

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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Администрирование систем и сетей**

**Москва
2022**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Поляк Р.И.
	Идентификатор	Rbc0e923e-PoliakRI-10208dd2

(подпись)

Р.И. Поляк

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной
программы

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка
подписи)

Заведующий
выпускающей кафедры

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(расшифровка
подписи)

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-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
2. ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
3. ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольное задание 1; Практическое задание № 1; (Контрольная работа)
2. Контрольное задание 2; Практическое задание № 2; (Контрольная работа)
3. Контрольное задание 3; Практическое задание № 3; (Контрольная работа)
4. Практическое задание № 4; Практическое задание № 5. (Контрольная работа)

БРС дисциплины

5 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ- 1	КМ- 2	КМ- 3	КМ- 4
	Срок КМ:	4	8	12	15
Введение в операционные системы					
Тема 1. Определение и основные функции операционных систем. Классификация операционных систем. История развития операционных систем	+				
Тема 2. Основные понятия операционных систем. Структура операционной системы	+				
Тема 3. Файловые системы. Файлы, каталоги. Реализация файловой системы. Примеры файловых систем			+		
Вычислительные сети					

Тема 4. Сети. Протоколы и основы работы в сети. Сетевые операционные системы			+	+
Основы администрирования серверных версий операционных систем семейства Microsoft Windows				
Тема 5. Операционные системы семейства Microsoft Windows				+
Тема 6. Администрирование операционных систем на примере ОС Microsoft Windows Server.				+
Тема 7. Сетевые службы в ОС Windows Server			+	+
Тема 8. Служба каталогов Active Directory			+	+
Тема 9. Основные понятия безопасности операционных систем и компьютерных сетей.		+		
Вес КМ:	20	20	20	40

\$Общая часть/Для промежуточной аттестации\$

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-4	ОПК-4(Компетенция)	Знать: модели и топологии информационных сетей; Уметь: использовать методы и средства мониторинга и конфигурирования сетевых служб и систем;	Контрольное задание 1; Практическое задание № 1; (Контрольная работа) Практическое задание № 4; Практическое задание № 5. (Контрольная работа)
ПК-1	ПК-1(Компетенция)	Знать: основы безопасности современных информационных сетей и базовая эталонная модель Международной организации стандартов (модель OSI); Уметь: применять сетевые программные и технические средства управления и администрирования информационными сетями;	Контрольное задание 2; Практическое задание № 2; (Контрольная работа) Контрольное задание 3; Практическое задание № 3; (Контрольная работа) Практическое задание № 4; Практическое задание № 5. (Контрольная работа)
ПК-3	ПК-3(Компетенция)	Знать: методы управления	Контрольное задание 2; Практическое задание № 2; (Контрольная работа)

		маршрутизацией информационных потоков в локальных сетях, основные инфраструктурные сетевые службы и методы управления ими; Уметь: применять информационные технологии в сети;	Контрольное задание 3; Практическое задание № 3; (Контрольная работа) Практическое задание № 4; Практическое задание № 5. (Контрольная работа)
--	--	---	---

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольное задание 1; Практическое задание № 1;

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: Практическое занятие

Краткое содержание задания:

1. Учитывая приведённое количество хостов и начальную сеть, разбить её на подсети для выделения хостов, используя максимально эффективную маску. Вычислить адрес сети и адрес домена широковещательной рассылки.

Изначальная сеть: 192.168.0.0

Количество хостов в конечных подсетях: 1000, 998, 543, 200, 135, 15, 1.

Контрольные вопросы/задания:

Знать: модели и топологии информационных сетей;	1. Что такое сетевой коммутатор? 2. Каково назначение сетевого коммутатора? 3. Каковы основные функции сетевого коммутатора?
---	--

Описание шкалы оценивания:

Оценка: 5

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

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

Нижний порог выполнения задания в процентах: 50

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

КМ-2. Контрольное задание 2; Практическое задание № 2;

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: Практическое занятие

Краткое содержание задания:

Пример расчета сети на 4 подсети.

Пусть есть адрес сети 192.168.1.0/24. Необходимо сеть разделить на 4 подсети.

