Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Северо-Кавказский федеральный университет»

Колледж СКФУ в г. Ставрополе

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к практическим занятиям

по (учебной) дисциплине ОП.07 КОМПЬЮТЕРНЫЕ СЕТИ

Специальность **09.02.11 Разработка и управление программным обеспечением**

Форма обучения очная

Ставрополь

Методические указания к практическим занятиям по дисциплине «ОП.07 Компьютерные сети» составлены в соответствии с требованиями ФГОС СПО и предназначены для студентов, обучающихся по специальности: 09.02.11 Разработка и управление программным обеспечением

.

Методические указания для учебной дисциплины разработаны:

1 Малецкой Н.В,., преподаватель колледжа СКФУ в Ставрополе

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Данные методические указания предназначаются для оказания помощи студентам в выполнении практических работ по учебной дисциплине «ОП.07 Компьютерные сети».

Раздел 2. Модель межсетевого взаимодействия OSI, TCP/IP

Тема 2.1. Физический уровень.

Практическое занятие Настройка сетевых устройств физического уровня с помощью эмулятора. Технология подключения к сети интернет ADSL, ADSL2+, SHDSL, WDSL, асимметрия.

Цель:

- Изучение и настройка устройств физического уровня для различных технологий подключения к сети интернет.
- Ознакомление с принципами работы и особенностями технологий ADSL, ADSL2+, SHDSL, WDSL.
- Изучение асимметричности в сетях.

Задания:

Подготовка среды:

Установите и настройте эмулятор GNS3 на своем компьютере.

Загрузите образы устройств Cisco, поддерживающих технологии ADSL, ADSL2+, SHDSL, WDSL.

Моделирование топологии сети:

Создайте простую топологию с использованием эмулятора, включающую маршрутизаторы и устройства, поддерживающие технологии ADSL, ADSL2+, SHDSL, WDSL.

Настройка маршрутизатора:

Настройте основной маршрутизатор для работы с выбранной технологией (например, ADSL).

Укажите параметры соединения, такие как VPI/VCI (для ADSL), скорость передачи данных, IP-адреса.

Настройка устройств DSLAM:

Если возможно, добавьте в топологию устройства DSLAM (Digital Subscriber Line Access Multiplexer), которые представляют оборудование на стороне провайдера.

Тестирование асимметрии:

Создайте сценарий для тестирования асимметрии в выбранной технологии.

Определите различия в скоростях передачи данных в направлениях от абонента к провайдеру и от провайдера к абоненту.

Анализ результатов:

Проанализируйте результаты тестирования асимметрии.

Рассмотрите возможные причины различий в скоростях передачи данных в асимметричных технологиях.

Отчет:

- Напишите отчет, включающий шаги выполненных заданий, конфигурацию устройств, полученные результаты тестирования и ваши выводы.

Критерии оценки:

- Корректная настройка устройств физического уровня.
- Понимание принципов работы технологий ADSL, ADSL2+, SHDSL, WDSL.
- Успешное проведение тестирования асимметрии и анализ результатов.

Подготовка среды:

Загрузите и установите эмулятор GNS3 с официального сайта.

Загрузите образы Cisco IOS, которые поддерживают технологии ADSL, ADSL2+, SHDSL, WDSL. Образы могут быть получены от Cisco, если у вас есть соответствующие права.

Создание топологии:

Запустите GNS3 и создайте новый проект.

Добавьте устройства (роутеры) и связи, создавая топологию, которая соответствует вашей задаче. Обратите внимание, что для поддержки технологий DSL (Digital Subscriber Line) может потребоваться использование модулей в роутерах.

Настройка маршрутизатора:

Выберите роутер, который будет использоваться для эмуляции абонентского оборудования.

Настройте параметры соединения, такие как VPI/VCI (для ADSL), скорость передачи данных и IP-адреса.

Добавление DSLAM:

Если выбранная технология включает в себя DSLAM, добавьте соответствующие устройства в топологию. Настройте их параметры.

Сценарий тестирования асимметрии:

Создайте сценарий тестирования, например, передачу файла с сервера провайдера на абонентское устройство и обратно.

Используйте инструменты GNS3 для мониторинга пропускной способности и времени отклика.

Анализ результатов:

Оцените различия в скоростях передачи данных в направлениях от абонента к провайдеру и от провайдера к абоненту.

Проанализируйте возможные причины асимметрии и её влияние на качество обслуживания.

Оформление отчета:

Внесите в отчет конфигурацию устройств и параметры сети.

Опишите шаги выполненных заданий.

Приведите результаты тестирования и сделайте выводы.

Презентация:

Подготовьте краткую презентацию, в которой расскажите о выполненной работе, представите основные моменты и ответите на возможные вопросы.

Дополнительные шаги:

По желанию, вы можете дополнить вашу топологию, добавив другие технологии DSL, экспериментировать с разными параметрами соединения и т.д.

Обсуждение:

Проведите обсуждение результатов с преподавателем и коллегами, обменяйтесь опытом и впечатлениями от работы.

Раздел 2. Модель межсетевого взаимодействия OSI, TCP/IP

Тема 2.2. Канальный уровень.

Практическое занятие Настройка коммутаторов L2 уровня, сетевая петля, IP адресация, маска подсети.

Цель:

- Опыт настройки коммутаторов на уровне L2.
- Понимание проблемы сетевой петли и методов ее предотвращения.
- Настройка IP-адресации и маски подсети для коммутаторов.

Задания:

Создание топологии:

Используя Cisco Packet Tracer, создайте сеть, состоящую из нескольких коммутаторов.

Подключите компьютеры к коммутаторам для формирования простой топологии.

Настройка IP-адресации:

Назначьте IP-адреса и маски подсети для интерфейсов коммутаторов.

