Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 09.03.03 Прикладная информатика

Наименование образовательной программы: Информационные технологии в теплоэнергетике

Уровень образования: высшее образование - бакалавриат

Форма обучения: Заочная

Оценочные материалы
по дисциплине
Администрирование защищенных операционных систем

Москва
2025

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Орлова М.А. Идентификатор: R42753cd2-OrlovaMA-6d7582a9	М.А. Орлова

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Щербатов И.А. Идентификатор: R6b2590a8-ShcherbatovIA-d91ec17	И.А. Щербатов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Щербатов И.А. Идентификатор: R6b2590a8-ShcherbatovIA-d91ec17	И.А. Щербатов

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-2 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

ИД-2 Применяет информационные технологии для поиска, хранения, обработки, анализа и представления информации

2. ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИД-1 Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасностикой культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

ИД-3 Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

и включает:

для текущего контроля успеваемости:

Форма реализации: Защита задания

1. Защита лабораторной работы "Инструменты администрирования защищенных операционных систем" (Контрольная работа)
2. Защита лабораторной работы "Настройка и диагностика сетевой подсистемы" (Контрольная работа)
3. Защита лабораторной работы "Настройка сервиса авторизации, диагностика и устранение неисправностей функционирования операционной системы" (Контрольная работа)
4. Защита лабораторной работы "Установка и настройка стандартного набора сервисов" (Контрольная работа)

БРС дисциплины

5 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Защита лабораторной работы "Настройка сервиса авторизации, диагностика и устранение

неисправностей функционирования операционной системы" (Контрольная работа)

КМ-2 Защита лабораторной работы "Установка и настройка стандартного набора сервисов" (Контрольная работа)

КМ-3 Защита лабораторной работы "Инструменты администрирования защищенных операционных систем" (Контрольная работа)

КМ-4 Защита лабораторной работы "Настройка и диагностика сетевой подсистемы" (Контрольная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	10
Основы компьютерной безопасности и базовые инструменты администрирования операционной системы					
Архитектура и компоненты операционных систем на базе ядра Linux		+			
Основы компьютерной безопасности		+			
Принципы сетевого взаимодействия и структура сетевой подсистемы защищенной операционной системы					
Основные протоколы стека TCP/IP.			+		
Межсетевой экран			+		
Установка и настройка стандартного набора сервисов					
Администрирование веб-сайтов и электронной почты.				+	
Администрирование базовых сетевых сервисов организации				+	
Диагностика					
Идентификация, аутентификация и авторизация пользователей					+
Диагностика неисправностей в защищенной операционной системы					+
	Вес КМ:	25	25	25	25

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-2	ИД-2$_{ОПК-2}$ Применяет информационные технологии для поиска, хранения, обработки, анализа и представления информации	Знать: протоколы базовых сетевых сервисов организации Уметь: настраивать межсетевой экран	КМ-1 Защита лабораторной работы "Инструменты администрирования защищенных операционных систем" (Контрольная работа) КМ-4 Защита лабораторной работы "Настройка сервиса авторизации, диагностика и устранение неисправностей функционирования операционной системы" (Контрольная работа)
ОПК-3	ИД-1$_{ОПК-3}$ Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасностикой культуры с применением информационно-коммуникационных	Уметь: искать и устранять неисправности в функционировании операционной системы	КМ-2 Защита лабораторной работы "Настройка и диагностика сетевой подсистемы" (Контрольная работа)

	технологий и с учетом основных требований информационной безопасности		
ОПК-3	ИД-$З_{ОПК-3}$ Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Знать: состав и структуру защищенных операционных систем	КМ-3 Защита лабораторной работы "Установка и настройка стандартного набора сервисов" (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Защита лабораторной работы "Настройка сервиса авторизации, диагностика и устранение неисправностей функционирования операционной системы"

Формы реализации: Защита задания
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Предварительная подготовка к выполнению лабораторной работы. Выполнение лабораторной работы в соответствии с заданием. Подготовка к защите по пройденным материалам.

