

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Магнитогорский государственный технический университет  
им. Г.И. Носова»  
Многопрофильный колледж



**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ  
ПРАКТИЧЕСКИХ РАБОТ**

**по ПМ.03 Техническое обслуживание и ремонт компьютерных систем и комплексов  
МДК.03.01 Техническое обслуживание и ремонт компьютерных систем и комплексов  
разделу 6Сетевая безопасность**

**для студентов специальности  
09.02.01 Компьютерные системы и комплексы  
(базовой подготовки)**

Магнитогорск, 2018

**ОДОБРЕНО:**

Предметно-цикловой комиссией  
«Информатики и вычислительной техники»  
Председатель И.Г. Зорина  
Протокол № 6 от 21.02.2018 г.

Методической комиссией МпК

Протокол №4 от «01» марта 2018г

**Составитель:**

преподаватель МпК ФГБОУ ВО «МГТУ им. Г.И. Носова» Анна Петровна Иванченко

Методические указания по выполнению практических работ разработаны на основе рабочей программы ПМ.03 Техническое обслуживание и ремонт компьютерных систем и комплексов, МДК.03.01 Техническое обслуживание и ремонт компьютерных систем и комплексов, разделу 6Сетевая безопасность.

Содержание практических работ ориентировано на формирование общих и профессиональных компетенций по программе подготовки специалистов среднего звена по специальности 09.02.01 Компьютерные системы и комплексы.

## СОДЕРЖАНИЕ

<b>1 ВВЕДЕНИЕ .....</b>	<b>4</b>
<b>2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ.....</b>	<b>6</b>
<b>Практическая работа № 1.....</b>	<b>6</b>
<b>Практическая работа № 2.....</b>	<b>7</b>
<b>Практическая работа № 3.....</b>	<b>8</b>
<b>Практическая работа № 4.....</b>	<b>9</b>
<b>Практическая работа № 5.....</b>	<b>10</b>
<b>Практическая работа № 6.....</b>	<b>11</b>
<b>Практическая работа № 7.....</b>	<b>13</b>
<b>Практическая работа № 8.....</b>	<b>14</b>
<b>Практическая работа № 9.....</b>	<b>15</b>
<b>Практическая работа № 10.....</b>	<b>16</b>
<b>Практическая работа № 11.....</b>	<b>17</b>

## 1 ВВЕДЕНИЕ

Важную часть теоретической и профессиональной практической подготовки обучающихся составляют практические занятия.

Состав и содержание практических занятий направлены на реализацию Федерального государственного образовательного стандарта среднего профессионального образования.

Ведущей дидактической целью практических занятий является формирование профессиональных практических умений (умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности) или учебных практических умений, необходимых в последующей учебной деятельности.

Ведущей дидактической целью практических занятий является экспериментальное подтверждение и проверка существенных теоретических положений (законов, зависимостей).

В соответствии с рабочей программой ПМ.03 Техническое обслуживание и ремонт компьютерных систем и комплексов, МДК.03.01 Техническое обслуживание и ремонт компьютерных систем и комплексов, разделу 6Сетевая безопасность предусмотрено проведение практических занятий.

В результате их выполнения, обучающийся должен:

**уметь:**

- проводить контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов;
- проводить системотехническое обслуживание компьютерных систем и комплексов;
- принимать участие в отладке и технических испытаниях компьютерных систем и комплексов;
- инсталляции, конфигурировании и настройке операционной системы, драйверов, резидентных программ;
- выполнять регламенты техники безопасности.

Содержание практических и лабораторных занятий ориентировано на формирование общих компетенций по профессиональному модулю программы подготовки специалистов среднего звена по специальности и овладению **профессиональными компетенциями**:

ПК 3.1. Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и комплексов.

ПК 3.2. Проводить системотехническое обслуживание компьютерных систем и комплексов.

ПК 3.3. Принимать участие в отладке и технических испытаниях компьютерных систем и комплексов; инсталляции, конфигурировании программного обеспечения.

А также формированию **общих компетенций**:

ОК 1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6 Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9 Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Выполнение обучающимися практических и/или лабораторных работ по ПМ.03 Техническое обслуживание и ремонт компьютерных систем и комплексов, МДК.03.01 Техническое обслуживание и ремонт компьютерных систем и комплексов, разделу 6 Сетевая безопасность направлено на:

- обобщение, систематизацию, углубление, закрепление, развитие и детализацию полученных теоретических знаний по конкретным темам учебной дисциплины;

- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;

- формирование и развитие умений: наблюдать, сравнивать, сопоставлять, анализировать, делать выводы и обобщения, самостоятельно вести исследования, пользоваться различными приемами измерений, оформлять результаты в виде таблиц, схем, графиков;

- приобретение навыков работы с различными приборами, аппаратурой, установками и другими техническими средствами для проведения опытов;

- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;

- выработку при решении поставленных задач профессионально значимых качеств, таких как самостоятельность, ответственность, точность, творческая инициатива.

Практические занятия проводятся после соответствующей темы, которая обеспечивает наличие знаний, необходимых для ее выполнения.

