ПРИЛОЖЕНИЕ

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«Рязанский государственный радиотехнический университет имени В.Ф. Уткина»**

КАФЕДРА «ЭЛЕКТРОННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ»

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ**

**«Администрирование сетевых сервисов»**

Направление подготовки

09.04.01 Информатика и вычислительная техника

Профиль

Вычислительные машины, системы, комплексы и сети

Квалификация (степень) выпускника — магистр

Форма обучения — очная, очно-заочная, заочная

Рязань

**1 ОБЩИЕ ПОЛОЖЕНИЯ**

Оценочные материалы – это совокупность учебно-методических материалов (практических заданий, описаний форм и процедур проверки), предназначенных для оценки качества освоения обучающимися данной дисциплины как части ОПОП.

Цель – оценить соответствие знаний, умений и владений, приобретенных обучающимся в процессе изучения дисциплины, целям и требованиям ОПОП в ходе проведения промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности компетенций, закрепленных за дисциплиной.

Контроль знаний обучающихся проводится в форме промежуточной аттестации. Промежуточная аттестация проводится в форме зачета.

Форма проведения зачета – тестирование, письменный опрос по теоретическим вопросам.

**2 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ**

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1. пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;
2. продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;
3. эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

**Уровень освоения компетенций, формируемых дисциплиной: Описание критериев и шкалы оценивания тестирования:**

|  |  |
| --- | --- |
| **Шкала оценивания** | **Критерий** |
| 3 балла  (эталонный уровень) | уровень усвоения материала, предусмотренного программой:  процент верных ответов на тестовые вопросы от 85 до 100% |
| 2 балла  (продвинутый уровень) | уровень усвоения материала, предусмотренного программой:  процент верных ответов на тестовые вопросы от 70 до 84% |
| 1 балл  (пороговый уровень) | уровень усвоения материала, предусмотренного программой:  процент верных ответов на тестовые вопросы от 50 до 69% |
| 0 баллов | уровень усвоения материала, предусмотренного программой:  процент верных ответов на тестовые вопросы от 0 до 49% |

**Описание критериев и шкалы оценивания теоретического вопроса:**

|  |  |
| --- | --- |
| **Шкала оценивания** | **Критерий** |
| 3 балла  (эталонный уровень) | выставляется студенту, который дал полный ответ на вопрос,  показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя |
| 2 балла (продвинутый уровень) | выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов |
| 1 балл (пороговый уровень) | выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя |
| 0 баллов | выставляется студенту, который не смог ответить на вопрос |

На промежуточную аттестацию (зачет) выносится тест, два теоретических вопроса. Максимально студент может набрать 6 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «зачтено», «не зачтено».

**Оценка «зачтено»** выставляется студенту, который набрал в сумме не менее 4 баллов (выполнил одно задание на эталонном уровне, другое – не ниже порогового, либо оба задания выполнит на продвинутом уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

**Оценка «не зачтено»** выставляется студенту, который набрал в сумме менее 4 баллов, либо имеет к моменту проведения промежуточной аттестации не сданные практические, либо лабораторные работы.

3. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Контролируемые разделы (темы) дисциплины** (результаты по разделам) | **Код контролируемой компетенции (или её части)** | **Наименование оценочного мероприятия** |
|
| 1 | 2 | 3 | 4 |
| 1 | Тема 1. Пакет OpenSSH | **ПК-3.1, ПК-3.2** | Зачет |
| 2 | Тема 2. Настройка сервера OpenSSH | **ПК-3.1, ПК-3.2** | Зачет |
| 3 | Тема 3. Протокол динамической конфигурации узлов (DHCP) | **ПК-3.1, ПК-3.2** | Зачет |
| 4 | Тема 4. Настройка сервера имен | **ПК-3.1, ПК-3.2** | Зачет |
| 5 | Тема 5. Запуск named | **ПК-3.1, ПК-3.2** | Зачет |
| 6 | Тема 6. TCP/IP Firewall | **ПК-3.1, ПК-3.2** | Зачет |
| 7 | Использование ipchains и iptables | **ПК-3.1, ПК-3.2** | Зачет |
| 8 | IP Accounting | **ПК-3.1, ПК-3.2** | Зачет |