Предотвращение сетевой петли:

Рассмотрите проблему сетевой петли и ее последствия.

Настройте протокол Spanning Tree (STP) на коммутаторах для предотвращения сетевой петли.

Тестирование:

Проверьте соединение между компьютерами, убедившись, что настройка IP-адресации корректна.

Проведите тесты на наличие сетевой петли, например, подключив дополнительный кабель между двумя портами одного коммутатора.

Отчет:

- Напишите отчет, включающий шаги выполненных заданий, конфигурацию коммутаторов, полученные результаты тестирования и ваши выводы.

Критерии оценки:

- Корректная настройка IP-адресации и масок подсетей.
- Настройка протокола Spanning Tree для предотвращения сетевой петли.
- Успешное проведение тестов и предотвращение сетевой петли.

Пример настройки:

Настройка IP-адресации на коммутаторе:

bash
Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# no shutdown

Настройка Spanning Tree Protocol (STP):

bash
Switch> enable
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 root primary

Дополнительные задания и настройки:

Безопасность:

Включите функцию Port Security на коммутаторах, чтобы ограничить доступ к сети только определенным устройствам по MAC-адресам.

Настройте пароль на коммутаторах для доступа к командному интерфейсу.

Обнаружение сетевых петель:

Включите механизмы обнаружения сетевых петель (Loop Guard, UDLD) для дополнительного обеспечения безопасности и стабильности сети.

Резервирование коммутаторов:

Настройте второй коммутатор как резервный, чтобы обеспечить отказоустойчивость сети в случае отказа первого коммутатора.

Документирование:

Создайте документацию, включающую схему топологии, настройки IP-адресации, конфигурации коммутаторов и прочую информацию.

Расширение топологии:

Добавьте дополнительные устройства, такие как маршрутизаторы, для создания более сложной сетевой топологии.

Настройте маршрутизацию между виртуальными локальными сетями (VLAN).

Тестирование на отказоустойчивость:

Проведите тесты на отказоустойчивость, отключив один из коммутаторов и убедившись, что сеть продолжает работать.

Пример дополнительной настройки:

Включение Port Security:

bash
Switch> enable

Switch# configure terminal
Switch(config)# interface range fa0/1 - 24
Switch(config-if-range)# switchport port-security
Switch(config-if-range)# switchport port-security maximum 2
Switch(config-if-range)# switchport port-security violation restrict
Switch(config-if-range)# switchport port-security mac-address sticky

Настройка безопасности доступа к коммутатору:

bash
Switch> enable
Switch# configure terminal
Switch(config)# enable secret ваш_пароль
Switch(config)# line vty 0 15
Switch(config-line)# password ваш_пароль
Switch(config-line)# login

Продвинутые задания и дополнительные конфигурации:

Виртуальные локальные сети (VLAN):

Создайте VLAN на коммутаторах и настройте их для обеспечения изоляции трафика между различными сегментами сети.

Настройте маршрутизацию между VLAN с использованием маршрутизатора.

Quality of Service (QoS):

Включите QoS на коммутаторах для управления приоритетами трафика, обеспечивая более высокое качество обслуживания для определенных приложений или сервисов.

EtherChannel (Link Aggregation):

Настройте группу портов в режиме EtherChannel для повышения пропускной способности и отказоустойчивости между коммутаторами.

Включение DHCP:

Настройте коммутаторы в роли DHCP-серверов для автоматического выделения IP-адресов клиентам в сети.

Мониторинг и логирование:

Настройте системы мониторинга и логирования на коммутаторах для отслеживания событий и выявления проблем в сети.

Обеспечение безопасности VLAN:

Используйте функции, такие как Private VLAN (PVLAN), для усиления безопасности между устройствами внутри одного VLAN.

Настройка SNMP (Simple Network Management Protocol):

Включите SNMP на коммутаторах для возможности удаленного мониторинга и управления сетевым оборудованием.

Примеры продвинутых настроек:

Настройка VLAN:

bash
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Отдел_1
Switch(config)# vlan 20
Switch(config-vlan)# name Отдел_2
Switch(config)# interface range fa0/1 - 12
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config)# interface range fa0/13 - 24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20

Включение EtherChannel:

bash

```
Switch> enable
Switch# configure terminal
Switch(config)# interface range gi0/1 - 2
Switch(config-if-range)# channel-group 1 mode desirable
Switch(config-if-range)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
```

Настройка DHCP:

bash

```
Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# exit
Switch(config)# ip dhcp pool Название_пула
Switch(dhcp-config)# network 192.168.1.0 255.255.255.0
Switch(dhcp-config)# default-router 192.168.1.1
Switch(dhcp-config)# exit
Switch(config)# service dhcp
```

Раздел 2. Модель межсетевого взаимодействия OSI, TCP/IP

Тема 2.3. Сетевой уровень.

Практическое занятие Настройка маршрутизатора, разноранговые сети, создание VPN тонеля ip sec, L2TP.

Определение интерфейсов:

Присвойте IP-адреса интерфейсам маршрутизатора, соответствующим различным сетям.

bash

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Повторите эти шаги для каждого интерфейса, находящегося в разных сетях.

