ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ТОМСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТОМСКИЙ ТЕХНИКУМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»
(ОГБПОУ «ТТИТ»)

УТВЕРЖДАЮ
Директор ОГБПОУ «ТТИТ»
_____/ Е.В.Дедюхина
«____»_____2025 г.

Подписано цифровой подписью: Дедюхина Елена Валентиновна
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России, CN=Федеральное казначейство
Причина: Я утвердил этот документ
Дата: 20 Июнь 2025 г. 16:09:20

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Техническая поддержка и администрирование информационных ресурсов
МДК 02.01 Настройка и сопровождение информационных ресурсов
МДК 02.02 Обеспечение безопасности информационных ресурсов
для специальности:
09.02.09, Веб-разработка
Квалификация: Разработчик веб-приложений
Форма обучения: очная
Базовая подготовка

Томск 2025 г.

РАССМОТРЕНО
на заседании ПЦК
«Информационные системы и программирование» (разработчик веб и мультимедийных приложений)
протокол №_____
от «____»_____2025 г.
Председатель ПЦК
_____/ М.Н. Фунтиков

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.09 Веб разработка (Приказ Министерства просвещения Российской Федерации от 21 ноября 2023 г. № 879).

Разработчик:
_____/ _____

_____/ _____

Преподаватели:
_____/ _____

_____/ _____

_____/ _____

_____/ _____

_____/ _____

_____/ _____

СОДЕРЖАНИЕ

1. ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ 4

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ 6

3. ОЦЕНКА ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 9

3.1. Формы и методы оценивания 9

3.2. Типовые задания для оценки освоения ПМ.02 Техническая поддержка и администрирование информационных ресурсов 11

4. КОНТРОЛЬ ПРИОБРЕТЕНИЯ ПРАКТИЧЕСКОГО ОПЫТА. ОЦЕНКА ПО УЧЕБНОЙ И (ИЛИ) ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ 29

5. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ 30

1. ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Планируемые результаты освоения профессионального модуля

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности «Проектирование и разработка информационных ресурсов» и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ПОП в целом.

1.1.1 Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
ОК 02.	Использовать современные средства поиска, анализа и интерпретации и информационные профессиональной деятельности;
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях;
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	Техническая поддержка и администрирование информационных ресурсов.
ПК 2.1.	Устанавливать прикладное программное обеспечение и модулей информационных ресурсов, включая их настройку.
ПК 2.2.	Проводить работы по резервному копированию и развертыванию резервной копии информационных ресурсов.
ПК 2.3.	Настраивать права пользователей в соответствии с функциональными задачами (ролями) и на основании информации о поведенческих факторах.
ПК 2.4.	Применять программные средства обеспечения безопасности информации веб приложений.
ПК 2.5	Обрабатывать запросы заказчика в службе технической поддержке в соответствии с трудовым заданием

1.2 Формы промежуточной аттестации по профессиональному модулю

Таблица 1

Элементы модуля, профессиональный модуль	**Формы промежуточной аттестации**
1	**2**
МДК 02.01 Настройка и сопровождение информационных ресурсов	Дифференцированный зачёт
МДК 02.02 Обеспечение безопасности информационных ресурсов	Дифференцированный зачёт
УП	Дифференцированный зачёт
ПП	Дифференцированный зачёт
ПМ	**Экзамен (квалификационный)**

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

2.1. В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Таблица 2

Код ПК, ОК	**Критерии оценки результата (показатели освоенности компетенций)**	**Формы контроля и методы оценки**
ПК 2.1	Оценка «отлично» - целевое веб-приложение способно выполняться согласно всем тестовым условиям и разработана необходимая документация Оценка «хорошо» - целевое веб-приложение способно выполняться согласно всем тестовым условиям. Оценка «удовлетворительно» - часть базовых компонентов ПО для веб-приложения установлено или подробно описаны требуемые операции.	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик Тестирование
ПК 2.2	Оценка«отлично»- Сформирован план создания резервных копий, настроено специальное ПО для резервирования, продемонстрирован процесс восстановления данных, в том числе автоматический. Оценка«хорошо»- Сформирован план создания резервных копий, настроено специальное ПО для резервирования. Оценка«удовлетворительно»- Сформирован план создания резервных копий, настроено специальное ПО для резервирования.	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик Тестирование
ПК 2.3	Оценка «отлично» - Настроены права доступа к ФС И БД, распределены роли в CMS, оформлен регламент доступа. Оценка «хорошо» - Настроены права доступа к ФС И БД, распределены роли в CMS. Оценка «удовлетворительно» - Распределены роли в CMS, оформлен регламент доступа.	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик Тестирование
ПК 2.4	Оценка «отлично» - проведен аудит безопасности веб-сервиса, настроено специальное ПО для обеспечения безопасности работы веб-приложения и составлен отчет с рекомендациями. Оценка «хорошо» - проведен аудит безопасности веб-сервиса, настроено специальное ПО для обеспечения безопасности работы веб-приложения и составлен отчет с рекомендациями по базовым характеристикам. Оценка «удовлетворительно» - проведен аудит безопасности веб-сервиса и составлен отчет с рекомендациями по базовым характеристикам.	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик Тестирование

ПК 2.5	Оценка «отлично» - составлена блок-схема работы оператора технической поддержки и решен инцидент от гипотетического пользователя. Оценка «хорошо» - составлена блок-схема работы оператора технической поддержки и решен инцидент от гипотетического пользователя с грубыми нарушениями. Оценка «удовлетворительно» - составлена блок-схема работы оператора технической поддержки или решен инцидент от гипотетического пользователя.	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик Тестирование
ОК 01	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик
ОК 02	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик
ОК 03	демонстрация ответственности за принятые решения обоснованность самоанализа и коррекция результатов собственной работы;	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик
ОК 04	взаимодействовать с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик
ОК 05	Демонстрировать грамотность устной и письменной речи, ясность формулирования и изложения мыслей	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик
ОК 07	эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик

ОК 08	эффективность использования средств физической культуры для сохранения и укрепления здоровья при выполнении профессиональной деятельности.	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик
ОК 09	эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экзамен/зачет Защита практических работ Наблюдение за выполнением различных видов работ во время учебной/ производственной практик

3. ОЦЕНКА ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Формы и методы оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по ПМ.02 Техническая поддержка и администрирование информационных ресурсов, направленные на формирование общих и профессиональных компетенций.

Текущий контроль знаний в рамках изучения профессионального модуля ПМ.02 Техническая поддержка и администрирование информационных ресурсов предполагает оценивание выполнения лабораторных работ по следующим междисциплинарным курсам:

МДК 02.01 Настройка и сопровождение информационных ресурсов

МДК 02.02 Обеспечение безопасности информационных ресурсов

Текущая оценка осуществляется посредством выполнения практических работ и компьютерного тестирования, в соответствии с установленными критериями.

Для всех тестов, применяемых для текущей оценки знаний применяется следующая шкала оценивания:

0-49% - неудовлетворительно

50-69% - удовлетворительно

70-84% - хорошо

85-100% - отлично.

До промежуточной аттестации по междисциплинарным курсам должны быть выполнены все предусмотренные программой тесты, а также все практические работы, предусмотренные рабочей программой. Промежуточная аттестация по междисциплинарным курсам включает в себя выполнение итогового тестирования и учитывает результаты работы в течение семестра.

Промежуточная аттестация по ПМ.02 Техническая поддержка и администрирование информационных ресурсов осуществляется в форме экзамена (квалификационного). До проведения квалификационного экзамена обучающемуся необходимо сдать экзамены по МДК 02.01 Настройка и сопровождение информационных ресурсов, МДК 02.02 Обеспечение безопасности информационных ресурсов, дифференцированные зачеты по учебной и производственной практикам.

Контроль и оценка освоения профессионального модуля

Элемент ПМ	**Формы и методы контроля**			
	Текущий контроль		**Промежуточная аттестация**	
	Форма контроля	**Проверяемые ОК, ПК**	**Форма контроля**	**Проверяемые ОК, ПК**
МДК 02.01 Настройка и сопровождение информационных ресурсов	Практическое занятие № 1. «Развертывание операционной системы» Практическое занятие № 2. «Установка и настройка WAMP подобного комплекта» Практическое занятие № 3. «Установка и настройка готовых систем CMS, LMS, CRM» Практическое занятие № 4. «Установка систем для функционирования технической поддержки»	ПК 2.1 ПК 2.5 ОК 1-5 ОК 7 ОК 9	Дифф. зачет Экзамен (квалификационный)	ПК 2.1 ПК 2.5 ОК 1-5 ОК 7 ОК 9

	Практическое занятие № 5. «Установка сред и платформ веб-разработки» Практическое занятие № 6. «Публикация веб-приложения на хостингах разного типа» Практическое занятие № 1. «Составление блок-схемы работы оператора технической поддержки» Практическое занятие № 2. «Выполнение обработки запросов в специализированной информационной системе» Практическое занятие № 3. «Решение и разбор примеров критических ситуаций в службе поддержки» Тест №1			
МДК 02.02 Обеспечение безопасности информационных ресурсов	Практическое занятие № 1. «Резервное копирование и восстановление файловой системы веб-браузера» Практическое занятие № 2. «Резервное копирование и восстановление базы данных веб-приложения» Практическое занятие № 3. «Использование сценариев и скриптов для организации процесса резервирования и восстановления данных» Практическое занятие № 1. «Настройка прав доступа к файловой системе и базе данных» Практическое занятие № 2. «Настройка ролей доступа пользователей в CMS, LMS или CRM» Практическое занятие № 1. «Анализ безопасности веб-сервиса на предмет наличия уязвимостей» Практическое занятие № 2. «Настройка веб-сервера с использованием протокола HTTPS» Практическое занятие № 3. «Настройка программного файрволла для веб-приложения» Тест №2	ПК 2.2 ПК 2.3 ПК 2.4 ОК 1-5 ОК 7 ОК 9	Дифф. зачет Экзамен (квалификационный)	ПК 2.2 ПК 2.3 ПК 2.4 ОК 1-5 ОК 7 ОК 9
Учебная практика	1. Проанализировать организацию заказчика и предложить алгоритм работы технической поддержки.	ПК 2.1 - ПК 2.5 ОК 1-5 ОК 7 ОК 9	Дифф. зачет Экзамен (квалификационный)	ПК 2.1 - ПК 2.5 ОК 1-5 ОК 7 ОК 9

	Учебная практика раздела 2. Обеспечение безопасности информационных ресурсов 2. Проанализировать организацию заказчика и разработать регламент по резервному копированию данных и доступу пользователей к системе.			
Производственная практика	1. Проанализировать организацию заказчика и разработать инструкцию по развертыванию используемого программного обеспечения для поддержания функционирования веб-приложений компании. Производственная практика раздела 2. Обеспечение безопасности информационных ресурсов 2.Проанализировать организацию заказчика и разработать регламент по обеспечению безопасности функционирования используемого веб-приложения.	ПК 2.1 - ПК 2.5 ОК 1-5 ОК 7 ОК 9	Дифф. зачет Экзамен (квалификационный)	ПК 2.1 - ПК 2.5 ОК 1-5 ОК 7 ОК 9

3.2. Типовые задания для оценки освоения ПМ.02 Техническая поддержка и администрирование информационных ресурсов

3.2.1. Типовые задания для оценки освоения МДК.02.01. Настройка и сопровождение информационных ресурсов

1) Задания в тестовой форме

Тест №1

1: Какой командой в Linux можно просмотреть содержимое текущей директории?
A) dir
B) ls
C) pwd
D) cd
Правильный ответ: B) ls
2: Какой из следующих файловых систем не является стандартной для Windows?
A) NTFS
B) FAT32
C) ext4
D) exFAT
Правильный ответ: C) ext4
3: Что означает аббревиатура DNS?
A) Domain Name Service
B) Domain Name System
C) Data Network Service
D) Data Name System
Правильный ответ: B) Domain Name System

4: Какой порт используется для HTTPS?
A) 80
B) 443
C) 21
D) 25
Правильный ответ: B) 443
5: Что означает аббревиатура LAMP?
A) Linux, Apache, MySQL, PHP
B) Linux, Apache, MongoDB, Python
C) Windows, Apache, MySQL, PHP
D) Windows, Nginx, MySQL, Perl
Правильный ответ: A) Linux, Apache, MySQL, PHP
6: Какой из следующих компонентов не входит в состав WAMP?
A) Windows
B) Apache
C) MySQL
D) Nginx
Правильный ответ: D) Nginx
7: Какой из следующих движков является популярной CMS?
A) Moodle
B) WordPress
C) Joomla!
D) Все вышеперечисленные
Правильный ответ: D) Все вышеперечисленные
8: Какой тип дополнений обычно используется в CMS для расширения функционала?
A) Модули
B) Плагины
C) Темы
D) Все вышеперечисленные
Правильный ответ: D) Все вышеперечисленные
9: Какой тип хостинга предоставляет пользователю полный доступ к серверу?
A) Виртуальный хостинг
B) VPS (Virtual Private Server)
C) Shared hosting (общий хостинг)
D) Cloud hosting (облачный хостинг)
Правильный ответ: B) VPS (Virtual Private Server)
10: Какой из следующих типов хостинга обычно используется для небольших сайтов и блогов?
A) Dedicated hosting (выделенный хостинг)
B) Shared hosting (общий хостинг)
C) VPS (Virtual Private Server)
D) Colocation hosting (колокационный хостинг)
Правильный ответ: B) Shared hosting (общий хостинг)
11: Какой командой в Windows можно открыть командную строку?
A) cmd.exe
B) command.com
C) terminal.exe
D) shell.exe
Правильный ответ: A) cmd.exe
12: Какой из следующих протоколов используется для передачи данных по защищенному каналу?
A) FTP
B) HTTP
C) HTTPS
D) SMTP
Правильный ответ: C) HTTPS
13: Что такое "кэширование" в контексте веб-приложений?
A) Сохранение данных на сервере для ускорения доступа к ним в будущем.
B) Процесс шифрования данных.
C) Удаление ненужных данных.
D) Создание резервной копии данных.
Правильный ответ: A) Сохранение данных на сервере для ускорения доступа к ним в будущем.
14: Какой из следующих инструментов позволяет управлять базами данных MySQL через графический интерфейс?
A) phpMyAdmin