Краткое содержание задания:
Ответьте на 40 вопросов теста, используя пройденный материал. Обратите внимание, что в некоторых вопросах может быть несколько правильных вариантов ответа, а также могут встретиться вопросы, где нужно ввести правильный ответ самостоятельно. Для успешного выполнения задания внимательно ознакомьтесь с каждым вопросом и выберите все правильные ответы, основываясь на знаниях, полученных на лекциях и в учебных материалах.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: протоколы базовых сетевых сервисов организации	1.**Вопрос:** Какова основная роль сессионного ключа в протоколе Kerberos? 1. Он используется для шифрования всех данных между клиентом и KDC. 2. Он обеспечивает временную аутентификацию клиента на сервере в рамках одной сессии. 3. Он используется для обмена ключами между клиентом и сервером. 4. Он служит для хранения учетных данных пользователя. 5. Он используется для генерации всех других ключей в Kerberos. 6. Он хранится на сервере для дальнейшего использования. 7. Он нужен для синхронизации времени между клиентом и сервером. 8. Он используется для создания билета службы (TGS). **Правильный ответ:** Он обеспечивает временную аутентификацию клиента на сервере в рамках одной сессии. 2.**Вопрос:** Рассмотрим следующую структуру LDAP-записи: dn: uid=jdoe,ou=IT,dc=example,dc=com objectClass: inetOrgPerson objectClass: organizationalPerson objectClass: person

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	objectClass: top cn: John Doe sn: Doe uid: jdoe mail: john.doe@example.com ou: IT Какие из следующих утверждений правильно описывают элементы информационной модели LDAP, присутствующие в этой записи? 1. dn (Distinguished Name) определяет уникальный путь к записи в LDAP-дереве. 2. objectClass определяет набор атрибутов, которые могут быть включены в запись. 3. Атрибут cn (Common Name) используется для хранения полного имени пользователя. 4. Атрибут sn (Surname) используется для хранения имени пользователя. 5. uid (User ID) является обязательным атрибутом для всех записей LDAP. 6. mail определяет электронную почту пользователя и должен быть уникальным для каждой записи. 7. Атрибут ou (Organizational Unit) указывает на подразделение пользователя в организации. 8. dc (Domain Component) используется для указания домена, к которому принадлежит запись. Выберите правильные утверждения: 1, 2, 3, 7 2, 3, 4, 6 1, 3, 5, 8 1, 2, 4, 6 1, 2, 3, 7, 8 2, 3, 6, 8 1, 4, 6, 7 3, 4, 5, 7 **Правильный ответ:** 1, 2, 3, 7, 8

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. Защита лабораторной работы "Установка и настройка стандартного набора сервисов"

Формы реализации: Защита задания
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Предварительная подготовка к выполнению лабораторной работы. Выполнение лабораторной работы в соответствии с заданием. Подготовка к защите по пройденным материалам.

Краткое содержание задания:
Ответьте на 40 вопросов теста, используя пройденный материал. Обратите внимание, что в некоторых вопросах может быть несколько правильных вариантов ответа, а также могут встретиться вопросы, где нужно ввести правильный ответ самостоятельно. Для успешного выполнения задания внимательно ознакомьтесь с каждым вопросом и выберите все правильные ответы, основываясь на знаниях, полученных на лекциях и в учебных материалах.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: состав и структуру защищенных операционных систем	1.**Вопрос:** Какие из следующих утверждений описывают принципы работы DHCP? 1. DHCP-сервер назначает IP-адреса устройствам в сети автоматически. 2. Клиент отправляет запрос на IP-адрес с помощью сообщения DHCPREQUEST. 3. DHCP-сервер использует протокол ICMP для проверки доступности IP-адресов. 4. DHCP-клиент начинает процесс аренды IP-адреса с отправки сообщения DHCPDISCOVER. 5. DHCP-клиент и сервер взаимодействуют по протоколу TCP. 6. DHCP-сервер может назначать устройства статические IP-адреса на основе их MAC-адресов. 7. Клиент должен вручную подтверждать назначение IP-адреса перед его использованием. 8. DHCP-сервер хранит информацию об арендах IP-адресов в специальной базе данных. **Правильный ответ:** 1, 2, 4, 6, 8 2.**Вопрос:** Как протокол DNS преобразует доменное имя в IP-адрес? Выберите правильные утверждения: 1. DNS использует протокол HTTP для передачи запросов и ответов между клиентом и сервером. 2. Клиент отправляет DNS-запрос на получение IP-адреса для доменного имени на DNS-сервер, используя

