**Федеральное государственное образовательное бюджетное учреждение  
высшего образования   
«Финансовый университет при Правительстве РФ»**

**КОЛЛЕДЖ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ**

Практическая работа № 11

по дисциплине Инфокоммуникационные системы и сети

Выполнил студент

Батхиев А.Б.

Группа 3ПКС-220

Проверил: Сибирев И.В.

\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

оценка подпись

Москва, 2023

Цель работы: разобраться в RDP.

RDP (Remote Desktop Protocol) — протокол подключения пользователя к удаленному рабочему столу через сервер терминалов.

Технология появилась в 90-х годах и до сих пор используется. Разработка полностью проприетарна, поставляется только в операционных системах семейства Windows. Однако подключаться можно и через другие ОС при помощи сторонних приложений.

Режим подключений

RDP используют в 3 режимах:

1. Подключение через протокол к серверной ОС для настройки или управления. Это связано с тем, что Windows Server поддерживает параллельно два удаленных подключения и один локальный вход, а рабочие станции – только один вариант.
2. RDP служит транспортом для соединения с терминальным сервером. Такой режим доступен только для серверных ОС. Количество подключений безлимитное, но потребуется установка сервера лицензий.
3. Подключение к рабочей станции. Пользователь, используя RDP, соединяется со своим офисным либо домашним компьютером для дальнейшей работы.

Если требуется установить соединение между ОС семейства Windows и Linux, то для второй используют приложения, которые поддерживают работу с протоколом RDP, например, Remmina, Rdesktop, Vinagre и др.

Принцип работы

Принцип работы RDP базируется на протоколе TCP. Соединение клиент-сервер происходит на транспортном уровне. После инициализации пользователь проходит аутентификацию. В случае успешного подтверждения сервер передает клиенту управление.

Протокол RDP внутри себя поддерживает виртуальные каналы, через которые пользователю передаются дополнительные функции операционной системы, например, можно распечатать документ, воспроизвести видео или скопировать файл в буфер обмена.

Безопасность

Технология обеспечивает безопасность подключения двумя способами. В первом используется внутренняя подсистема (Standard RDP Security). На удаленной машине генерируется пара ключей RSA и сертификат открытого ключа, который подписывается одним из них.

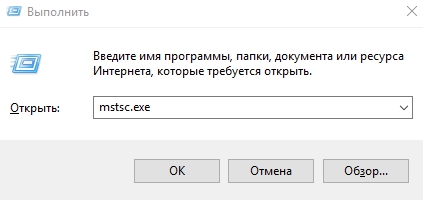
Во время подключения клиент получает подписанный сертификат и открытый ключ, который используется для выбора технологии шифрования данных. Длина ключа шифрования зависит от версии операционной системы, в старых версиях Windows Server 2008 значение составляло 168 бит. Авторизация происходит после подтверждения сертификата и ввода пароля.

Второй способ предлагает использовать внешние средства обеспечения безопасности (Enhanced RDP Security). В качестве примера расскажем про протокол TLS. Во время инициализации подключения он шифрует соединение и проверяет разрешение пользователя на вход. Такой подход снижает нагрузку на терминальный сервер при большом количестве одновременных подключений. Принцип работы аналогичен первому варианту. Как правило, крупные компании используют второй вариант, а небольшие – первый.

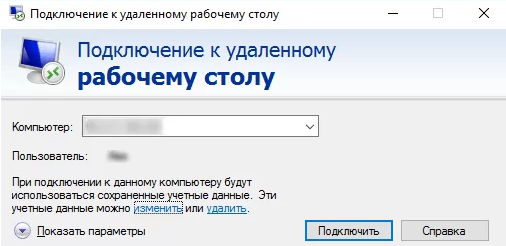
Протокол RDP используется для удаленного подключения только в среде Windows. Соединение полностью безопасно, так как использует шифрование и процедуру аутентификации пользователей. Для других операционных систем существует специальное ПО, которое поддерживает работу с RDP.

Рассмотрим пример подключения к серверу по RDP

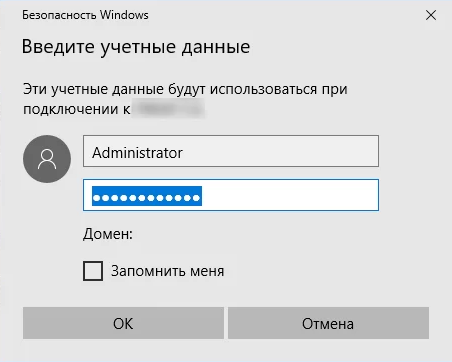
1. Для подключения необходимо знать IP-адрес и данные доступа администратора (логин/пароль) сервера, к которому мы будем подключаться.
2. Используем стандартную программу от Windows «Подключение к удаленному рабочему столу», набираем сочетание клавиш «Win+R» и вводим в поле команду «mstsc», затем нажимаем «ОК».



1. В открывшемся окне вводим IP-адрес сервера.



1. Затем вводим данные доступа администратора из панели управления сервером.



Вывод: разобрался в протоколе RDP.