

## Практическая работа №20

### «Настройка удаленного доступа к компьютеру»

**Цель работы:** изучить технологии удаленного доступа (RDP, TeamViewer, VNC, SSH); освоить настройку и подключение к удаленному рабочему столу в ОС Windows; получить навыки безопасной организации удаленного доступа в локальной сети и через Интернет.

**Оборудование:** два ПК с ОС Windows (или один ПК и виртуальная машина), подключение к локальной сети, доступ в Интернет.

**Время выполнения:** 90 минут.

### ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. С разрешения преподавателя включите компьютеры, дождитесь завершения загрузки операционной системы Windows на обоих ПК (или запустите виртуальную машину).

2. **Определите сетевые параметры обоих компьютеров:**

- На каждом ПК откройте командную строку (Win+R → cmd).
- Выполните команду: ipconfig
- Запишите IP-адреса обоих компьютеров (например, ПК1 — 192.168.1.100, ПК2 — 192.168.1.101).
- Убедитесь, что компьютеры «видят» друг друга (выполните ping с одного ПК на другой).

Сделайте **screenshot** окна командной строки с результатами ping и вставьте в отчет.

3. **Настройка удаленного рабочего стола (RDP) в Windows:**

- (a) На ПК1 (к которому будем подключаться) откройте: **Панель управления → Система и безопасность → Система → Дополнительные параметры системы**.
- (b) Перейдите на вкладку **Удаленный доступ**.
- (c) Установите переключатель в положение: **«Разрешать удаленные подключения к этому компьютеру»**.
- (d) Снимите галочку **«Разрешать подключения только с компьютеров, работающих под управлением удаленного рабочего стола с проверкой подлинности на уровне сети»** (для совместимости).
- (e) Нажмите **«Выбрать пользователей»** и добавьте пользователя, которому разрешен удаленный доступ (например, Администратор или текущего пользователя).
- (f) Запомните имя компьютера (оно отображается там же).

Сделайте скриншот окна настроек удаленного доступа и вставьте в отчет.

4. **Подключение к удаленному рабочему столу:**

- (a) На ПК2 откройте приложение **«Подключение к удаленному рабочему столу»** (Пуск → mstsc или введите в поиске).
- (b) В поле **«Компьютер»** введите IP-адрес ПК1 (например, 192.168.1.100).

- (с) Нажмите **«Подключить»**.
- (d) Введите имя пользователя и пароль от учетной записи на ПК1.
- (е) При предупреждении о сертификате нажмите **«Да»**.

Вы должны увидеть рабочий стол удаленного компьютера. Сделайте скриншот окна с удаленным рабочим столом (на ПК2 отображается рабочий стол ПК1).

#### 5. **Настройка альтернативного способа удаленного доступа — TeamViewer (или аналог):**

- (a) Скачайте TeamViewer (QuickSupport версию) с официального сайта на оба ПК (или используйте портативную версию).
- (b) На ПК1 запустите TeamViewer, запишите **ID** и **пароль**, который сгенерировала программа.
- (с) На ПК2 запустите TeamViewer, в поле «ID партнера» введите ID ПК1, нажмите «Подключиться».
- (d) Введите пароль, который отображается на ПК1.
- (е) После подключения вы увидите удаленный экран ПК1 в окне TeamViewer.

Сделайте скриншот окна TeamViewer с активным сеансом удаленного управления.

#### 6. **Настройка удаленного доступа через SSH (для Linux или Windows с OpenSSH):**

- Если доступен компьютер с Linux или в Windows включен компонент OpenSSH Server, выполните:
- На сервере: `sudo apt install openssh-server` (Linux) или установка через «Дополнительные компоненты» в Windows.
- На клиенте выполните подключение: `ssh пользователь@IP-адрес`
- Сделайте скриншот окна терминала с успешным подключением по SSH.

#### 7. **Настройка сетевого экрана (брандмауэра) для удаленного доступа:**

- (a) Откройте **Панель управления → Брандмауэр Windows → Разрешить приложение**.
- (b) Убедитесь, что в списке разрешенных есть **«Удаленный рабочий стол»** (для частной и доменной сети).
- (с) При необходимости добавьте правило для порта 3389 (TCP) вручную.

#### 8. **Подключение через Интернет (при наличии внешнего IP или настройки проброса портов):**

- Если ваш роутер поддерживает проброс портов (port forwarding), настройте перенаправление внешнего порта 3389 на внутренний IP-адрес ПК1 (порт 3389).
- С внешнего компьютера подключитесь по `внешний_IP:3389` через mstsc.
- **Внимание!** Для безопасности после выполнения работы отключите проброс портов.

#### 9. **Дополнительное задание:** Настройте автоматическое подключение к удаленному рабочему столу с сохранением пароля (.rdp-файл):

- В mstsc введите параметры, нажмите "Сохранить как".
- Откройте сохраненный .rdp-файл в блокноте, найдите строку "username:s:..."
- Добавьте параметр "password 51:b:зашифрованный\_пароль" (или используйте Credential Manager).

## 10. Завершение работы:

- Завершите все сеансы удаленного доступа.
- Отключите разрешение на удаленные подключения в настройках системы (если это не требуется далее).
- Сохраните отчет в своей папке на сервере или распечатайте на сетевом принтере.
- Покажите выполненную работу преподавателю.

## СПРАВОЧНЫЕ СВЕДЕНИЯ

### Используемые порты:

- RDP (Remote Desktop Protocol) — порт TCP 3389.
- TeamViewer — использует динамические порты (80, 443, 5938 и др.).
- SSH — порт TCP 22.
- VNC — порт TCP 5900.

### Команды для проверки удаленного доступа:

```
netstat -an | findstr "3389" # проверка, слушает ли компьютер порт RDP
telnet IP-адрес 3389 # проверка доступности порта (если telnet включен)
Test-NetConnection IP-адрес -Port 3389 # PowerShell
```

## КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие протоколы используются для удаленного доступа? Назовите основные различия между RDP, VNC и SSH.
2. Какой порт используется по умолчанию для службы удаленного рабочего стола Windows (RDP)?
3. Какие меры безопасности необходимо соблюдать при организации удаленного доступа через Интернет?
4. В чем отличие между TeamViewer и встроенным RDP?
5. Как разрешить удаленные подключения к компьютеру в ОС Windows?
6. Что такое проброс портов (port forwarding) и зачем он нужен?
7. Как проверить, активен ли удаленный рабочий стол на компьютере, не подключаясь к нему?
8. Какие права должен иметь пользователь для подключения по RDP?