## 2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

### Тема 6.1. Безопасность сетей Ethernet

#### Практическая работа № 1 Аудит безопасности протокола SNMP

**Цель работы:** Изучение способов мониторинга и управления сетью на основе протокола SNMP с использованием собственных механизмов безопасности.

**Выполнив работу, Вы будете:**

*уметь:*

- управлять сетью на основе протокола SNMP;

**Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

**Порядок выполнения работы:**

1. Постройте топологию сети, показанную на рисунке 1.

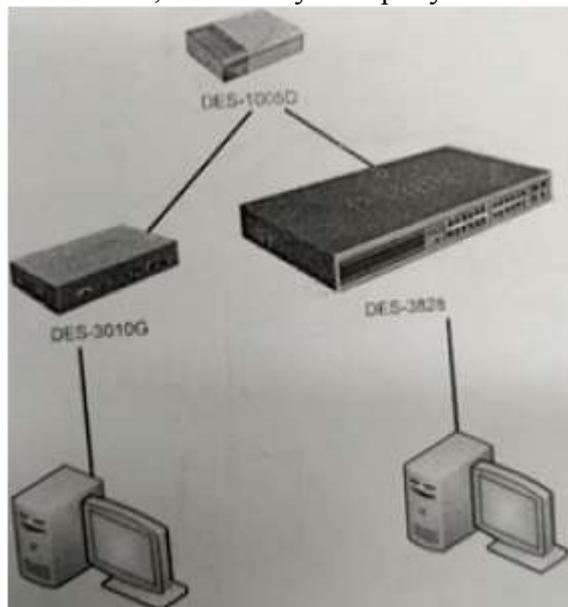


Рисунок 1

2. Изучите раздел «Протокол SNMP» теоретического пособия.
3. Настройте SNMP-протокол на коммутаторах.
4. Изучите раздел «Утилиты управления сетью по протоколу SNMP».
5. Запустите утилиту Reasoning MIB Browser.
6. Загрузите базу MIB RFC-1213.
7. На обоих коммутаторах (DES-3010 и DES-3828) выясните следующие параметры:
  - название устройства, время работы устройства, службы, запущенные на устройстве (ветвь system);
  - количество интерфейсов на устройстве, содержимое таблицы интерфейсов, название двух дополнительных виртуальных портов (ветвь interfaces);
  - IP-адрес устройства, содержимое таблицы маршрутизации (ветвь ip);
  - TCP-соединения, установленные устройством (ветвь tcp).
8. Загрузите базы MIB Time, DES-3010G-L2MGMT из каталога root/Desktop/SNMP/DES3000-MIB/private/.

9. Определите текущее системное время коммутатора.
10. Определите состояние портов коммутатора (база DES-3010G-L2MGMT, ветвь swL2PortinfoTable, таблица swL2PortMgmt).

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

**Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

## **Практическая работа № 2** **Аудит безопасности протокола STP**

**Цель работы:** Изучение уязвимостей алгоритма SpanningTreeи RapidSpanningTree

**Выполнив работу, Вы будете:**

*уметь:*

- выполнять аудит безопасности протокола STP;

**Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

**Порядок выполнения работы:**

1. Изучите раздел «Аудит безопасности протокола связующего дерева STP» теоретического пособия и раздел «L2 Features» (меню «Spanning Tree»).
2. Соберите сеть с топологией, представленной на рисунке 2.

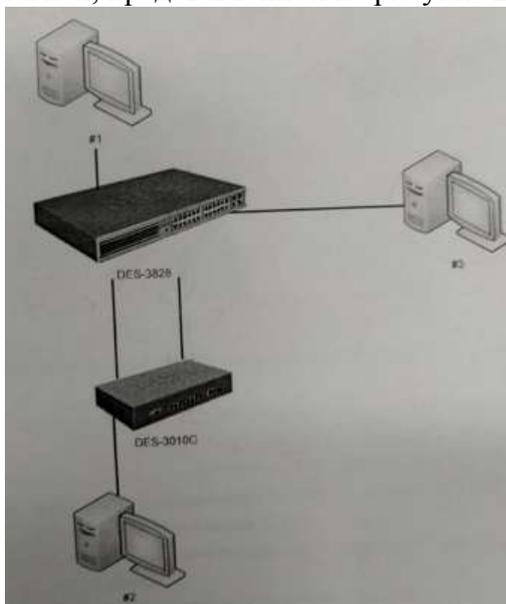


Рисунок 2

3. Настройтеиактивизируйте на коммутаторах протокол SpanningTree(замечание: по причине недоработки компанией D-Link программного обеспечения коммутатора DES-3828 приоритет коммутатора на данной модели выставить невозможно.Поэтому приоритет коммутатора DES-3828 постоянен и равен 32768, что не мешает выполнению лабораторной работы).

4. Параллельно с шагом 3 запустите на машине #3 утилите tcdump и выясните MAC-адреса коммутаторов, анализируя содержимое пакетов BPDU.
5. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

**Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

### Практическая работа № 3 Базовые механизмы коммутаторов

**Цель работы:** Изучение технологий TrustedHosts, IP-MACBinding и PortSecurity.

**Выполнив работу, Вы будете:**

*уметь:*

- контролировать доступ компьютеров в сеть на основе их IP и MAC-адресов, а также порта подключения;

**Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

**Порядок выполнения работы:**

1. Соберите топологию сети, представленную на рисунке 3.

