МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный технический университет»

Кафедра радиоэлектронных устройств и систем

СЕТЕВЫЕ ТЕХНОЛОГИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ №5-7
для студентов специальности 11.05.01
«Радиоэлектронные системы и комплексы»
очной формы обучения

Воронеж 2024

УДК 621.396.6(07)
ББК 32.844я7

Составитель: А. И. Сукачев

Сетевые технологии в радиоэлектронных системах: методические указания к выполнению лабораторных работ №5-7 для студентов специальности 11.05.01 «Радиоэлектронные системы и комплексы» очной формы обучения / ФГБОУ ВО «Воронежский государственный технический университет»; сост.: А. И. Сукачев. – Воронеж: Изд-во ВГТУ, 2024. – 29 с.

В соответствии с рабочими учебными программами дисциплин приведены описания методов измерений и методик выполнения лабораторных работ, изложены теоретические сведения, содержащие основы использования микро-процессорной техники. По каждой лабораторной работе в описание включены: теоретические материалы, используемое оборудование и приборы, порядок подготовки и проведения работы.

Предназначены для студентов специальности 11.05.01 «Радиоэлектронные системы и комплексы» очной формы обучения.

Методические указания подготовлены в электронном виде и содержатся в файле МУ_СТвРЭС_ЛР 5-7.pdf.

Ил. 21. Библиогр.: 6 назв.

УДК 621.396.6(07)
ББК 32.844я7

Рецензент – А. В. Останков, д-р техн. наук, профессор кафедры радиотехники ВГТУ

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

1. ЛАБОРАТОРНАЯ РАБОТА №5
ПРОКСИ-СЕРВЕР

1.1. ЦЕЛЬ РАБОТЫ

Изучить работу прокси-сервера.

1.2. ЗАДАЧИ РАБОТЫ

Установить Squid;

Настроить работу Squid;

Проверить работу Squid.

1.3. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.4. ПРОКСИ-СЕРВЕР SQUID

Squid - программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS. Разработан сообществом как программа с открытым исходным кодом (распространяется в соответствии с GNU GPL). Все запросы выполняет как один неблокируемый процесс ввода/вывода. Используется в UNIX- системах и в операционных системах семейства Windows NT. Имеет возможность взаимодействия с Active Directory Windows Server путём аутентификации через LDAP, что позволяет использовать разграничения доступа к интернет-ресурсам пользователей, которые имеют учётные записи на Windows Server, также позволяет организовать «нарезку» интернет-трафика для различных пользователей. Сервер Squid развивается в течение уже многих лет. Обеспечивает совместимость с большинством важнейших протоколов Интернета.

Для установки Squid запустите в терминале следующую команду (рис. 1):

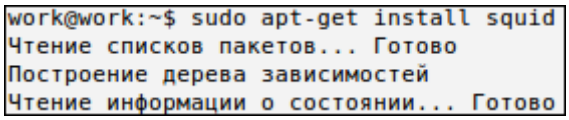

Рис. 1. Установка Squid

Конфигурация для Squid находится в файле /etc/squid/squid.conf. Оставим все настройки по умолчанию. Изменим лишь некоторые правила:

Для аутентификации пользователей добавим следующие строки:

auth_param basic program /usr/lib/squid/ncsa_auth

/etc/squid/internet_users

auth_param basic children 5

auth_param basic realm Enter Login/Password auth_param basic credentialsttl 2 hours

auth_param basic casesensitive off

В директории /usr/lib/squid/ncsa_auth находится программа, для аутентификации; в директории /etc/squid/internet_users – список пользователей и их пароли в зашифрованном виде. Текст «Enter Login/Password» обозначает приглашение к аутентификации.

Добавим строку http_access allow localnet. Это имя правила.

Теперь напишем и сами правила (рис. 2):

```
alc localnet src 10.0.0.0/8     #RFC1918 possible internal network
alc localnet src 172.16.0.0/12  #RFC1918 possible internal network
alc localnet src 192.168.0.0/24 #RFC1918 possible internal network
```

Рис. 2. Правила

Аналогичным образом добавим правило с именем «password» и его описание:

acl password proxy_auth REQUIRED

После этого сохраняем файл-конфигурации и перезапускаем squid следующей командой:

```
work@work:~$ sudo service squid restart
squid start/running, process 2010
```

Рис. 3. Перезапуск squid

Дальше проверим работу нашего прокси сервера. Например, создадим ещё одну виртуальную машину с любой операционной системой. К примеру, будем использовать Windows XP.

Меняем настройки виртуальной машины с Linux Ubuntu: в категории «Сеть» добавляем второй адаптер. При этом тип подключения «Внутренняя сеть», имя: «intent».

Меняем настройки виртуальной машины с Windows XP (или другой любой операционной системой): в категории «Сеть» для адаптера 1 тип подключения «Внутренняя сеть», имя: «intent».

В самих операционных системах приписываем статический IP- адрес, например, для Linux Ubuntu 192.168.0.1, для Windows XP – 192.168.0.2.

Далее, в Windows XP необходимо использовать подключение к LAN через прокси-сервер. В браузере Internet Explorer это можно сделать следующим образом:

Сервис > Свойство обозревателя > Подключение > Настройка LAN. Далее выделить пункт «Использовать прокси-сервер». В адресе прописать IP-адрес Ubuntu (192.168.0.1) и порт, который был прописан в файле-конфигурации squid (3128).

1.5. ПРАКТИЧЕСКАЯ РАБОТА

1. Отключите межсетевой экран. Установите Squid на вашу операционную систему Linux;
2. Создайте новое правило работы Squid: разрешить доступ подсети 192.168.0.0/24;
3. Проверьте работу Squid следующим образом: создайте ещё две виртуальные машины с операционными системами Windows и Linux. Настройте второй адаптер вашей Linux Ubuntu и адаптеры у вспомогательных операционных систем. Не забудьте указать в браузерах вспомогательных операционных систем, что подключение бу-

дет осуществлятся через прокси-сервер. Если у вас всё настроено правильно и в вашей Linux Ubuntu есть подключение к Internet, то и во вспомогательных операционных системах так же должен быть доступ к Internet;

4. Измените предыдущее правило работы Squid: доступ подсети 192.168.0.0/24 должен быть разрешен в период рабочего времени (с 8.00 до 17.00) и только в рабочие дни (понедельник, вторник, среда, четверг, пятница).