Настройка маршрутизации:

Включите маршрутизацию на маршрутизаторе, чтобы он мог пересылать пакеты между различными сетями.

bash

```
Router(config)# ip routing
```

Настройка статических маршрутов (при необходимости):

Добавьте статические маршруты для достижения удалённых сетей, если ваша сеть использует несколько маршрутизаторов.

bash

```
Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.2
```

Создание VPN-туннеля с использованием IPSec и L2TP:

Настройка IPSec:

Включите IPSec на маршрутизаторе и настройте параметры шифрования и аутентификации.

bash

Router(config)# crypto isakmp policy 10
Router(config-isakmp)# encr aes
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 2
Router(config-isakmp)# exit

Router(config)# crypto isakmp key ВАШ_ПАРОЛЬ address 0.0.0.0
Router(config)# crypto ipsec transform-set MY_TRANSFORM_SET esp-aes esp-sha-hmac
Router(config)# crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
Router(config-crypto-map)# set peer УДАЛЕННЫЙ_IP
Router(config-crypto-map)# set transform-set MY_TRANSFORM_SET
Router(config-crypto-map)# match address VPN_ACL

Настройка L2TP:

Включите L2TP и настройте параметры, такие как IP-адрес пула для назначения клиентам.

bash
Router(config)# bba-group pppoe global
Router(config-bba-group)# virtual-template 1
Router(config)# interface Virtual-Template1
Router(config-if)# mtu 1492
Router(config-if)# peer default ip address pool VPN_POOL

Настройка IP-адресов для клиентов:

Создайте пул IP-адресов, который будет использоваться для назначения клиентам при подключении.

bash
Router(config)# ip local pool VPN_POOL 192.168.3.1 192.168.3.10

Настройка ACL (Access Control List):

Создайте ACL для определения трафика, который будет направляться через VPN-туннель.

bash
Router(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

Привязка VPN-туннеля к интерфейсу:

Привяжите VPN-туннель к интерфейсу, через который будет обрабатываться трафик.

bash
Router(config)# interface GigabitEthernet0/0
Router(config-if)# crypto map MY_CRYPTO_MAP

Пример настройки клиента:

Для клиента настройте подключение с использованием L2TP и указанием параметров IPSec (ключ, IP-адрес сервера, шифрование и т. д.) в настройках VPN-подключения.

Обратите внимание, что данная конфигурация предоставляет общий обзор процесса настройки VPN-туннеля с использованием IPSec и L2TP. Перед применением подобной конфигурации в реальной сети рекомендуется ознакомиться с документацией вашего оборудования и внести необходимые изменения согласно требованиям вашей сети и политикам безопасности.

Продолжение настройки VPN-туннеля с использованием IPSec и L2TP:

Настройка L2TP на интерфейсе WAN:

Включите L2TP на интерфейсе WAN маршрутизатора.

bash
Router(config)# interface GigabitEthernet0/1 # Здесь GigabitEthernet0/1 - ваш интерфейс WAN
Router(config-if)# pppoe enable group global

Настройка параметров IPSec для L2TP:

Укажите параметры IPSec для L2TP.

bash

```
Router(config)# crypto isakmp policy 20
Router(config-isakmp)# encr aes
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 2
Router(config-isakmp)# exit

Router(config)# crypto isakmp key ВАШ_ПАРОЛЬ address 0.0.0.0
```

Настройка L2TP:

Включите L2TP и определите параметры, такие как IP-адрес сервера, предварительно распределённые ключи, аутентификация и шифрование.

bash

```
Router(config)# virtual-template 1
Router(config)# interface Virtual-Template1
Router(config-if)# peer default ip address pool VPN_POOL
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# exit

Router(config)# bba-group pppoe global
Router(config-bba-group)# virtual-template 1
```

Настройка ACL (Access Control List):

Создайте ACL для определения трафика, который будет направляться через VPN-туннель.

bash

```
Router(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Привязка VPN-туннеля к интерфейсу WAN:

Привяжите VPN-туннель к интерфейсу WAN.

bash

```
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# pppoe enable group global
Router(config-if)# pppoe-client dial-pool-number 1
```

Настройка IP-адресов для клиентов:

Создайте пул IP-адресов, который будет использоваться для назначения клиентам при подключении.

bash

```
Router(config)# ip local pool VPN_POOL 192.168.3.1 192.168.3.10
```

Пример настройки клиента:

Настройка подключения:

Настройте VPN-подключение на клиенте, используя протокол L2TP и указав параметры IPSec, такие как ключ, IP-адрес сервера, шифрование и аутентификацию.

Подключение:

Запустите VPN-подключение на клиенте и убедитесь в успешном соединении с удалённой сетью через L2TP/IPSec.

Настройка IPSec:

Настройка протокола IPSec:

bash

/ip ipsec proposal
set [find default=yes] enc-algorithms=aes-256-cbc
/ip ipsec peer
add address=УДАЛЕННЫЙ_IP auth-method=pre-shared-key secret=ВАШ_ПАРОЛЬ

Настройка политики IPSec:

bash
/ip ipsec policy
add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 sa-dst-address=УДАЛЕННЫЙ_IP \
tunnel=yes proposal=default

Настройка L2TP:

Настройка L2TP-сервера:

bash
/interface l2tp-server server
set authentication=mschap2 default-profile=default enabled=yes use-ipsec=required

Настройка пула IP-адресов для клиентов:

bash
/ip pool
add name=VPN_POOL ranges=192.168.3.1-192.168.3.10

Настройка профиля L2TP:

bash
/ppp profile
add dns-server=8.8.8.8 local-address=192.168.1.1 name=default \
remote-address=VPN_POOL use-encryption=yes

Настройка пользователя для аутентификации:

bash
/ppp secret
add name=ВАШ_ЛОГИН password=ВАШ_ПАРОЛЬ profile=default

Примечания:

В приведенных примерах "УДАЛЕННЫЙ_IP" - это IP-адрес удаленного сервера, "ВАШ_ПАРОЛЬ" - это предварительно согласованный пароль для IPSec, "ВАШ_ЛОГИН" и "ВАШ_ПАРОЛЬ" - учетные данные пользователя L2TP.

Убедитесь, что на маршрутизаторе MikroTik включена поддержка L2TP и IPSec. Это можно проверить, используя команду /interface l2tp-server print и /ip ipsec print.

Раздел 2. Модель межсетевого взаимодействия OSI, TCP/IP

Тема 2.4. Транспортный уровень.

Практическое занятие IPv4-адресация, IPv6-адресация, Популярные диапазоны частных IP-адресов: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8.

IPv4 и IPv6 предоставляют уникальные адресные пространства для идентификации устройств в сети. Давайте рассмотрим адресацию в IPv4 и IPv6, а также популярные диапазоны частных IP-адресов в IPv4.

IPv4-адресация:

IPv4-адрес:

IPv4 использует 32-битные адреса и записывается в виде четырех десятичных чисел, разделенных точками (например, 192.168.1.1).

Подсети и маска подсети:

IPv4-адреса могут быть разделены на подсети с использованием маски подсети. Например, адрес 192.168.1.1/24 означает, что первые 24 бита представляют собой сетевую часть, а остальные 8 бит - хостовую.

IPv6-адресация:

IPv6-адрес:

IPv6 использует 128-битные адреса и записывается в виде восьми групп четырех шестнадцатеричных цифр, разделенных двоеточиями (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Сокращение записи:

Нули в IPv6-адресах могут быть сокращены. Например, 2001:0db8:0000:0042:0000:8a2e:0370:7334 может быть записан как 2001:db8:0:42:0:8a2e:370:7334.

Популярные диапазоны частных IP-адресов в IPv4:

192.168.0.0/16:

Этот диапазон (192.168.0.0 - 192.168.255.255) является одним из наиболее часто используемых для построения частных сетей.

172.16.0.0/12:

Диапазон 172.16.0.0 - 172.31.255.255 также предназначен для частных сетей и часто используется в корпоративных средах.

10.0.0.0/8:

Диапазон 10.0.0.0 - 10.255.255.255 также зарезервирован для частных сетей и широко применяется в различных сценариях.

Эти частные адреса не маршрутизируются в интернете и могут быть использованы в локальных сетях.

Рекомендации:

Использование частных IP-адресов:

Рекомендуется использовать частные IP-адреса внутри локальных сетей, чтобы избежать конфликтов с глобальными IP-адресами в интернете.

IPv6-переход:

С увеличением числа подключенных устройств и ограниченности адресов IPv4, важен переход к IPv6 для обеспечения достаточного адресного пространства.

Дополнительные сведения по IPv4 и IPv6:

IPv4:

Структура IPv4-адреса:

IPv4-адрес представляет собой 32 бита, разделенные на 4 октета (байта) по 8 бит каждый. Каждый октет записывается в десятичной системе счисления и разделяется точками.

Public vs. Private IPv4:

Публичные IP-адреса используются для доступа к сети из интернета, тогда как частные IP-адреса предназначены для внутренних сетей.

NAT (Network Address Translation):

Используется для преобразования множества частных IP-адресов в один (или несколько) публичных IP-адресов для выхода в интернет.

IPv6:

Структура IPv6-адреса:

IPv6-адрес состоит из 8 групп по 4 символа в шестнадцатеричной системе счисления. Каждая группа представляет собой 16 бит.

Уникальность IPv6:

IPv6 предоставляет значительно больше уникальных адресов (2^128), что решает проблему нехватки адресов IPv4.

Отсутствие необходимости в NAT:

Использование IPv6 уменьшает или устраняет потребность в Network Address Translation (NAT) благодаря большому адресному пространству.

Практическое использование:

Работа с IPv6-адресами:

Воспользуйтесь IPv6-адресами, чтобы обеспечить устройствам уникальные и постоянные идентификаторы в сети.

Тестирование совместимости:

Проверьте совместимость вашего сетевого оборудования и программного обеспечения с IPv6 для подготовки к будущему переходу.

Поддержка обоих протоколов:

Многие сетевые устройства и системы поддерживают оба протокола (IPv4 и IPv6), что позволяет сети функционировать в смешанных средах.

Обучение и сертификация:

Работники сетевых специальностей должны обладать знаниями и навыками по IPv4 и IPv6. Получение сертификации IPv6 может быть полезным.

Внедрение IPv6 важно для обеспечения устойчивости и расширяемости сетей, особенно с увеличением числа подключенных устройств. Помните о том, что IPv6 является неотъемлемой частью будущего интернета.

Раздел 2. Модель межсетевого взаимодействия OSI, TCP/IP

Тема 2.5. Прикладной уровень.

Практическое занятие Веб-браузеры (Chrome, Firefox, Safari) для просмотра веб-страниц по протоколу HTTP. Электронная почта (Outlook, Gmail) для обмена электронными письмами по протоколам SMTP, POP3 и IMAP. Файловые клиенты (FileZilla) для передачи файлов по протоколу FTP. Мессенджеры (WhatsApp, Telegram) для обмена мгновенными сообщениями. Клиент-серверное взаимодействие.

Веб-браузеры:

Google Chrome:

Google Chrome является одним из наиболее популярных веб-браузеров. Он поддерживает множество расширений и имеет высокую скорость работы.

Mozilla Firefox:

Firefox от Mozilla - браузер с открытым исходным кодом, который предоставляет высокую степень настраиваемости и защиты приватности.

Safari:

Safari является стандартным браузером для устройств Apple. Он хорошо интегрирован с macOS и iOS, обеспечивает высокую производительность и энергоэффективность.

Электронная почта:

Microsoft Outlook:

Outlook является частью пакета Microsoft Office и предоставляет расширенные функции для работы с электронной почтой, календарем и задачами.

Gmail:

Gmail от Google - веб-почтовый сервис с множеством функций, включая умные фильтры и хороший интегрированный поиск.

Протоколы электронной почты:

SMTP (Simple Mail Transfer Protocol):

Используется для отправки электронных писем. Клиент отправляет сообщение на сервер по протоколу SMTP.

POP3 (Post Office Protocol 3):

Позволяет клиентским приложениям загружать электронные сообщения с почтового сервера на локальный компьютер.

IMAP (Internet Message Access Protocol):

Позволяет клиентам управлять электронной почтой непосредственно на сервере, а не загружать её на локальное устройство.

Файловые клиенты:

FileZilla:

FileZilla - мощный и легкий в использовании FTP-клиент, который поддерживает FTP, SFTP и FTPS протоколы.

Мессенджеры:

WhatsApp:

WhatsApp - мессенджер с широким распространением, позволяющий обмениваться текстовыми сообщениями, звонками и видео.

Telegram:

Telegram - мессенджер с фокусом на безопасность и скорость передачи данных. Поддерживает шифрование и ботов.

Клиент-серверное взаимодействие:

Клиент:

Клиент - это устройство или приложение, которое обращается к серверу для получения данных или выполнения определенных задач.

Сервер:

Сервер - это устройство или приложение, которое предоставляет ресурсы или услуги клиентам через сеть.

Протоколы для клиент-серверного взаимодействия:

HTTP (Hypertext Transfer Protocol), HTTPS (HTTP Secure), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), и другие.

Клиент-серверная модель является фундаментальной для многих сетевых приложений, включая веб, электронную почту и передачу файлов. В этой модели клиенты и серверы взаимодействуют, отправляя и принимая данные через определенные протоколы.

Веб-браузеры:

Открытие браузера:

Запустите выбранный вами веб-браузер (например, Chrome, Firefox, Safari).

Ввод адреса:

Введите адрес веб-сайта в адресной строке или используйте поисковый движок для поиска информации.

Навигация:

Используйте кнопки навигации (назад, вперёд), закладки и другие функции для удобного перемещения по веб-страницам.

Отправка данных:

Заполняйте формы, отправляйте комментарии, пользуйтесь интерактивными элементами на веб-страницах.

Работа с вкладками:

Открывайте новые вкладки для параллельного просмотра нескольких веб-страниц.

Электронная почта:

Открытие почтового клиента:

Запустите почтовый клиент (Outlook, Gmail и т.д.).

Аутентификация:

Введите учетные данные для входа в почтовый аккаунт.

Чтение писем:

Открывайте и читайте входящие письма.

Отправка писем:

Создавайте новые письма, вводите адреса получателей, добавляйте вложения и отправляйте сообщения.

Организация писем:

Используйте папки, метки или категории для организации ваших писем.

Файловые клиенты (FileZilla):

Открытие FileZilla:

Запустите FileZilla или аналогичный FTP-клиент.

Установка соединения:

Введите адрес FTP-сервера, имя пользователя и пароль для установки соединения.

Передача файлов:

Перетаскивайте файлы между локальной и удаленной сторонами, используя интерфейс клиента.

Управление структурой каталогов:

Создавайте новые папки, перемещайте и удаляйте файлы на удаленном сервере.

Мессенджеры (WhatsApp, Telegram):

Открытие мессенджера:

Запустите выбранный мессенджер (WhatsApp, Telegram).

Аутентификация:

Введите номер телефона и проходите процедуру аутентификации.

Обмен сообщениями:

Отправляйте текстовые сообщения, медиа-файлы, видео, и используйте другие функции обмена информацией.

Групповые чаты:

Создавайте или присоединяйтесь к групповым чатам для общения с несколькими участниками.

Клиент-серверное взаимодействие:

Клиентская сторона:

Клиент отправляет запросы серверу для получения данных или выполнения определенных операций.

Серверная сторона:

Сервер принимает запросы от клиентов, обрабатывает их и отправляет обратно результаты или необходимую информацию.

Протоколы:

Различные протоколы (HTTP, SMTP, FTP) используются для обеспечения стандартного взаимодействия между клиентами и серверами.

Безопасность веб-браузеров:

Обеспечьте безопасность браузера с помощью расширений или настроек, например, блокировки вредоносных сайтов и использования защищенного протокола HTTPS.

Обновления:

Регулярно обновляйте браузеры, почтовые клиенты и другие программы для обеспечения безопасности и доступа к последним функциям.

Настройка электронной почты:

Конфигурируйте почтовые клиенты с учетом параметров протоколов SMTP, POP3 или IMAP в зависимости от требований вашего почтового провайдера.

Интеграция файловых клиентов:

Возможность синхронизации или обмена файлами напрямую из файловых клиентов с другими приложениями и облачными хранилищами.

Шифрование сообщений в мессенджерах:

В случае мессенджеров, активируйте функции шифрования для обеспечения конфиденциальности ваших сообщений.

Работа с кукис в браузерах:

Понимание и управление файлами cookie в настройках браузера для контроля вашей онлайн-активности и конфиденциальности.

Отладка сетевых проблем:

При возникновении проблем с сетью используйте инструменты отладки, такие как инспектор браузера, средства разработчика, чтобы определить причину и решение проблем.

Многозадачность:

Используйте встроенные функции многозадачности браузеров и программ для эффективной работы с несколькими задачами одновременно.

Клиент-серверные приложения:

Разработка собственных клиент-серверных приложений с использованием соответствующих API и технологий.

Понимание протоколов:

Глубокое понимание протоколов, таких как HTTP, SMTP, POP3, IMAP, FTP, для эффективной работы и устранения возможных проблем.

Раздел 4. Беспроводные сети.

Тема 4.2. Управление беспроводными сетями.

Практическое занятие Управление каналами, Мониторинг и Обнаружение, Обнаружение и Реагирование на Инциденты, Обновление ПО и Firmware, Оптимизация сети.

Управление каналами:

Конфигурация и мониторинг сетевых устройств:

Определите и настройте каналы на маршрутизаторах, коммутаторах и других устройствах для оптимального распределения трафика.

Качество обслуживания (QoS):

Используйте QoS для приоритизации трафика и обеспечения оптимального качества обслуживания для различных типов данных.

Мониторинг пропускной способности:

Используйте инструменты мониторинга, чтобы отслеживать использование пропускной способности и выявлять возможные узкие места.

Обеспечение безопасности каналов:

Применяйте шифрование (например, VPN) для обеспечения безопасности передаваемых данных по каналам.

Мониторинг и Обнаружение:

Использование систем мониторинга:

Внедрите системы мониторинга сети для отслеживания состояния устройств, пропускной способности и других параметров.

Обнаружение аномалий:

Используйте средства для обнаружения аномалий в сетевом трафике, что может свидетельствовать о возможных атаках или сбоях.

Системы логирования:

Настройте системы логирования на сетевых устройствах и серверах для регистрации событий и обеспечения возможности анализа.

Обнаружение и Реагирование на Инциденты:

План инцидентного реагирования:

Разработайте и документируйте план реагирования на инциденты, определяя шаги по обнаружению, анализу и устранению проблем.

Использование SIEM (Security Information and Event Management):

Внедрите SIEM-системы для сбора и анализа данных о безопасности, что обеспечит раннее обнаружение инцидентов.

Обучение персонала:

Обучите персонал методам обнаружения и реагирования на инциденты, а также эффективному взаимодействию с инструментами безопасности.

Обновление ПО и Firmware:

Регулярные обновления:

Установка регулярных обновлений программного обеспечения (OS, приложений) и прошивок устройств для исправления уязвимостей.

Автоматизация обновлений:

Используйте инструменты для автоматизации процесса обновления, чтобы минимизировать риск от неприменения патчей.

Тестирование перед обновлением:

Проводите тестирование обновлений в контролируемой среде перед их применением в производственной сети.

Оптимизация сети:

Анализ трафика:

Проведите анализ трафика сети, чтобы выявить и устранить узкие места и оптимизировать использование пропускной способности.

Оптимизация маршрутизации:

Настройте маршрутизацию с учетом оптимального использования сетевых ресурсов и минимизации задержек.

Кэширование и сжатие данных:

Применяйте техники кэширования и сжатия данных для сокращения времени загрузки и использования пропускной способности.

Балансировка нагрузки:

Используйте балансировку нагрузки для распределения трафика между серверами, обеспечивая равномерную загрузку.

Оптимизация производительности протоколов:

Настройте параметры протоколов (TCP/IP, UDP) с учетом требований конкретных приложений для оптимальной производительности.

Управление каналами, мониторинг, обнаружение инцидентов, обновление ПО и firmware, а также оптимизация сети, являются важными аспектами сетевого администрирования для обеспечения стабильности, безопасности и эффективности сетевой инфраструктуры.

Управление каналами:

Анализ Требований:

Определите требования к пропускной способности, задержкам и другим параметрам сети для эффективного управления каналами.

Конфигурация Сетевого Оборудования:

Настройте маршрутизаторы, коммутаторы и другие устройства для оптимального управления трафиком в соответствии с выявленными требованиями.

Внедрение QoS:

Реализуйте QoS-политики для приоритизации важного трафика и управления пропускной способностью сети.

Мониторинг Пропускной Способности:

Используйте инструменты мониторинга для постоянного отслеживания использования пропускной способности и выявления возможных узких мест.

Мониторинг и Обнаружение:

Выбор Инструментов Мониторинга:

Разработайте стратегию мониторинга и выберите подходящие инструменты (Nagios, Zabbix, PRTG) для наблюдения за состоянием сетевых устройств.

Конфигурация Систем Мониторинга:

Настройте системы мониторинга для отслеживания параметров, таких как доступность устройств, загрузка CPU, использование памяти и другие.

Обнаружение Аномалий:

Внедрите решения для обнаружения аномалий в трафике, используя технологии, такие как IDS/IPS (системы обнаружения и предотвращения вторжений).

Обнаружение и Реагирование на Инциденты:

Разработка Плана Реагирования:

Создайте подробный план реагирования на инциденты, который включает шаги по обнаружению, анализу и устранению угроз.

Интеграция SIEM:

Внедрите SIEM-систему для централизованного сбора и анализа данных о безопасности для раннего обнаружения инцидентов.

Обучение Команды:

Обучите команду по обнаружению инцидентов, проводите регулярные учения и обновляйте навыки персонала.

Обновление ПО и Firmware:

Определение Обновлений:

Регулярно отслеживайте выход новых версий программного обеспечения, операционных систем и прошивок для сетевого оборудования.

Разработка Плана Обновлений:

Создайте план регулярных обновлений, включая тестирование в безопасной среде перед внедрением.

Автоматизация Обновлений:

Используйте инструменты автоматизации для управления процессом обновлений, чтобы минимизировать риски и снизить время простоя.

Оптимизация Сети:

Анализ Трафика:

Проведите анализ трафика, выявляя часто используемые маршруты и определяя паттерны использования сети.

Оптимизация Маршрутизации:

Настройте маршрутизацию для оптимизации путей следования данных и уменьшения задержек.

Применение Техник Кэширования и Сжатия:

Внедрите техники кэширования и сжатия данных, чтобы сократить время загрузки и использование пропускной способности.

Балансировка Нагрузки:

Используйте механизмы балансировки нагрузки для равномерного распределения трафика между серверами.

Оптимизация Протоколов:

Настройте параметры протоколов (TCP/IP, UDP) для максимальной производительности и эффективности.

Раздел 5. Виртуализация сетей.

Тема 5.1. Виртуальные локальные сети.

Практическое занятие Облачные вычисления, Центры обработки данных, Корпоративные сети, Тестирование и разработка.

Облачные вычисления:

Выбор Облачного Поставщика:

Проанализируйте требования организации и выберите подходящего облачного поставщика (AWS, Azure, Google Cloud).

Развертывание Ресурсов:

Разверните виртуальные машины, хранилища данных и другие ресурсы в облаке в соответствии с бизнес-потребностями.

Управление Ресурсами:

Используйте средства управления облаком для мониторинга и оптимизации использования ресурсов.

Безопасность в Облаке:

Реализуйте меры безопасности, такие как шифрование данных, контроль доступа и мониторинг безопасности для защиты информации в облаке.

Центры Обработки Данных (ЦОД):

Дизайн и Строительство ЦОД:

Разработайте проект ЦОД, включая выбор местоположения, охлаждение, электропитание и оборудование.

Управление Инфраструктурой:

Разверните и управляйте серверами, сетевым оборудованием и хранилищами данных в ЦОД.

Мониторинг и Обслуживание:

Установите системы мониторинга для отслеживания температуры, энергопотребления и работы оборудования в реальном времени.

Энергоэффективность:

Оптимизируйте энергопотребление, используя энергосберегающие технологии и мониторинг эффективности.

Корпоративные Сети:

Проектирование Сети:

Разработайте корпоративную сеть, учитывая требования по пропускной способности, надежности и безопасности.

Управление Трафиком:

Используйте средства управления трафиком для обеспечения эффективного распределения ресурсов и минимизации задержек.

VPN и Безопасность:

Настройте виртуальные частные сети (VPN) и применяйте средства шифрования для защиты корпоративного трафика.

Безопасность Сети:

Реализуйте меры безопасности, такие как брандмауэры, системы обнаружения вторжений и регулярное обновление программного обеспечения.

Тестирование и Разработка:

Выбор Методологии Тестирования:

Определите методологию тестирования (например, Agile, Scrum) и инструменты для эффективного тестирования ПО.

Разработка Тестовых Сценариев:

Создайте тестовые сценарии, охватывающие функциональность, производительность и безопасность разрабатываемого ПО.

Автоматизация Тестирования:

Автоматизируйте тестирование с использованием инструментов автоматизации для ускорения процесса и повышения точности результатов.

Континуальная Интеграция:

Реализуйте систему непрерывной интеграции (CI), чтобы автоматизировать процесс сборки и тестирования кода при каждом его изменении.

Обеспечение Качества ПО:

Внедрите процессы обеспечения качества, включая регулярные код-ревью и тестирование на всех этапах разработки.

Ход Работы:

Анализ Потребностей:

Определите потребности организации в облачных вычислениях, ЦОД, корпоративных сетях и разработке ПО.

Проектирование Инфраструктуры:

Разработайте планы по созданию и развертыванию необходимой инфраструктуры с учетом всех вышеуказанных аспектов.

Развертывание и Настройка:

Поставьте в эксплуатацию облачные ресурсы, ЦОД, корпоративную сеть и настройте их согласно требованиям.

Тестирование и Отладка:

Проведите тестирование новой инфраструктуры и программного обеспечения, выявляя и устраняя возможные проблемы.

Внедрение и Масштабирование:

Внедрите инфраструктуру в работу и масштабируйте ее в соответствии с ростом организации и изменением требований.

Обучение Персонала:

Обучите персонал работе с новой инфраструктурой и внедренными технологиями.

Облачные вычисления:

Выбор Облачного Поставщика:

Пример: Организация выбрала Amazon Web Services (AWS) для развертывания своей инфраструктуры в облаке из-за широкого спектра услуг и гибкости.

Развертывание Ресурсов:

Пример: Развертывание виртуальных машин, баз данных и хранилища данных в облаке для обеспечения отказоустойчивости и масштабируемости.

Управление Ресурсами:

Пример: Использование AWS Management Console для мониторинга и управления ресурсами, такими как EC2-инстансы и S3-хранилища.

Безопасность в Облаке:

Пример: Внедрение AWS Identity and Access Management (IAM) для управления доступом и шифрования данных в Amazon S3.

Центры Обработки Данных (ЦОД):

Пример: Построение ЦОД с учетом требований к энергоэффективности, с использованием холодильных систем и резервного электропитания.

Управление Инфраструктурой:

Пример: Использование инструментов управления ЦОД, таких как Data Center Infrastructure Management (DCIM), для мониторинга и контроля оборудования.

Мониторинг и Обслуживание:

Пример: Реализация системы мониторинга температуры и энергопотребления в режиме реального времени.

Энергоэффективность:

Пример: Использование технологий виртуализации серверов для уменьшения числа физических серверов и, как следствие, сокращения энергопотребления.

Корпоративные Сети:

Пример: Разработка корпоративной сети с учетом логической структуры, сегментации и высокой доступности.

Управление Трафиком:

Пример: Использование технологий Quality of Service (QoS) для приоритизации голосового трафика в корпоративной VoIP-сети.

VPN и Безопасность:

Пример: Настройка Virtual Private Network (VPN) для обеспечения защищенного удаленного доступа к корпоративным ресурсам.

Безопасность Сети:

Пример: Внедрение брандмауэров, систем обнаружения вторжений (IDS) и регулярное обновление антивирусных баз.

Тестирование и Разработка:

Выбор Методологии Тестирования:

Пример: Внедрение Agile-методологии разработки и тестирования для обеспечения гибкости и быстрого внедрения изменений.

Разработка Тестовых Сценариев:

Пример: Создание тестовых сценариев, включающих тестирование функциональности, производительности и безопасности.

Автоматизация Тестирования:

Пример: Использование инструментов автоматизации тестирования, таких как Selenium или JUnit, для ускорения процесса.

Континуальная Интеграция:

Пример: Реализация системы Continuous Integration (CI) с использованием Jenkins для автоматизации сборки и тестирования кода.

Обеспечение Качества ПО:

Пример: Внедрение процессов регулярных код-ревью и тестирования на всех этапах разработки для обеспечения высокого качества ПО.

Список информационных источников

Основные печатные и/или электронные издания

1. Акмаров, П. Б. Компьютерные сети. Лабораторный практикум / П. Б. Акмаров. — Санкт-Петербург : Лань, 2024. — 120 с. — ISBN 978-5-507-48068-5. — Текст : электронный

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск : ЮРГПУ (НПИ), 2022. — 216 с. — ISBN 978-5-9997-0805-2. — Текст : электронный

3. Кузин, А. В. Компьютерные сети : учебное пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2025. — 190 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-453-3. - Текст: электронный.

4. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. - Москва ; Вологда : Инфра-Инженерия, 2022. - 460 с. - ISBN 978-5-9729-0962-9. - Текст : электронный.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Северо-Кавказский федеральный университет»

Колледж СКФУ в г. Ставрополе

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к самостоятельной работе

по (учебной) дисциплине	**ОП.11 Компьютерные сети**
Специальность	09.02.07 Информационные системы и программирование
Форма обучения	очная

Ставрополь

1. Пояснительная записка

Методические указания для самостоятельной работы студентов при изучении учебной дисциплины ОП.11 Компьютерные сети предназначены для обучающихся по специальности 09.02.07 Информационные системы и программирование.

При организации СР важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

По учебному плану специальности 09.02.07 Информационные системы и программирование/ в учебной дисциплине ОП.11 Компьютерные сети на внеаудиторную самостоятельную работу обучающихся отводится 6 часов.

2. План-график выполнения СРС

№ п/п	Наименование разделов и тем дисциплины	Краткое содержание самостоятельной работы	Форма контроля	Объем часов
1	**Тема 1.3.** Классификация сетей по масштабу и топологии.	Подготовить презентацию классификации сетей, топологии сети преимущества и недостатки.	проверка презентаций	2
2	**Тема 3.3.** Брандмауэры и средства защиты.	Презентация на тему «Безопасность в сети Интернет».	проверка презентаций	2
3	**Тема 4.3.** Безопасность в беспроводных сетях.	Работа с литературой по темам: Скрытие SSID, Разделение сетей и Гостевой Доступ, Безопасность клиентов, Отключение автоматического подключения.	проверка конспекта	2
Итого				**6**

3. Методические рекомендации по выполнению самостоятельной работы

3.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

3.2 Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и

выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

3.3 Методические рекомендации по созданию презентаций:

1. Оформление.

– Создание первых слайдов обязано привлекать внимание.

– Лучше выдержать особый стиль оформления. Не используйте шаблоны: будьте оригинальны.

– Презентация не должна утомлять своей пестротой. 3-4 цвета – оптимальный вариант.

– Текст должен быть читабелен. На темном фоне – светлые символы и наоборот.

– Не перегружайте презентацию текстами. В ней должны быть ориентиры для вашего красноречия. Конец презентации тоже должен быть запоминающимся. Поработайте над оформлением в редакторах. Цвет и анимация должны соответствовать теме.

2. Содержание.

– Информация должна быть полной, достоверной, актуальной.

– Соответствовать учебной программе.

– Тезаурус для целевой аудитории.

– Могут быть переходы по ссылкам.

3. Вербализация.

– Звук, мелодия сопровождения презентации должны быть гармоничны с оформлением и содержанием. Звук не должен заглушать говорящего.

– Без надобности не используйте песни, распыляющие внимание слушающих.

– Не перегружайте аудио- и видеопотоками презентацию.

4. Количество слайдов: 12-15.

Общие требования:

Средний расчет времени, необходимого на презентацию, ведется исходя из количества слайдов. Обычно на один слайд необходимо не более 2-3 минут. Необходимо использовать максимальное пространство слайда – например, растянув рисунки. По возможности используйте ¾ экрана в верхней части слайда, т.к. с последних рядов нижняя часть экрана обычно не видна. Дизайн должен быть простым и лаконичным. Каждый слайд должен иметь заголовок. Слайды могут быть пронумерованы с указанием общего количества слайдов в презентации. Завершить презентацию следует кратким резюме, содержащим ее основные положения, важные данные, прозвучавшие в докладе.

В оформлении презентаций выделяют два блока: оформление слайдов и представление информации на них. Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к оформлению данных блоков.

Информационное обеспечение реализации программы

Основные печатные и электронные издания

1. Уймин, А. Г. Компьютерные сети. L2-технологии: практикум / А. Г. Уймин. — Москва: Ай Пи Ар Медиа, 2024. — 191 с. — ISBN 978-5-4497-2539-4. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/135259

2. Зиангирова, Л. Ф. Инфокоммуникационные системы и сети: учебное пособие для СПО / Л. Ф. Зиангирова. — 2-е изд. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2024. — 128 с. — ISBN 978-5-4488-2176-9, 978-5-4497-3427-3. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/142221

Дополнительные источники

1. Ибе, О. Компьютерные сети и службы удаленного доступа / О. Ибе; перевод И. В. Синицын. — 3-е изд. — Саратов: Профобразование, 2024. — 335 с. — ISBN 978-5-4488-0054-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/145916

Основные электронные издания

1. Федеральный центр информационно-образовательных ресурсов — URL: www.fcior.edu.ru
2. Единая коллекция цифровых образовательных ресурсов — URL: www.school-collection.edu.ru
3. Единое окно доступа к образовательным ресурсам Российской Федерации — URL: http://window.edu.ru/