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	протокол UDP по порту 53. 3. Если DNS-сервер не знает IP-адрес, он рекурсивно отправляет запрос к другим DNS-серверам, начиная с корневых серверов. 4. DNS-запросы всегда проходят через SSL/TLS для обеспечения безопасности. 5. DNS может использовать протокол TCP, если размер ответа превышает 512 байт. 6. DNS-запросы могут кэшироваться на промежуточных серверах для уменьшения времени отклика. 7. Клиент отправляет DNS-запросы непосредственно на корневые DNS-серверы. 8. DNS-сервер возвращает IP-адрес доменного имени или сообщение об ошибке, если имя не может быть разрешено. Выберите правильные утверждения: 2, 3, 5, 6, 8 1, 2, 3, 4, 7 2, 4, 5, 6, 8 1, 3, 5, 6, 8 3, 4, 5, 7, 8 2, 3, 6, 7, 8 1, 2, 4, 6, 8 2, 3, 4, 5, 8 **Правильный ответ:** 2, 3, 5, 6, 8

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. Защита лабораторной работы "Инструменты администрирования защищенных операционных систем"

Формы реализации: Защита задания

Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Предварительная подготовка к выполнению лабораторной работы. Выполнение лабораторной работы в соответствии с заданием. Подготовка к защите по пройденным материалам.

Краткое содержание задания:

Ответьте на 40 вопросов теста, используя пройденный материал. Обратите внимание, что в некоторых вопросах может быть несколько правильных вариантов ответа, а также могут встретиться вопросы, где нужно ввести правильный ответ самостоятельно. Для успешного выполнения задания внимательно ознакомьтесь с каждым вопросом и выберите все правильные ответы, основываясь на знаниях, полученных на лекциях и в учебных материалах.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: настраивать межсетевой экран	1.**Вопрос:** Какая команда используется для поиска файлов размером больше 50 MB в папке /home/user1? 1. find /home/user1 -size +50M 2. grep /home/user1 -size 50M 3. search /home/user1 -size >50M 4. locate /home/user1 -size 50M 5. find /home/user1 -size >50M 6. find /home/user1 -name +50M 7. search /home/user1 -name 50M 8. locate /home/user1 -name +50M **Правильный ответ:** find /home/user1 -size +50M 2.**Вопрос:** Какой символ используется в Bash для передачи вывода одной команды в качестве ввода для другой команды? > < | & ; && || * **Правильный ответ:** |

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Защита лабораторной работы "Настройка и диагностика сетевой подсистемы"

Формы реализации: Защита задания
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Предварительная подготовка к выполнению лабораторной работы. Выполнение лабораторной работы в соответствии с заданием. Подготовка к защите по пройденным материалам.