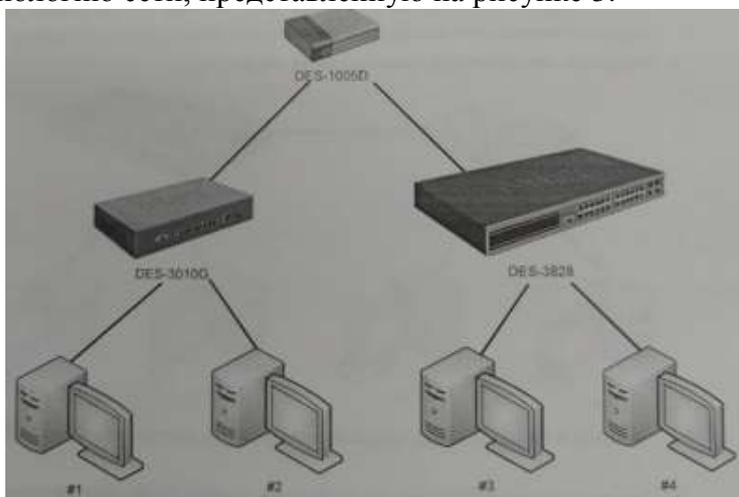


Рисунок 3

2. Изучите разделы «Ограничение количества управляющих компьютеров», «Настройка безопасности индивидуального порта» и «Технология фильтрации IP-MACBinding» теоретического пособия.
3. Изучите раздел «Security» (меню «Trusted Hosts»).
4. Настройте коммутаторы таким образом, чтобы ими могли управлять только машины #1 и #3.
5. Проверьте выполненные настройки.
6. Изучите раздел «Security» (меню «Port Security»).
7. Очистите таблицы коммутации на всех коммутаторах.
8. С машин #1 и #2 «пропингуйте» машину #3.

9. Убедитесь, что в таблицах коммутации не присутствует аппаратного адреса машины #4.
10. Заблокируйте на обоих коммутаторах таблица коммутации в режиме Permanent.
11. Попробуйте осуществить взаимодействие с 4-ым компьютером с любого компьютера. Объясните полученный результат.
12. Изучите раздел. «Administration» (меню «IP-MAC Binding»).
13. Сбросьте блокировку таблиц коммутации.
14. Используя технологию IP-MacBinding, настройте на коммутаторах фильтры таким образом, чтобы в сети могли работать только машины #1 и #3.
15. Сбросьте настройки коммутаторов в заводские и перезагрузите его.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

#### **Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

### **Практическая работа № 4** **Списки контроля доступа ACL**

**Цель работы:** Изучение технологии AccessControlLists.

#### **Выполнив работу, Вы будете:**

*уметь:*

- ограничивать типы приложений, разрешенных для использования в сети;
- контролировать доступ пользователей к сети;
- определять устройства, к которым они могут подключаться

#### **Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

#### **Порядок выполнения работы:**

1. Соберите сеть с топологией, представленной на рисунке 4.

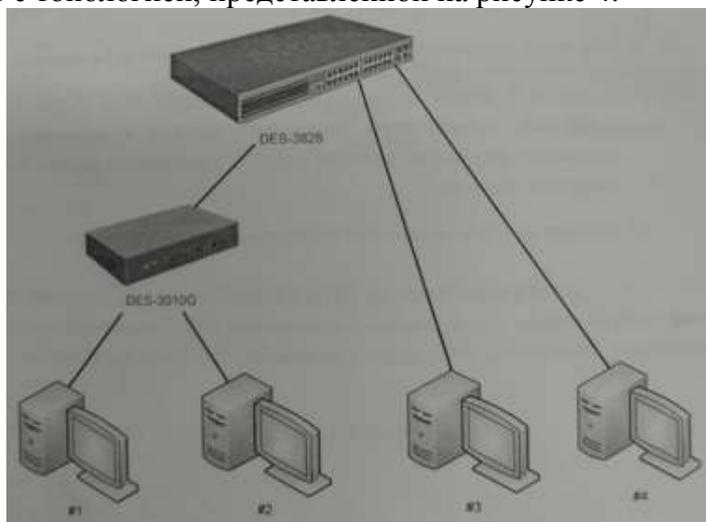


Рисунок 4

- Изучите раздел «Списки контроля доступа» теоретического пособия и раздел «ACL» (меню «Access Profile Table»).
- Настройте списки контроля доступа таким образом, чтобы:
  - ни один из коммутаторов DES-3010 не мог «пропинговать» машину #4;
  - машина #1 могла «пропинговать» машину #3, но не могла – машину #4;
  - машина #2 могла скачивать файл с машины #4 (используя ftp-протокол), но не могла получить почтовые сообщения;
  - только тот трафик, который идет от машины #2 к машине #3 «зеркалировался» на порт машины #4.
- Проверьте созданные настройки.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

**Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

**Тема 6.2. Механизмы обеспечения безопасности беспроводных локальных сетей**

**Практическая работа № 5**

**Шифрование канала с использованием протокола WEP**

**Цель работы:** Получение навыков построения сетей Wi-Fi с использованием механизма шифрования WEP.

**Выполнив работу, Вы будете:**

*уметь:*

- использовать алгоритм обеспечения безопасности сетей Wi-Fi;

**Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

**Порядок выполнения работы:**

- Постройте сеть, топология которой представлена на рисунке 5.