B) MySQL Workbench
C) Adminer
D) Все вышеперечисленные
Правильный ответ: D) Все вышеперечисленные
15: Какой из следующих факторов не влияет на выбор хостинга для веб-сайта?
A) Трафик сайта
B) Необходимость в поддержке определенного языка программирования
C) Личное предпочтение дизайна сайта
D) Уровень безопасности
Правильный ответ: C) Личное предпочтение дизайна сайта
16: Какой из следующих факторов не является причиной конфликтов в деловом взаимодействии?
A) Разные цели и интересы
B) Неясность ролей
C) Эмоциональная привязанность
D) Высокий уровень доверия
Правильный ответ: D) Высокий уровень доверия
Вопрос 17: Какой стиль управления конфликтами предполагает сотрудничество сторон для нахождения взаимовыгодного решения?
A) Конкуренция
B) Избежание
C) Компромисс
D) Сотрудничество
Правильный ответ: D) Сотрудничество
18: Какой из следующих инструментов является наиболее эффективным для групповой работы?
A) Электронная почта
B) Видеоконференция
C) Телефонный звонок
D) Личное общение
Правильный ответ: B) Видеоконференция
19: Какой из следующих методов коммуникации наилучшим образом подходит для передачи сложной информации?
A) Устная речь
B) Письменное сообщение
C) Визуальные средства (графики, схемы)
D) Обсуждение в группе
Правильный ответ: C) Визуальные средства (графики, схемы)
20: Какой из следующих этапов является первым в процессе управления изменениями?
A) Оценка изменений
B) Подготовка к изменениям
C) Идентификация изменений
D) Реализация изменений
Правильный ответ: C) Идентификация изменений
21: Какой метод часто используется для оценки влияния изменений на бизнес-процессы?
A) SWOT-анализ
B) PEST-анализ
C) Анализ рисков
D) Диаграмма Исикавы
Правильный ответ: C) Анализ рисков
22: Какой из процессов ITIL отвечает за управление инцидентами?
A) Управление изменениями
B) Управление инцидентами
C) Управление проблемами
D) Управление конфигурациями
Правильный ответ: B) Управление инцидентами
23: Какое из утверждений о методологии ITIL является верным?
A) ITIL фокусируется только на технических аспектах ИТ.
B) ITIL не включает в себя процессы управления изменениями.
C) ITIL помогает организациям повысить качество ИТ-услуг.
D) ITIL не предназначен для использования в малом бизнесе.
Правильный ответ: C) ITIL помогает организациям повысить качество ИТ-услуг.
24: Какой из следующих принципов является ключевым для эффективной работы службы технической поддержки?
A) Игнорирование запросов пользователей

B) Быстрая реакция на инциденты
C) Отказ от документирования процессов
D) Минимизация взаимодействия с пользователями
Правильный ответ: B) Быстрая реакция на инциденты
25: Какой из следующих показателей используется для оценки эффективности службы технической поддержки?
A) Количество сотрудников в службе поддержки
B) Среднее время решения инцидента
C) Количество полученных звонков от пользователей
D) Количество открытых тикетов на конец месяца
Правильный ответ: B) Среднее время решения инцидента

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%

3) Практическое занятие № 1. «Развертывание операционной системы»

Цель работы: формирование умения осуществлять развертывание операционной системы.
Формируемые компетенции: ПК 2.1, ПК 2.5, ОК 1-5, ОК 7, ОК 9

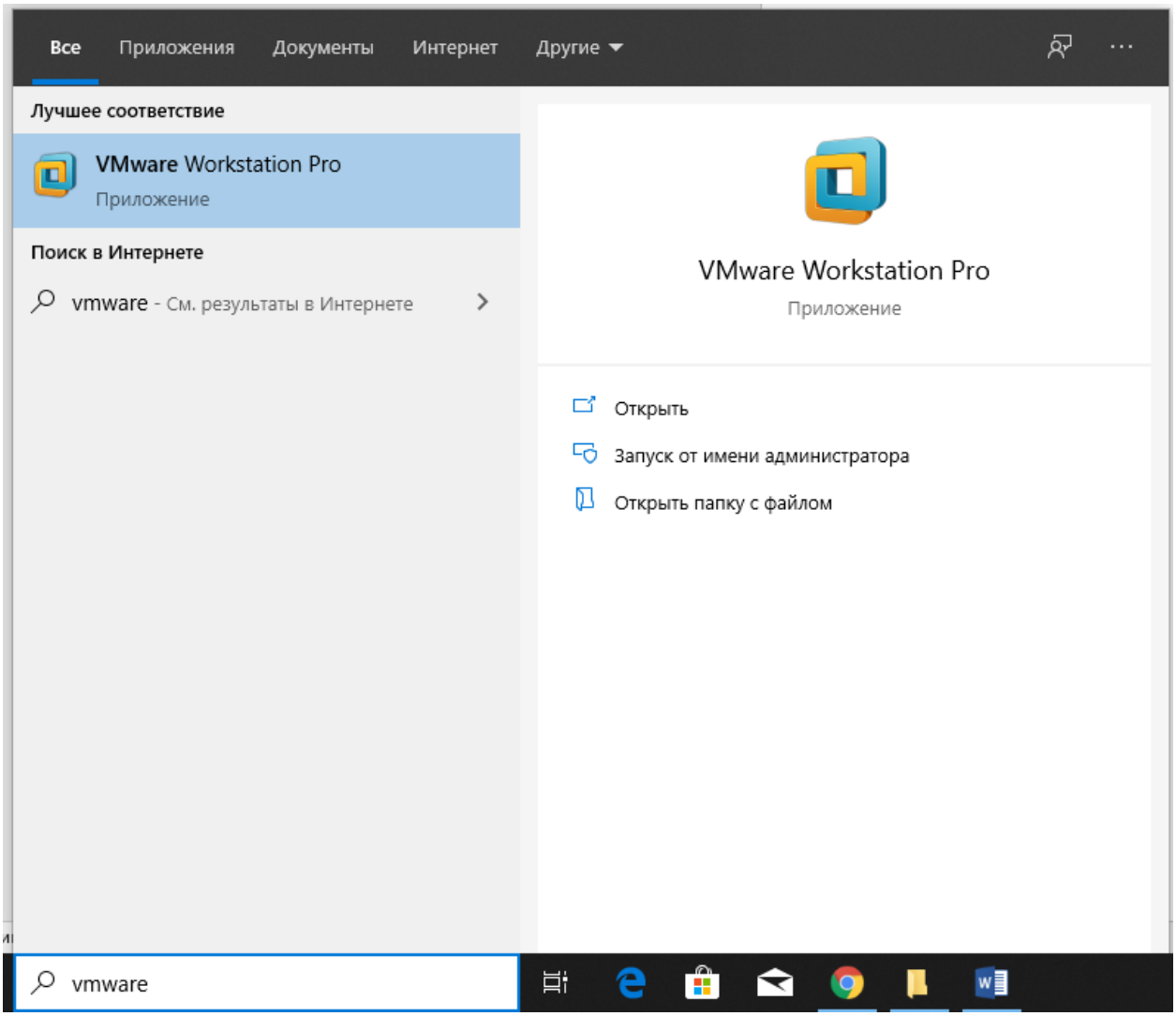
Ход работы:
1. Выполнить упражнения.
2. Ответить на контрольные вопросы.
3. Составить отчёт.

Упражнения:
1. Создать виртуальную машину и установить на ней ОС Windows 10
2. Создать виртуальную машину и установить на ней ОС Xubuntu 20.04

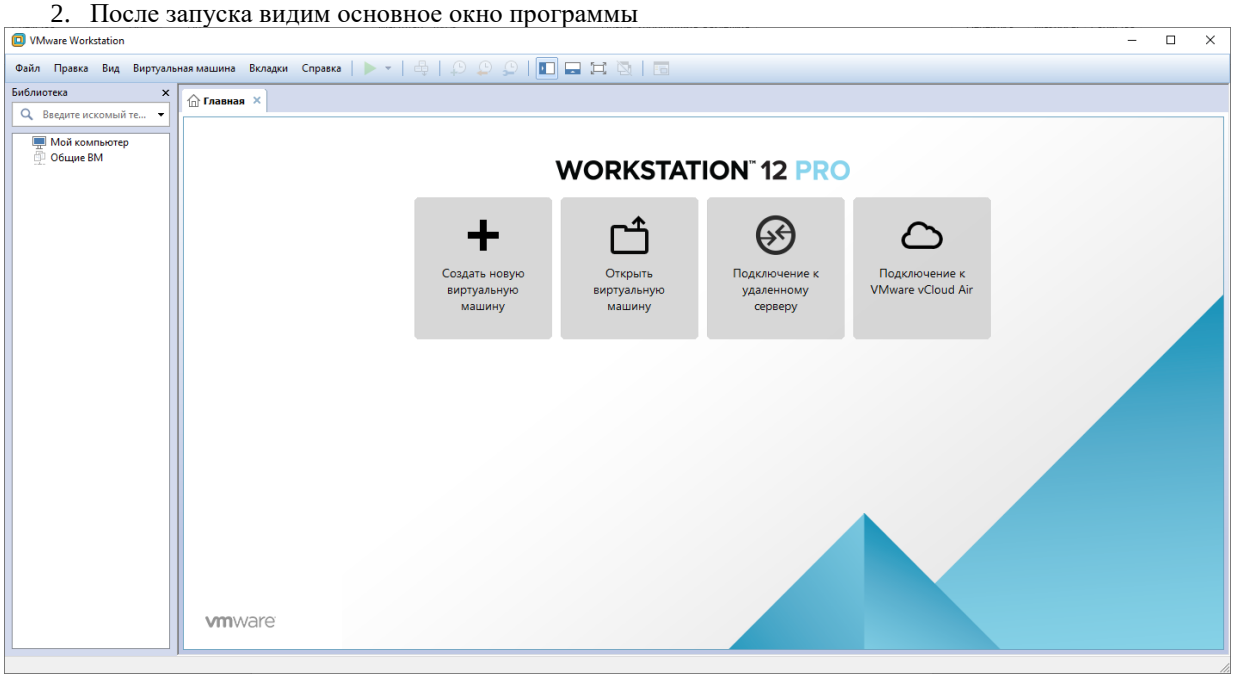
При установке везде где это необходимо вводить данные в формате “Группа, инициалы”.
Контрольные вопросы:
1. Какие есть различия в установках этих ОС?
2. Какая ОС больше использует ресурсов? (Пояснения + скрины)
3. В чём различия ОС x64, x32, x86?

Основные источники:
Поддержка и тестирование программных модулей: учебник для среднего профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2025. — 145 с. — (Профессиональное образование). — ISBN 978-5-534-19290-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580603

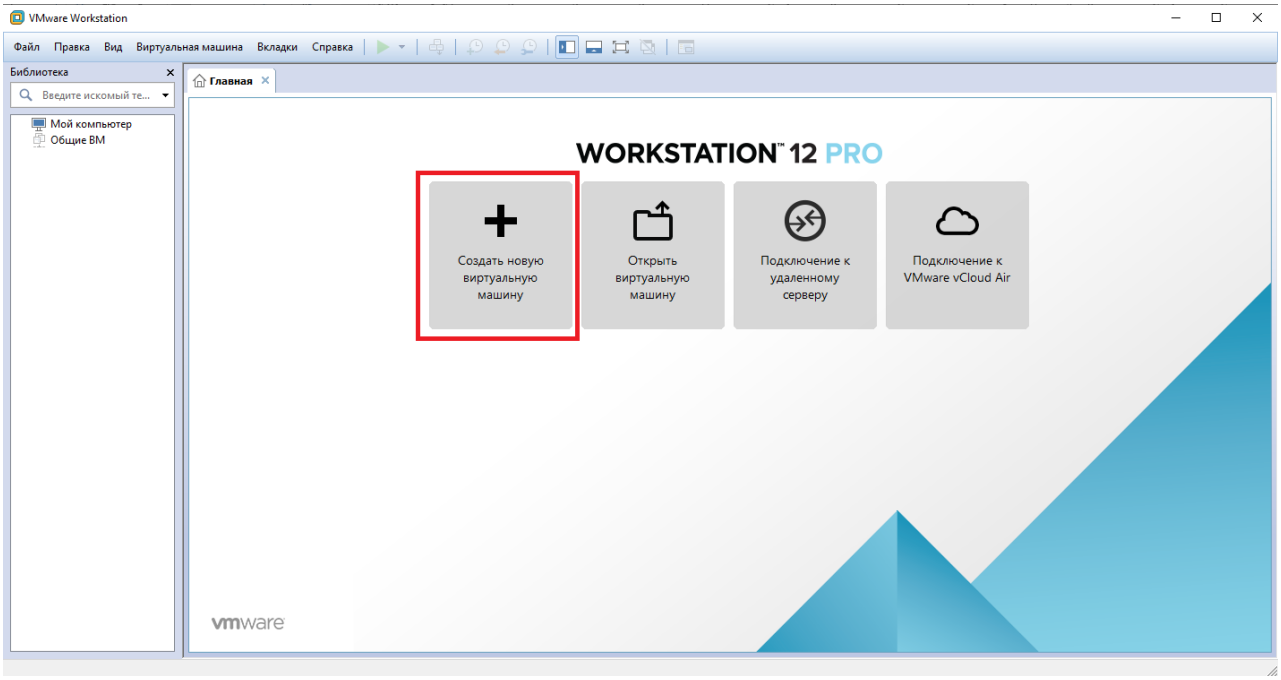
Справочный материал:
1. Найти и запусти программу VMWare



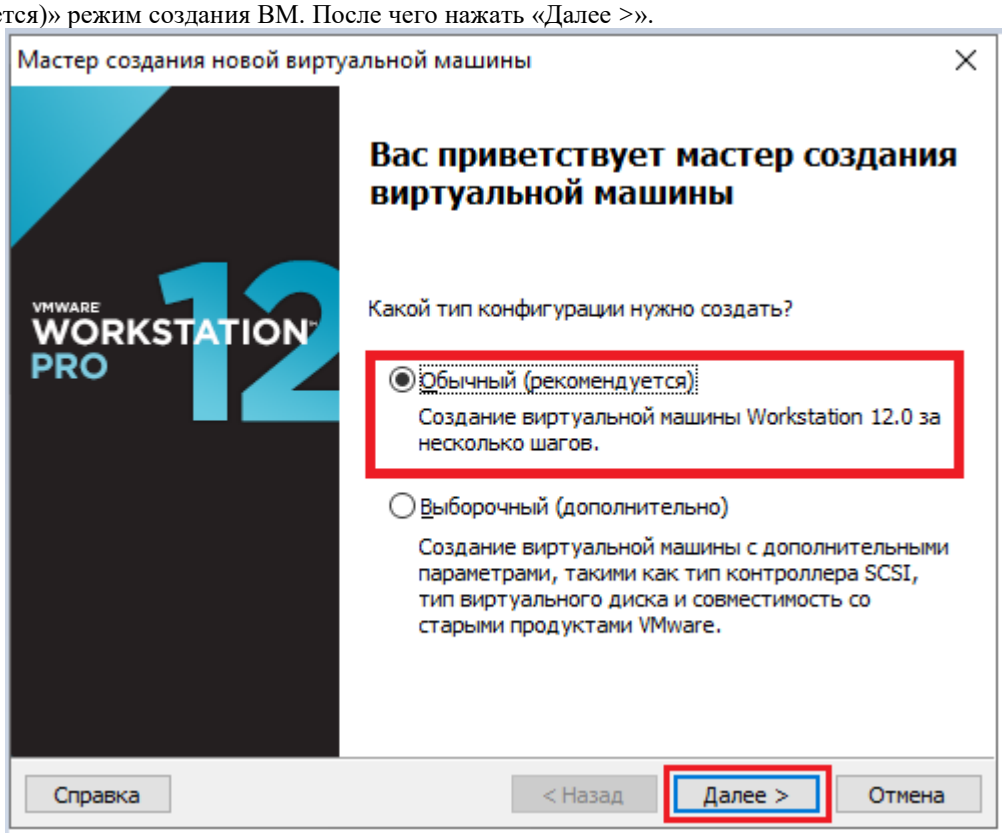
2. После запуска видим основное окно программы



