

**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 автоматизированных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очно-заочная**

**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. ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации

ПК-1.1 Администрирует системы защиты информации автоматизированных систем

2. ПК-3 Способен администрировать средства защиты информации в компьютерных системах и сетях

ПК-3.1 Администрирует подсистемы защиты информации в операционных системах

ПК-3.3 Администрирует средства защиты информации прикладного и системного программного обеспечения

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

7 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  |
|--------------------|---|---|--|
| ПК-1               | ПК-1.1 <sub>ПК-1</sub><br>Администрирует системы защиты информации автоматизированных систем                          | Уметь:<br>применять информационные технологии в сети;   | Практическое задание № 4; Практическое задание № 5. (Контрольная работа)   |
| ПК-3               | ПК-3.1 <sub>ПК-3</sub><br>Администрирует подсистемы защиты информации в операционных системах                         | Знать:<br>методы управления маршрутизацией информационных потоков в локальных сетях, основные инфраструктурные сетевые службы и методы управления ими;<br>Уметь:<br>использовать методы и средства мониторинга и конфигурирования сетевых служб и систем; | Контрольное задание 2; Практическое задание № 2; (Контрольная работа)<br>Контрольное задание 3; Практическое задание № 3; (Контрольная работа)   |
| ПК-3               | ПК-3.3 <sub>ПК-3</sub><br>Администрирует средства защиты информации прикладного и системного программного обеспечения | Знать:<br>модели и топологии информационных сетей;<br>основы безопасности современных информационных сетей и  | Контрольное задание 1; Практическое задание № 1; (Контрольная работа)<br>Контрольное задание 2; Практическое задание № 2; (Контрольная работа)<br>Практическое задание № 4; Практическое задание № 5. (Контрольная работа) |

|  |  |  |  |
|--|--|--|--|
|  |  | базовая эталонная модель<br>Международной<br>организации стандартов<br>(модель OSI);<br>Уметь:<br>применять сетевые<br>программные и<br>технические средства<br>управления и<br>администрирования<br>информационными сетями; |  |
|--|--|--|--|

## 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. Каково назначение 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 изменяется на /26.

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

1) 11000000.10101000.00000001.**00**000000;

2) 11000000.10101000.00000001.**01**000000;

3) 11000000.10101000.00000001.10000000;

4) 11000000.10101000.00000001.11000000.

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

1) **11000000.10101000.00000001.00000000** = 192.168.1.0/26;

2) **11000000.10101000.00000001.01000000** = 192.168.1.64/26;

3) **11000000.10101000.00000001.10000000** = 192.168.1.128/26

4) **11000000.10101000.00000001.11000000** = 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:

|   |   |
|---|---|
| Знать: методы управления маршрутизацией информационных потоков в локальных сетях, основные инфраструктурные сетевые службы и методы управления ими; | 1.Перечислите основные режимы работы маршрутизатора |
| Знать: основы безопасности современных информационных сетей и базовая эталонная модель Международной организации стандартов (модель OSI);           | 1.Каковы основные функции маршрутизатора?           |

### 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:

|  |                                       |
|--|---------------------------------------|
| Уметь: использовать методы и средства мониторинга и конфигурирования сетевых служб и систем; | 1. Где лучше ставить стандартный ACL? |
|--|---------------------------------------|

### 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:

|  |  |
|--|--|
| Уметь: применять информационные технологии в сети;                       | 1. Каков синтаксис команды Ping?           |
| Уметь: применять сетевые программные и технические средства управления и | 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

7 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

|   |  |  |
|---|--|--|
| <b>НИУ<br/>МЭИ</b>  | <b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1</b><br>Кафедра <i>Безопасности и информационных технологий</i><br>Дисциплина «Администрирование систем и сетей»<br><b>Инженерно-экономический институт</b> | <i>Утверждаю:<br/>Зав. каф. БИТ<br/>А.Ю.Невский<br/>Протокол НМК ИЭБ<br/>№</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.<br/>Изначальная сеть: 192.168.0.0<br/>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:** ПК-1.1<sub>ПК-1</sub> Администрирует системы защиты информации автоматизированных систем

### **Вопросы, задания**

- 1.Что такое сеть?
- 2.Модель OSI. Характеристика, область применения.
- 3.Коллизии трафика. Описание, методы защиты
- 4.Стыковочные сети. Понятие и область применения.
- 5.Траблшутинг. Процесс поиска проблем на сети.
- 6.Траблшутинг в коммутации: примеры проблем и их решение

### **Материалы для проверки остаточных знаний**

#### **1. 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.

**2. Компетенция/Индикатор:** ПК-3.1<sub>ПК-3</sub> Администрирует подсистемы защиты информации в операционных системах

### **Вопросы, задания**

- 1.Классификация сетей передачи данных. Понятия «коммутатор», «коммутация», их общая характеристика.
- 2.Развитие технологий коммутации. Хабы, мосты, коммутаторы. Общая характеристика.
- 3.Процесс коммутации пакетов внутри сети. Широковещательная рассылка и ARP-запросы.
- 4.Технология DNS. Принцип работы.
- 5.Понятие маршрутизации. Процесс маршрутизации пакетов

### **Материалы для проверки остаточных знаний**

- 1.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. Компетенция/Индикатор:** ПК-3.3<sub>ПК-3</sub> Администрирует средства защиты информации прикладного и системного программного обеспечения

### **Вопросы, задания**

- 1.Структура кадра 802.3. Общая характеристика заполнения кадра типа Ethernet.
- 2.Петли коммутации. Условия возникновения и способы борьбы с петлями.
- 3.Дуплексная передача данных. Понятия полу- и полного дуплекса. Общая характеристика, область применения.

### **Материалы для проверки остаточных знаний**

- 1.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.

## **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*