В соответствии с **Cisco-формулой** 2^n рассчитаем сколько необходимо занять бит от хоста: $2^2 = 4$. Таким образом, префикс маски сети изменится на /26.

Запишем адреса 4 подсетей, где «захваченный» бит выделен жирным шрифтом:

1) 11000000.10101000.00000001.**00000000**;

- 2) 11000000.10101000.00000001.**01**000000;
- 3) 11000000.10101000.00000001.**10**000000;
- 4) 11000000.10101000.00000001.**11**000000.

Как в предыдущем примере, выделена жирным шрифтом порция подсети, а без выделения - порция хоста:

- 1) **11000000.10101000.00000001.00**000000 = 192.168.1.0/26;
- 2) **11000000.10101000.00000001.01**000000 = 192.168.1.64/26;
- 3) **11000000.10101000.00000001.10**000000 = 192.168.1.128/26
- 4) **11000000.10101000.00000001.11**000000 = 192.168.1.192/26

Таким образом, сеть разделена на 4 подсети. При этом порция хоста теперь составляет 6 бит, а, следовательно, $2^6 - 2 = 62$ хостов. Выпишем составляющие адреса для каждой подсети в двоичном и десятичном виде:

- 11000000.10101000.00000001.00000000 = 192.168.1.0/26 (адрес сети первой подсети)
 11000000.10101000.00000001.00111111 = 192.168.1.63/26 (широковещательный адрес первой подсети)
 11000000.10101000.00000001.01000000 = 192.168.1.64/26 (адрес сети второй подсети)
 11000000.10101000.00000001.01111111 = 192.168.1.127/26 (широковещательный адрес второй подсети)
 11000000.10101000.00000001.10000000 = 192.168.1.128/26 (адрес сети третьей подсети)
 11000000.10101000.00000001.10111111 = 192.168.1.191/26 (широковещательный адрес третьей подсети)
 11000000.10101000.00000001.11000000 = 192.168.1.192/26 (адрес сети четвертой подсети)
 11000000.10101000.00000001.11111111 = 192.168.1.255/26 (широковещательный адрес четвертой подсети).

Контрольные вопросы/задания:

<p>Знать: основы безопасности современных информационных сетей и базовая эталонная модель Международной организации стандартов (модель OSI);</p>	<ol style="list-style-type: none"> 1. Каковы основные функции маршрутизатора? 2. Каким образом производится настройка маршрутизатора 3. Перечислите основные режимы работы маршрутизатора
<p>Уметь: применять информационные технологии в сети;</p>	<ol style="list-style-type: none"> 1. Каковы основные функции специального ПО «Cisco Packet Tracer» и «PuTTY»? 2. Каким образом можно настроить маршрутизатор на работу в режиме шлюза? 3. Как выбрать адрес для настройки на конечном устройстве (ПК) таким образом, чтобы он мог работать со шлюзом?

Описание шкалы оценивания:

Оценка: 5

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

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

Нижний порог выполнения задания в процентах: 50

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

КМ-3. Контрольное задание 3; Практическое задание № 3;

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: Практическое задание

Краткое содержание задания:

Задача управления доступом является весьма важной проблемой, решать которую приходится администратору сети. При этом необходимо предусмотреть:

- ограничение доступа к серверу;
- запрет на доступ к некоторым сетевым ресурсам и сервисам, например запрещенным интернет-сайтам;
- разграничение прав пользователей.

Данная задача решается настройкой **списков управления доступом (ACL – Access Control List)** – таблиц, которые определяют, какие операции можно совершать над тем или иным сетевым компонентом.

В сущности ACL – это мини-файрволлы, фильтрующие трафик, направленный к хосту, от хоста, к подсети или от подсети.

ACL – мощный инструмент управления трафиком. С их помощью можно обезопасить сеть, ограничить объем трафика, разграничить пользователей по правам. Надо лишь уметь их правильно применять.

Итак, списки управления доступом бывают:

1. Стандартные (Standard ACLs), позволяющие фильтровать трафик только по адресу отправителя (правила синтаксиса), в котором отражён лишь IP-адрес устройства, с которого должен фильтроваться поток данных.

```
router(conf)# access-list <1-99> <permit | deny | remark> source [source-wildcard]
```

Пример

```
router(conf)# access-list 10 permit 192.168.0.0 0.0.0.255
```

Из примера видно, что любой ACL имеет строгую структуру. У него есть идентификатор (в данном примере – 10), который позволяет осуществить привязку ACL к устройству; правило, которое определяет действия с трафиком (в данном примере «permit - разрешить») и, собственно, адрес отправителя, с которого был отправлен пакет данных. Работает это следующим образом: если трафик пришёл из сети 192.168.0.0/24, то, руководствуясь списком доступа под номером 10, он пропускается.

Примечание: в синтаксисе стандартных Access-lists используется обратная **маска – wildcard** типа 0.0.0.255. Ей будет соответствовать прямая маска - 255.255.255.0.

Встает вопрос: Что делать с трафиком, который не попадает под это правило?

Для этого в конце любого ACL существует «неявное» (англ. «implicit») правило отброса всего остального трафика. Это означает, что любой поток данных, попадающий под действие списка управления доступом с номером 10 и не исходит из сети 192.168.0.0/24, будет отброшен.

Отсюда вытекает другой вопрос: Как определить попадает ли трафик под действие ACL?

Для этого списки управления доступом привязываются к **интерфейсам**. Происходит это при помощи команды связки:

```
router(conf-if)# ip access-group <1-99> <in | out>
```

Пример

```
router(conf-if)# ip access-group 10 in
```

Как видно из примера, настройка происходит из режима конфигурации интерфейса (conf-if) и ACL будет иметь имя Access-group.

Кроме определения того, на каком порту устройства применяется список управления доступом, необходимо указать направление, в котором трафик будет фильтроваться (на вход или на выход).

Для стандартных ACL имеет смысл ставить режим «на вход», так как фильтрация осуществляется, исходя из IP-адреса отправителя.

Побочным эффектом является то, что такие ACL ставятся как можно ближе к пункту назначения, чтобы охватить весь поток трафика и не отфильтровывать нужный трафик, идущий по другим направлениям через тот же маршрутизатор.

Контрольные вопросы/задания:

Знать: методы управления маршрутизацией информационных потоков в локальных сетях, основные инфраструктурные сетевые службы и методы управления ими;	1. Как выбрать адрес для настройки на конечном устройстве (ПК) таким образом, чтобы он мог работать со шлюзом?
Уметь: применять сетевые программные и технические средства управления и администрирования информационными сетями;	1. Чем стандартный ACL отличается от расширенного? 2. Где лучше ставить стандартный ACL? 3. Перечислите основные элементы сетевой топологии в данной лабораторной работе

Описание шкалы оценивания:

Оценка: 5

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

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

Нижний порог выполнения задания в процентах: 50

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

КМ-4. Практическое задание № 4; Практическое задание № 5.

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 40

Процедура проведения контрольного мероприятия: Практическое задание

Краткое содержание задания:

Задача управления доступом является весьма важной проблемой, решать которую приходится администратору сети. При этом необходимо предусмотреть:

- ограничение доступа к серверу;
- запрет на доступ к некоторым сетевым ресурсам и сервисам, например запрещенным интернет-сайтам;
- разграничение прав пользователей.

Данная задача решается настройкой **списков управления доступом (ACL – Access Control List)** – таблиц, которые определяют, какие операции можно совершать над тем или иным сетевым компонентом.

В сущности ACL – это мини-файрволлы, фильтрующие трафик, направленный к хосту, от хоста, к подсети или от подсети.

ACL – мощный инструмент управления трафиком. С их помощью можно обезопасить сеть, ограничить объем трафика, разграничить пользователей по правам. Надо лишь уметь их правильно применять.

Итак, списки управления доступом бывают:

1. Стандартные (Standard ACLs), позволяющие фильтровать трафик только по адресу отправителя (правила синтаксиса), в котором отражён лишь IP-адрес устройства, с которого должен фильтроваться поток данных.

```
router(conf)# access-list <1-99> <permit | deny | remark> source [source-wildcard]
```

Пример

```
router(conf)# access-list 10 permit 192.168.0.0 0.0.0.255
```

Из примера видно, что любой ACL имеет строгую структуру. У него есть идентификатор (в данном примере – 10), который позволяет осуществить привязку ACL к устройству; правило, которое определяет действия с трафиком (в данном примере «permit - разрешить») и, собственно, адрес отправителя, с которого был отправлен пакет данных. Работает это следующим образом: если трафик пришёл из сети 192.168.0.0/24, то, руководствуясь списком доступа под номером 10, он пропускается.

Примечание: в синтаксисе стандартных Access-lists используется обратная **маска – wildcard** типа 0.0.0.255. Ей будет соответствовать прямая маска - 255.255.255.0.

Встает вопрос: Что делать с трафиком, который не попадает под это правило?

Для этого в конце любого ACL существует «неявное» (англ. «implicit») правило отброса всего остального трафика. Это означает, что любой поток данных, попадающий под действие списка управления доступом с номером 10 и не исходит из сети 192.168.0.0/24, будет отброшен.

Отсюда вытекает другой вопрос: Как определить попадает ли трафик под действие ACL?

Для этого списки управления доступом привязываются к **интерфейсам**. Происходит это при помощи команды связки:

```
router(conf-if)# ip access-group <1-99> <in | out>
```

Пример

```
router(conf-if)# ip access-group 10 in
```

Как видно из примера, настройка происходит из режима конфигурации интерфейса (conf-if) и ACL будет иметь имя Access-group.

Кроме определения того, на каком порту устройства применяется список управления доступом, необходимо указать направление, в котором трафик будет фильтроваться (на вход или на выход).

Для стандартных ACL имеет смысл ставить режим «на вход», так как фильтрация осуществляется, исходя из IP-адреса отправителя.

Побочным эффектом является то, что такие ACL ставятся как можно ближе к пункту назначения, чтобы охватить весь поток трафика и не отфильтровывать нужный трафик, идущий по другим направлениям через тот же маршрутизатор.

Контрольные вопросы/задания:

Знать: методы управления маршрутизацией информационных потоков в локальных сетях, основные инфраструктурные сетевые службы и методы управления ими;	1.Каким образом можно настроить маршрутизатор на работу в режиме шлюза?
Уметь: использовать методы и средства мониторинга и конфигурирования сетевых служб и систем;	1.Что такое утилизация адресного пространства? 2. Каков синтаксис команды Ping?
Уметь: применять сетевые программные и технические средства управления и администрирования информационными сетями;	1.Какие параметры можно передавать в EACL

Описание шкалы оценивания:

Оценка: 5

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

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

Нижний порог выполнения задания в процентах: 50

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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1 Кафедра <i>Безопасности и информационных технологий</i> Дисциплина «Администрирование систем и сетей» Инженерно-экономический институт	<i>Утверждаю: Зав. каф. БИТ А.Ю.Невский Протокол НМК ИЭБ №</i>
<p>1. Что такое сеть? Физические компоненты сети.</p> <p>2. Атаки на коммутаторы. Принцип проведения атак и способы защиты.</p> <p>3. Учитывая приведённое количество хостов и начальную сеть, разбить её на подсети для выделения хостов, используя максимально эффективную маску. Вычислить адрес сети и адрес домена широковещательной рассылки. Изначальная сеть: 192.168.0.0 Количество хостов в конечных подсетях: 1000, 998, 543, 200, 135, 15, 1.</p>		

Процедура проведения

Письменная форма по билету

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

1. Компетенция/Индикатор: ОПК-4(Компетенция)

Вопросы, задания

1. Модель OSI. Характеристика, область применения.
2. Дуплексная передача данных. Понятия полу- и полного дуплекса. Общая характеристика, область применения.
3. Коллизии трафика. Описание, методы защиты

Материалы для проверки остаточных знаний

1. Дать определение Хост
Верный ответ: Хост (от англ. host - «хозяин, принимающий гостей») - любое устройство, предоставляющее сервисы типа «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах.
2. Что такое расширенные списки управления доступом?
Верный ответ: Расширенные списки управления доступом – это более гибкий инструмент управления. Кроме адреса отправителя, они могут содержать в себе протокол, порт или/и адрес получателя. Соответственно, их функционал гораздо богаче, а список функций – шире.
3. **Что делает Динамический NAT?**
Верный ответ: Динамический NAT отображает набор частных адресов на некое множество публичных IP-адресов. Если число локальных хостов не превышает число имеющихся публичных адресов, каждому локальному адресу будет

гарантироваться соответствие публичного адреса. В противном случае, число хостов, которые могут одновременно получить доступ во внешние сети, будет ограничено количеством публичных адресов.

4. Для чего нужна технология **РАТ**

Верный ответ: Для решения такой задачи существует технология РАТ (Port Address Translation, трансляция порт-адрес). Иногда ее называют NAT overload или NATPT. Технология РАТ применима в случае, если число активных устройств превышает число выделенных адресов. При этом для доступа в интернет будет использован один адрес + порт, который для каждого хоста локальной сети будет отличаться. Пример: Наш выделенный IP - 11.0.0.2. Необходимо, чтобы одновременно Интернетом пользовались хосты с адресами: 192.168.0.11, 192.168.0.12, 192.168.0.13, 192.168.0.14. В этом случае каждый из них будет выходить в глобальную сеть, имея следующую привязку адрес+порт

2. Компетенция/Индикатор: ПК-1(Компетенция)

Вопросы, задания

1. Развитие технологий коммутации. Хаббы, мосты, коммутаторы. Общая характеристика.
2. Понятия инкапсуляции и де-инкапсуляции в сетях передачи данных. Область применения.
3. Структура кадра 802.3. Общая характеристика наполнения кадра типа Ethernet.

Материалы для проверки остаточных знаний

1. Что такое Локальная вычислительная сеть
Верный ответ: Локальная вычислительная сеть (ЛВС, англ. LAN, Local area Network) – компьютерная сеть предприятия (домашняя, офисная и др.), все хосты которой объединены территориальным признаком.
2. Компоненты, составляющие локальную сеть?
Верный ответ: ● хост; ● сетевой концентратор - хаб; ● сетевой коммутаторы - свитч; ● сетевой мост - бридж; ● точки доступа к беспроводной сети.
3. Что такое **MAC-адрес**
Верный ответ: MAC-адрес – это записанный в шестнадцатеричном виде буквенно-цифровой код, который присваивается любой единице сетевого оборудования производителем. Поскольку каждый MAC-адрес уникален, его удобно использовать для идентификации компьютера в сети. Хранится этот шифр в микросхеме ПЗУ, встроенной в сетевое устройство

3. Компетенция/Индикатор: ПК-3(Компетенция)

Вопросы, задания

1. Что такое сеть?
2. Стыковочные сети. Понятие и область применения.
3. Статическая и динамическая маршрутизация. Отличия и область применения
4. Траблшутинг. Процесс поиска проблем на сети.

Материалы для проверки остаточных знаний

1. Что такое Таблица маршрутизации (Routing Table)
Верный ответ: Таблица маршрутизации (Routing Table) – это набор записей, содержащий варианты достижения той или иной подсети при помощи известного пути.
2. Что содержит в себе таблица маршрутизации
Верный ответ: Обычно, таблица маршрутизации содержит в себе: ● обозначение протокола, по которому был получен маршрут (R, C, S); ● сеть, до которой известен

путь с указанием маски (172.16.0.0/16); ●адрес следующего хопа (устройства, через которое пойдет трафик для достижения указанной сети назначения – via 209.165.200.1); ● интерфейс (физический порт), через который будет отправлен трафик (Serial1/0); ●административное расстояние (Administrative distance, цена маршрута) и метрика (120/1).

3.Преимущества статической маршрутизации

Верный ответ: Преимущества статической маршрутизации: ●минимальные затраты процессора и памяти; ●отсутствие нагрузки на линию связи на обновления между маршрутизаторами; ●детальный контроль маршрутизации трафика. Недостатки статической маршрутизации: ●настройки изменяются только вручную; ●нет динамической отказоустойчивости если какой-либо канал связи перестанет работать; ●не практично для больших сетей.

4.Что такое списков управления доступом (ACL – Access Control List)

Верный ответ: списков управления доступом (ACL – Access Control List) – таблиц, которые определяют, какие операции можно совершать над тем или иным сетевым компонентом.

II. Описание шкалы оценивания

Оценка: 5

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

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

Нижний порог выполнения задания в процентах: 50

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

III. Правила выставления итоговой оценки по курсу