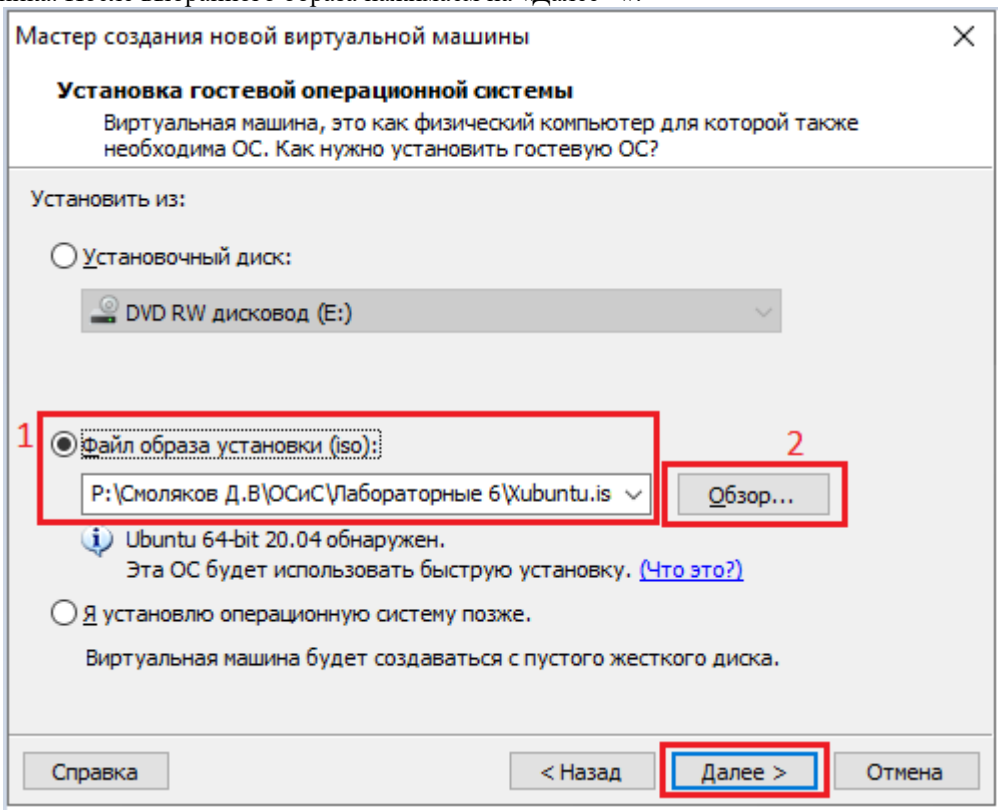
3. Нажимаем кнопку «Создать новую виртуальную машину»



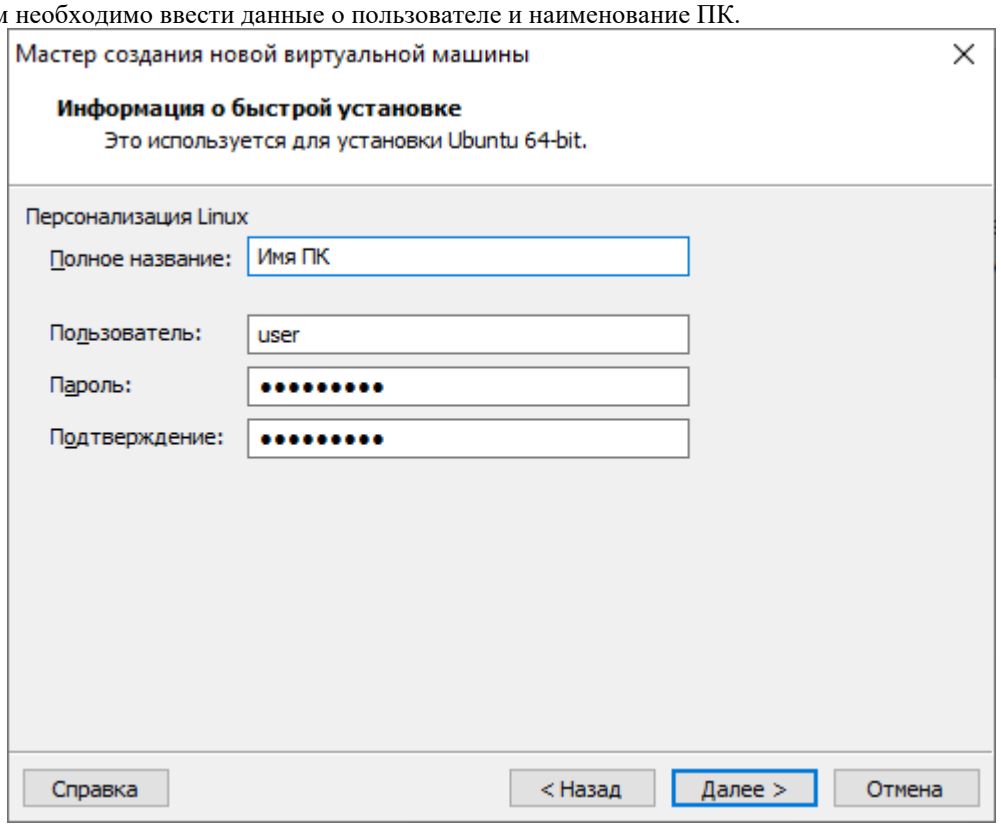
4. Начинаем работу с диалоговым окном создания. Рекомендуется выбирать «Обычный (рекомендуется)» режим создания ВМ. После чего нажать «Далее >».



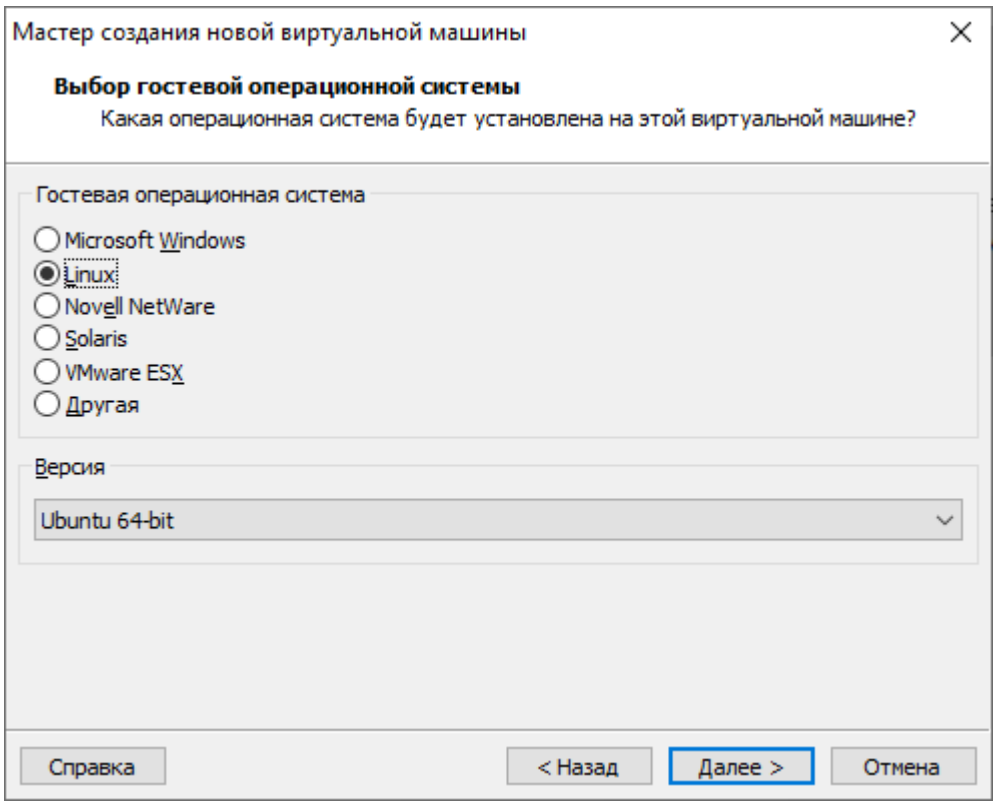
5. На следующем шаге мы выбираем образ операционной системы для ВМ. Для это нужно выбрать «Файл образа установки»(1) и нажать «Обзор…»(2). Следящим шагом выбрать образ в окне проводника (путь до образа ОС узнать у преподавателя) и выбрать его, нажатием по нему и нажатием на кнопку «Открыть» в окне проводника. После выбранного образа нажимаем на «Далее >».



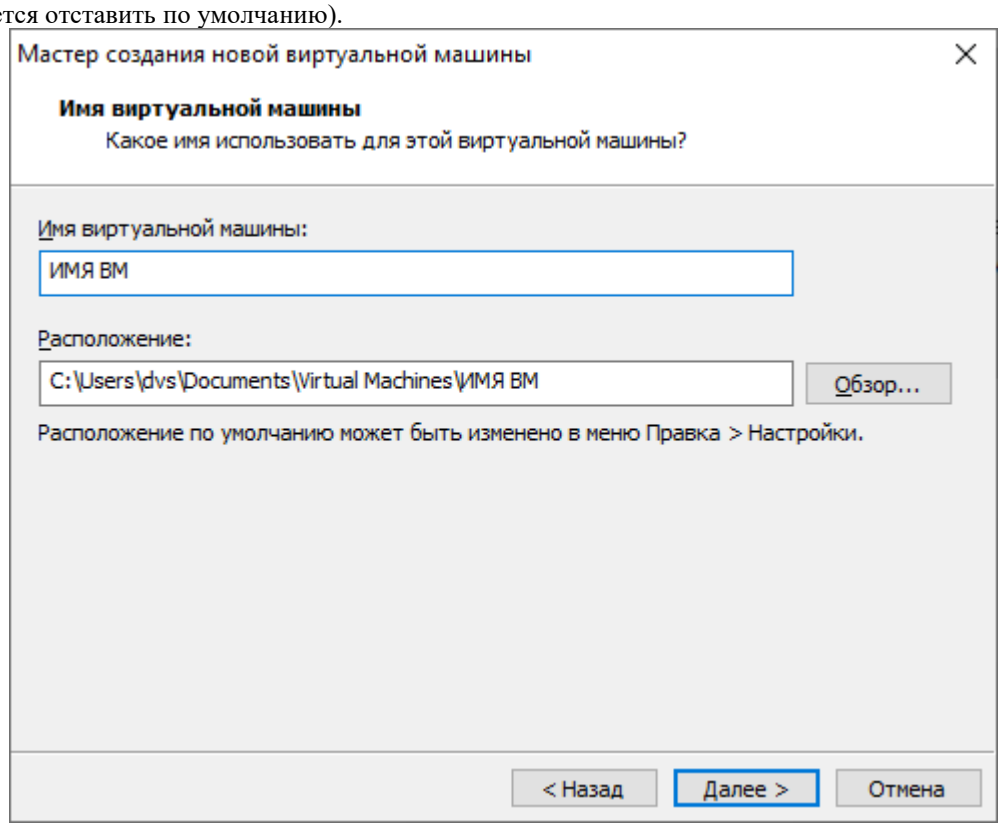
6. Следующие шаги для разных операционных систем разные. Если вы устанавливаете дистрибутив Linux, то вам необходимо ввести данные о пользователе и наименование ПК.



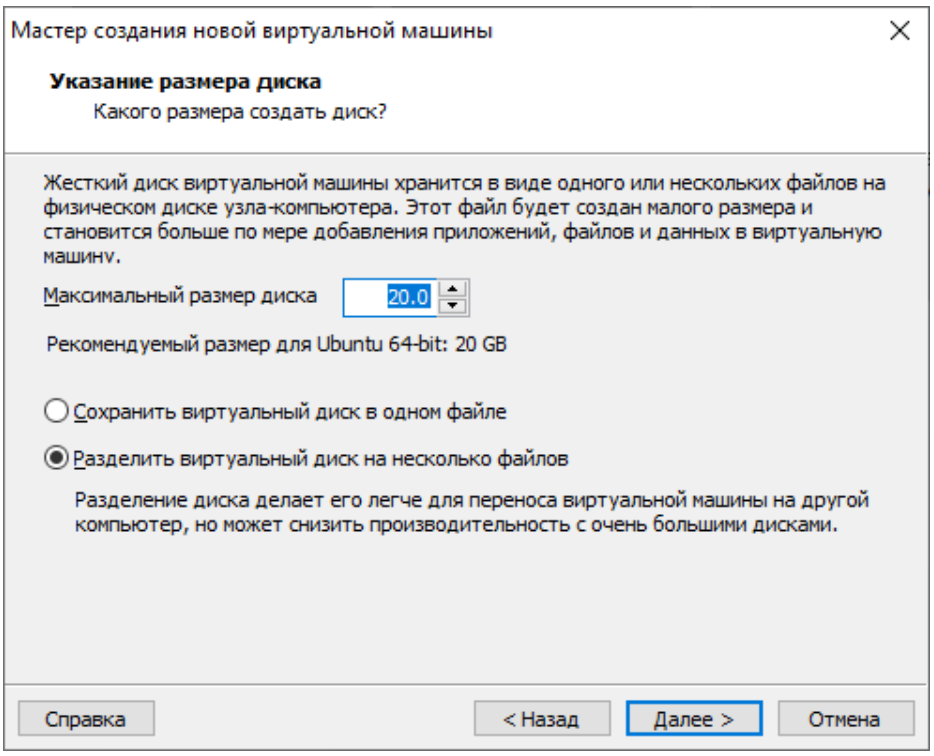
7. Если вы устанавливаете операционную систему семейства Windows, то вас встретит диалоговое окно с уточнение операционной системы. Где необходимо выбрать семейство ОС и версию в выпадающем списке (семейство и версию можно уточнить у преподавателя).



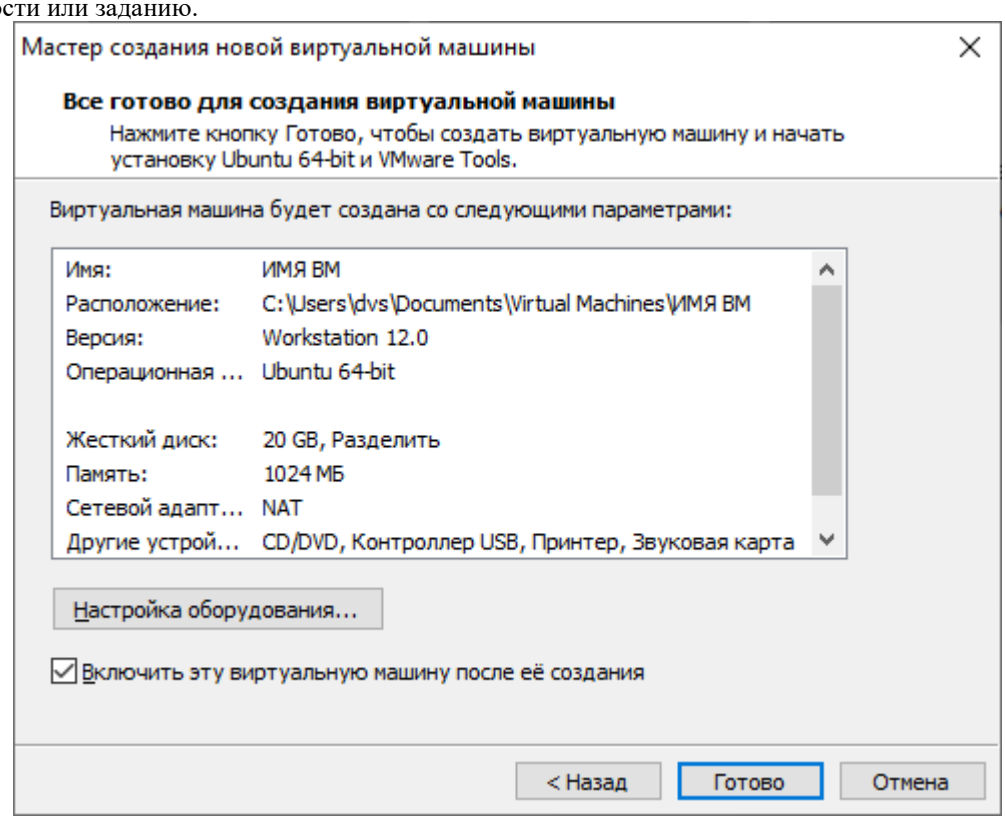
8. Следующее диалоговое окно попросит нас ввести имя виртуальной машины (по необходимости или заданию), и выбрать путь расположения файлом ВМ который можно поменять по необходимости или заданию (рекомендуется отставить по умолчанию).



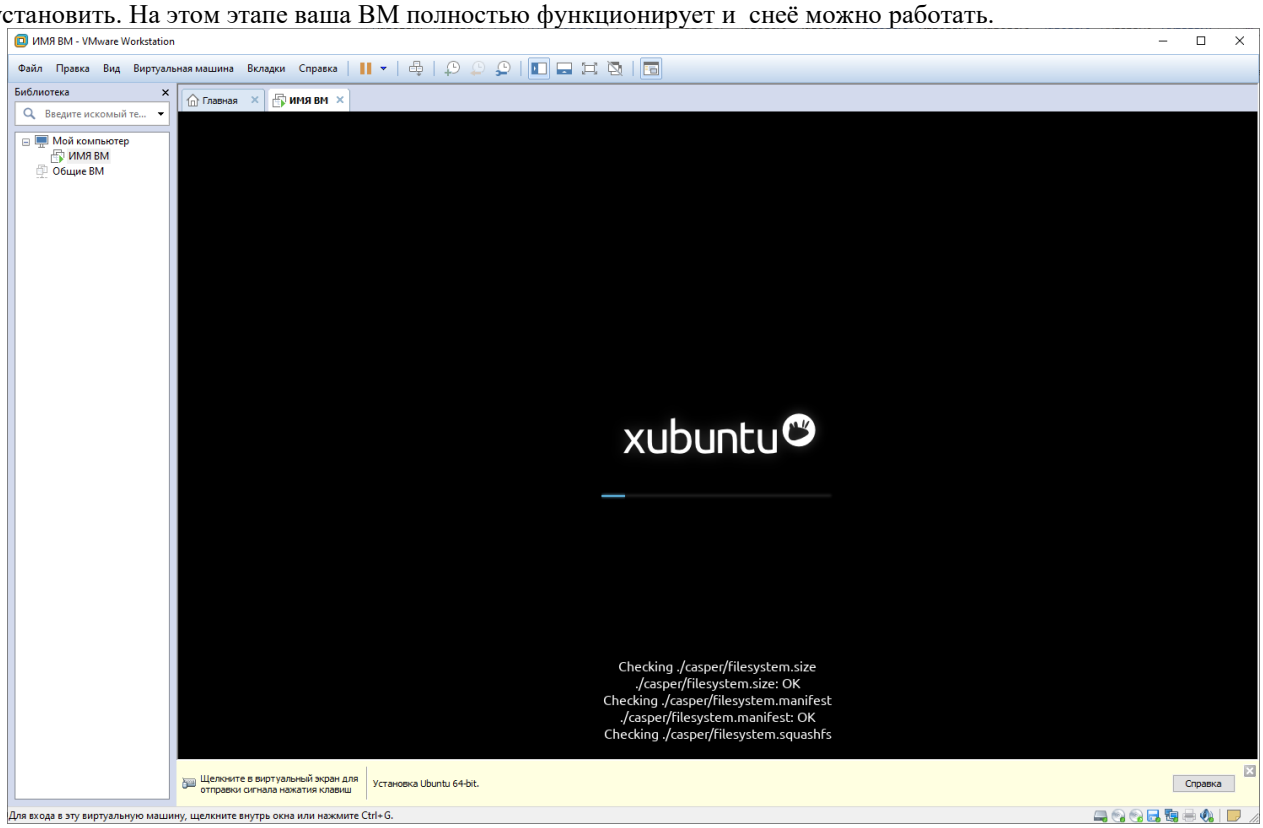
9. После чего, следующее диалоговое окно просит указать размер жесткого диска вашей ВМ и указать вариант хранения этих файлов (в одном/в нескольких). Оба этих параметра можно изменить по необходимости или заданию (рекомендуется отставить по умолчанию).



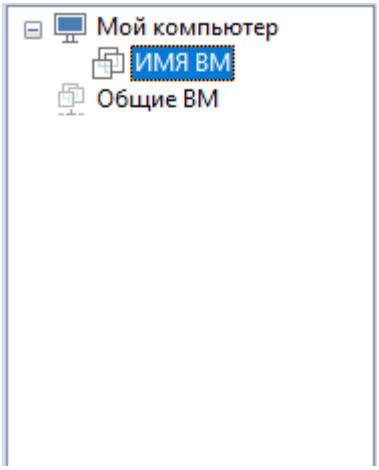
10. ВМ почти готова. Остался последний шаг, где необходимо убедить в правильности настроек для ВМ, и внести изменения поменять по необходимости или заданию (рекомендуется отставить по умолчанию). Так же можно убрать «галочку» с параметра «Включить эту виртуальную машину после её создания» по необходимости или заданию.



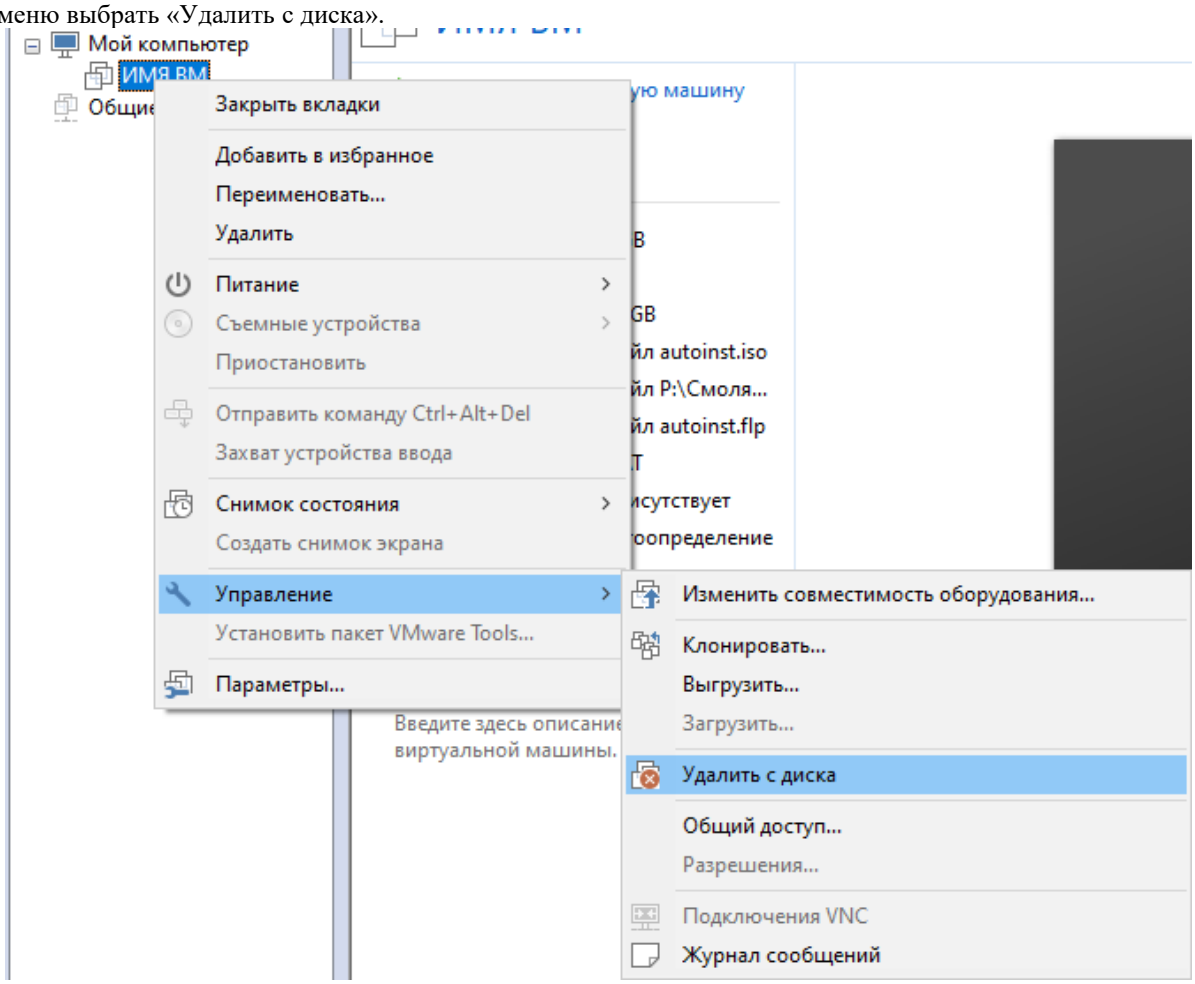
11. После включения ВМ сразу начнёт загружать ту операционную систему, которую вы хотите установить. На этом этапе ваша ВМ полностью функционирует и снеё можно работать.



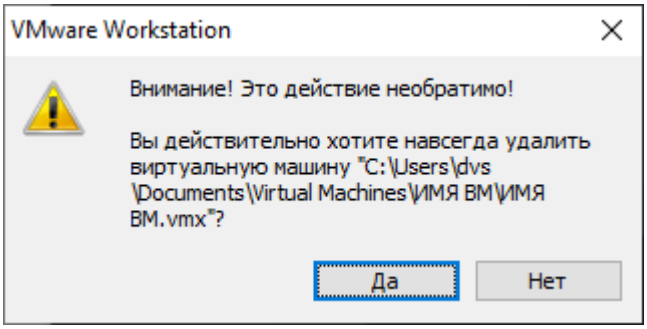
12. После работы, будьте добры удалить вашу ВМ. Для этого, нужно выбрать вашу ВМ в списке основного окна программы.



13. После этого, нажать ПКМ (правая кнопка мыши) по ней, выбрать пункт «Управление», а в этом подменю выбрать «Удалить с диска».



14. Подтвердить своё действие.



15. Готово, ваша ВМ удалена.

Критерии оценки:

№	Критерий	Баллы
1	Виртуальная машина создана, на ней установлена ОС Windows 10	10
2	Виртуальная машина создана, на ней установлена ОС Xubuntu 20.04	10
3	Оформление отчета соответствует требованиям (шрифт, поля, отступы, интервалы, оформление рисунков, автоматическое оглавление)	10
4	Ответы на контрольные вопросы	10
Итого		40

Перевод в пятибалльную систему оценивания

Оценка	Кол-во баллов
«отлично»	от 34 до 40

«хорошо»	от 29 до 33
«удовлетворительно»	от 21 до 28
«неудовлетворительно»	менее 20

3.2.2. Типовые задания для оценки освоения МДК.02.02. Обеспечение безопасности информационных ресурсов

1) Задания в тестовой форме

Тест №2

1: Что такое безопасность данных?
A) Защита данных от несанкционированного доступа и потери
B) Процесс создания резервных копий данных
C) Хранение данных в облаке
D) Удаление ненужных данных
Правильный ответ: A) Защита данных от несанкционированного доступа и потери
2: Какой из следующих методов не относится к безопасности данных?
A) Шифрование данных
B) Аутентификация пользователей
C) Оптимизация базы данных
D) Резервное копирование данных
Правильный ответ: C) Оптимизация базы данных
3: Какой тип резервного копирования предполагает создание полной копии всех данных?
A) Полное резервное копирование
B) Инкрементное резервное копирование
C) Дифференциальное резервное копирование
D) Мульти-резервное копирование
Правильный ответ: A) Полное резервное копирование
4: Какой из следующих методов восстановления данных является наиболее быстрым?
A) Полное восстановление из резервной копии
B) Восстановление отдельных файлов из резервной копии
C) Восстановление системы с помощью образа диска
D) Восстановление через облачное хранилище
Правильный ответ: B) Восстановление отдельных файлов из резервной копии
5: Какой из следующих типов файловых систем используется в Windows?
A) ext4
B) NTFS
C) HFS+
D) XFS
Правильный ответ: B) NTFS
6: Что такое "файловая система"?
A) Программа для редактирования текстов
B) Способ организации и хранения файлов на носителе информации
C) Устройство для хранения данных
D) Метод создания резервных копий данных
Правильный ответ: B) Способ организации и хранения файлов на носителе информации
7: Какой язык используется для работы с реляционными базами данных?
A) HTML
B) SQL
C) Python
D) JavaScript
Правильный ответ: B) SQL
8: Что такое "нормализация" в контексте баз данных?
A) Процесс удаления дубликатов данных
B) Процесс упрощения структуры базы данных
C) Процесс оптимизации запросов к базе данных
D) Процесс распределения данных по нескольким таблицам
Правильный ответ: D) Процесс распределения данных по нескольким таблицам

9: Какой тип хостинга обеспечивает пользователю полный контроль над сервером?
A) Shared hosting (общий хостинг)
B) VPS (виртуальный частный сервер)
C) Dedicated hosting (выделенный хостинг)
D) Cloud hosting (облачный хостинг)
Правильный ответ: C) Dedicated hosting (выделенный хостинг)
10: Какой из следующих типов хостинга обычно используется для небольших веб-сайтов?
A) VPS (виртуальный частный сервер)
B) Shared hosting (общий хостинг)
C) Dedicated hosting (выделенный хостинг)
D) Colocation hosting (колокационный хостинг)
Правильный ответ: B) Shared hosting (общий хостинг)
11: Какой из следующих методов контроля доступа основан на ролях пользователей?
A) DAC (Discretionary Access Control - Дискреционный контроль доступа)
B) MAC (Mandatory Access Control - Обязательный контроль доступа)
C) RBAC (Role-Based Access Control - Контроль доступа на основе ролей)
D) ABAC (Attribute-Based Access Control - Контроль доступа на основе атрибутов)
Правильный ответ: C) RBAC (Role-Based Access Control - Контроль доступа на основе ролей)
12: Что такое "дискреционный контроль доступа"?
A) Контроль доступа, основанный на политике безопасности организации
B) Контроль доступа, предоставляемый владельцем объекта ресурсов
C) Контроль доступа, основанный на атрибутах пользователя
D) Контроль доступа, который невозможно изменить
Правильный ответ: B) Контроль доступа, предоставляемый владельцем объекта ресурсов
13: Какой документ описывает политику доступа к информационным системам организации?
A) Положение о конфиденциальности
B) Политика безопасности информации
C) Регламент работы службы поддержки
D) Договор о неразглашении
Правильный ответ: B) Политика безопасности информации
14: Какое действие необходимо предпринять для учета доступа пользователей к системам?
A) Хранить пароли в открытом виде
B) Вести журналы аудита доступа
C) Игнорировать несанкционированные попытки доступа
D) Удалить все учетные записи пользователей после завершения проекта
Правильный ответ: B) Вести журналы аудита доступа
15: Какой из следующих методов используется для аутентификации пользователей?
A) Шифрование данных
B) Брандмауэр
C) Парольная защита
D) Резервное копирование
Правильный ответ: C) Парольная защита
16: Что такое многофакторная аутентификация?
A) Использование одного метода аутентификации
B) Использование нескольких методов аутентификации
C) Использование только паролей
D) Аутентификация без пароля
Правильный ответ: B) Использование нескольких методов аутентификации
17: Какой из следующих методов контроля прав пользователей считается наиболее безопасным?
A) Пароль
B) Биометрическая аутентификация
C) Секретные вопросы
D) SMS-код
Правильный ответ: B) Биометрическая аутентификация
18: Что такое "аудит безопасности"?
A) Процесс создания резервных копий
B) Оценка системы на предмет уязвимостей
C) Процесс шифрования данных
D) Оценка качества обслуживания клиентов
Правильный ответ: B) Оценка системы на предмет уязвимостей
19: Какой из следующих методов защиты данных предполагает их шифрование перед отправкой по сети?
A) Аутентификация
B) Доступ по паролю

C) VPN (Virtual Private Network - виртуальная частная сеть）

D）Брандмауэр

Правильный ответ: C）VPN (Virtual Private Network - виртуальная частная сеть）

20: Что такое "распределенный контроль доступа"?

A）Контроль доступа, который осуществляется централизованно

B）Контроль доступа, который осуществляется несколькими системами

C）Контроль доступа, который основан только на паролях

D）Контроль доступа, который невозможно изменить

Правильный ответ: B）Контроль доступа, который осуществляется несколькими системами

Критерии оценки:

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%

2)Практическое занятие № 1. «Анализ безопасности веб-сервиса на предмет наличия уязвимостей»

Цель: формирование умения применять методы и средства идентификации и эксплуатации уязвимостей в веб-приложениях

Формируемые компетенции: ПК 2.2, ПК 2.3, ПК 2.4, ОК 1-5, ОК 7, ОК 9

Инструкция по выполнению:

1. Ознакомиться с заданием.
2. Скачать образ и создать виртуальную машину на его основе.
3. Выполнить идентификацию и эксплуатацию уязвимостей к атакам SQLinjection согласно представленным шагам.
4. Отправить на проверку отчет, содержащий:
5. Список выполненных действий с кратким описанием.
6. Скриншоты ключевых этапов выполнения работы.
7. Защитить работу, представив основные шаги выполнения работы.

1. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Атака внедрения операторов SQL (SQL-injection) – это внедрение во входные данные, обрабатываемые веб-приложением, операторов языка SQL.

Необходимым условием уязвимости к атаке SQL-injection является недостаточная обработка входных недоверенных данных при формировании веб-приложением SQL-запросов, зависящих от этих данных.

Атака SQLinjection позволяет злоумышленнику получить непосредственный доступ к данным через механизмы СУБД в обход логики веб-приложения.

В зависимости от используемой веб-приложением СУБД и условий внедрения выделяют следующие разновидности атак SQL-injection:

− классическая;
− «слепая» типа boolean-based;
− «слепая» типа time-based;
− error-based;
− вложенная;
− фрагментированная.

Рассмотрим примеры базовых тестов, обнаруживающих уязвимость параметра id к атаке SQL-injection:

− http://www.test.app.com/index?id=1'
− http://www.test.app.com/index?id=1"
− http://www.test.app.com/index?id=1' order by 1000
− http://www.test.app.com/index?id=1"--
− http://www.test.app.com/index?id=1'/*
− http://www.test.app.com/index?id=1"#
− http://www.test.app.com/index?id=1 and 1=1—
− http://www.test.app.com/index?id=1 and 1=2-

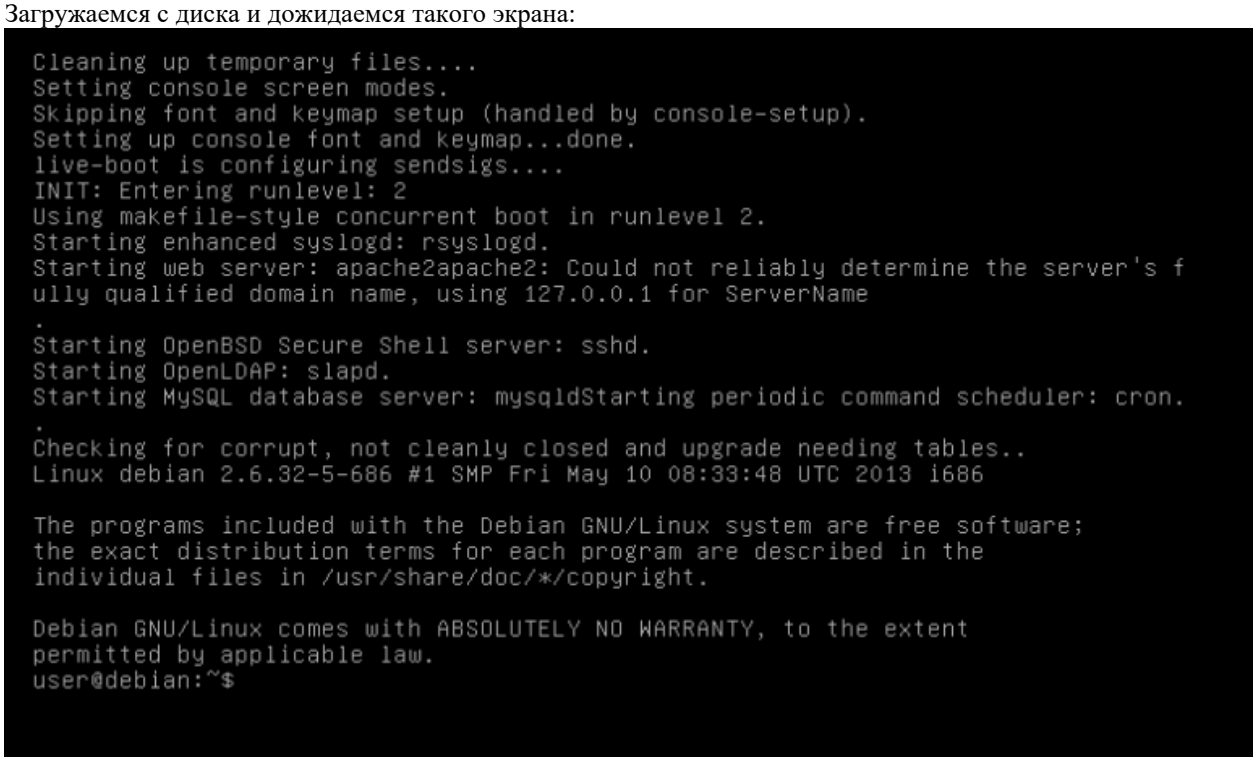
− http://www.test.app.com/index?id=1' and '1'='1
− http://www.test.app.com/index?id=1' and '1'='2

Последовательность действий

Шаг 1. Скачать образ «Web For Pentesters» с веб-сайта www.pentesterlab.com.

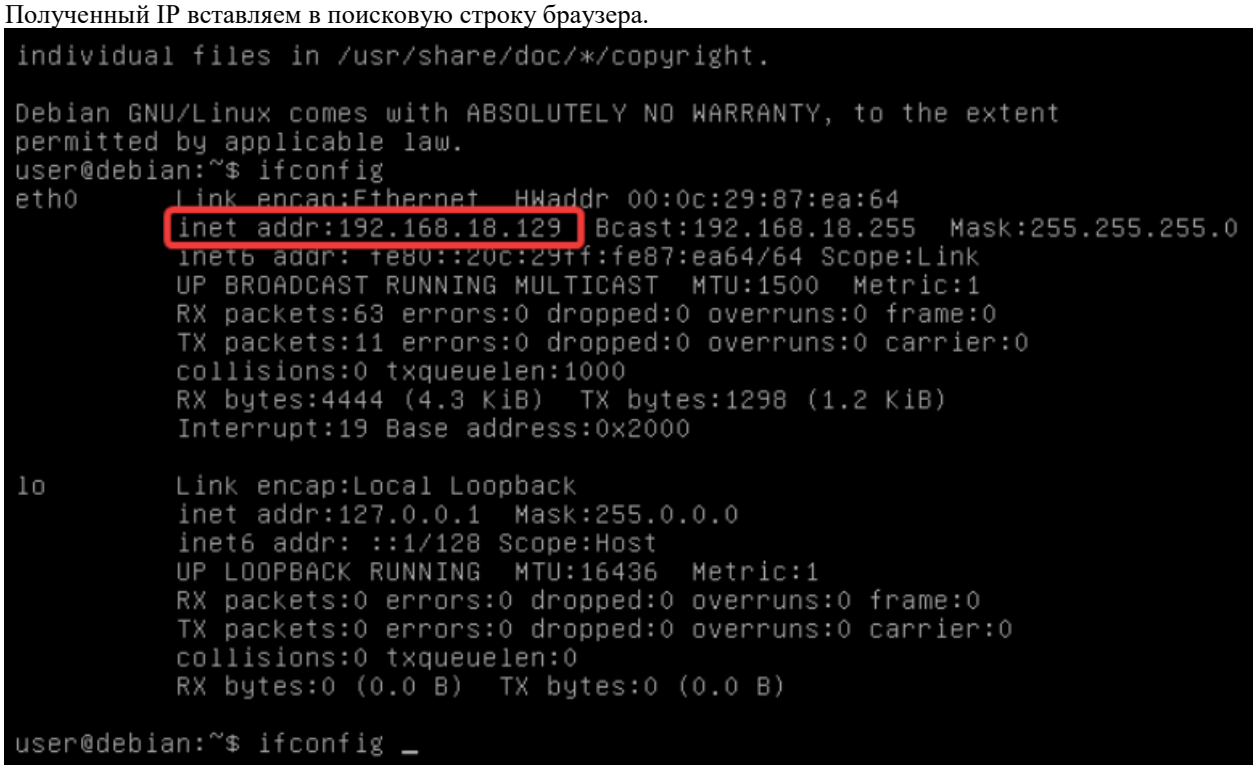
Создаем виртуальную машину.

Загружаемся с диска и дожидаемся такого экрана:



Пишем в строку ifconfig.

Полученный IP вставляем в поисковую строку браузера.



Шаг 2. Перейти по ссылке «SQL injections → Example 1». Проанализировать логику функционирования веб-приложения. Последовательно ввести следующие запросы, обращая внимание на вывод веб-приложения, сделать предположение о структуре используемого SQL-запроса:

− sqli/example1.php?name=root'
− sqli/example1.php?name=root''
− sqli/example1.php?name=root'%201=1

− sqli/example1.php?name=root'%201=1#
− sqli/example1.php?name=root'%201=1%20-
− sqli/example1.php?name=root'%201=1%20/*
− sqli/example1.php?name=root'%20'1'='1
− sqli/example1.php?name=root'%20'1'='2
− sqli/example1.php?name=root'%23sqli
Последние три запроса позволяют сделать вывод об уязвимости параметра name к атаке SQL-injection.
Шаг 3. Перейти по ссылке «SQL injections → Example 2». Проанализировать логику функционирования веб-приложения. Последовательно ввести следующие запросы, обращая внимание на вывод веб-приложения, сделать предположение о структуре используемого SQL-запроса:
− sqli/example2.php?name=root%20and%201=1
− sqli/example2.php?name=root'%09and%09'1'='1
− sqli/example2.php?name=root'%09and%09'1'='2
− sqli/example2.php?name=root'%2b%2b'
Последние три запроса позволяют сделать вывод об уязвимости параметра name к атаке SQL-injection.
Шаг 4. Перейти по ссылке «SQL injections → Example 3». Проанализировать логику функционирования веб-приложения. Последовательно ввести следующие запросы, обращая внимание на вывод веб-приложения, сделать предположение о структуре используемого SQL-запроса:
− sqli/example3.php?name=root%20and%201=1
− sqli/example3.php?name=root'/**/and/**/'1'='1
− sqli/example3.php?name=root'/**/and/**/'1'='2
− sqli/example3.php?name=root'%2b%2b'
Последние три запроса позволяют сделать вывод об уязвимости параметра name к атаке SQL-injection.
Шаг 5. Перейти по ссылке «SQL injections → Example 4». Проанализировать логику функционирования веб-приложения. Последовательно ввести следующие запросы, обращая внимание на вывод веб-приложения, сделать предположение о структуре используемого SQL-запроса:
− sqli/example4.php?id=2
− sqli/example4.php?id=2'
− sqli/example4.php?id=2"
− sqli/example4.php?id=1%2b1
− sqli/example4.php?id=0%2b2
− sqli/example4.php?id=3-1
Последние три запроса позволяют сделать вывод об уязвимости параметра id к атаке SQL-injection.
Просмотреть исходный код PHP-сценария.
Шаг 6. Перейти по ссылке «SQL injections → Example 5». Проанализировать логику функционирования веб-приложения. Последовательно ввести следующие запросы, обращая внимание на вывод веб-приложения, сделать предположение о структуре используемого SQL-запроса:
− sqli/example5.php?id=2
− sqli/example5.php?id=2'
− sqli/example5.php?id=2"
− sqli/example5.php?id=1%2b1
− sqli/example5.php?id=0%2b2
− sqli/example5.php?id=3-1
Последние три запроса позволяют сделать вывод об уязвимости параметра id к атаке SQL-injection.
Просмотреть исходный код PHP-сценария.
Шаг 7. Перейти по ссылке «SQL injections → Example 6». Проанализировать логику функционирования веб-приложения. Последовательно ввести следующие запросы, обращая внимание на вывод веб-приложения, сделать предположение о структуре используемого SQL-запроса:
− sqli/example6.php?id=2
− sqli/example6.php?id=2'
− sqli/example6.php?id=2"
− sqli/example6.php?id=1%2b1
− sqli/example6.php?id=0%2b2
− sqli/example6.php?id=3-1
− sqli/example6.php?id=5-3
Последние три запроса позволяют сделать вывод об уязвимости параметра id к атаке SQL-injection.
Просмотреть исходный код PHP-сценария.
Шаг 8. Перейти по ссылке «SQL injections → Example 7». Проанализировать логику функционирования веб-приложения. Последовательно ввести следующие запросы, обращая внимание на вывод веб-приложения, сделать предположение о структуре используемого SQL-запроса:
− sqli/example7.php?id=2
− sqli/example7.php?id=2'
− sqli/example7.php?id=2"

− sqli/example7.php?id=1%2b1
− sqli/example7.php?id=3-1
− sqli/example7.php?id=2%0Aand%201=1
− sqli/example7.php?id=2%0Aand%201=2
− sqli/example7.php?id=2%0A%23sqli
Последние три запроса позволяют сделать вывод об уязвимости параметра id к атаке SQL-injection.
Выполнить следующие запросы для извлечения данных из СУБД:
− sqli/example7.php?id=2%0Aunion%20select%201
− sqli/example7.php?id=2%0Aunion%20select%201,2
− sqli/example7.php?id=2%0Aunion%20select%201,2,3
− sqli/example7.php?id=2%0Aunion%20select%201,2,3,4 45
− sqli/example7.php?id=2%0Aunion%20select%201,2,3,4, 5
− sqli/example7.php?id=2%0Aunion%20select%20name, passwd,1,1,1 from users
Ручными методами получить данные из базы данных. Просмотреть исходный
код PHP-сценария.

Требования к отчету
Общие требования:
1. Шрифт – PT ASTRA SERIF, 14 пт.
2. Интервалы: междустрочный – 1,5 строки, интервал до и после абзаца – 0 пт.
3. Отступ первой строки – 1,25
4. Рисунки и подписи к ним выравниваются по центру.

Требования к структуре отчета:
1. Титульный лист
2. Содержание
3. Основная часть:
4. Отчет по решению заданий для выполнения. (Если предусмотрены)
5. Отчет по решению индивидуальных заданий
6. Выводы по работе
7. Ответы на контрольные вопросы (если предусмотрены)

Основные источники:

1.Щербак, А. В. Информационная безопасность: учебникдля среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/557735

2.Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособиедля среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/542339

3.Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособиедля среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/542340

4.Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособиедля среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/542339

5.Организационное и правовое обеспечение информационной безопасности: учебникдля среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/555949

Критерии оценки:

№ п.п	Критерий	Баллы
1	Идентификация и эксплуатация уязвимостей к атакам SQLinjection выполнена согласно представленным шагам	5

2	Отражённый в отчёте анализ достаточно подробно описывает действия и результаты выполненной работы	10
3	Отчет оформлен корректно	10
4	Работа защищена	20
	Итого	45

Перевод в пятибалльную систему оценивания

Оценка	Кол-во баллов
«отлично»	от 40 до 45
«хорошо»	от 34 до 39
«удовлетворительно»	от 26 до 33
«неудовлетворительно»	менее 26

4. КОНТРОЛЬ ПРИОБРЕТЕНИЯ ПРАКТИЧЕСКОГО ОПЫТА. ОЦЕНКА ПО УЧЕБНОЙ И (ИЛИ) ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

4.1. Общие положения

Оценка по учебной и (или) производственной практике выставляется на основании данных характеристики профессиональной деятельности обучающегося/студента на практике с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

4.2. Виды работ практики и проверяемые результаты обучения по профессиональному модулю

Таблица 3

Код ПК	Виды и объем работ на учебной практике	Документ, подтверждающий качество выполнения работ
1	**2**	**3**
ПК 2.1 ПК 2.5 ОК 1-5, ОК 7, ОК 9	Проанализировать организацию заказчика и предложить алгоритм работы технической поддержки.	Отчет по учебной практике
ПК 2.2 ПК 2.3 ПК 2.4 ОК 1-5, ОК 7, ОК 9	Проанализировать организацию заказчика и разработать регламент по резервному копированию данных и доступу пользователей к системе.	Отчет по учебной практике

Таблица 4

Код ПК	Виды и объем работ на учебной практике	Документ, подтверждающий качество выполнения работ
1	**2**	**3**
ПК 2.1 ПК 2.5 ОК 1-5, ОК 7, ОК 9	Проанализировать организацию заказчика и разработать инструкцию по развертыванию используемого программного обеспечения для поддержания функционирования веб-приложений компании.	Отзыв с места практики Отчет по производственной практике
ПК 2.2 ПК 2.3 ПК 2.4 ОК 1-5, ОК 7, ОК 9	Проанализировать организацию заказчика и разработать регламент по обеспечению безопасности функционирования используемого веб-приложения.	Отзыв с места практики Отчет по производственной практике

5. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

5.1.1. Контрольно-оценочные материалы для дифференцированного зачета МДК 02.01 Настройка и сопровождение информационных ресурсов

I. ПАСПОРТ

Назначение:

Контрольно-оценочные материалы предназначены для контроля и оценки результатов освоения междисциплинарного курса
Настройка и сопровождение информационных ресурсов
по специальности СПО:
09.02.09, Веб-разработка
Промежуточная аттестация включает в себя ответ на тестовые вопросы открытого и закрытого типов.

II. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ. Вариант № 1

Инструкция: дайте ответы на представленные ниже вопросы.
Время выполнения задания: 60 минут

1. Какая из операционных систем предпочтительна для использования в целях защиты информации и для работы с информацией разного уровня секретности, в том числе со степенью «совершенно секретно»?
   1) Astra Linux Common Edition
   2) Astra Linux Special Edition
   3) Windows
   4) MacOS
2. Укажите участников взаимодействия по протоколу http
   1) Клиент
   2) Сервер
   3) Персональное устройство пользователя (ПК, мобильное устройство)
   4) Маршрутизатор
3. Какой из протоколов передачи данных необходимо выбирать при организации веб-страниц с с конфиденциальными данными?
   1) http
   2) https
   3) ftp
   4) smtp
4. Установите правильный порядок действий, выполняемых DNS при связи одного компьютера с другим в интернете:
   1) Запрос компьютера к DNS серверу для получения IP-адреса
   2) Если имя не найдено в кэше, то перенаправление к корневому серверу
   3) Поиск запрошенного доменного имени в кэше DNS сервера
   4) Связь с веб-сервером по IP-адресу и получение доступа к веб-странице
   5) Возвращение IP-адреса

5. Установите соответствие между наименованиями стеков для разработки динамических веб-сайтов и их назначением:

1) WAMP
2) LAMP
3) LEMP

A) стек открытого серверного программного обеспечения, который состоит из операционной системы Linux, веб-сервера Apache, системы управления базами данных (СУБД) MySQL и языка программирования PHP.

B) стек для разработки и развертывания веб-приложений из операционной системы Linux, веб-сервера Nginx, системы управления базами данных (СУБД) MySQL и языка программирования PHP.

C) стек для разработки динамических веб-сайтов и приложений, состоящий из Windows, веб-сервера Apache, системы управления базами данных (СУБД) MySQL и языка программирования PHP.

6. Дополните предложение: Один из самых популярных конструкторов сайтов, позволяющий онлайн собирать и публиковать сайты из готовых блоков

7. Вставьте пропущенное слово: CMS — это системы управления _____.

8. Как называется процесс установки и настройки системы управления контентом (CMS) на сервере для запуска сайта или веб-приложения

9. Как называется услуга, которая позволяет разместить сайт на сервере, доступном для пользователей интернета.

10. Назовите, какой тип хостинга (сервера) выбрать для большого интернет-магазина с высоким трафиком, имеющих сложную систему корзины и оплаты

11. Какая профессиональная документация может использоваться сотрудником технической поддержки в области настройки и сопровождения информационных ресурсов?

1) Технические руководства
2) Стандарты и регламенты
3) Руководство программиста
4) Техническое задание

12. Документ, который предоставляет пользователям информацию о том, как использовать определенное программное обеспечение, оборудование или систему - это

1) Техническое задание
2) Руководство пользователя
3) Руководство администратора
4) Спецификация

13. Какой документ следует выбрать, чтобы получить пошаговые инструкции по установке программного обеспечения или оборудования?

1) Техническое задание
2) Руководство пользователя
3) Руководство администратора
4) Спецификация

14. Установите правильный порядок действий, выполняемых DNS при связи одного компьютера с другим в интернете:

1) Введение и общие сведения
2) Управление пользователями
3) Установка и настройка
4) Резервное копирование, управление производительностью и безопасность системы
5) Устранение неполадок

15. Установите соответствие между наименованием документа и его назначением:

1) Руководство пользователя
2) Руководство Программиста
3) Руководство администратора

A) Обеспечение необходимыми знаниями для установки, настройки и эффективного управления системами, обеспечения их безопасности и надежности.

B) Обеспечение необходимой информацией об архитектуре системы и ее компонентов, использованию API, библиотек и фреймворков при разработке модулей и компонентов программного обеспечения, для создания новых функций и интеграции с другими системами.

C) Обеспечение необходимыми знаниями о продукте и его функциональности, об установке и первоначальной настройке программного обеспечения, об основных функциях и их выполнении и пользовательском интерфейсе.

16. Вставьте пропущенное слово: В процессе устранения ошибок и настройки использования информационных ресурсов специалист может обратиться к записям о работе программ и ошибках, которые появились в процессе работы. Такие записи собираются и хранятся в виде текстовых файлов, называемых _____

17. Дополните предложение: Правила и рекомендации по обеспечению безопасности сети и данных, используемые при настройке и сопровождении информационных ресурсов – это _____.

18. Как называются руководства, содержащие инструкции по регулярному обслуживанию и технической поддержке информационных ресурсов

19. Дополните предложение: Онлайн-ресурсы, где можно найти информацию о решении проблем и получить помощь от других специалистов – это

20. Какой тип логов следует выбрать, чтобы проанализировать информацию о сетевых соединениях и трафике

21. Какие виды настроек относятся к настройкам пользовательского интерфейса операционной системы?

1) Настройка рабочего стола
2) Настройка темы оформления
3) Настройка клавиатуры и мыши
4) Настройка запускаемых программ при входе в систему

22. Одним из первых действий после установки ОС Astra Linux является...

1) Настройка пользователей
2) Настройка печати
3) Проверка и установка обновлений
4) Настройка звука

23. Какую СУБД следует выбрать для небольших и средних веб-проектов, блогов, форумов, CMS, где важна простота использования и интеграции с PHP?

1) PostgreSQL
2) MongoDB
3) MySQL
4) Oracle

24. Установите правильный порядок установки систем для функционирования технической поддержки :

1) Приобретение лицензии/подписки
2) Установка и настройка
3) Выбор программного обеспечения
4) Интеграция с другими системами

25. Установите соответствие между наименованиями категорий программного обеспечения и их назначением:

1) Системы управления контентом (CMS)
2) Системы управления базами данных
3) Программы для работы с файлами
4) Веб-браузеры

A) Обработка, редактирование, создание и управление файлами разных форматов.
B) Создание, редактирование, управление и публикация контента на веб-сайтах.
C) Хранение, обработка и извлечение данных в структурированном виде.
D) Просмотр веб-страниц, загрузка файлов, взаимодействие с веб-приложениями

26. Вставьте пропущенное слово: Обработка основных запросов и инцидентов, предоставление первичной помощи – это _____ уровень технической поддержки

27. Дополните предложение: Централизованный ресурс, который содержит информацию, полезную для решения различных проблем и вопросов пользователей – _____.

28. Как называется процесс разделения физического диска на логические разделы, которые могут использоваться для установки операционной системы, хранения данных и других задач
29. Назовите рекомендуемый тип файловой системы для раздела пользовательских данных (/home) в Astra Linux
30. Каким образом внедрение базы знаний может снизить нагрузку на службу поддержки:
31. Одна из самых популярных платформ для управления тикетами, которая предлагает широкий спектр функций, включая автоматизацию, базы знаний и интеграцию с другими сервисами?

1) ZenDesk
2) Trello
3) Google Ticket
4) Яндекс.Scout

32. Укажите каналы, через которые пользователи могут создавать запросы технической поддержке

1) Чат
2) Телефон
3) Личное обращение в офис
4) Форумы и обсуждения

33. Какая встроенная функция чата Zendesk Chat позволяет общаться с клиентами в реальном времени на веб-сайте компании?

1) Live Chat
2) WhatsApp
3) Telegram
4) WeChat

34. Установите правильный порядок действий сотрудника технической поддержки после получения и регистрации заявки от клиента на решение проблемы:

1) Изучение заявки
2) Решение проблемы
3) Диагностика и общение с клиентом
4) Закрытие задачи с указанием статуса решения проблемы

35. Установите соответствие между запросами клиентов и видами технических проблем:

1) Проблемы с доступом
2) Сбои в работе ПО
3) Проблемы с оборудованием
4) Проблемы с интеграцией

A) Несовместимость программного обеспечения, некорректная синхронизация данных.
B) Затруднения с входом в систему, паролем, аккаунтом.
C) Неисправность устройства, неработающий принтер, ошибка сети.
D) Некорректная работа программного обеспечения, ошибки, зависания, вылеты

36. Ответьте на вопрос одним словом: Как называется категория обращений клиентов из-за неудовлетворительного качества продукта, из-за проблем с обслуживанием или доставкой, из-за нарушений условий договора
37. Вставьте пропущенное словосочетание: Одним из основных методов коммуникации, заключающемся в понимании потребностей клиента, задавании вопросов, перефразировании сказанного является _____.
38. Вставьте пропущенное слово: Чат-боты в службах технической поддержки используются для _____ ответов на часто задаваемые вопросы и обработки простых запросов
39. К какой категории обращений клиентов относятся запросы с проблемами компьютерных вирусов, взломов, утечки данных, подозрительной активности.
40. Перечислите и кратко поясните ключевые принципы эффективной коммуникации

Критерии оценки

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%

III. ПАКЕТ ЭКЗАМЕНАТОРА

1. УСЛОВИЯ

Количество вариантов каждого задания / пакетов заданий для экзаменующегося: не менее 10.

Ответы:

1. Правильный ответ: 2
2. Правильные ответы: 1, 2
3. Правильные ответы: 2
4. Правильная последовательность этапов: 1 -3 - 2 - 5 - 4
5. Правильный вариант соответствия: 1–C, 2–A, 3–B
6. Правильный ответ: Тильда (Tilda)
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
7. Правильный ответ: контентом
8. Правильный ответ: развертывание
9. Правильный ответ: хостинг
10. Правильный ответ: В данной ситуации надо выбрать выделенный сервер, так как он позволяет получить максимальную производительность, контроль и безопасность для вашего сайта
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
11. Правильные ответы: 1, 2
12. Правильный ответ: 2
13. Правильный ответ: 3
14. Правильная последовательность этапов: 1 -3 - 2 - 4 - 5
15. Правильный вариант соответствия: 1–C, 2–B, 3–A
16. Правильный ответ: логи (логами, log, log-файлами)
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
17. Правильный ответ: политика безопасности
18. Правильный ответ: руководства по сопровождению
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
19. Правильный ответ: Форумы (сообщества)
20. Правильный ответ: Сетевые логи
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
21. Правильный ответ: 1, 2, 4
22.Правильные ответы: 3
23.Правильный ответ: 3
24.Правильная последовательность этапов: 3 - 1 - 2 - 4
25.Правильный вариант соответствия: 1–B, 2–C, 3–A, 4–D
26.Правильный ответ: первый (1, 1-ый)
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
27.Правильный ответ: база знаний
28.Правильный ответ: разметка диска (разметка)
29. Правильный ответ: ext4

30. Правильный ответ: Пользователи могут самостоятельно находить ответы на свои вопросы, что уменьшает количество обращений в службу поддержки и позволяет специалистам сосредоточиться на более сложных запросах.
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
31.Правильный ответ: 1
32.Правильные ответы: 1, 2
33.Правильный ответ: 1
34.Правильная последовательность этапов: 1 -3 - 2 - 4
35.Правильный вариант соответствия: 1–B, 2–D, 3–C, 4–A
36.Правильный ответ: Жалобы (жалоба)
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
37.Правильный ответ: активное слушание (метод активного слушания)
38.Правильный ответ: автоматизации
39.Правильный ответ: проблемы с безопасностью (безопасность)
40.Правильный ответ: 1) В центре внимания всегда должен быть клиент и его потребности; 2) Информацию необходимо излагать просто и доступно для понимания; 3) Инициатива должна исходить от сотрудника, необходимо опережать ожидания клиентов; 4) необходимо сделать взаимодействие с клиентом приятным и полезным.
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)

Критерии оценки

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%

5.1.2. Контрольно-оценочные материалы для дифференцированного зачета по МДК 02.02 Обеспечение безопасности информационных ресурсов

I. ПАСПОРТ

Назначение:

Контрольно-оценочные материалы предназначены для контроля и оценки результатов освоения междисциплинарного курса
Обеспечение безопасности информационных ресурсов
по специальности СПО:
09.02.09, Веб-разработка
Промежуточная аттестация включает в себя ответы на теоретические вопросы в тестовой форме открытого и закрытого типов
Экзаменационный билет включает в себя тестовые вопросы открытой и закрытой формы.

II. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ. Вариант № 1

Инструкция: дайте ответы на представленные ниже вопросы.
Время выполнения задания: 60 минут

1. Комплекс мер, направленных на защиту информации от несанкционированного доступа, изменения, уничтожения или раскрытия - это

1) Безопасность информационных ресурсов
2) Защита данных
3) Обеспечение конфиденциальности
4) Защита от неправомерного доступа

2. Укажите основные элементы обеспечения безопасности информационных ресурсов, входящие в категорию «политики безопасности»:
1) Политика паролей
2) Политика доступа
3) Политика конфиденциальности
4) Политика защиты данных

3. Какие технические средства защиты информационных ресурсов необходимы для установки на компьютер с операционной системой Windows?
1) Антивирусная программа
2) Система видеонаблюдения
3) Правила использования информационных ресурсов в организации
4) Правила создания, хранения и использования паролей

4. Установите правильный порядок действий, выполняемых на этапе планирования и подготовки проверки безопасности:
1) Определение целей проверки
2) Выбор методик проверки
3) Определение области проверки
4) Получение разрешений
5) Создание плана проверки

5. Установите соответствие технических средств защиты с их назначением:
1) Антивирусное ПО
2) Брандмауэры
3) Шифрование

A) Защита от вредоносных программ.
B) Защита информации от несанкционированного доступа путем преобразования ее в нечитаемый формат.
C) Контроль сетевого трафика и блокировка нежелательных соединений.

Правильный вариант соответствия: 1–A, 2–C, 3–B

6. Дополните предложение: процесс создания копий данных, которые могут быть использованы для восстановления системы в случае возникновения проблем, таких как сбой оборудования, стихийные бедствия, ошибки в работе программного обеспечения, кибератаки и т.д. – это _____

7. Вставьте пропущенное слово: способность программы резервного копирования создавать резервные копии файлов по расписанию, например непрерывно (все время), ежечасно, еженедельно и т.д. – это _____ резервного копирования.

8. Команда для выполнения резервного копирования для MySQL

9. Сценарий mysqldump создает резервную копию базы данных в файл _____
Правильный ответ: backup.sql

10. Назовите, какие факторы влияют на выбор частоты резервного копирования базы данных

11. Модель управления доступом, где владелец ресурса (пользователь или группа) имеет право определять, кто может получить доступ к этому ресурсу и какие действия с ним можно выполнять.
1) Дискреционный контроль доступа.
2) Мандатный контроль доступа.
3) Ролевой контроль доступа.

12. К сценариям резервного копирования относятся: (выберите два верных варианта ответа)
1) Сценарии для создания резервных копий баз данных.
2) Сценарии для копирования файлов и папок.
3) Сценарии для импорта данных из резервных копий.
4) Сценарии для разархивирования данных

13. Какой контроль доступа необходимо использовать в организациях, занимающихся обработкой секретной информации?

1) Дискреционный контроль доступа.
2) Мандатный контроль доступа.
3) Ролевой контроль доступа.

14. Установите правильный порядок действий по восстановлению базы данных:
1) Выбор резервной копии
2) Проверка работоспособности
3) Восстановление базы данных

5. Установите соответствие типа контроля доступа с принципом его работы:
1) Дискреционный контроль доступа (DAC)
2) Мандатный контроль доступа (MAC)
3) Ролевой контроль доступа (RBAC)

A) Владелец ресурса (пользователь или группа) определяет, кто имеет к нему доступ.
B) Пользователи принадлежат к ролям, а каждая роль имеет определенный набор прав доступа к ресурсам.
C) Система определяет доступ к ресурсам на основе правил безопасности и классификации пользователей и ресурсов.

16. Вставьте пропущенное слово: Разграничение доступа субъектов к объектам, основанное на назначении метки (мандата) конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности – это _____контроль доступа

17. Как называется проверка подлинности пользователей при входе в систему?

18. Какие команды нужно использовать для настройки прав доступа к базам данных, таблицам и колонкам MySQL и PostgreSQL?

19. Назовите типовые роли в CMS

20. Дополните определение: криптографический аналог собственноручной подписи, который используется для подтверждения подлинности и целостности электронных документов – это

21. Какие функции обеспечивает применение электронно-цифровой подписи (ЭЦП)?
1) Идентификация
2) Целостность данных
3) Конфиденциальность
4) Проверка достоверности

22. Может ли подписавший документ впоследствии отказаться от своей подписи, выполненной с помощью ЭЦП (электронно-цифровой подписи)
1) Да
2) Нет
3) После предварительного запроса на переподписание документа

23. Какой вид подписи удобнее использовать, если требуется документы обрабатывать и хранить в электронном виде, при отправке заявлений, отчетов или других документов в государственные органы ?
1) Электронно-цифровая подпись
2) Ручная подпись
3) Нотариальная подпись
4) Упрощенная электронная подпись

24. Установите правильный порядок порядок получения электронной цифровой подписи:
1) Выбор удостоверяющего центра (УЦ)
2) Идентификация и создание ключевой пары
3) Подготовка документов и заполнение заявления
4) Получение и настройка ЭЦП

25. Установите соответствие между криптографическими ключами и их назначением:
1) Открытый ключ
2) Закрытый ключ

A) Это ключ, который можно свободно распространять. Он используется для проверки подписи. Такой ключ обычно хранится в реестре удостоверяющего центра (УЦ) и доступен для всех, кто хочет проверить подпись.

B) Это секретный ключ, который должен храниться в безопасности и не разглашаться. Он используется для создания цифровой подписи. Только владелец закрытого ключа может подписывать документы, используя этот ключ.

26. Вставьте пропущенное слово: _____ ключ хранится в реестре УЦ и доступен для всех, кто хочет проверить подпись.

27. Перечислите, на каких носителях может хранится закрытый ключ ЭЦП

28. Вставьте пропущенное слово: При подписании документа с помощью ЭЦП для создания подписи используется _____ ключ

29. Дополните предложение: важный компонент безопасности веб-приложений, который помогает защищать их от различных типов атак – это

Правильный ответ: Web Application Firewall (WAF)10. Опишите способы защиты от XSS уязвимостей в веб-приложениях, позволяющих злоумышленникам внедрять и выполнять вредоносный скрипт на веб-страницах, просматриваемых другими пользователями

30. Какие виды резервного копирования существуют?

1) Полное резервное копирование
2) Инкрементное резервное копирование
3) Неполное резервное копирование
4) Однократное резервное копирование

31. Действие, позволяющее проверить резервные копии на предмет целостности и доступности, чтобы убедиться, что данные могут быть восстановлены...

1) Проверка целостности резервных копий
2) Хранение резервных копий
3) Проверка объема резервной копии
4) Настройка частоты резервного копирования

32. Какую СУБД следует выбрать для небольших и средних веб-проектов, блогов, форумов, CMS, где важна простота использования и интеграции с PHP?

1) PostgreSQL
2) MongoDB
3) MySQL
4) Oracle

33. Установите правильный порядок установки систем для функционирования технической поддержки:

1) Приобретение лицензии/подписки
2) Установка и настройка
3) Выбор программного обеспечения
4) Интеграция с другими системами

34. Установите соответствие между наименованиями категорий программного обеспечения и их назначением:

1) Системы управления контентом (CMS)
2) Системы управления базами данных
3) Программы для работы с файлами
4) Веб-браузеры

A) Обработка, редактирование, создание и управление файлами разных форматов.
B) Создание, редактирование, управление и публикация контента на веб-сайтах.
C) Хранение, обработка и извлечение данных в структурированном виде.
D) Просмотр веб-страниц, загрузка файлов, взаимодействие с веб-приложениями

35. Запишите термин, к которому дано следующее определение: процесс создания копий данных, которые можно использовать для восстановления системы в случае возникновения проблем – это

36. Вставьте пропущенное слово: Способ защиты резервных копий от несанкционированного доступа – _____.

37. Дополните предложение: Ключ шифрования - это _____

38. Опишите преимущества шифрования резервных копий

39. Назовите тип шифрования, в том случае если используются два ключа: публичный ключ для шифрования и частный ключ для расшифровки.

40. Какой принцип настройки прав доступа используется в случае их настройки в зависимости от данных о поведении пользователей?

1) Настройка прав на основе поведенческих факторов
2) Настройка прав на основе функциональных задач (ролей)
3) Настройка прав на основе максимальных привилегий

41. Анализ каких данных может влиять на настройку прав на основе поведенческих факторов?
1) Анализ активности в системе
2) Анализ действий
3) Анализ местоположения
4) Анализ личных данных
5) Анализ социальной активности

42. Системы, предназначенные для управления идентификацией и доступом пользователей к ресурсам, которые позволяют создавать роли, настраивать права доступа на основе ролей и поведенческих факторов - это
1) Системы управления доступом
2) Системы управления информационной безопасностью
3) Программное обеспечение для управления политиками безопасности
4) Системы управления базами данных

43. Установите правильный порядок действий по настройке прав доступа:
1) Планирование
2) Настройка прав доступа на основе ролей
3) Настройка системы управления доступом
4) Настройка прав доступа на основе поведенческих факторов
5) Тестирование и внедрение

44. Установите соответствие этапа настройка прав доступа на основе поведенческих факторов с действием, которое необходимо выполнить на этом этапе:
1) Сбор данных
2) Создание правил
3) Включение динамической настройки

A) Создайте правила настройки прав доступа на основе поведенческих факторов.
B) Соберите данные о поведении пользователей (например, активность в системе, местоположение, тип устройства).
C) Включите динамическую настройку прав доступа на основе поведенческих факторов

45. Вставьте словосочетание: Принцип _____ заключается в предоставлении пользователям только тех права, которые необходимы им для выполнения своих задач
Правильный ответ: наименьших привилегий

46. Вставьте пропущенное словосочетание: набор инструкций, которые определяют, кто может получить доступ к определенным ресурсам, и какие действия с ними можно выполнять - _____.

47. Как настройка прав доступа на основе ролей может быть использована для улучшения безопасности системы

48. Какая технология позволяет управлять идентификацией и доступом пользователей к ресурсам?

49. Представьте, что вы разрабатываете систему управления доступом для online-курсов. В системе есть роли “Преподаватель”, “Студент” и “Администратор”. Опишите как можно использовать поведенческие факторы для настройки прав доступа к системе. Приведите минимум три примера.

50. Какой из следующих типов атак может быть предотвращен с помощью использования веб-файрвола (WAF)?
1) SQL-инъекция
2) Фишинг
3) Вирусные атаки
4) Атаки типа "отказ в обслуживании" (DoS)

51. Какие категории программных средств для обеспечения безопасности веб-приложений существуют?
1) Веб-файрвол (Web Application Firewalls, WAF)
2) Инструменты для статического и динамического анализа кода
3) Проактивное предсказание уязвимостей (PVP)

4) Automatic Repair Engine (ARE) - автоматическое обнаружение и исправление уязвимостей в реальном времени

52. Что такое XSS (Cross-Site Scripting) и как его можно предотвратить?
1) Это атака на сервер, которая требует использования SSL.
2) Это атака, при которой злоумышленник вставляет вредоносный скрипт на веб-страницу. Предотвращается экранированием пользовательского ввода.
3) Это атака, при которой злоумышленник перехватывает сетевой трафик. Предотвращается использованием VPN.
4) Это атака на базу данных. Предотвращается шифрованием данных.

53. Установите правильный порядок действий при обеспечении безопасности веб-приложения:
1) Провести тестирование на проникновение.
2) Реализовать многофакторную аутентификацию.
3) Обновить все используемые библиотеки и фреймворки.
4) Настроить веб-файрвол (WAF).
5) Провести аудит безопасности и анализ уязвимостей.

54. Установите соответствие инструмента анализа кода и его принципа работы:
1) Статический анализ (SAST)
2) Динамический анализ (DAST)

A) тестирует приложение во время его работы, выявляя уязвимости в реальном времени.
B) помогает находить уязвимости в исходном коде до его выполнения.

Правильный вариант соответствия: 1–B, 2–A,

55. Ответьте на вопрос: Какое программное средство может быть использовано для автоматического обнаружения уязвимостей в веб-приложении?

56. Вставьте пропущенное словосочетание: Метод аутентификации, считающийся наиболее безопасным для веб-приложений - _____.

57. Опишите, какой тип уязвимости позволяет злоумышленнику выполнить произвольный код на сервере через ввод данных и какие способы защиты от него необходимо использовать?

58. Что такое "SQL-инъекция"?

59. Представьте, что вы разрабатываете веб-приложение для онлайн-магазина. Опишите три программных средства обеспечения безопасности, которые вы бы использовали для защиты данных пользователей и предотвращения атак. Для каждого средства укажите его основное назначение и как оно поможет в обеспечении безопасности.

Критерии оценки

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%

III. ПАКЕТ ЭКЗАМЕНАТОРА

1. УСЛОВИЯ

Количество вариантов каждого задания / пакетов заданий для экзаменующегося: не менее 10.

Ответы:

1. Правильный ответ: 1
2. Правильные ответы: 1, 2
3. Правильные ответы: 1
4. Правильная последовательность этапов: 1 -3 - 2 - 5 - 4
5. Правильный вариант соответствия: 1–A, 2–C, 3–B
6. Правильный ответ: Резервное копирование (бэкап)
7. Правильный ответ: частота

8. Правильный ответ: mysqldump
9. Правильный ответ: backup.sql
10. Правильный ответ: критичность данных, скорость изменения данных, объем данных, доступные ресурсы, требования безопасности
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
11. Правильный ответ: 1
12. Правильный ответ: 1, 2
13. Правильные ответы: 2
14. Правильная последовательность этапов: 1 -3 - 2
15. Правильный вариант соответствия:1–A,2–C,3–B
16. Правильный ответ: мандатный
17. Правильный ответ: аутентификация
18. Правильный ответ: GRANT и REVOKE
19. Правильный ответ: Администратор, Редактор, Автор, Читатель
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
20. Правильный ответ: электронно-цифровая подпись (ЭЦП)
21. Правильные ответы: 1, 2
22.Правильный ответ: 2
23. Правильный ответ: 1
24. Правильная последовательность этапов: 1 -3 - 2 - 4
25. Правильный вариант соответствия: 1–A,2–B
26. Правильный ответ: открытый
27. Правильный ответ: USB-ключи с аппаратной защитой, смарт-карты, защищенные программные приложения на компьютерах или мобильных устройствах.
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
28. Правильный ответ: закрытый
29. Правильный ответ: Web Application Firewall (WAF)10. Опишите способы защиты от XSS уязвимостей в веб-приложениях, позволяющих злоумышленникам внедрять и выполнять вредоносный скрипт на веб-страницах, просматриваемых другими пользователями
Правильный ответ: экранирование данных, валидация и фильтрация ввода, использование безопасных методов разработки
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
30.Правильный ответ: 1, 2
31. Правильные ответы: 1
32. Правильный ответ: 3
33. Правильная последовательность этапов: 3 - 1 - 2 - 4
34. Правильный вариант соответствия: 1–B, 2–C, 3–A, 4–D
35. Правильный ответ: Резервное копирование (бэкап, backup)
36. Правильный ответ: шифрование
37. Правильный ответ: секретный код, необходимый для расшифровки зашифрованных данных
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
38.Правильный ответ: Защита от несанкционированного доступа, увеличение уровня безопасности, соответствие нормативным требованиям
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
39. Правильный ответ: ассиметричное (Асимметричное шифрование)
40. Правильный ответ: 1
41. Правильные ответы: 1, 2, 3
42. Правильный ответ: 1
43. Правильная последовательность этапов: 1 -3 - 2 - 4 - 5
44. Правильный вариант соответствия: 1–B, 2–A, 3–C
45. Правильный ответ: наименьших привилегий

46. Правильный ответ: права доступа / политика доступа.
47. Правильный ответ: Минимизация прав доступа: каждая роль имеет ограниченный набор прав, что снижает риск несанкционированного доступа к данным и системе, упрощение управления доступом: не нужно настраивать права для каждого пользователя вручную.
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
48. Правильный ответ: IAM (Identity and Access Management)
49. Правильный ответ: Анализ активности: если студент не заходил в систему в течение месяца, он может получить уведомление с предложением продолжить обучение, иначе права в ближайшее время будут ограничены; анализ действий: если студент не сдавал тесты или не выполнял задания в течение недели, он может получить уведомление с предложением обратиться за помощью; анализ ввода: если преподаватель вводит неправильный пароль несколько раз, его аккаунт может быть заблокирован.
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
50. Правильный ответ: 1
51. Правильные ответы: 1, 2
52. Правильный ответ: 2
53. Правильная последовательность этапов: 5 - 3 - 4 - 1 - 2
54. Правильный вариант соответствия: 1–В, 2–А,
55. Правильный ответ: Сканер уязвимостей
56. Правильный ответ: Многофакторная аутентификация
57. Правильный ответ: SQL-инъекции предотвращаются следующими способами: валидацией и фильтрацией входных данных, минимизацией привилегий учетных записей БД, отслеживание подозрительной активности
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
58. Правильный ответ: Это уязвимость, позволяющая злоумышленнику выполнять произвольные SQL-запросы к базе данных приложения.
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)
59. Правильный ответ: 1) Web Application Firewall (WAF) фильтрует и мониторит HTTP-трафик к веб-приложению, защищая его от распространенных угроз, таких как SQL-инъекции и XSS-атаки. Он помогает блокировать вредоносные запросы до того, как они достигнут сервера, 2) Использование SSL-сертификатов обеспечивает шифрование данных между клиентом и сервером, что защищает конфиденциальную информацию, такую как пароли и номера кредитных карт, от перехвата злоумышленниками, 3) Реализация ролевого управления доступом позволяет ограничить права пользователей в зависимости от их роли, что минимизирует риск несанкционированного доступа к чувствительным данным и функциям приложения.
(ответ студента может быть написан в собственной трактовке, эквивалентной по смыслу приведенному правильному ответу)

Критерии оценки

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%

5.2.1. Контрольно-оценочные материалы для экзамена (квалификационного)

I. ПАСПОРТ

Назначение:

Контрольно-оценочные материалы предназначены для контроля и оценки результатов освоения профессионального модуля

ПМ.02 Техническая поддержка и администрирование информационных ресурсов
по специальности СПО:

09.02.09, Веб-разработка

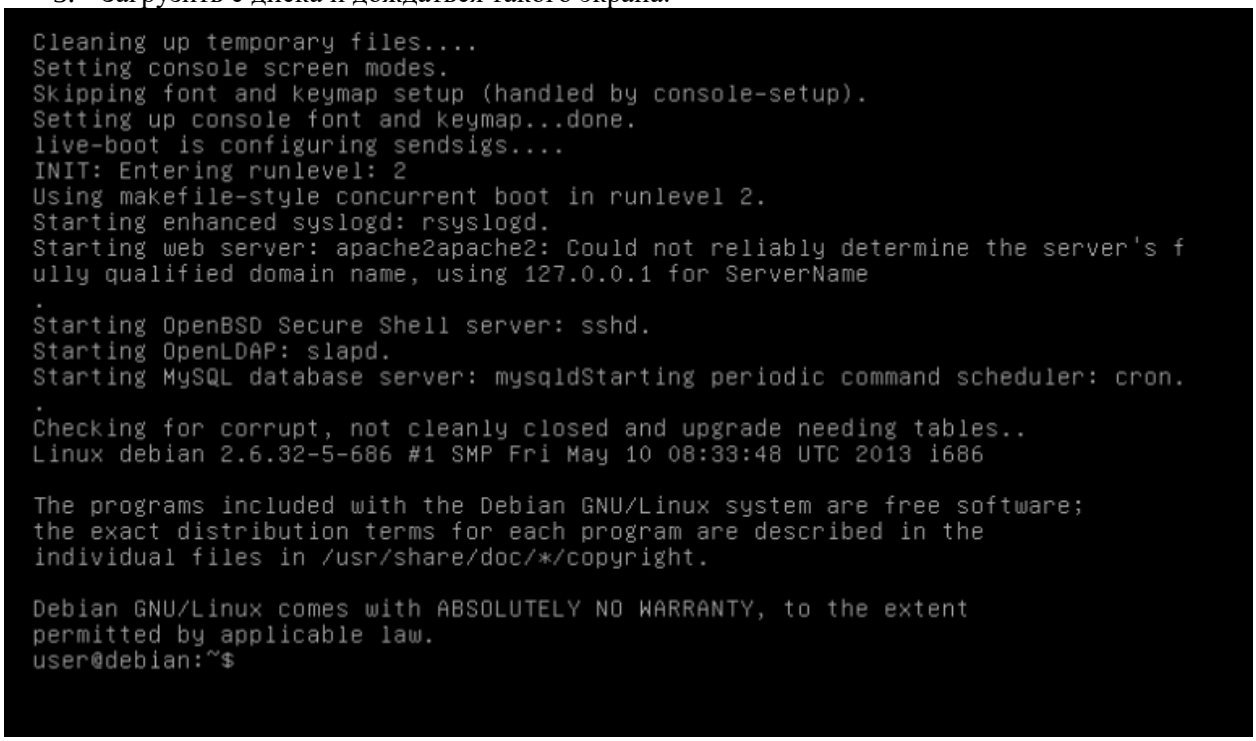
II. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ. Вариант №1

Задание 1
Коды проверяемых профессиональных и общих компетенций: ПК 2.1, ПК 2.5, ОК 1-5, ОК 7, ОК 9
Время выполнения задания – 60 минут

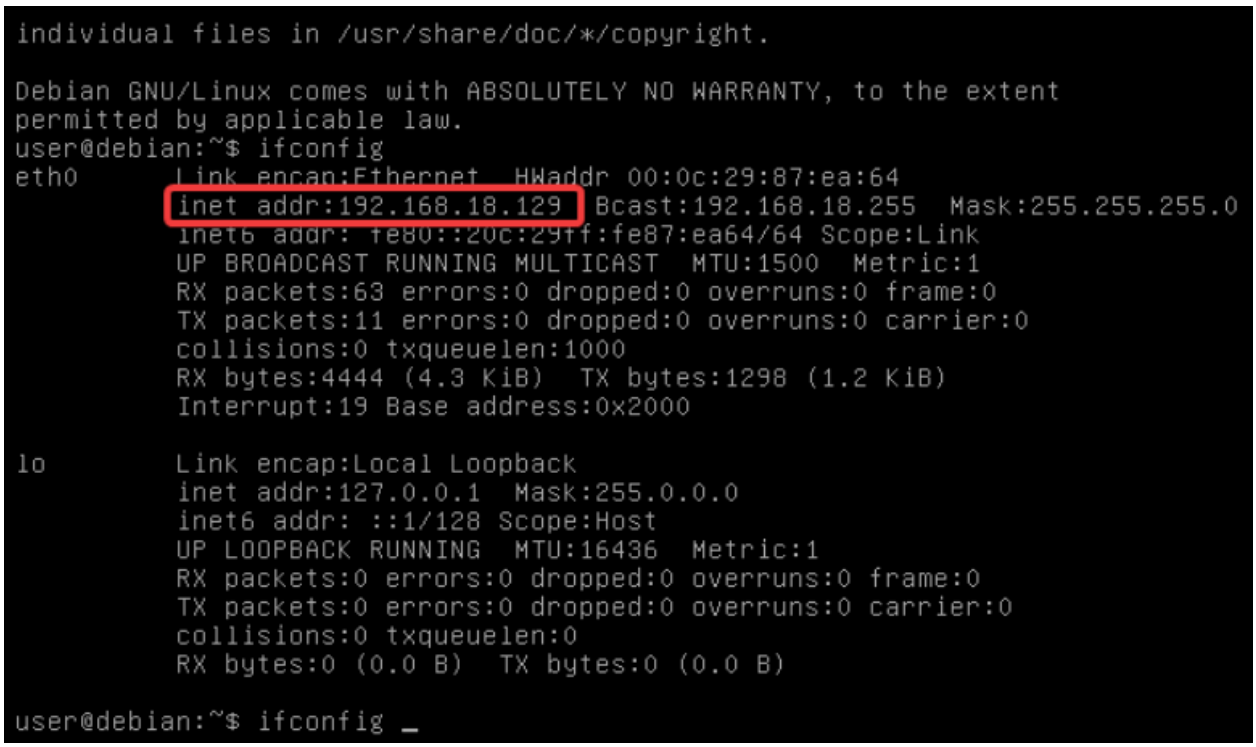
1. Выполнить установку и первичную настройку LMS Moodle.
2. Описать решение и сделать разбор ситуации в службе технической поддержки, связанной с негативным отзывом или жалобой клиента, вызвавшей резонанс в социальных сетях

Задание 2
Коды проверяемых профессиональных и общих компетенций: ПК 2.2, ПК 2.3, ПК. 2.4, ОК 1-5, ОК 7, ОК 9
Время выполнения задания – 60 минут

1. Скачать образ «Web For Pentesters» с веб-сайта www.pentesterlab.com.
2. Создать виртуальную машину.
3. Загрузить с диска и дождаться такого экрана:



4. Написать в строку ifconfig.
5. Полученный IP вставить в поисковую строку браузера.



6. Осуществить поиск уязвимостей к атакам XSS

Показатели оценивания

№ п.п	Критерий	Баллы
1	Выполнена установка и настройка программного обеспечения	20
2	Описано решение критической ситуации	10
3	Представлен детальный разбор ситуации	10
4	Виртуальная машина создана и настроена	10
5	Поиск уязвимостей выполнен	20
	Итого	70

Критерии оценки

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%

III. ПАКЕТ ЭКЗАМЕНАТОРА

1. УСЛОВИЯ

Количество вариантов каждого задания / пакетов заданий для экзаменующегося: не менее 10 (по количеству обучающихся)
Время выполнения каждого задания:
Задание 1 – 60 минут
Задание 2 – 60 минут

Оборудование: текстовый редактор, табличный редактор

Примерный перечень программного обеспечения для установки и настройки:

1. Операционная система
2. WAMP подобный комплект
3. CMS, LMS, CRM
4. Система для функционирования технической поддержки
5. Среды и платформы веб-разработки

Примерный перечень критических ситуаций для службы поддержки:

1. Проблема с доступом к основному сервису (например, не работает сайт или приложение).
2. Негативный отзыв или жалоба клиента, вызвавшая резонанс в социальных сетях
3. Угроза безопасности данных

2. КРИТЕРИИ ОЦЕНКИ

Показатели оценивания

№ п.п	Критерий	Баллы
1	Выполнена установка и настройка программного обеспечения	20
2	Описано решение критической ситуации	10
3	Представлен детальный разбор ситуации	10
4	Виртуальная машина создана и настроена	10
5	Поиск уязвимостей выполнен	20
	Итого	70

Критерии оценки

Оценка	Кол-во баллов
«отлично»	от 85% до 100%
«хорошо»	от 70% до 84%
«удовлетворительно»	от 50% до 69%
«неудовлетворительно»	менее 50%