

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**



**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ «ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт

компьютерных наук

Кафедра

---

автоматизированных систем управления

---

**ЛАБОРАТОРНАЯ РАБОТА №6**

По дисциплине "Операционные системы Linux"

На тему "Работа с SSH"

Студент

ПИ-22-1

---

подпись, дата

Кистерёв В.А.

Руководитель

канд.техн.наук, доцент

ученая степень, ученое звание

---

подпись, дата

Кургасов В.В.

Липецк, 2024 г.

## **Оглавление**

Цель работы .....	3
Ход работы .....	4
Установка пакетов .....	4
Подключение через Telnet .....	6
Подключение через SSH.....	8
Вывод.....	12
Контрольные вопросы.....	13

## **Цель работы**

Практическое ознакомление с программным обеспечением удаленного доступа к распределенным системам обработки данных.

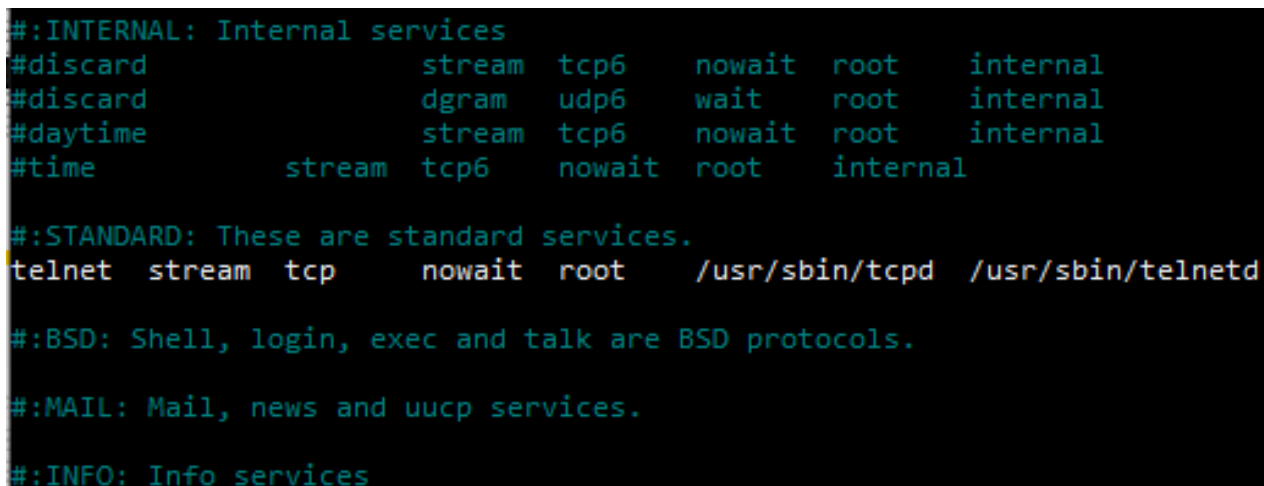
## Ход работы

### Установка пакетов

Установим необходимые для удалённого подключения пакеты:

- openssh-server (сервер OpenSSH)
- telnetd (демон Telnet для удаленного подключения)
- tcpdump (анализатор сетевого трафика)
- screen (утилита управления сеансами командой строки)
- inetd (суперсервер, отвечающий за управление сетевыми службами)

После установки inetd необходимо отредактировать конфигурационный файл. Для этого откроем файл командой: - `sudo nano /etc/inetd.conf` В файле необходимо раскомментировать строку, представленную на рисунке 1. Это действие позволяет активировать Telnet-сервис. После применения конфигурации необходимо перезапустить inetd: `sudo systemctl restart inetd`.



```
#:INTERNAL: Internal services
#discard          stream  tcp6      nowait  root    internal
#discard          dgram   udp6      wait    root    internal
#daytime          stream  tcp6      nowait  root    internal
#time             stream  tcp6      nowait  root    internal

#:STANDARD: These are standard services.
telnet stream tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/telnetd

#:BSD: Shell, login, exec and talk are BSD protocols.

#:MAIL: Mail, news and uucp services.

#:INFO: Info services
```

Рисунок 1 – Раскомментированная строка

Для запуска и активации ssh сервера воспользуемся следующими командами:

- `sudo systemctl enable ssh`
- `sudo systemctl start ssh`
- `sudo systemctl status ssh`

Воспользуемся командой `ss -lt` для того, чтобы определить, какие порты TCP на сервере находятся в состоянии ожидания входящих соединений, и

проверить, какие службы активно слушают сеть. Результат представлен на рисунке 2.

```
user@labs:~$ sudo systemctl restart inetd
user@labs:~$ ss -lt
State      Recv-Q      Send-Q       Local Address:Port      Peer Address:Port      Process
LISTEN     0            128          0.0.0.0:telnet           0.0.0.0:*
LISTEN     0            128          0.0.0.0:ssh              0.0.0.0:*
LISTEN     0            244          127.0.0.1:postgresql    0.0.0.0:*
LISTEN     0            128          [::]:telnet             [::]:*
LISTEN     0            128          [::]:ssh                 [::]:*
LISTEN     0            244          [::1]:postgresql        [::]:*
```

Рисунок 2 – Состояния TCP портов

Как видно из рисунка 2, telnet и ssh прослушиваются и готовы к подключениям.

## Подключение через Telnet

Для подключения через Telnet необходимо активировать клиент Telnet на хостовой системе. На Windows это делается в «Компоненты Windows» (рисунок 3).

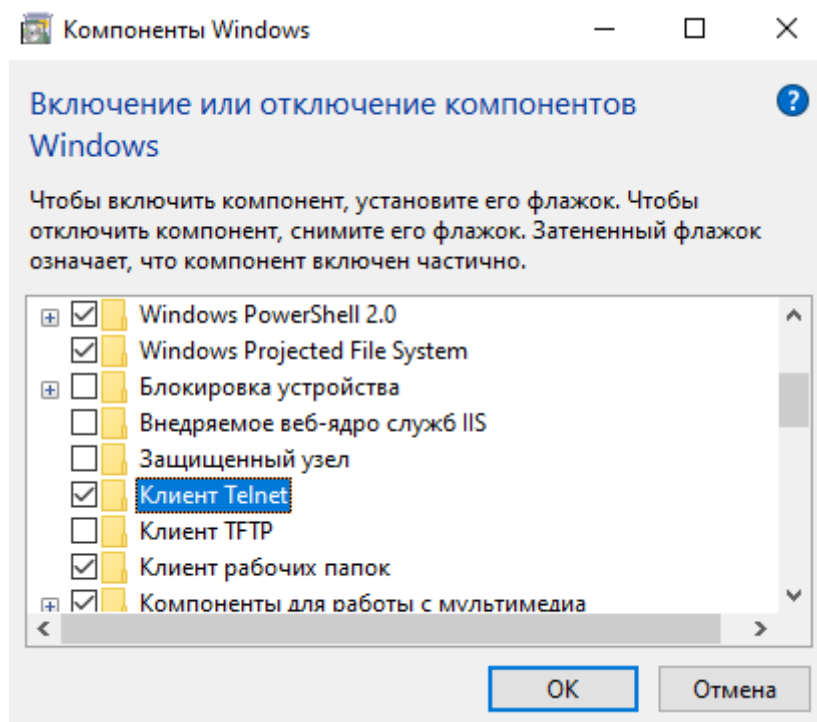


Рисунок 3 – Компоненты Windows

На сервере включаем анализ сетевого трафика с фильтрацией:

– `sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log` ("-l": вывод в реальном времени, "-v": подробный формат вывода, "-nn": отключение разрешения имен хостов и служб, tcp: фильтрация только трафика TCP, src port 23 or dst port 23: анализ трафика с исходным или целевым портом 23, tee telnet.log: запись вывода команды в файл telnet.log).