1.6. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каково назначение Squid?
2. Каким образом изменяются настройки работы Squid?
3. Каким образом прописываются правила работы Squid? Опишите синтаксис.

2. ЛАБОРАТОРНАЯ РАБОТА №6
УДАЛЕННОЕ ХРАНЕНИЕ ДАННЫХ

2.1. ЦЕЛЬ РАБОТЫ

Изучить технологии удаленного доступа к файлам.

2.2. ЗАДАЧИ РАБОТЫ

Изучить работу Samba;

Изучить работу Network File System.

2.3. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

2.3.1. SAMBA

Samba - программа, которая позволяет обращаться к сетевым дискам на различных операционных системах по протоколу SMB/CIFS. Имеет клиентскую и серверную части. Является свободным программным обеспечением, выпущена под лицензией GPL.

Samba работает на большинстве Unix-подобных систем, таких как GNU/Linux, POSIX-совместимых Solaris и Mac OS X Server, на различных вариантах BSD, в OS/2. Samba включена практически во все дистрибутивы GNU/Linux, в том числе, конечно, и в Ubuntu.

2.3.2. УСТАНОВКА И НАСТРОЙКА SAMBA

Для установки достаточно открыть терминал и ввести команду (рис. 4):

```
work@work:~$ sudo apt-get install samba
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 4. Установка Samba

Приложение будет автоматически загружено и установлено.

2.4. КОНФИГУРИРОВАНИЕ АВТОНОМНОГО ФАЙЛОВОГО СЕРВЕРА

Файл конфигурации находится в директории: /etc/samba/smb.conf.

Домен Active Directory есть далеко не у всех. Поэтому часто возникает необходимость организовать на Linux машине автономное файловое хранилище со своей собственной системой авторизации. Это сделать очень просто.

Основной особенностью такой организации файлового хранилища будет то, что вся информация о пользователях будет храниться в базе данных Samba, соответственно добавлять и удалять пользователей на Samba надо будет вручную.

Самое главное - определиться с используемым способом доступа к ресурсу. Для его изменения надо правильно установить значение параметра security в секции [global] файла

/etc/samba/smb.conf. Обычно используется значение share или user.

Параметр security влияет на то, как будут себя вести клиенты Samba и это один из наиболее важных параметров файла smb.conf.

2.4.1. SECURITY = SHARE

Когда клиенты присоединяются к ресурсу с security = share им не нужно регистрироваться с использованием действительного имени пользователя и пароля. Вместо этого, клиенты посылают информацию аутентификации (пароли) на конкретный ресурс, в тот момент, когда хотят получить доступ к этому ресурсу.

Заметьте, что при использовании уровня безопасности share может быть очень сложно определить какой же пользователь UNIX будет использован в конечном счете.

2.4.2. SECURITY = USER

При этом режиме клиент должен сначала произвести вход (logon), с существующим именем пользователя и паролем (имя может быть транслировано с помощью параметра username map). Шифрованные пароли также могут быть использованы в этом режиме.

Заметьте, что имя запрошенного ресурса не будет послано серверу до тех пор, пока сервер не аутентифицирует клиента. Именно поэтому гостевые учетки не работают в режиме user, не позволяя серверу преобразовывать неопознанных пользователей в гостей.

2.4.3. SECURITY = DOMAIN

Такой режим будет работать только в том случае, если была использована команда net для добавления этого компьютера в домен Windows NT. Это требует установленного параметра encrypted passwords = yes.

В этом режиме Samba попытается опознать имя пользователя и пароль, передав их первичному или резервному домен контроллерам Windows NT, т.е. сделает тоже самое, что сделал бы сервер Windows NT.

Заметьте, что реальный пользователь UNIX все-таки должен быть, потому что Samba придется проверять права доступа пользователя UNIX, к файлу в файловой системе UNIX. С точки зрения клиента, нет разницы между режимами domain и user. Это затрагивает лишь то, как сервер проводит аутентификацию, только и всего.

Имя запрошенного ресурса не будет послано серверу до тех пор, пока сервер не аутентифицирует клиента. Именно поэтому гостевые шары не работают в режиме user, не позволяя серверу преобразовывать неопознанных пользователей в гостей, чтобы сервер аутентифицировал пользователя, используются параметр guest account.

2.4.4. SECURITY = SERVER

В этом режиме Samba попытается определить правильность пары пользователь/пароль, передав ее другому серверу SMB, такому как NT. Если это не получится, будет работать security = user.

2.4.5. SECURITY = ADS

В этом режиме Samba работает как член домена AD.

Для работы в этом режиме, компьютеру, на котором запущена Samba, необходим будет установленный и настроенный Kerberos, и Samba должна быть присоединена к области AD с использованием утилиты net.

Делаем так, что для того, чтобы залогинится на сервере samba обязательно нужно использовать учётную запись самой Ubuntu, то есть для того, чтобы создать samba-юзера надо сделать следующее (рис. 5):

```
work@work:~$ cd /etc/samba
work@work:/etc/samba$ sudo smbpasswd -a work
New SMB password:
Retype new SMB password:
```

Рис. 5. Запись пользователя в БД SMB

Вам будет предложено ввести пароль, пользователь будет добавлен в базу, теперь необходимо включить этого пользователя:

```
work@work:/etc/samba$ sudo smbpasswd -e work
Enabled user work.
```

Рис. 6. Включение пользователя

Открыть доступ на какую-нибудь папку очень просто. Допустим, мы хоти сделать три доступных каталога: usershare – доступный только определённым пользователям, download – откуда можно только скачивать файлы и upload – папка для закачки файлов на сервер. Для начала создадим три директории /home/share/usershare, /home/share/download и /home/share/upload, сделать каталог upload доступным для записи

```
sudo chmod 777 /home/share/upload
```

И запишем в конец конфигурационного файла /etc/samba/smb.conf следующий текст:

```
[usershare]
comment = User share
path = /home/shares/usershare valid users = username
create mask = 0660
```

```
directory mask = 0771 writable = yes
[download]
comment = All users download path = /home/share/download
create mode = 0700
directory mask = 0700 available = yes
browsable = yes public = yes
writable = no [upload]
comment = All users upload path = /home/share/upload
create mode = 0777
directory mask = 0777 available = yes
browsable = yes public = yes
writable = yes
```

Не забудьте перезапустить samba после изменений (рис. 7):

```
work@work:/etc/samba$ sudo service smbd restart
smbd start/running, process 2048
```

Рис. 7. Перезапуск Samba

2.5. ПРИЛОЖЕНИЯ ДЛЯ НАСТРОЙКИ

Так же существуют приложения, позволяющие производить настройку Samba через графический интерфейс (см. GUI приложения для работы с Samba).

Установить самый простой GUI для Samba можно командой (рис. 8):

```
work@work:~$ sudo apt-get install system-config-samba
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 8. Установка приложения для работы с Samba

Запускается он командой (рис. 9):

```
work@work:~$ sudo system-config-samba
```

Рис. 9. Запуск приложения для работы с Samba

Все изменения он записывает в конфигурационный файл samba.
Интерфейс приложения приведен на рис. 10.

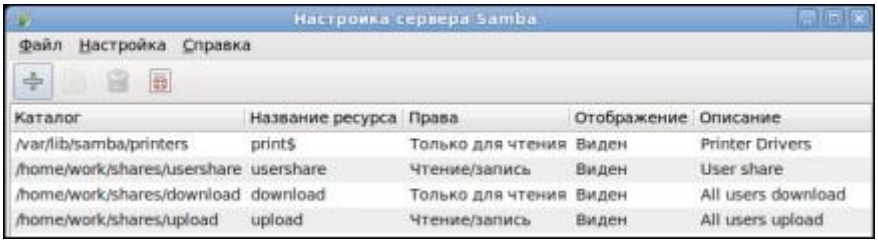

Рис. 10. Приложение для работы с Samba

Для удалённого администрирования Samba в качестве web-интерфейса для Samba отлично подойдёт webmin.

2.6. NETWORK FILE SYSTEM

Network File System (NFS) позволяет системе предоставлять в общий сетевой доступ каталоги и файлы. Посредством NFS, пользователи и программы могут получать доступ к файлам на удаленных машинах так же легко, как будто это файлы на их локальном компьютере.

2.6.1. УСТАНОВКА И НАСТРОЙКА NFS-СЕРВЕРА

Для работы NFS-сервера должны быть установлены пакеты (рис. 11):

- nfs-kernel-server;
- nfs-common;
- portmap.

```
work@work:~$ sudo apt-get install nfs-kernel-se
rver nfs-commom portmap
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 11. Установка пакетов для работы с NFS

Настраиваем, какие именно директории мы хотим открыть для совместного пользования и кому. Все это делается в файле /etc/exports. Записи в этом файле имеют следующий формат:

каталог (или файловая система)

client1 (option1, option2) client2 (option1, option2)

Выделим директорию /homeshare (директория с данными на сервере) в совместное пользование всем компьютерам с IP - 192.168.0.0/24 с правами чтения и записи:

```
/homeshare
192.168.0.0/24 |( rw,sync,no_subtree_check,all_squash)|
```

Рис. 12. Настройка NFS

Опции:

- ro - права только на чтение. Можно и не указывать, так как она установлена по умолчанию;
- rw - дает клиентам право на запись;
- async - этот параметр может повысить производительность, но он может также вызвать потерю данных при перезапуске NFS-сервера без предварительной процедуры остановки NFS-демона;
- sync - более безопастный режим. Выставлен по умолчанию;
- no_wdelay - актуален только в режиме async. Отключает задержку при записи;
- no_subtree_check - этот параметр отключает контроль подкаталогов, выполняющийся для некоторых проверок системой защиты.

Например, могут проверяться права на все подкаталоги монтируемой директории. Параметр по умолчанию - разрешить контроль подкаталогов;

- noaccess - запрещает доступ к указанной директории. Может быть полезной, если перед этим задан доступ всем пользователям сети к определенной директории, и нужно ограничить доступ в поддиректории лишь некоторым пользователям.

Опции отображения пользователей:

- root_squash - этот параметр не позволяет пользователю root обращаться к смонтированному NFS-тому;
- no_root_squash - этот параметр позволяет пользователю root обращаться к смонтированному NFS-тому;
- all_squash - этот параметр, полезный для NFS-томов с открытым доступом, подавляет все UID и GID и использует только учетную запись анонимного пользователя. Установка по умолчанию - no_all_squash;
- anonuid и anongid - эти параметры меняют UID и GID анонимного пользователя на указанную учетную запись.

2.6.2. УСТАНОВКА И НАСТРОЙКА NFS-КЛИЕНТА

На клиентской машине необходимо установить следующие пакеты:

- nfs-common;
- portmap.

Далее, создать точку монтирования. Для того, чтобы не создавать точку монтирования каждый раз, необходимо добавить в файл /ets/fstab следующие строки:

Создаем точку монтирования (если её нет):

$mkdir data (мы же используем как точку монтирования (/ home)

Монтировать можно двумя способами - каждый раз вручную или прописав опции монтирования в файл /etc/fstab (рис. 13):

```
Device mountpoint fs-type options dump fsckorder 192.168.0.1|:/homeshare /home
nfs rw,hard,intr,sync 0 0
```

Рис. 13. Монтирование директории на клиентской ОС

NFS клиент может обрабатывать сбои сервера в работе. Есть две опции монтирования: hard и soft.

soft: если запрос на получение файла не выполнен, NFS клиент сообщит об ошибке процессу, который пытается получить доступ к файлу. Некоторые программы умеют это обрабатывать, большая же часть - нет. Разработчики nfs не рекомендуют использовать эту опцию — это прямой путь к повреждённым данным и потере информации. hard: Программа, осуществляющая доступ к файлу, повиснет при смерти сервера. Процесс не может быть прерван или убит (только «sure kill»), пока вы не укажете опцию intr. Когда NFS сервер вернётся к работе, программа продолжит работу с того места, где остановилась. Разработ-

чики NFS рекомендуют использование опций hard, intr со всеми монтируемые NFS файловые системы.

2.7. КОМПОНЕНТЫ WINDOWS

Для работы Windows с NFS необходимо добавить службу Майкрософт для Network File System. Для этого проделаем следующее:

1. Установка и удаления программ > Установка компонентов Windows;
2. Другие службы доступа к файлам и принтерам сети -> Служба Microsoft для NFS.

И выбираем там:

- Администрирование служб Microsoft для NFS;
- Внешнее представление данных RPC;
- Клиент для NFS.

После установки и перезагрузки появляется возможность примонтировать NFS.

2.8. ПРАКТИЧЕСКАЯ РАБОТА

1. Установите Samba на вашу Linux Ubuntu;
2. Измените настройки Samba так, что бы вход осуществлялся с существующим именем пользователя и паролем;
3. Создайте Samba-юзера, его имя и пароль должны совпадать с именем и паролем учетной записи. Включите этого пользователя.
4. Создайте каталог /home/share и в нем три каталога: usershare, download и update. Настройте их так, что бы первый был для доступа только определенных пользователей, второй - для скачанных файлов, третий - для закачки файлов на сервер. Проверьте работоспособность в дополнительных операционных системах – Linux и Windows;
5. Установите NFS-сервер на вашу Linux Ubuntu, а NFS-клиент на вспомогательную виртуальную машину с Linux. Создайте в основной операционной системе общий каталог – homeshare;
6. Проверьте работоспособность NFS в дополнительных операционных системах – Linux и Windows.

2.9. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каково назначение Samba?
2. Каким образом производится настройка Samba?
3. Какие приложение для настройки Samba существуют?
4. Какого назначение NFS?
5. Каким образом производится настройка NFS?
6. Что такое монтирование, каким образом оно осуществляется и какие способы монтирования бывают?

3. ЛАБОРАТОРНАЯ РАБОТА №7
УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ

3.1. ЦЕЛЬ РАБОТЫ

Изучить основы удаленного администрирования.

3.2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

3.2.1. WEBMIN

Webmin - это графический web интерфейс для управления сервером на базе Unix подобных операционных систем. То есть установив Webmin вы можете удалённо конфигурировать и управлять Linux сервер в удобном графическом интерфейсе на русском языке через браузер.

Возможности:

- Полное управление ОС (загрузка, процессы, состояние, log- файлы);
- Управлять пользователями и группами и их правами;
- Управлять всеми серверами (Apache, FTP, SSH, Samba);
- Настройка сети в том числе и Firewall;
- Проводить резервное копирование, и многое другое;

3.2.2. УСТАНОВКА WEBMIN

Установить webmin можно двумя путями. Первый путь:

Скачайте установочный пакет с webmin сайта www.webmin.com.

Для установки выполните (рис. 14).

```
work@work:~$ sudo dpkg -i webmin_1.570_all.deb
```

Рис. 14. Установка Webmin

В ходе установки появится сообщение об ошибке из-за отсутствия необходимых пакетов в системе.

Для устранения зависимостей выполните команду, представленную на рис. 15.

```
work@work:~$ sudo apt-get install -f
```

Рис. 15. Устранение зависимостей

Все зависимости будут разрешены. Настройка пакета webmin выполнится автоматически после разрешения зависимостей.

Второй путь устранения ошибки: необходимо добавить в список репозитария сайт wibmin'a. Для этого необходимо открыть для редактирования файл: /etc/apt/sources.list. В данный список необходимо в конец добавить следующую строку:

deb http://download.webmin.com/download/repository
sarge contrib

Сохраните файл. Теперь можно установить Webmin привычным способом (рис. 16):

```
work@work:~$ sudo apt-get install webmin
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 16. Установка Webmin

Запустить Webmin можно через браузер для этого введите следующий адресу в строку url: https://localhost:10000.

Примите сертификат (рис. 17).

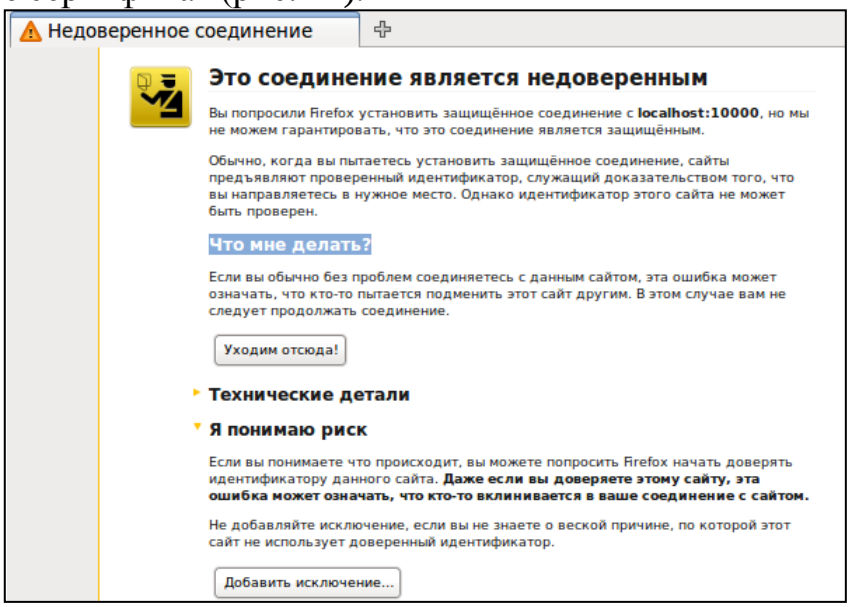

Рис. 17. Добавление в исключение

3.3. ИНТЕРФЕЙС

При входе в Wibmin вам будет предложено авторизоваться (рис. 18).

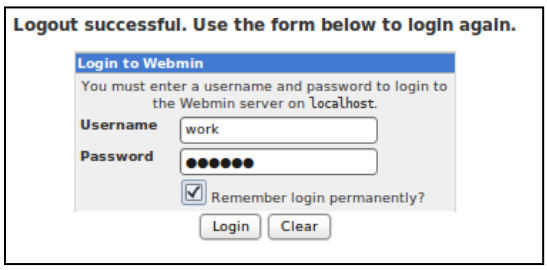

Рис. 18. Авторизация

Введите логин и пароль от вашей учетной записи. Далее вы попадете на страницу управления сервером (рис. 19).

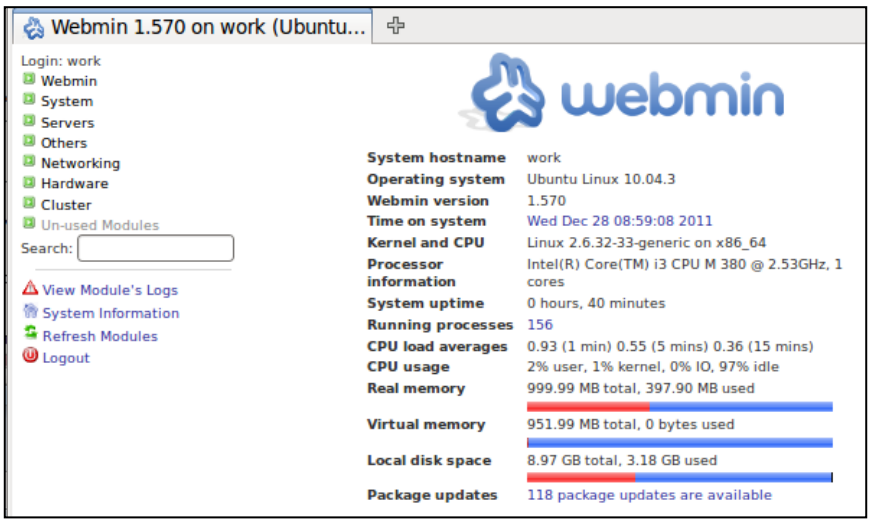

Рис. 19. Главная страница Webmin

С левой стороны находится список возможных конфигураций.

Для смены языка нажмите Wemin > Выбрать язык.

Все сервисы находятся в пункте Service. Рассмотрим, например, конфигурацию Squid и просмотр журнала событий. Для начала, установим sarg – сервис, позволяющий вести статистику по работе Squid (рис. 20).

```
work@work:~$ sudo apt-get install sarg
[sudo] password for work:
Чтение списков пакетов... Готово
Построение дерева зависимостей
```

Рис. 20. Установка sarg

Для настройки sarg зайдите в пункт Неиспользуемые модули (Un-user Modules). Там выберите Squid Report Generator (рис. 21). Для настройки нажмите «Настройки модуля» и введите путь для файла конфигурации: /etc/sarg/sarg.conf.

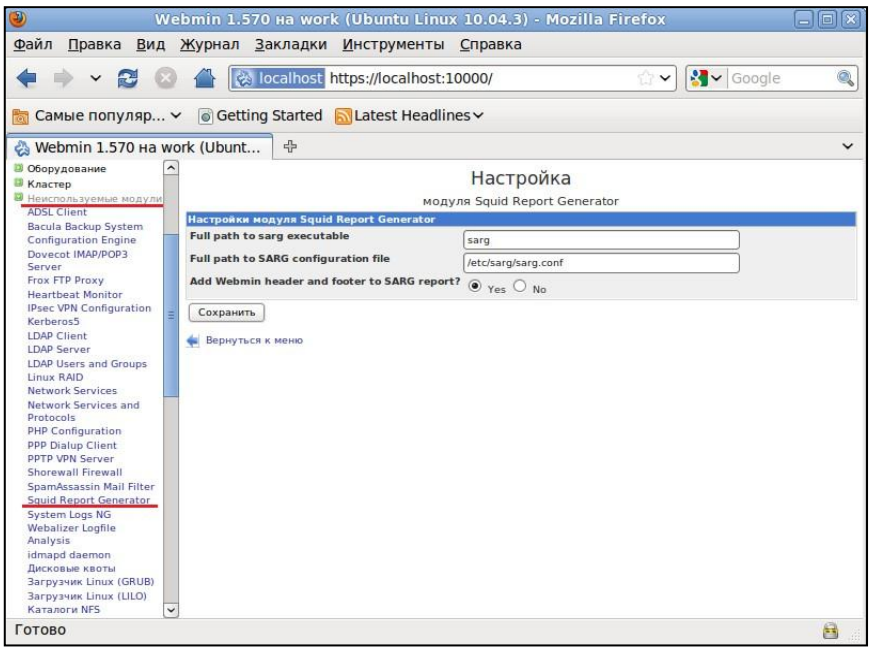

Рис. 21. Настройка sarg

Сохраните настройки и перезагрузить страницу. После этого Squid Report Generator появится в пункте Сервисы (Servers).

3.4. PHPMYADMIN

phpMyAdmin - это программа написанная на PHP и предназначенная для управления сервером MySQL через всемирную сеть. phpMyAdmin поддерживает широкий набор операций над MySQL. Наиболее часто используемые операции поддерживаются с помощью пользовательского интерфейса (управление базами данных, таблицами, полями, связями, индексами, пользователями, правами, и т. д.), одновременно вы можете напрямую выполнить любой SQL запрос.

phpMyAdmin обладает большим разделом документации и все пользователи приглашаются для обновления наших вики страниц для обмена идеями и способами применений различных операций. Команда phpMyAdmin постарается помочь вам при возникновении проблем, вы можете использовать различные каналы связи для получения поддержки.

Возможности phpMyAdmin:

1. интуитивно понятный веб-интерфейс;
2. поддержка большинства функций MySQL:

– просмотр и удаление баз данных, таблиц, вьюшек, полей и индексов;
– создание, копирование, удаление, переименование и изменение баз данных, таблиц, полей и индексов;
– управление сервером, базами данных и таблицами, с советами по настройке сервера;
– выполнение, редакция и сохранение любого SQL- выражения, включая пакетные запросы;

- управление пользователями MySQL и их привилегиями;
- работа с хранимыми процедурами и триггерами.

3. поддержка импорта данных из CSV и SQL;
4. поддержка экспорта в различные форматы CSV, SQL, XML, PDF, ISO/IEC 26300 - OpenDocument текст и таблицы, Word, Excel, LATEX и другие;
5. администрирование нескольких серверов;
6. генерирование наглядных схем баз данных в виде PDF;
7. создание комплексных запросов с помощью функции Запрос по шаблону;
8. глобальный или частичный поиск в базе данных;
9. трансформация данных в любой формат, используя набор предназначенных функций вроде отображения BLOB- данных в виде картинки или ссылки для скачивания;
10. это не все, лишь часть возможностей phpMyAdmin которых, впрочем, достаточно чтобы объяснить его международную популярнсть.

3.5. ПРАКТИЧЕСКАЯ РАБОТА

1. Установите Webmin на вашу Linux Ubuntu;
2. С помощью Webmin’а добавите новую группу пользователей и добавьте в неё нового пользователя;
3. С помощью Webmin’а измените конфигурацию Squid;
4. С помощью Webmin’а просмотрите файловый журнал Squid.

3.6. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое Webmin?
2. Какие основные возможности Webmin?
3. Каково назначение PHPmyAdmin?
4. Каковы возможности PHPmyAdmin?

ПРИЛОЖЕНИЕ

ОСНОВНЫЕ КОМАНДЫ LINUX

Таблица П.1

Список общих команд

# uname -a	Отобразить версию ядра Linux;
# lsb_release -a	Отобразить на экране информации о версии операционной системы;
# man hier	Отобразить описания иерархии файловой системы;
# clear	Осуществить очищение экрана терминала;
# wall Hello	Осуществить отправление на терминалы других пользователей сообщение «Hello»;
# date	Отобразить текущую дату и время;
# cal -3	Отобразить в удобной форме предыдущий, текущий и последующий месяц;
# uptime	Отобразить текущее время и работу системы без перезагрузки и выключения;
# hostname	Отобразить сетевое имя компьютера;
# whois linux.org	Отобразить информацию о доменом имени linux.org;
# pppconfig	Осуществить создание и настройка Dial-Up соединения для выхода в Интернет по модему;
# pppoeconf	Осуществить создание и настройка выхода в Интернет через ADSL-модем;
# !!	Осуществить повторение последней выполненной команды;
# history | tail -50	Отобразить последние 50 набранных команд;
# exit	Осуществить завершение сеанса текущего пользователя;
# passwd	Осуществить изменение пароля текущего пользователя;
# shutdown -h now	Осуществить выход из Linux;
# poweroff	Осуществить выход из Linux;
# reboot	Осуществить перезагрузку системы;
# last reboot	Отобразить статистику перезагрузок;
# host site.ru	Отобразить IP-адрес введенного сайта;

Таблица П.2

Список команд для работы с файлами и директориями

# pwd	Отобразить текущий путь;
# ls	Отобразить список файлов и каталогов по порядку;
# ls -la X	Отобразить форматированный список всех файлов и директорий, включая скрытые;
# cd	Осуществить переход в домашнюю директорию;
# cd /home	Осуществить переход в директорию /home;
# touch /home/file	Осуществить создание пустого файла /home/file;
# cat /home/file	Отобразить содержимое файла /home/file;
# tail /var/log/file	Отобразить окончание файла (последние строки данного файла, которые поместятся на экран). Удобно при работе с логами и большими файлами;
# nano /home/file	Осуществить редактирование файла /home/file;
# gedit /home/file	Осуществить редактирование файла /home/file;
# echo «the End»| sudo tee -a /home/file	Осуществить добавление к концу файла «the End» в файл /home/file;
# cp /home/work/primer.txt /home/primer.txt	Осуществить копирование /home/work/primer.tx в home/primer.txt;
# ln -s /home/work/primer.txt /home/primer	Осуществить создание символической ссылки /home/primer к файлу /home/work/primer.txt;
# mkdir /home/work/ dir	Осуществить создание директории с именем dir;
# rmdir /home/work/ dir	Осуществить удаление директории с именем dir;
# rm -rf /home/work/ dir	Осуществить удаление директории с вложенными фалами;
# cp -la /dir1 /dir2	Осуществить копирование директорий;
# mv /dir1 /dir2	Осуществить переименование директории;

Окончание табл. П.2

# du -sh /home/work/	Отобразить на экран размер заданной директории. Можно использовать для определения размера файлов;
# locate primer	Осуществить поиск всех файлов с именем primer;
# [sudo] chmod 0777 /home/	Осуществить изменение прав доступа к директории только для /home. 0777 – разрешение на чтение/запись/исполнение для всех групп;
# [sudo] chmod -R 0777 /home/	Осуществить рекурсивное изменение прав доступа к директории /home. 777 – разрешение на чтение/запись/исполнение для всех групп. Все вложенные директории и файлы будут иметь права 0777;
# [sudo] chown work:test /home/primer.txt	Осуществить изменение владельца и группы только для файла /home/primer.txt;
# [sudo] chown -R work /home/	Осуществить изменение владельца для всего содержимого директории /home;

Таблица П.3

Работа с архивами

# tar cf primer.tar /home/primer.txt	Осуществить создание tar-архива с именем primer.tar содержащий /home/primer.txt;
# tar czf primer.tar.gz /home/primer.txt	Осуществить создание tar-архива с сжатием Gzip по имени primer.tar.gz;
# tar cjf primer.tar.bz2 /home/primer.txt	Осуществить создание tar-архива с сжатием Bzip2 по имени primer.tar.bz;
# tar xf primer.tar	Осуществить распаковку архива primer.tar в текущую папку;
# tar xzf primer.tar.gz	Осуществить распаковку tar-архива с Gzip;
# tar xjf primer.tar.bz	Осуществить распаковку tar-архива с Bzip2;

Таблица П.4

Команды установки программ (RPM-дистрибутивы)

# rpm -qa	Отобразить список установленных пакетов RPM в системе;
# [sudo] rpm -i pkgname.rpm	Осуществить установку RPM пакета pkgname.rpm;
# [sudo] rpm -e pkgname	Осуществить удаление RPM пакета pkgname;
# [sudo] dpkg -i *.rpm	Осуществить установку всех пакетов в директории;

Таблица П.5

Команды установки программ (DEB-дистрибутивы)

# dpkg -l |more	Отрбразить список установленных пакетов DEB в системе;
# apt-cache search pack	Осуществить поиск в индексах наличее доступного пакета и выводит на экран краткую информацию о пакете pack (очень полезная команда для поиска и установки программ из консоли);
# apt-cache showpkg pack	Отрбразить полную информация о пакете pack;
# [sudo] apt-get update	Осуществить обновление списка доступных пакетов из Internet;
# [sudo] apt-get upgrade	Осуществить обновление доступной версии установленных пакетов в системе;
# [sudo] apt-get install pkgname	Осуществить установку DEB пакета pkgname;
# [sudo] apt-get remove pkgname	Осуществить удаление DEB пакета pkgname;
# [sudo] dpkg -i *.deb	Осуществить установку всех пакетов в директории;

Таблица П.6

Мониторинг работы и просмотр логов

# top	Отобразить информацию в реальном времени о загруженных процессах, потребление ОЗУ;
# dmesg	Отобразить log-файл загрузки ОС и нахождения новых устройств;

Окончание табл. П.6

# mpstat 1	Отобразить расширенную статистику потребления ресурсов системы в процентах (для некоторых дистрибутивов необходима установка пакета sysstat);
# vmstat 2	Отобразить расширенную статистику по использованию виртуальной памяти;
# iostat 2	Отобразить расширенную статистику прерываний по устройствам;

Таблица П.7

Информация об устройствах

# lsdev	Отобразить информацию об уже установленных устройствах;
# cat /proc/cpuinfo	Отобразить полную информацию о модели процессора (частота, поддерживаемые инструкции и т.д.);
# cat /proc/meminfo	Отобразить расширенную информацию о занимаемой оперативной памяти (MemTotal, MemFree, Buffers, Cached, SwapCached,HighTotal, HighFree, LowTotal и т. д.);
# grep SwapTotal /proc/meminfo	Отобразить размер раздела выделенного под swap;
# watch -n1 'cat /proc/interrupts '	Отобразить информацию о прерываниях;
# free -m	Отобразить информацию о используемой и свободной ОЗУ и Swap-файле (-m указывает, что отображать нужно в Мб);
# lshal	Отобразить список всех устройств и их параметров;
# cat /proc/devices	Отобразить все устройства в системе (названия взяты из директории /proc/devices);
# lspci -tv	Отобразить обнаруженные PCI-устройства;
# lsusb -tv	Отобразить обнаруженные USB-устройства;
# [sudo] dmidecode	Отобразить информацию о версии BIOS компьютера;
# gtf 1024 768 75	Отобразить строку ModeLine для Вашего монитора на параметрах экрана 1024x768x75Hz;

Таблица П.8

Жесткие диски и файловая система

# fdisk -l	Отобразить информацию о всех подключенных жестких и сменных дисках;
# [sudo] hdparm -I /dev/sda	Отобразить полную информацию о IDE/ATA жестких дисках;
# smartctl -a /dev/sda1	Отобразить SMART-информацию о разделе жесткого диска /dev/sda1 (необходима установка пакета smartmontools);
# [sudo] blkid	Отобразить UUID всех доступных накопителей информации в системе;
# [sudo] hdparm -tT /dev/sda	Отобразить производительность жесткого диска;
# mount | column -t	Отобразить полную информацию о примонтированных устройсвах;
# cat /proc/partitions	Отобразить только примонтированные разделы жесткого диска;
# df	Отобразить свободное место на разделах;
# [sudo] mount /dev/sda1 /mnt	Осуществить монтирование раздел /dev/sda1 к точке монтирования /mnt;
# [sudo] mount -t auto /dev/cdrom /mnt/cdrom	Осуществить монтирование большинство CD-ROM`ов;
# [sudo] mount /dev/hdc -t iso9660 -r /cdrom	Осуществить монтирование IDE CD-ROM;
# [sudo] mount /dev/scd0 -t iso9660 -r /cdrom	Осуществить монтирование SCSI CD-ROM;
# [sudo] mount -t smbfs -o username=vasja ,password=pupk in //pup/Video	Осуществить монтирование сетевых ресурсов (SMB);

Окончание табл. П.8

# [sudo] mount-t iso9660 -o loop /home/file.iso /home/iso	Осуществить монтирование ISO-образов;
# [sudo] mount /dev/sdb1 -t vfat -o rw /mnt	Осуществить монтирование раздел с файловой системой FAT 16/32 (к примеру USB-накопитель) к точки монтирования /mnt с возможностью записи;
# [sudo] umount /mnt	Осуществить демонтирование раздел от точки монтирования /mnt;

Таблица П.9

Настройка сети

# ifconfig	Отобразить параметры всех сетевых интерфейсов;
# ifconfig eth0	Отобразить параметры сетевого интерфейса eth0;
# [sudo] ethtool eth0	Отобразить состояние сетевого интерфейса. Команда ethtool применяется только для проводных подключений, не работает с беспроводными интерфейсами;
# [sudo] ethtool -s eth0 speed 100 duplex full autoneg off	Осуществить принудительное задание скорости сетевому интерфейсу 100Mbit и режим Full duplex и отключить автоматическое определение;
# ifconfig eth0 192.168.50.254 netmask 255.255.255.0	Осуществить задание основного IP-адреса сетевому интерфейсу eth0;
# ip addr add 192.168.50.254 /24 dev eth0	Осуществить задание основного IP-адреса сетевому интерфейсу eth0;
# ifconfig eth0:0 192.168.51.254 netmask 255.255.255.0	Осуществить задание дополнительного IP-адреса сетевому интерфейсу eth0;
# ip addr add 192.168.51.254 /24 dev eth0 label eth0:1	Осуществить задание дополнительного IP адреса сетевому интерфейсу eth0;
# [sudo] ifconfig eth0 up	Осуществить запуск сетевого интерфейса eth0;

Продолжение табл. П.9

# [sudo] ifconfig eth0 down	Осуществить отключение сетевого интерфейса eth0;
# ifconfig eth0 hw ether 00:01:02:03:04:05	Осуществить смену MAC адреса;
# [sudo] /etc/init.d/dhcpd restart	Осуществить перезагрузка DHCP клиента;
# ping 192.168.0.2	Осуществить проверку сетевого соединения. Проверяется доступность IP адрес 192.168.0.2;
# route -n	Отобразить на экране таблицу маршрутизации;
# netstat -rn	Отобразить на экране таблицу маршрутизации;
# netstat -an | grep LISTEN	Отобразить список всех открытых портов;
# lsof -i	Отобразить список всех открытых портов в сеть Internet;
# [sudo] netstat -tup	Отобразить активные соединения с интернетом;
# socklist	Отобразить все открытые сокеты;
# [sudo] netstat -anp --udp --tcp | grep LISTEN	Отобразить список приложений, которые открывают порты;
# [sudo] iptables -L -n - v	Отобразить статус firewall (статус iptables);
# [sudo] iptables -P INPUT ACCEPT	Осуществить открытие доступа ко всем портам;
# [sudo] iptables -P FORWARD ACCEPT	Осуществить открытие доступа ко всем портам;
# [sudo] iptables -P OUTPUT ACCEPT	Осуществить открытие доступа ко всем портам;
# [sudo] iptables -X	Осуществить удаление всей цепочки;
# [sudo] iptables -t nat - A POSTROUTING -o eth0 -j MASQUERADE	Осуществить включение NAT на интерфейсе eth0;

Окончание табл. П.9

# [sudo] iptables -t nat - A PREROUTING -p tcp -d 78.31.70.238 --dport 20022 -j DNAT --to 192.168.16.44:22	Осуществить перенаправление порта 20022, который используется для ssh;
# [sudo] iptables -t nat - A PREROUTING -p tcp -d 78.31.70.238 --dport 993:995 - j DNAT --to 192.168.16.254 :993-995	Осуществить перенаправление диапазона портов 993-995;
# iptables -L -t nat	Осуществить проверку статуса NAT;

Таблица П.10

Создание и запись ISO образов

# cdrecord -scanbus	Отобразить все доступные CD-ROM;
# dd if=/dev/hdc of=/tmp/mycd.iso bs=2048 conv=notrunc	Осуществить создание ISO образов с диска CD-ROM;
Пользователи и группы	
# id	Отобразить сводную информацию по текущему пользователю (логин, UID, GID, группы);
# finger work	Отобразить информацию о пользователе work;
# last	Отобразить список последних зарегистрированных пользователей;
# who	Отобразить имя текущего пользователя и время входа;
# useradd work	Осуществить добавление нового пользователя work;
# groupadd test	Осуществить добавление группы test;
# usermod -a -G test work	Осуществить добавление пользователя work в группу test;
# groupmod -A work test	Осуществить добавление пользователя work в группу test;

Окончание табл. П.10

# userdel work	Осуществить удаление пользователя work;
# groupdel test	Осуществить удаление группы test;

Таблица П.11

Печать на принтере

# export PRINTER=lbp2900	Осуществить выбор принтера по-умолчанию. В примере выбран принтер Canon LBP-2900;
# lpr #2 name.txt	Осуществить печать на принтере Canon LBP-2900 две копии файла name.txt;
# lprm -	Осуществить удаление всех задач с принтера по умолчанию.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Блек Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы / Пер. с англ. – М.:Мир, 1990. – 506с.
2. Дж.Мартин. Вычислительные сети и распределенная обработка данных: программное обеспечение, методы и архитектура / Пер. с англ.; Предисл. В.С.Штаркмана. – Вып.2. – М.: Финансы и статистика, 1986. – 269с.
3. Семёнов Ю.А. Протоколы и ресурсы Internet. – М.: Радио и связь, 1996. – 320с.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Издательство «Питер», 2000. – 672с.
5. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – СПб.: СпбГУ, 1998. – 328с.
6. Кульгин М.В. Коммутация и маршрутизация IP/IPX–трафика. – М.: Компьютер-Пресс, 1998. – 320с.

ОГЛАВЛЕНИЕ

1. ЛАБОРАТОРНАЯ РАБОТА №5. Прокси-сервер 3
1.1. Цель работы 3
1.2. Задачи работы 3
1.3. Теоретическая часть 3
1.4. Прокси-сервер Squid 3
1.5. Практическая работа 4
1.6. Контрольные вопросы 5
2. ЛАБОРАТОРНАЯ РАБОТА №6. Удаленное хранение данных. 5
2.1. Цель работы 5
2.2. Задачи работы 5
2.3. Теоретическая часть 5
2.3.1. Samba 5
2.3.2 .Установка и настройка Samba 5
2.4. Конфигурирование автономного файлового сервера 5
2.4.1. Security = share 6
2.4.2. Security = user 6
2.4.3. Security = domain 6
2.4.4. Security = server 7
2.4.5. Security = ADS 7
2.5. Приложения для настройки 8
2.6. Network File System 9
2.6.1. Установка и настройка NFS-сервера 9
2.6.2. Установка и настройка NFS-клиента 10
2.7. Компоненты Windows 11
2.8. Практическая работа 11
2.9. Контрольные вопросы 11
3. ЛАБОРАТОРНАЯ РАБОТА №7. Удаленное администрирование 12
3.1. Цель работы 12
3.2.Теоретическая часть 12
3.2.1. Webmin 12
3.2.2. Установка Webmin 12
3.3. Интерфейс 13
3.4. PHPmyAdmin 15
3.5. Практическая работа 16
3.6. Контрольные вопросы 16
ПРИЛОЖЕНИЕ . Основные команды Linux 17
Библиографический список 27

СЕТЕВЫЕ ТЕХНОЛОГИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ №5-7
для студентов специальности 11.05.01
«Радиоэлектронные системы и комплексы»
очной формы обучения

Составитель
Сукачев Александр Игоревич

Издается в авторской редакции

Подписано к изданию 19.03.2024.
Уч.-изд. л. 1,4

ФГБОУ ВО «Воронежский государственный технический университет»
394006 Воронеж, ул. 20-летия Октября, 84