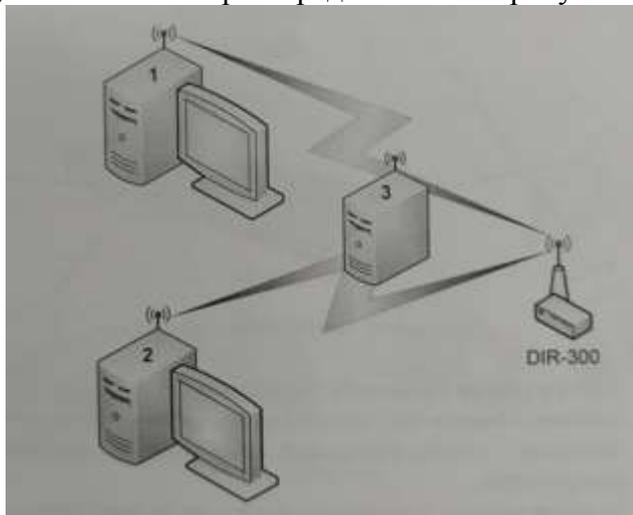


Рисунок 5

2. Изучите раздел «Механизмы шифрования в беспроводных сетях» теоретического пособия.
3. Включите точку доступа, настройте канал и имя сети. Включите внутренний DHCP-сервер. Включите шифрование WEP, используя 40-битный ключ.
4. Ассоциируйте два компьютера с этой точкой доступа.
5. Запустите на третьем компьютере утилиту «Airodump-ng» для перехвата пакетов.
6. Выполните взаимодействие между компьютерами 1 и 2.
7. Убедитесь (по экрану airodump-ng), что несколько пакетов с данными было перехвачено.
8. Сгенерируйте файл словаря, содержащий несколько произвольных ключей и добавьте в конец файла заданный ключ. Длина словаря должна быть не меньше 10000 записей. Скрипт для генерации находится на диске в каталоге /root/Desktop/Scripts/wep.
9. Используя полученный словарь и перехваченные пакеты выполните атаку на файл с перехваченными пакетами с помощью утилиты «WepAttack».
10. Выполните эти же действия, изменяя длину ключа и используя в качестве перехватчика Kismet вместо airodump. Варьируйте размер файла словаря, добавляя или удаляя записи. Сделайте вывод о влиянии длины ключа и размера словаря на скорость атаки.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

**Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

## **Практическая работа № 6**

### **Шифрование канала с использованием протокола WPA**

**Цель работы:** Получение навыков построения сетей Wi-Fi с использованием механизма шифрования WPA.

**Выполнив работу, Вы будете:**

*уметь:*

- контролировать доступ к беспроводным сетям;

**Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

**Порядок выполнения работы:**

1. Постройте сеть, топология которой представлена на рисунке 6.

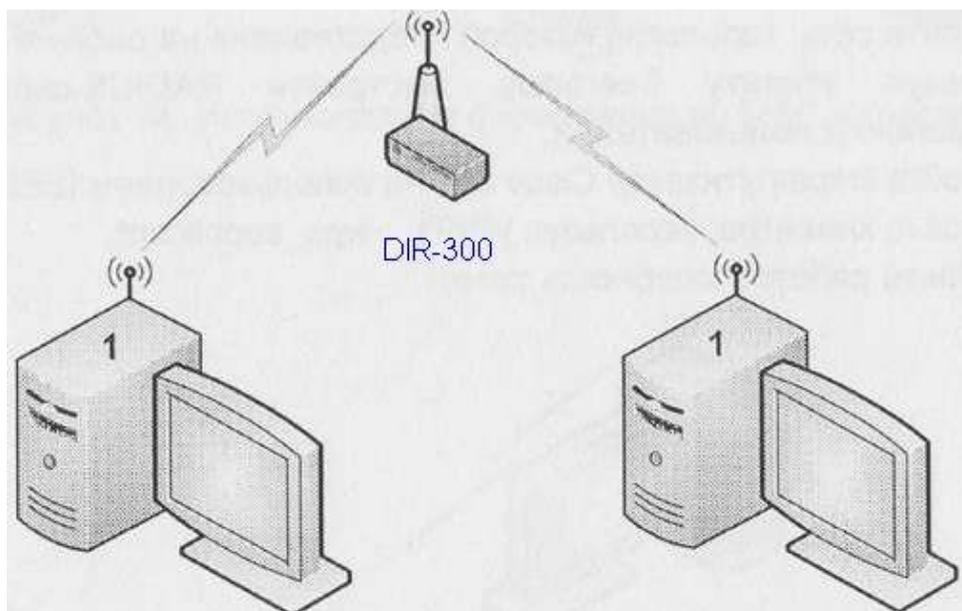


Рисунок 6

2. Используйте утилиту `wpa_supplicant`, настройте защищенную сеть с использованием аутентификации WPA и системой шифрования TKIP.
3. Используя `ssh`, сравните полезную пропускную способность канала до и после использования WPA.

