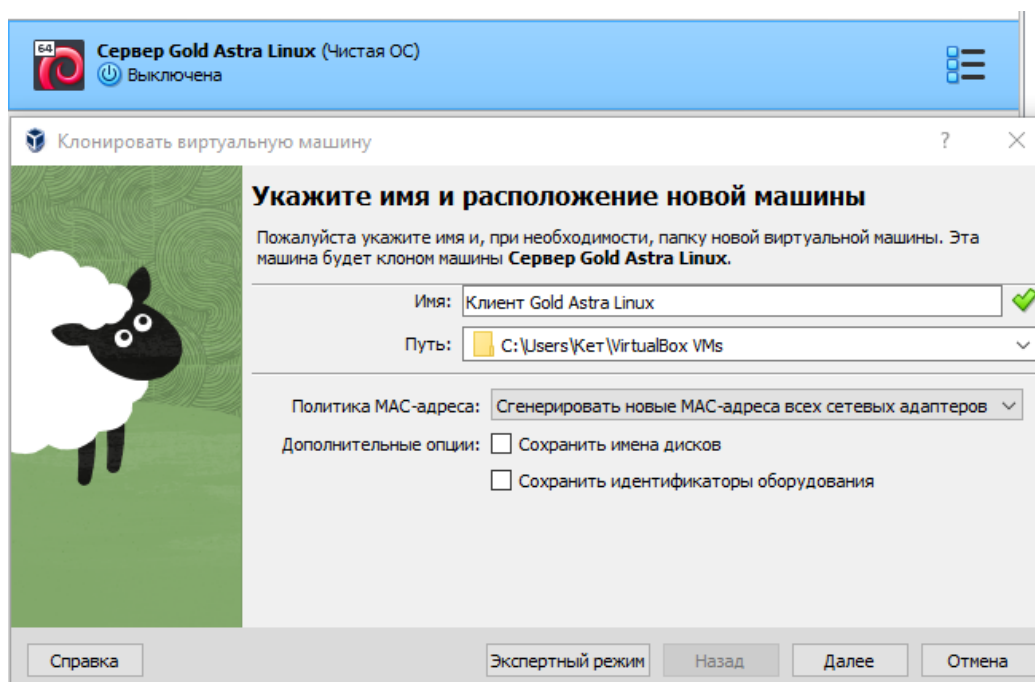


ДИСЦИПЛИНА НАСТРОЙКА СЕТЕВЫХ СЕРВИСОВ  
ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАТИКИ  
КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ  
ВИД УЧЕБНОГО МАТЕРИАЛА ПРАКТИКА  
ПРЕПОДАВАТЕЛЬ ЗАБОТКИНА ЕКАТЕРИНА МИХАЙЛОВНА  
СЕМЕСТР СЕДЬМОЙ, 2024/2025

## Практическая работа № 9. Настройка удаленного доступа по SSH

### 0. Клонирование ВМ

Сделайте клонирование вашей ВМ. Старую ВМ переименуйте в «Сервер Gold Astra Linux», а новую назовите – «Клиент Gold Astra Linux».



Далее выберите «Полное клонирование», цель клонирования – «Все». После этого нажмите на кнопку «Готово».

### 1. Настройка службы SSH

Предварительно через графическую утилиту необходимо задать IP-адресацию для проводного соединения 1 (тип подключения «Внутренняя сеть»):

Сервер: IP-адрес и маска – 192.168.1.10/24.

Клиент: IP-адрес и маска – 192.168.1.20/24.

Далее идет пример настройки IP-адреса на сервере. Важно: необходимо выбрать метод «Вручную».

Имя соединения: Проводное соединение 1

Основное Ethernet Безопасность 802.1x DCB Прокси **Параметры IPv4** Параметры IPv6

Метод: Вручную

**Адреса**

| Адрес        | Маска сети | Шлюз |                                        |
|--------------|------------|------|----------------------------------------|
| 192.168.1.10 | 24         |      | <div>Добавить</div> <div>Удалить</div> |

Серверы DNS:

Поисковый домен:

ID клиента DHCP:

☐ Требовать адресацию IPv4 для этого соединения

Маршруты...

1.1. Установите службу `ssh` на клиенте и сервере.

```
sudo apt install ssh
```

1.2. Сгенерируйте ключи SSH на клиенте и сервере. Пароль и место хранения ключа можно не задавать.

```
ssh-keygen
```

1.3. Загрузите ключ с клиента на сервер.

```
ssh-copy-id sa@192.168.1.10
```

Примечание: утилита подключится к удаленному серверу, а затем использует содержимое ключа `id_rsa.pub` для загрузки его на сервер в файл `~/.ssh/authorized_keys`. Дальше вы можете выполнять аутентификацию с помощью этого ключа.

Если такой способ по какой-либо причине для вас не работает, вы можете скопировать ключ по SSH вручную. Здесь создается каталог `~/.ssh`, а затем помещается ключ в файл `authorized_keys` с помощью символа `>>`, это позволит не перезаписывать существующие ключи:

```
cat ~/.ssh/id_rsa.pub | ssh username@remote_host "mkdir -p
~/.ssh && cat >>
~/.ssh/authorized_keys"
```

1.4. На сервере посмотрите содержимое файла ~/.ssh/authorized\_keys.

```
cat ~/.ssh/authorized_keys
```

1.5. На клиенте посмотрите содержимое файла ~/.ssh/id\_rsa.pub. Убедитесь в том, что значение ключей на сервере и клиенте совпадают.

```
cat ~/.ssh/id_rsa.pub
```

1.6. Подключитесь с клиента на сервер по SSH.

```
ssh sa@192.168.1.10
```

Примечание: если вы не захотели создать SSH ключ с доступом по паролю, то вы сразу же будете авторизованы, что очень удобно. Иначе, сначала придется ввести фразу-пароль для расшифровки ключа. Для выхода в сессию клиента можно ввести `exit`.

1.7. Изучите конфигурационный файл SSH-сервера. Какой порт SSH используется для подключения к серверу?

```
cat /etc/ssh/sshd_config
```

1.8. Измените порт по умолчанию на значение 2222 и уберите значок комментария (решетка #).

```
sudo nano /etc/ssh/sshd_config
```

```
Port 2222
```

1.9. Перезапустите службу ssh и посмотрите ее статус.

```
sudo systemctl restart ssh
```

```
sudo systemctl status ssh
```

1.10. Подключитесь с клиента на сервер по SSH с использованием порта 2222.

```
ssh -p 2222 sa@192.168.1.10
```

## **2. Безопасное копирование файлов**

2.1. Скопируйте файл и директорию с клиента на сервер. Для этого на клиенте:

```
touch file_for_scp
```

```
scp -P 2222 file_for_scp sa@192.168.1.10:~/
```

```
mkdir dir_for_scp && cp file_for_scp dir_for_scp
```

```
scp -P 2222 -r dir_for_scp sa@192.168.1.10:~/
```

2.2. Проверьте, что файл и директория были скопированы на сервер. Для этого на сервере:

```
ls -l
```