1. **ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ**
   1. **Промежуточная аттестация в форме зачета**

|  |
| --- |
| **ПК-3: Способен администрировать сетевые устройства и программное обеспечение** |
| **Знать:**  **основы администрирования вычислительных сетей средствами операционных систем** |
| **Уметь:**  **конфигурировать серверы, управляющие сетевым взаимодействием** |
| **Владеть:**  **навыками практической работы с серверами, управляющими сетевым взаимодействием** |
| **ПК-3.1: Оценивает производительность сетевых устройств и программного обеспечения** |
| **Знать**  основные методы оценки производительности сетевых устройств |
| **Уметь**  оценивать производительность сетевых устройств |
| **Владеть**  навыками сбора статистики для определения производительности сетевых устройств |
| ПК-3.2: Планирует необходимую производительность администрируемых устройств |
| **Знать**  **основные методы определения необходимой производительности сетевых устройств** |
| **Уметь**  **определять требуемую производительность сетевых устройств** |
| **Владеть**  **навыками планирования необходимой производительности сетевых устройств** |

***а) типовые тестовые вопросы закрытого типа:***

1. Утилита ssh пакета OpenSSH используется для замены:

1. **rlogin**;
2. rcp;
3. **telnet**;
4. ftp

2. Протокол SSH относится к следующему уровню модели OSI:

1. **7. Прикладной (application)***;*

2. 6. Представления (presentation);

3. 5. Сеансовый (session);

4. 4. Транспортный (transport).

3. Для генерации пары ключей в пакете OpenSSH используется утилита:

1. ssh-keyscan*;*
2. **ssh-keygen**;
3. ssh-add;
4. ssh-agent***.***

4. IP firewall защитит от:

1. эксплуатации слабостей в сетевых сервисах;
2. подслушивания;
3. ***несанкционированного доступа;***
4. ***IP spoofing.***

5. Сетевая маска 255.255.255.0 соответствует следующему количеству бит маски:

1. 8
2. 16
3. 28
4. ***24***

6. Следующая команда IP Firewall позволяет удалить правило:

1. -a [policy]
2. -i [policy]
3. -p policy;
4. ***-d [policy].***

7. Apache имеет следующий каталог для документов веб-сервера:

1. ***htdocs;***
2. conf;
3. cgi-bin;

8. Squid - это:

1. ***Кеширующий прокси-сервер;***
2. север имен;
3. веб-сервер;

9. Кеширующие и проксирующие способности Squid можно использовать, пропуская через сервер:

1. Исходящие запросы на внешние серверы;
2. Входящие запросы на внутренние компьютеры;
3. ***входящие запросы на внутренние серверы;***
4. Исходящие запросы на внешние компьютеры.

10. Squid может запросить ресурс у вышестоящего сервера, который называется:

1. sibling peer;
2. ***parent peer***;
3. near peer;
4. front peer.

***б) типовые тестовые вопросы открытого типа:***

1. OpenSSH \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ весь трафик (включая пароли) для предотвращения подслушивания, перехвата соединений и других видов сетевых атак.

***Ответ: шифрует***;

2. Команда \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ является безопасной заменой команд rlogin, rsh и telnet. Она позволяет вам регистрироваться и выполнять команды на удалённом компьютере.

***Ответ: ssh***;

3. Команда \_\_\_\_\_\_\_\_\_\_\_\_\_ используется для передачи файлов между компьютерами через защищённое шифрованием соединение. Она похожа на rcp

***Ответ: scp***;

4. Веб-сервер в его простейшей форме - это компьютер со специальным программным обеспечением и подключением к \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, которое позволяет ему взаимодействовать с другими устройствами.

***Ответ: Интернету***;

5. Основная роль Apache связана с коммуникацией по сетям и использует протокол \_\_\_\_\_\_\_\_\_\_\_ (протокол управления передачей / интернет-протокол, который позволяет устройствам с IP-адресами в одной сети взаимодействовать друг с другом).

***Ответ: TCP / IP***;

6. Утилита iptables входит в пакет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Ответ: netfilter***;

7. После ввода правил можно попросить ipfwadm их показать в виде списка: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Ответ: # ipfwadm -F -l***;

8. Команда \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ читает текущую конфигурацию firewall и пишет упрощенную форму в стандартный вывод

***Ответ: ipchains-save***;

9. Если прокси-сервер — одновременно и \_\_\_\_\_\_\_\_\_\_\_\_\_, весь сетевой трафик в любом случае его не обойдёт.

***Ответ: маршрутизатор***;

10. Непосредственно после установки прокси-сервера он уже выполняет кеширующие функции.