Примечание –

Для проверки скорости соединения воспользуйтесь SSH

1. На первом компьютере задайте пароль пользователю `root`: `passwd`.
2. На втором компьютере для копирования файла выполните команду:

**`scp ip_адрес_компьютера_1:путь_к_файлу /dev/null`**

Эта команда скопирует указанный файл с первого компьютера на второй, причем файл не будет сохранен на диске, что позволит оценить реальную пропускную способность сети. Скорость передачи данных будет указана в выводе команды `scp`.

4. Используя утилиту `tcpdump` осуществите перехват пакетов. Изучите содержимое перехваченных пакетов до и после применения WPA.
5. Используя утилиту `wpa_supplicant`, настройте защищенную сеть с использованием аутентификации WPA2/PSK и системой шифрования TKIP.
6. Используя `ssh`, сравните полезную пропускную способность канала до и после использования WPA2/PSK.
7. Используя утилиту `wpa_supplicant`, настройте защищенную сеть с использованием аутентификации WPA2/PSK и системой шифрования AES.
8. Используя `ssh`, сравните полезную пропускную способность канала с использованием системы шифрования TKIP с системой шифрования AES.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

#### **Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

## Практическая работа № 7

### Аутентификация беспроводных клиентов на основе учетных записей пользователей и аппаратных адресов компьютеров

**Цель работы:** получение навыков построения защищенных Wi-Fi сетей с использованием RADIUS-сервера и фильтрации по MAC-адресам.

**Выполнив работу, Вы будете:**

*уметь:*

- выполнять проверку пользователей и устройств при их подключении;

**Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

**Порядок выполнения работы:**

1. Постройте сеть, топология которой представлена на рисунке 7.
2. Используя утилиту freeradius, настройте RADIUS-сервер и создайте двух произвольных пользователей.
3. Настройте маршрутизатор DIR-300 на использование IEEE 802.1x.
4. Настройте клиентов, используя утилиту wpa\_supplicant.
5. Проверьте работоспособность сети.

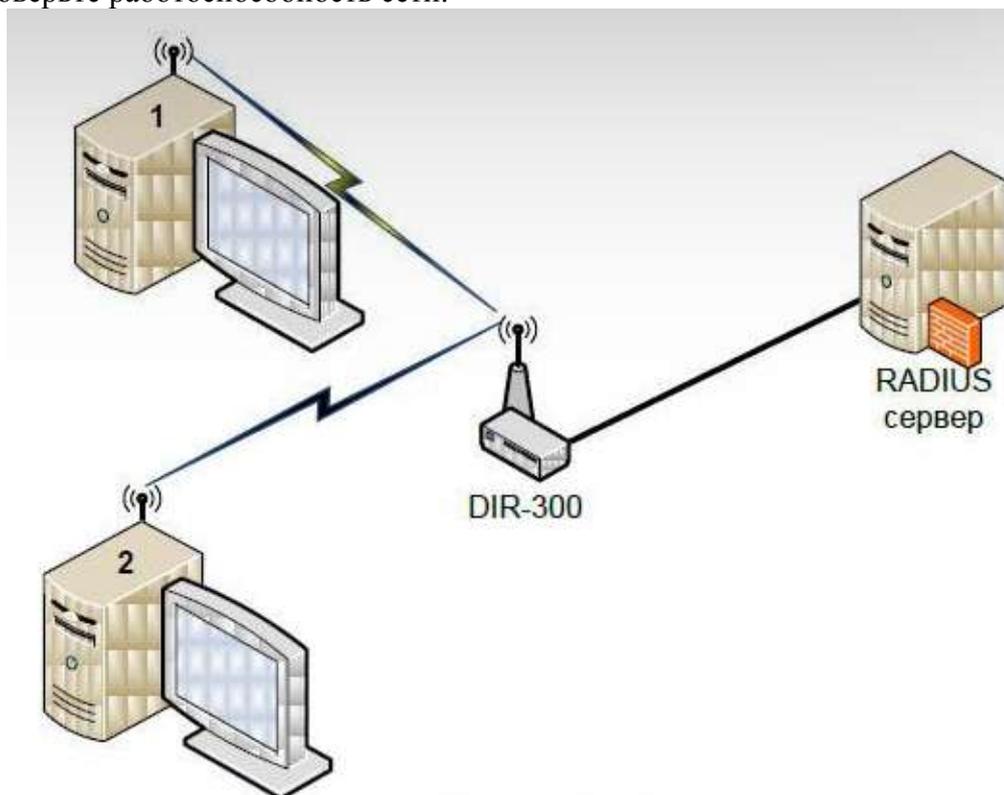


Рисунок 7

6. Соберите топологию, представленную на рисунке 8.
7. К точке доступа 1 разрешить подключение компьютеров 1 и 2 с помощью разрешенных списков MAC-адресов. К точке доступа 2 запретить подключение с компьютера А с помощью запрещенных списков MAC-адресов.
8. Проверьте правильность выполненных настроек.