Краткое содержание задания:
Ответьте на 40 вопросов теста, используя пройденный материал. Обратите внимание, что в некоторых вопросах может быть несколько правильных вариантов ответа, а также могут встретиться вопросы, где нужно ввести правильный ответ самостоятельно. Для успешного выполнения задания внимательно ознакомьтесь с каждым вопросом и выберите все правильные ответы, основываясь на знаниях, полученных на лекциях и в учебных материалах.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: искать и устранять неисправности в функционировании операционной системы	1.**Вопрос:** Какие параметры и файл используются для настройки ARP в операционной системе, и что они означают? 1. gc_stale_time (время хранения устаревших записей), base_reachable_time_ms (базовое время доступности соседей), gc_thresh1 (пороговое значение для запуска сбора мусора) - /proc/sys/net/ipv4/neigh/default 2. base_reachable_time_ms (время доступности записи в миллисекундах), retrans_time_ms (интервал повторных запросов), delay_first_probe_time (задержка перед первым запросом) - /etc/network/interfaces 3. base_reachable_time_ms (базовое время доступности соседей), retrans_time_ms (время между повторными запросами), delay_first_probe_time (задержка перед первой проверкой) - /proc/sys/net/ipv4/neigh/default 4. proxy_arp (включение/выключение proxy ARP), ucast_solicit (максимальное количество запросов для одноадресного ответа) - /proc/sys/net/ipv4/arp_config 5. proxy_arp (включение/выключение проксирования ARP), gc_stale_time (время хранения устаревших записей), ucast_solicit (максимальное количество одноадресных

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	запросов) - /proc/sys/net/ipv4/neigh/default 6. gc_thresh3 (максимальное количество записей в кэше), app_solicit (максимальное количество запросов приложения) - /etc/arp.conf **Правильный ответ:** gc_stale_time (время хранения устаревших записей), base_reachable_time_ms (базовое время доступности соседей), gc_thresh1 (пороговое значение для запуска сбора мусора) - /proc/sys/net/ipv4/neigh/default 2.**Вопрос:** Какие из перечисленных шагов являются правильными для настройки SSH доступа с использованием публичного ключа? 1. Генерация пары ключей (приватного и публичного) на клиенте. 2. Копирование приватного ключа на удалённый хост. 3. Копирование публичного ключа на удалённый хост с использованием `ssh-copy-id`. 4. Добавление публичного ключа в файл `authorized_keys` на удалённом хосте. 5. Установка правильных прав доступа на файл `authorized_keys` и каталог `.ssh` на удалённом хосте. 6. Удаление публичного ключа с клиентской машины. 7. Проверка подключения к удалённому хосту с использованием SSH. 8. Изменение пароля root пользователя на клиентской машине. Выберите правильные шаги: 1, 3, 4, 5, 7 2, 4, 5, 6, 7 1, 2, 3, 4, 8 3, 5, 6, 7, 8 1, 4, 5, 7, 8 2, 3, 4, 6, 7 1, 2, 4, 5, 7 1, 3, 5, 7, 8 **Правильный ответ:** 1, 3, 4, 5, 7

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

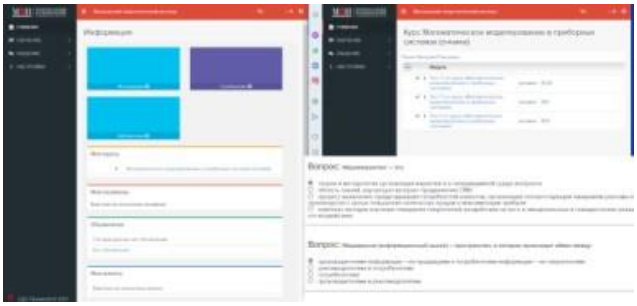
Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета



Процедура проведения

В тесте 20 вопросов встречаются вопросы следующих типов:
1. с одним вариантом ответа (в вопросах «один из многих», система сравнивает ответ слушателя с правильным ответом и автоматически выставляет за него назначенный балл)
2. с выбором нескольких вариантов ответов (в вопросах «многие из многих» система оценивает каждый ответ отдельно; есть возможность разрешить слушателю получить за вопрос 0,75 балла, если он выберет 3 правильных ответа из 4)
3. на соответствие слушатель должен привести в соответствие левую и правую часть ответа (в вопросах «соответствие» система оценивает каждый ответ отдельно; можно разрешить слушателю получить за вопрос 0,75 балла, если он выберет 3 правильных ответа из 4)
4. развернутый ответ, вводится в вручную в специально отведенное поле (ручная оценка преподавателем)

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-2$_{ОПК-2}$ Применяет информационные технологии для поиска, хранения, обработки, анализа и представления информации

Вопросы, задания

1.Как ядро Linux взаимодействует с пользовательскими программами и оборудованием?
2.Что такое системные вызовы и как они обеспечивают взаимодействие приложений с ядром Linux?
3.Как организована файловая система в Linux? Какие основные каталоги существуют и каково их назначение?

