилению безопасности.

16. Сгенерируйте самоподписанный SSL-сертификат с помощью OpenSSL. Настройте веб-сервер Apache (или Nginx) для работы по HTTPS с использованием этого сертификата. Настройте принудительный редирект с HTTP на HTTPS.

17. Настройте брандмауэр (ufw для Linux или брандмауэр Windows) таким образом, чтобы:

- были открыты только порты 22 (SSH), 80 (HTTP) и 443 (HTTPS);
- все остальные входящие соединения были заблокированы.

Проверьте доступность сервера по открытым портам и недоступность по закрытым (например, телнетом).

18. Установите и настройте плагин безопасности для WordPress (например, Wordfence или iThemes Security). Выполните базовую настройку: включите защиту от брутфорса, скройте страницу входа.

19. Разработайте блок-схему алгоритма действий оператора первой линии технической поддержки при поступлении новой заявки. Отрадите этапы: регистрация, категоризация, приоритизация, диагностика, решение, эскалация, закрытие.

20. Установите одну из систем Service Desk (например, osTicket). Создайте в ней отделы (ИТ, Бухгалтерия), сотрудников и несколько тестовых заявок. Продемонстрируйте процесс назначения заявки, изменения статуса и добавления комментария.

21. Смоделируйте диалог с недовольным пользователем. Преподаватель описывает проблему

22. Составьте инструкцию (базу знаний) для пользователей по часто возникающей проблеме: «Как сбросить пароль от учетной записи в корпоративном портале». Инструкция должна быть понятной для неспециалиста.

23. Проанализируйте описание инцидента: *«Пользователь сообщает, что при попытке зайти в систему видит ошибку "403 Forbidden". До вчерашнего дня все работало»*. Предложите гипотезы о причинах (не менее 3-х) и опишите ваши действия по диагностике и решению проблемы для каждой гипотезы.