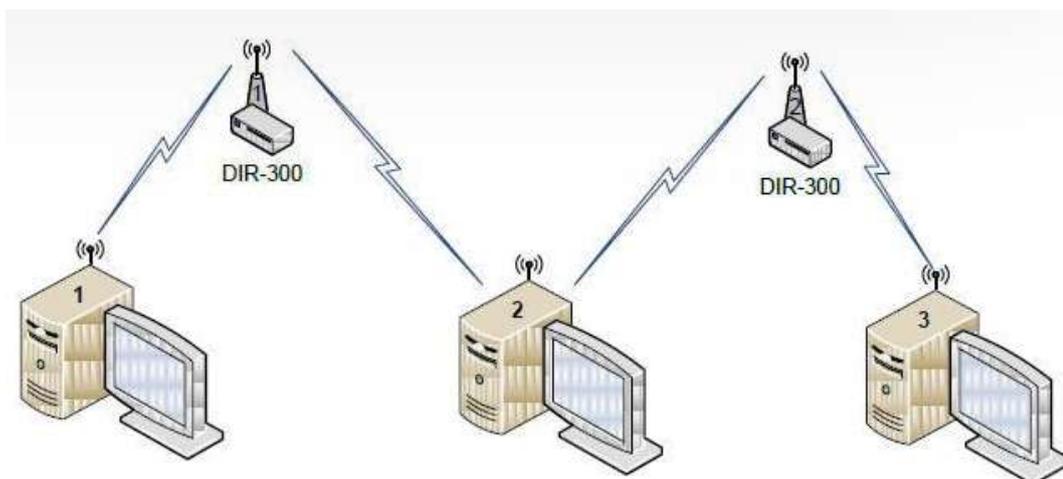


Рисунок 8

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

**Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

**Тема 6.3. Механизмы построения защищенных сетей с использованием брандмауэров  
Практическая работа № 8  
Протокол PPPoE**

**Цель работы:** Изучение протокола PPPoE и способов его настройки и использования в OCLinux и брандмауэре D-Link DFL-800.

**Выполнив работу, Вы будете:**

*уметь:*

- настраивать (или инкапсулировать) IP или другие протоколы, которые настраиваются на PPP, через соединения Ethernet, но с программными возможностями PPP-соединений;

**Материальное обеспечение:**

учебно-лабораторный стенд «Сетевая безопасность»

**Порядок выполнения работы:**

1. Соберите топологию сети, представленную на рисунке 9.

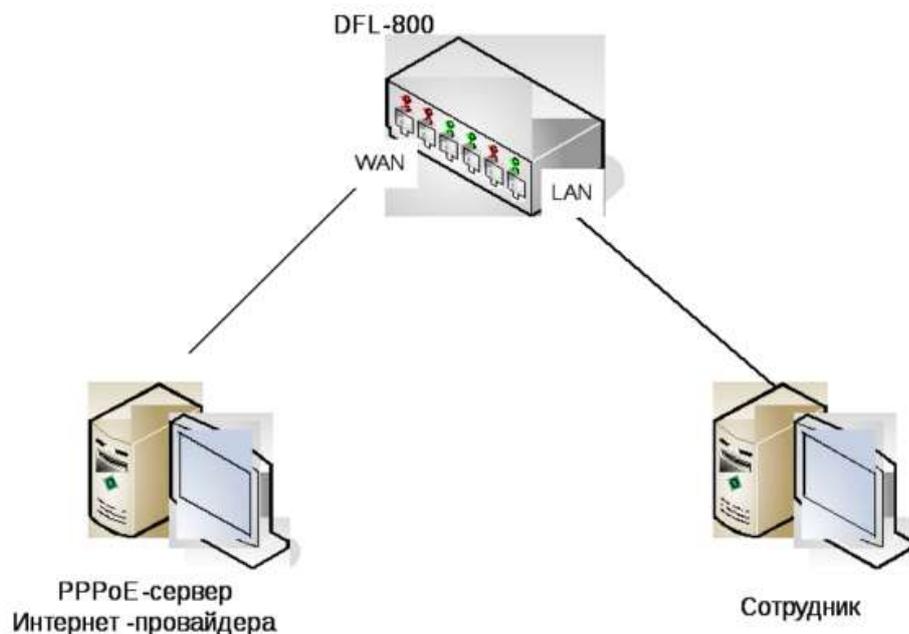


Рисунок 9

2. Настройте рабочие станции и брандмауэр таким образом, чтобы WAN-интерфейс DFL-800 и PPPoE-сервер принадлежали одной IP-подсети, а LAN-интерфейс DFL-800 и машина сотрудника – другой.
3. Изучите главу 8.1 «Протокол PPPoE» теоретического пособия, а также главы 4.7 «Настройка PPPoE-клиента на D-LinkDFL-800» и 5.14 «Протокол PPPoE».
4. Используя утилиту гр-pppoe, настройте PPPoE-сервер на машине Интернет-провайдера.
5. Настройте DFL-800 в качестве PPPoE-клиента (используя созданную в п.5 учетную запись пользователя). Установите PPPoE-туннель.
6. Осуществите доступ с машины сотрудника в сеть Интернет, то есть к машине провайдера.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

**Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

**Практическая работа № 9  
Виртуальные частные сети**

**Цель работы:** изучение протокола IPSec и способа его настройки в ОС Linux на брандмауэре D-LinkDFL-800.

**Выполнив работу, Вы будете:**

*уметь:*

- использовать протокол IPSec и способ его настройки в ОС Linux на брандмауэре D-LinkDFL-800;

### Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

### Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 10.

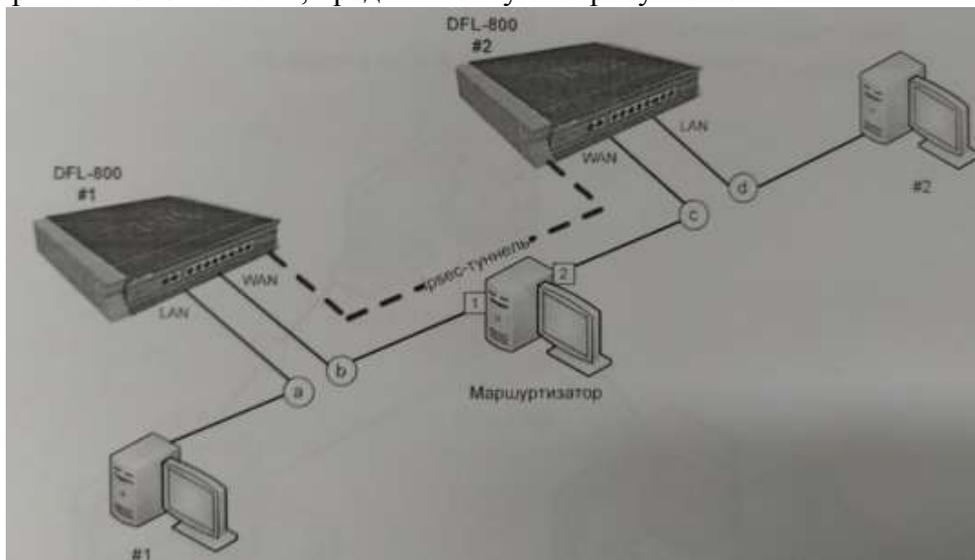


Рисунок 10

2. Настройте рабочие станции и брандмауэры таким образом, чтобы создать четыре различных IP-подсети: a, b, c и d (в соответствии с рисунком 10).
3. Изучите главу «Протокол IPSec» теоретического пособия, а также главы «Настройка протокола IPSec на D-Link DFL-800» и «Протокол IPSec».
4. Настройте IPSec-туннель, как это показано на рисунке 10.
5. Проверьте работоспособность сети, обратившись с машины #1 на машину #2.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

### Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

## Практическая работа № 10

### Туннелирование соединений с использованием протокола SSL

**Цель работы:** изучение принципов безопасного обмена информации с использованием протокола SSL в OCLinux.

### Выполнив работу, Вы будете:

*уметь:*

- создавать защищённое соединение между клиентом и сервером;

### Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

### Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 11.