Материалы для проверки остаточных знаний

1.Какие основные компоненты составляют архитектуру операционной системы на базе ядра Linux? Перечислите их функции и назначение.

Ответы:

Перечислены основные компоненты.

Верный ответ: Ядро (Kernel) Ядро является центральным компонентом операционной системы Linux. Оно управляет основными системными ресурсами, такими как память, процессоры, и устройства ввода-вывода. Ядро также предоставляет интерфейсы для взаимодействия с аппаратным обеспечением.

Пример: Когда программа запрашивает файл на диске, ядро обрабатывает запрос, взаимодействуя с файловой системой и драйверами диска, чтобы извлечь необходимые данные. Оболочка (Shell) Оболочка — это интерфейс между пользователем и ядром. Она интерпретирует команды, вводимые пользователем, и передает их ядру для выполнения. Оболочка может быть командной строкой (например, Bash) или графическим интерфейсом. Пример: Пользователь вводит команду ls в оболочке Bash, и оболочка передает эту команду ядру, которое выполняет соответствующую системную функцию для отображения списка файлов. Файловая система Файловая система управляет хранением и доступом к данным на жестких дисках и других устройствах хранения. Она организует данные в виде файлов и каталогов и предоставляет интерфейс для их чтения и записи. Пример: Файловая система ext4 обеспечивает надежное хранение данных с поддержкой журналирования, что помогает защитить данные от повреждения при сбоях системы. Драйверы устройств Драйверы устройств — это специальные модули, которые позволяют ядру взаимодействовать с аппаратным обеспечением, таким как сетевые карты, жесткие диски, принтеры и т. д. Они абстрагируют детали работы устройств, предоставляя унифицированный интерфейс для ядра. Пример: Драйвер сетевой карты обеспечивает передачу данных между ядром Linux и сетевым адаптером, позволяя системе подключаться к сети. Системные библиотеки Системные библиотеки предоставляют множество функций, которые могут использоваться приложениями. Они включают в себя библиотеку C (glibc), которая содержит функции для работы с файлами, строками, процессами и многими другими базовыми операциями. Пример: Когда приложение использует функцию printf для вывода текста на экран, эта функция предоставляется системной библиотекой glibc.

2.Какие существуют системные вызовы в Linux, и какова их роль?

Ответы:

Дано определение. Приведены примеры.

Верный ответ: Описание: Системные вызовы — это интерфейс между пользовательским пространством и ядром операционной системы. Они позволяют приложениям запрашивать услуги, предоставляемые ядром, такие как управление процессами, файловыми системами, сетевыми взаимодействиями и аппаратными ресурсами. Пример: Системный вызов open() используется для открытия файла. Когда приложение вызывает open(), ядро открывает указанный файл и возвращает файловый дескриптор, который приложение затем может использовать для чтения или записи данных. Основные категории системных вызовов

3.Как работает протокол ARP, и какую роль он играет в сетевых взаимодействиях?

Ответы:

Дано правильное определение протокола и его основной функции.

Верный ответ: ARP (Address Resolution Protocol) используется для преобразования IP-адресов в MAC-адреса. Когда устройство хочет отправить данные в локальной сети, оно запрашивает MAC-адрес по известному IP-адресу с помощью ARP-запроса.

2. Компетенция/Индикатор: ИД-1$_{ОПК-3}$ Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасностикой культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

Вопросы, задания

1.Какова структура и основные компоненты архитектуры операционной системы на базе ядра Linux?

2.Как осуществляется управление пользователями и группами в Linux? Какие команды и файлы используются для этого?

3.Какие методы управления процессами существуют в Linux, и как они реализованы?

Материалы для проверки остаточных знаний

1.Как работают модели доступа к защищённой информации в ОС?