***Ответ: кеширующие***;

***в) типовые практические задания:***

**Задание 1.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Установить с ним соединение

**Задание 2.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Удаленно создать на нем каталог /*home/stud/tmp*

**Задание 3.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Удаленно переименовать на нем каталог /*home/stud/tmp в /home/stud/temp*

**Задание 4.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Вывести на консоль содержимое его каталога /*home/stud/tmp*

**Задание 5.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Удаленно удалить файл /*home/stud/tmp/list.txt*

**Задание 6.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Удаленно вывести на консоль содержимое файла /*home/stud/tmp/list.txt*

**Задание 7.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Скопировать на него в каталог /*home/stud/tmp* файл /*home/stud/tmp/lessons.txt* со своего компьютера

**Задание 8.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Скопировать из него файл /*home/stud/tmp/friends.txt* на свой компьютер в каталог /*home/stud/tmp/*

**Задание 9.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Запустить на нем удаленно браузер firefox с отображение в окне на своем компьютере

**Задание 10.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Удаленно завершить работы этого компьютера.

**Задание 11.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Создать для безопасного соединения пару ключей

**Задание 12.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Для неоднократного соединения с ним добавить ключ в агент OpenSSH

**Задание 13.** На компьютере с сетевым адресом 192.168.0.1 установлен сервер OpenSSH.

Соединится с ним в консольном режиме и запустить файловый менеджер mc

**Задание 14. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipfadm

Удалить все правила для пересылаемых пакетов

**Задание 15. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipfadm

для пересылки пакетов назначить запретительную стратегию по умолчанию.

**Задание 16. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipfadm

Удалить все правила для входящих пакетов

**Задание 17. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipfadm

для входящих пакетов назначить разрешительную стратегию по умолчанию.

**Задание 18. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipfadm

разрешить нашим tcp пакетам по порту 80 выходить из внутренней сети наружу

**Задание 19. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipfadm

разрешить приходить ответным tcp пакетам по порту 80

**Задание 20. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipfadm

вывести в виде списка набор правил для пересылаемых пакетов

**Задание 21. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipchains

создать новую цепочку tcpin

**Задание 22. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipchains

в определенной пользователем цепочке tcpin создать правило, которое не выполняет никаких действий

**Задание 23. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipchains

в определенной пользователем цепочке tcpin создать разрешающее правило, которое соответствует любому пакету, который предназначен для нашей локальной сети и порта ssh

**Задание 24. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipchains

сохранить текущие настройки сетевого фильтра в файле /var/state/ipchains/firewall.state

**Задание 25. С**еть имеет 24-битную сетевую маску (класс C) и ее сетевой адрес 172.16.1.0.

С помощью утилиты ipchains

восстановить настройки сетевого фильтра из файла /var/state/ipchains/firewall.state

**Типовые теоретические вопросы для зачета по дисциплине**

1. Пакет OpenSSH
2. Настройка клиента OpenSSH.
3. Использование команды ssh.
4. Использование команды sftp
5. Создание пар ключей. Создание пары ключей DSA.
6. Настройка ssh-agent
7. Настройка сервера OpenSSH
8. Методы атаки . Что такое firewall?. Что такое IP Filtering?. Установка Firewall в Linux. Настройка ядра для IP Firewall.
9. Утилита ipfwadm. Обзор параметров ipfwadm.
10. IP Firewall Chains Использование ipchains и iptables
11. Синтаксис команды ipchains. Просмотр наших правил в ipchains.
12. Правильное использование цепочек. Netfilter и таблицы IP. Обратная совместимость с ipfwadm и ipchains
13. Управление битами TOS. Задание TOS-битов с помощью ipfwadm или ipchains. Установка TOS- битов с помощью iptables .
14. Проверка конфигурации Firewall.
15. IP Accounting
16. Настройка ядра для IP Accounting. Настройка IP Accounting. Учет по адресам . Учет по портам сервисов. Учет по пакетам ICMP. Учет по протоколам. Использование результатов IP Accounting
17. Просмотр данных с помощью ipfwadm . Просмотр данных с помощью ipchains. Просмотр данных с помощью iptables.
18. Перезапуск счетчиков. Удаление набора правил.
19. Пассивные коллекции данных доступа
20. HTTP-сервер Apache
21. Как работает Apache
22. Общая структура Apache