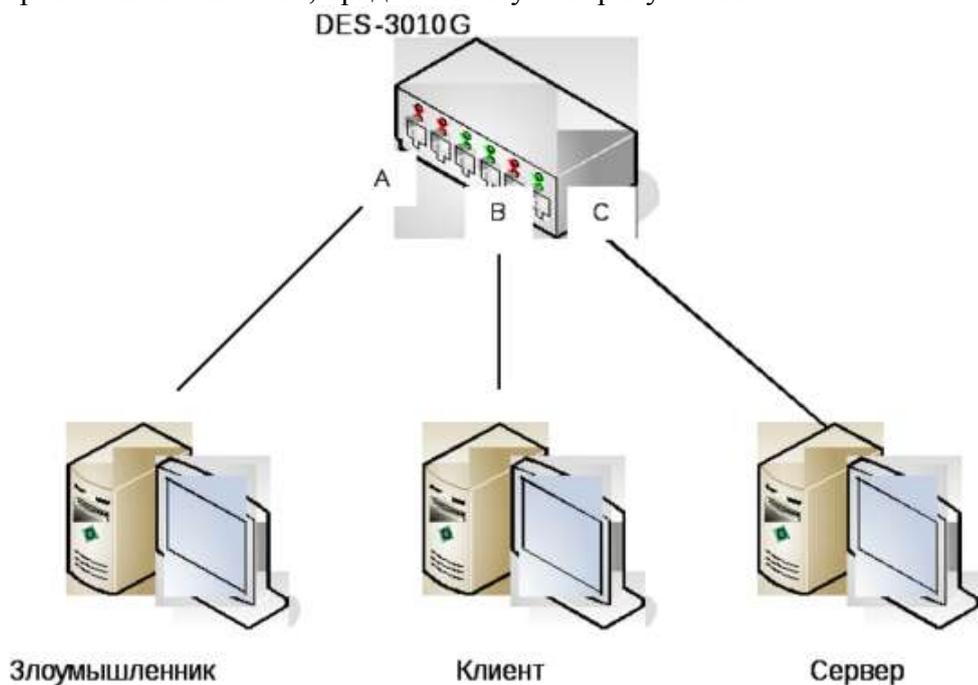


Рисунок 11

2. Настройте «зеркалирование» (PortMirroring) на коммутаторе следующим образом: порт «а» - приемник, порт «b» - источник. Таким образом, злоумышленник сможет «прослушивать» весь трафик клиента.
3. Изучите главу «Протокол SSL/TLS» теоретического пособия, а также главу «Шифратор TCP-соединения Stunnel».
4. Запустите на сервер POP3-сервер с авторизацией через /etc/passwd.
5. Получите почту пользователя rootc машины клиента. Параллельно с этим процессом запустите утилиту tcpdump на компьютере злоумышленника. Обнаружьте пароль на почтовый ящик в перехваченных пакетах.
6. На сервере запустите утилиту stunnel на 995 порту для запуска почтового сервера.
7. Включите использование SSL/TLS на клиенте. Выполните шаг 5.
8. Сравните перехваченные утилитой tcpdump пакеты.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

### Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

## Практическая работа № 11

### Удаленное управление по защищенному протоколу SSH

**Цель работы:** Изучение протокола SSH и способов его применения в OCLinux.

### Выполнив работу, Вы будете:

уметь:

- удаленно управлять компьютером пользователя по протоколу SSH;

### Материальное обеспечение:

учебно-лабораторный стенд «Сетевая безопасность»

### Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке 12.

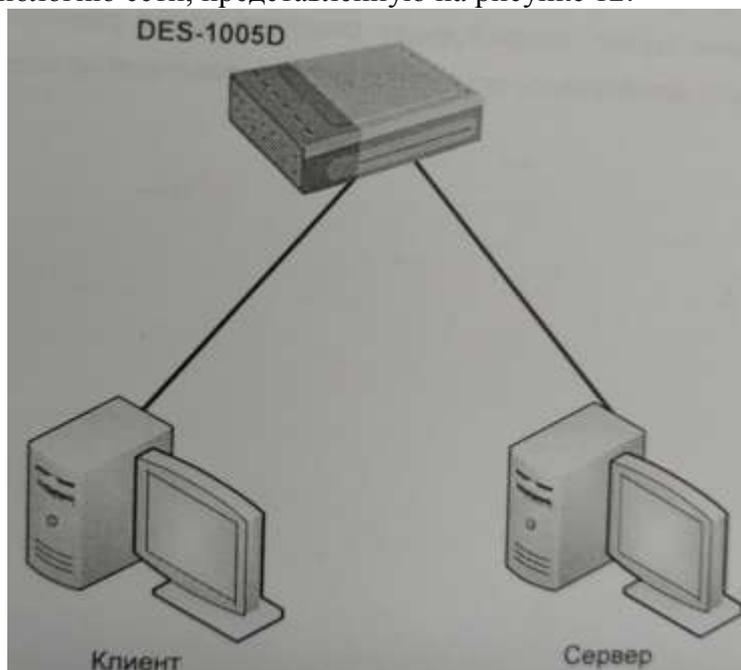


Рисунок 12

2. Изучите главу «Протокол SSH» теоретического пособия, а также главу «Пакет OpenSSH».
3. Проверьте, работает ли на компьютерах ssh-сервер (**psax | grepssh**). Если не работает, то запустите его командой.
4. Попробуйте подключиться с клиента на сервер с использованием протокола SSH. Изучите переданные пакеты с помощью **tcpdump**. Посмотрите, какие события были отмечены в файле журнала **/var/log/auth.log**.
5. Перезагрузите удаленный сервер, не подключаясь к нему.
6. Удаленно перезапустите демон **ssh** без подключения.
7. Подключитесь к удаленному серверу и перезапустите демон **ssh**. Обратите внимание на то, что сеанс не завершился.
8. Запустите FTP-сервис на сервере.
9. Выполните передачу файла через FTP с помощью утилиты **wget**. Анализируйте проходящие пакеты с помощью утилиты **tcpdump (-XX)**. Запомните скорость передачи.
10. Выполните передачу файла через **ssh**. Анализируйте проходящие пакеты с помощью **tcpdump (-XX)**. Запомните скорость передачи. Сравните передаваемые пакеты и скорость передачи данных.
11. Включите сжатие **ssh** и повторите замер скорости. В каждом тесте анализируйте результаты для файла, состоящего из нулей, для файла, содержащего случайную последовательность (**ddif=/dev/urandomof=filebs=1Mcount=10**), для текстового конфигурационного файла и для бинарного файла.
12. Напишите скрипт, который будет создавать файл размером 10МБ со случайными данными, архивировать его и передать с удаленной на локальную машину.

**Форма представления результата:** Отчет о проделанной работе, выполненная работа.

**Критерии оценки:**

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.