Ответы:

Перечислены модели контроля доступа

Верный ответ: Существуют модели контроля доступа, такие как Discretionary Access Control (DAC), Mandatory Access Control (MAC) и Role-Based Access Control (RBAC). Они определяют, кто и как может получить доступ к ресурсам системы на основе предопределённых правил и политик.

2.Этапы обработки сетевого пакета в операционной системе Linux

Ответы:

Перечислены этапы обработки сетевого пакета в ОС

Верный ответ: 1. Получение сетевого пакета на интерфейсе Когда пакет поступает на сетевой интерфейс (например, Ethernet), сетевой адаптер принимает его и передаёт в сетевой стек ядра Linux. Пример: При получении ICMP-запроса (ping) на сетевой интерфейс eth0, драйвер сетевой карты передаёт пакет в ядро. 2. Обработка на уровне сетевого драйвера Драйвер сетевого адаптера копирует пакет из аппаратного буфера в оперативную память. Затем пакет передается в сетевой стек ядра для дальнейшей обработки. Пример: Пакет ICMP (ping) передаётся драйвером сетевой карты в стек TCP/IP для дальнейшей маршрутизации. 3. Фильтрация и обработка пакета в Netfilter Netfilter — это подсистема Linux, ответственная за фильтрацию пакетов. Пакет проходит через цепочки PREROUTING, INPUT, FORWARD, OUTPUT, и POSTROUTING в зависимости от назначения и происхождения. Пример: Если настроено правило в iptables, которое блокирует ICMP-запросы, пакет будет отфильтрован и отклонён на этапе INPUT. 4. Маршрутизация пакета Если пакет не отфильтрован, ядро проверяет таблицу маршрутизации, чтобы определить, нужно ли передать пакет локальному процессу или маршрутизировать его на другой узел в сети. Пример: Если IP-адрес назначения соответствует локальному адресу, пакет направляется на обработку локальному процессу; иначе — переадресовывается через соответствующий интерфейс. 5. Протоколы уровня транспортного уровня Если пакет предназначен для локального хоста, ядро обрабатывает его на уровне транспортного протокола (например, TCP, UDP, ICMP). Сначала проверяется порт назначения, чтобы передать пакет соответствующему приложению. Пример: Если это TCP-пакет, он будет ассоциирован с соответствующим сокетом приложения через порт. 6. Передача пакета приложению Пакет передается в соответствующий сокет или приложение, например, в случае web-сервера пакет HTTP передается веб-серверу, такому как Apache или Nginx. Пример: Если это пакет TCP, предназначенный для веб-сервера на порту 80, он будет передан веб-серверу Apache для обработки HTTP-запроса. 7.

Ответ на запрос или последующая передача Если пакет требует ответа (например, для запроса ICMP), соответствующее приложение или ядро генерируют ответный пакет, который затем проходит аналогичные этапы обработки, но в обратном порядке: отправляется через стек TCP/IP, фильтруется в Netfilter и передаётся обратно через сетевой интерфейс. Пример: В случае ICMP-запроса приложение или ядро генерируют ICMP-ответ, который отправляется обратно отправителю через интерфейс eth0.

3.Принципы функционирования системы электронной почты

Ответы:

Перечислены основные принципы.

Верный ответ: Система электронной почты позволяет пользователям отправлять и получать сообщения через Интернет. Основными компонентами являются почтовые клиенты, почтовые серверы и протоколы, такие как SMTP, POP3 и IMAP. Когда пользователь отправляет электронное письмо, почтовый клиент передаёт сообщение на исходящий сервер с помощью протокола SMTP. Сервер доставляет сообщение на сервер получателя, где оно хранится до тех пор, пока получатель не запросит его через свой почтовый клиент. Протоколы POP3 и IMAP используются для получения сообщений: POP3 загружает письма на устройство пользователя и обычно удаляет их с сервера, тогда как IMAP сохраняет сообщения на сервере, синхронизируя их между несколькими устройствами. Система электронной почты также включает функции фильтрации спама, шифрования сообщений и управление контактами.