На хостовой машине подключаемся к серверу через Telnet:

– `telnet <IP адрес>`

Успешное подключение к серверу через Telnet представлено на рисунке 4.

```
Telnet 188.130.154.70

Linux 6.1.0-21-amd64 (labs.novalocal) (pts/2)
labs login: user
Password:
Linux labs 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jan  2 21:35:19 UTC 2025 from 176.212.149.64 on pts/0
user@labs:~$ ps
  PID TTY          TIME CMD
 1352 pts/2    00:00:00 bash
 1357 pts/2    00:00:00 ps
user@labs:~$
user@labs:~$
```

```
user@labs: ~
502, length 1
21:43:14.022455 IP (tos 0x70, ttl 120, id 17078, offset 0, flags [DF], proto TCP (6), length 40)
176.212.149.64.53270 > 188.130.154.70.23: Flags [.], cksum 0x3298 (correct), ack 656, win 510, length 0
21:43:16.059573 IP (tos 0x70, ttl 120, id 17080, offset 0, flags [DF], proto TCP (6), length 42)
176.212.149.64.53270 > 188.130.154.70.23: Flags [P.], cksum 0x2584 (correct), seq 107:109, ack 656, win 5
2
21:43:16.059894 IP (tos 0x0, ttl 64, id 34083, offset 0, flags [DF], proto TCP (6), length 42)
188.130.154.70.23 > 176.212.149.64.53270: Flags [P.], cksum 0x9cfa (incorrect -> 0x258a), seq 656:658, ac
502, length 2
21:43:16.135619 IP (tos 0x70, ttl 120, id 17081, offset 0, flags [DF], proto TCP (6), length 40)
176.212.149.64.53270 > 188.130.154.70.23: Flags [.], cksum 0x3294 (correct), ack 658, win 510, length 0
21:43:16.135686 IP (tos 0x0, ttl 64, id 34084, offset 0, flags [DF], proto TCP (6), length 197)
188.130.154.70.23 > 176.212.149.64.53270: Flags [P.], cksum 0x9d95 (incorrect -> 0x8665), seq 658:815, ac
502, length 157
21:43:16.214038 IP (tos 0x70, ttl 120, id 17083, offset 0, flags [DF], proto TCP (6), length 40)
176.212.149.64.53270 > 188.130.154.70.23: Flags [.], cksum 0x31f8 (correct), ack 815, win 509, length 0
```

Рисунок 4 – Подключение к серверу через Telnet

Для разрыва соединения на хостовой машине необходимо прописать exit.

Пакеты инициализации и завершения сессии представлены на рисунке 5.

```
user@labs:~$ cat telnet.log | grep -P '\[[SF].*\]' telnet.log
cat: 176.212.149.64.53270 > 188.130.154.70.23: Flags [S], cksum 0xe34d (incorrect -> 0xe3e5), seq 1459604686, win 64240, options [mss 1300,nop,wscale 8,nop,nop,sackOK], length 0
telnet.log: No such file or directory
176.212.149.64.53270 > 188.130.154.70.23: Flags [S], cksum 0xe34d (incorrect -> 0xe3e5), seq 1459604686, win 64240, options [mss 1300,nop,wscale 8,nop,nop,sackOK], length 0
188.130.154.70.23 > 176.212.149.64.53270: Flags [S.], cksum 0x9d04 (incorrect -> 0xfbc9), seq 1539935136, ack 1459604687, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
188.130.154.70.23 > 176.212.149.64.53270: Flags [FP.], cksum 0x9d0a (incorrect -> 0x0f34), seq 841:859, ack 124, win 502, length 18
176.212.149.64.53270 > 188.130.154.70.23: Flags [F.], cksum 0x31bb (correct), seq 124, ack 860, win 509, length 0
```

Рисунок 5 – Пакеты инициализации и завершения сессии

## Подключение через SSH

На сервере включаем анализ сетевого трафика с фильтрацией:

– `sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log`

(порт 22 – используется для SSH).

Подключимся к серверу через ssh:

– `ssh <пользователь>@<ip адрес>`

Успешное подключение к серверу через SSH представлено на рисунке 6.

```
Connection to 188.130.154.70 closed.
PS C:\Users\SP> ssh user@188.130.154.70
user@188.130.154.70's password:
Linux labs 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jan  2 21:46:07 2025 from 176.212.149.64
user@labs:~$ uname -a
Linux labs 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64 GNU/Linux
user@labs:~$
```

Рисунок 6 – Подключение к серверу через SSH

Чтобы передать файл по ssh, необходимо воспользоваться командой `scp`:

– `scp <путь к файлу> <пользователь>@<ip адрес>:<путь на сервере>`.

Пример передачи файла представлен на рисунке 7.

```
PS C:\Users\SP> scp C:\Users\SP\Desktop\test.txt user@188.130.154.70:/home/user
user@188.130.154.70's password:
test.txt
PS C:\Users\SP>
```

Рисунок 7 – Передача файла через ssh

```
user@labs:~$ ls -l
total 4724
drwxr-xr-x 3 user user 4096 Dec 23 00:20 env
drwxr-xr-x 5 user user 4096 Dec 30 14:26 lb
-rwxr-xr-x 1 user user 19136 Dec 13 21:36 lb3
-rw-r--r-- 1 user user 4771369 Jan  2 21:51 ssh.log
-rw-r--r-- 1 user user 30250 Jan  2 21:45 telnet.log
drwxr-xr-x 3 user user 4096 Dec 12 18:39 test
user@labs:~$ ls -l
total 15828
drwxr-xr-x 3 user user 4096 Dec 23 00:20 env
drwxr-xr-x 5 user user 4096 Dec 30 14:26 lb
-rwxr-xr-x 1 user user 19136 Dec 13 21:36 lb3
-rw-r--r-- 1 user user 16142313 Jan  2 22:00 ssh.log
-rw-r--r-- 1 user user 30250 Jan  2 21:45 telnet.log
drwxr-xr-x 3 user user 4096 Dec 12 18:39 test
-rw-r--r-- 1 user user 0 Jan  2 22:00 test.txt
user@labs:~$
```

Рисунок 8 – Проверка файла на сервере



Настроим подключение по ssh через SSH-ключи. Для этого создадим папку .ssh (задать права 700 – все права для владельца) и файл authorized\_keys (задать права 600 – только владелец может читать и записывать файл) на сервере. Пример создания представлен на рисунке 9.

```
user@labs:~$ mkdir .ssh
user@labs:~$ chmod 700 /home/user/.ssh
user@labs:~$ touch /home/user/.ssh/authorized_keys
user@labs:~$ chmod 600 /home/user/.ssh/authorized_keys
```

Рисунок 9 – Создание папки и файла

Командой ssh-keygen сгенерируем ssh ключ на хостовой машине (рисунок 10).

```
PS C:\Users\SP\.ssh> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\SP\.ssh/id_ed25519): lab
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in lab
Your public key has been saved in lab.pub
The key fingerprint is:
SHA256:5No4h9e4z8b4xaLA0NvA3rLt1nTcwh19EFZmRKB0XOQ sp@DESKTOP-8S3LTDL
The key's randomart image is:
+--[ED25519 256]--+
|      ..=00      |
|      . +o+      |
|      . .. .E     |
|    o o . . .    |
|  . + So + .     |
|  + X.o*..       |
|    @.B=o.o      |
|    O++oo        |
|    .o=++        |
+-----[SHA256]-----+
PS C:\Users\SP\.ssh> ls

Каталог: C:\Users\SP\.ssh

Mode                LastWriteTime         Length Name
----                -
-a----             09.12.2024    21:28           464 banana
-a----             09.12.2024    21:28           101 banana.pub
-a----            24.12.2024     2:43          1775 known_hosts
-a----            12.12.2024    18:08           937 known_hosts.old
-a----            03.01.2025     1:06           411 lab
-a----            03.01.2025     1:06           101 lab.pub
-a----             09.12.2024    21:56           411 rtunnel
-a----             09.12.2024    21:56           101 rtunnel.pub
```

Рисунок 10 – Генерация ssh ключа

Скопируем ключ на сервер в папку .ssh (рисунок 11).

```
PS C:\Users\SP\.ssh> scp C:\Users\SP\.ssh\lab.pub user@188.130.154.70:/home/user/.ssh
user@188.130.154.70's password:
lab.pub                                100% 101    3.3KB/s  00:00
```

Рисунок 11 – Копирование ключа на сервер

Скопируем ключ в файл `authorized_keys` (рисунок 12).

```
user@labs:~/.ssh$ ls
authorized_keys  lab.pub
user@labs:~/.ssh$ nano lab.pub
user@labs:~/.ssh$ nano authorized_keys
user@labs:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK2axoH5lqWS1bqxaXpJXtGHLKxyaQiHfrxdp0BfBi4k sp@DESKTOP-8SJLTDL
user@labs:~/.ssh$
```

Рисунок 12 – Копирование ключа

Теперь для подключения по `ssh` можно указать путь до `ssh` ключа (через -  
i). Пример представлен на рисунке 13.

```
PS C:\Users\SP> ssh user@188.130.154.70 -i C:\Users\SP\.ssh\lab
Linux labs 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jan  2 21:51:14 2025 from 176.212.149.64
user@labs:~$
```

Рисунок 13 – Подключение через `ssh` ключ

Таким же образом можно без указания пароля скопировать файл на сервер  
(рисунок 14).

```
PS C:\Users\SP> scp -i C:\Users\SP\.ssh\lab C:\Users\SP\Desktop\test2.txt user@188.130.154.70:/home/user
test2.txt                                     100% 44    1.7KB/s   00:00
PS C:\Users\SP>
```

Рисунок 14 – Копирование файла на сервер через `ssh` ключ

```
user@labs:~$ ls -l
total 39692
drwxr-xr-x 3 user user    4096 Dec 23 00:20 env
drwxr-xr-x 5 user user    4096 Dec 30 14:26 lb
-rwxr-xr-x 1 user user   19136 Dec 13 21:36 lb3
-rw-r--r-- 1 user user 40569151 Jan  2 22:17 ssh.log
-rw-r--r-- 1 user user   30250 Jan  2 21:45 telnet.log
drwxr-xr-x 3 user user    4096 Dec 12 18:39 test
-rw-r--r-- 1 user user      0 Jan  2 22:00 test.txt
-rw-r--r-- 1 user user     44 Jan  2 22:16 test2.txt
user@labs:~$ cat test2.txt
Проверка передачи файлаuser@labs:~$
user@labs:~$
```

Рисунок 15 – Проверка файла на сервере

Чтобы избежать постоянного указания пути к ключу, создаем файл  
конфигурации `~/.ssh/config` на хостовой машине (рисунок 16).

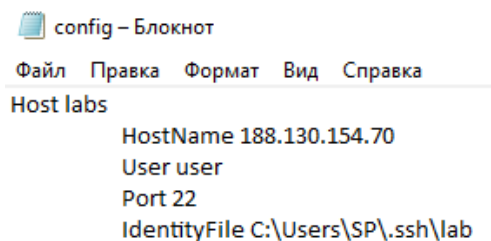


Рисунок 16 – Конфигурационный файл

Теперь можно подключиться к серверу по названию из конфига (labs).

Пример представлен на рисунке 17.

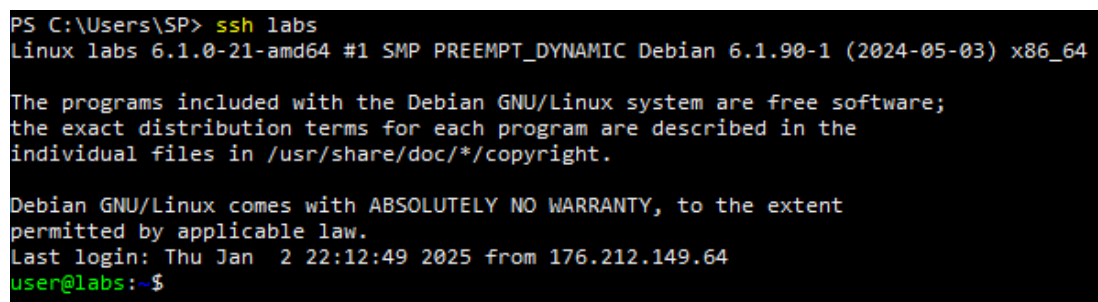


Рисунок 17 – Подключение к серверу с помощью конфига

Также можно отключить вход по паролю и запретим доступ для root. На сервере отредактируем файл конфигурации SSH: `sudo nano /etc/ssh/sshd_config` (рисунок 18).



Рисунок 18 – Отредактированные параметры

- PermitRootLogin no (запрет входа для root)
- PubkeyAuthentication yes (включение авторизации по ключам)
- PasswordAuthentication no (отключение авторизации по паролю)
- PermitEmptyPassword no (запрет входа без пароля)

Содержимое файла `ssh.log` представлено на рисунке 19.

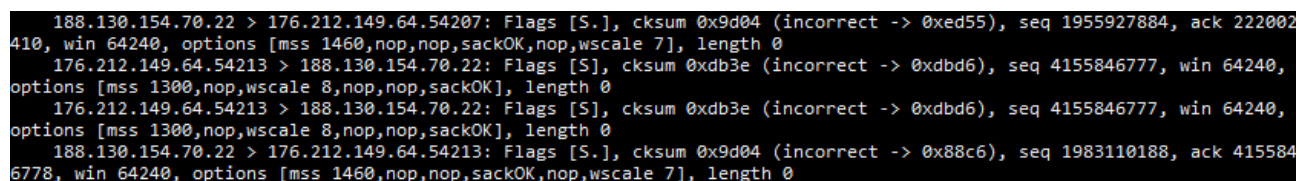


Рисунок 19 – Содержимое файла `ssh.log`

## **Вывод**

В ходе выполнения лабораторной работы было выполнено практическое ознакомление с программным обеспечением для удаленного доступа к распределенным системам обработки данных.

## Контрольные вопросы

1. Определите основные цели и задачи решаемые с помощью ПО удаленного доступа?

– удаленное управление устройствами: позволяет администраторам и пользователям управлять удаленными компьютерами, серверами или устройствами.

– мониторинг и устранение проблем: используется для быстрого выявления и устранения неисправностей в сети или на устройствах.

– управление файлами: доступ к удаленным файлам, их редактирование и перемещение.

– снижение затрат на обслуживание: устраняет необходимость физического присутствия для обслуживания оборудования.

– поддержка пользователей: обеспечивает техническую помощь и консультации удаленно.

2. Выделите отличительные особенности между режимами работы удаленного доступа по протоколам Telnet и SSH?

Критерий	Telnet	SSH
Безопасность	Данные передаются в открытом виде.	Использует шифрование для защиты данных.
Протокол	Не использует шифрование.	Применяет асимметричное шифрование (RSA).
Аутентификация	Простая аутентификация (логин и пароль).	Поддерживает ключи и пароли.
Применение	Подходит для локальных сетей.	Используется в публичных и защищенных сетях.

3. Опишите способы установления соединения при использовании протокола SSH? Охарактеризуйте положительные и отрицательные аспекты приведенных методов.

– Аутентификация с использованием пароля.

Преимущества: Простота настройки.

Недостатки: Уязвимость при переборе паролей (brute-force).

– Аутентификация с помощью SSH-ключей (генерация пары ключей (закрытого и открытого), где открытый ключ размещается на сервере).

Преимущества: высокая безопасность, исключение необходимости ввода пароля.

Недостатки: требуется предварительная настройка, потеря закрытого ключа может привести к блокировке доступа.

– Аутентификация на основе сертификатов (используются сертификаты для идентификации клиента).

Преимущества: дополнительный уровень безопасности.

Недостатки: сложность настройки.

4. Основываясь на заданиях лабораторной работы, приведите практический пример использования систем удаленного доступа?

Администратор IT компании использует SSH для управления сервером базы данных, расположенным в удаленном дата-центре:

1) Подключается к серверу через SSH.

2) Выполняет обновление системы или устраняет сбой в работе базы данных.

5. Перечислите распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH? Приведите пример использования службы передачи файлов по безопасному туннелю?

SCP (Secure Copy Protocol): используется для безопасной передачи файлов между устройствами (копирование конфигурационного файла с сервера на локальный компьютер).

SFTP (Secure File Transfer Protocol): обеспечивает безопасную передачу файлов с использованием шифрованного соединения (загрузка резервных копий данных на удаленный сервер).

SSH Tunneling: создает защищенные туннели для передачи данных между клиентом и сервером (прокси-сервер для обхода ограничений в сети).

Git по SSH: безопасный доступ к репозиториям для разработчиков (работа с удаленными репозиториями Git через SSH).