3. Компетенция/Индикатор: ИД-$З_{ОПК-3}$ Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Вопросы, задания

1.Как можно контролировать и управлять процессами с помощью команд и системных вызовов в Linux?

2.Как система Linux обрабатывает приоритеты процессов и что такое планировщик задач?

3.Каковы основные методы установки и обновления программ в Linux?

4.Как автоматизировать задачи в Linux с помощью shell-скриптов и ansible?

Материалы для проверки остаточных знаний

1.Как работает SSH и как он обеспечивает безопасное подключение к удалённым системам?

Ответы:

Дано корректное определение.

Верный ответ: SSH (Secure Shell) обеспечивает шифрование данных при удалённом управлении системами. Подключение происходит через аутентификацию (пароль или ключ) с использованием шифрования данных сессии. Для настройки используются файл /etc/ssh/sshd_config.

2.Сравнение системы управления идентификацией на основе LDAP и Kerberos

Ответы:

Перечислены основные функции протоколов LDAP и Kerberos.

Верный ответ: Назначение и область применения: LDAP: LDAP используется для хранения и управления данными о пользователях, группах, устройствах и других объектах в иерархической структуре. Он обеспечивает централизованную базу данных для хранения информации, которая может быть использована различными службами для аутентификации и авторизации пользователей. Пример использования: LDAP часто применяется для организации централизованного каталога, который используется для управления пользователями в корпоративной

сети, а также для предоставления сервисов, таких как адресная книга, сервисы электронной почты и другие службы. Kerberos: Kerberos — это протокол аутентификации, который предоставляет безопасную и надежную аутентификацию пользователей и сервисов в сети. Он работает на основе системы тикетов, что позволяет пользователям аутентифицироваться один раз и получать доступ к множеству сервисов без необходимости повторной аутентификации. Пример использования: Kerberos широко используется в системах, где требуется высокая безопасность, таких как Active Directory, для обеспечения централизованного управления доступом и аутентификацией в сети. Механизмы работы: LDAP: LDAP работает по принципу запроса и ответа. Клиент отправляет запрос к LDAP-серверу для поиска, добавления, изменения или удаления данных в каталоге. LDAP использует протокол TCP/IP для передачи данных и может работать по защищенному соединению через LDAPS (LDAP over SSL). LDAP не занимается аутентификацией пользователей, но предоставляет данные, необходимые для аутентификации (например, хранение паролей, хешей). Kerberos: Kerberos использует симметричное шифрование и систему тикетов для аутентификации. Когда пользователь проходит аутентификацию, Kerberos выдает тикет-доступ (Ticket Granting Ticket, TGT), который используется для получения других тикетов для доступа к различным сервисам в сети без повторного ввода пароля. Kerberos работает по протоколу UDP и может использовать TCP для передачи больших данных или в случае высокой надежности соединения. Безопасность: LDAP: LDAP не предоставляет встроенных механизмов для аутентификации и шифрования, поэтому он часто используется в связке с другими протоколами, такими как Kerberos, для повышения безопасности. LDAP может использовать SSL/TLS для защиты данных в процессе передачи. Kerberos: Kerberos обеспечивает высокий уровень безопасности, используя механизм взаимной аутентификации и шифрования на основе симметричных ключей. Все данные, передаваемые между клиентом и сервером, шифруются, что предотвращает перехват или подделку данных. Интеграция и использование: LDAP: LDAP может интегрироваться с различными сервисами и приложениями, такими как почтовые серверы, веб-приложения, системы управления доступом и т.д. LDAP часто используется в качестве базы данных для хранения информации о пользователях, которая затем используется для аутентификации в других системах. Kerberos: Kerberos используется в системах, где необходима безопасная аутентификация пользователей и сервисов, часто в средах, где требуется поддержка SSO (Single Sign-On). Он может интегрироваться с LDAP для получения данных о пользователях, но сам Kerberos занимается только процессом аутентификации.

II. Описание шкалы оценивания

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно.

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ».