Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По лабораторной работе №11**

Студент: Демьянов Артём Сергеевич

Дисциплина/Профессиональный модуль: Инфокоммуникационные системы и сети

Группа: 3ПКС-220

Вариант: 10

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2023г.**

**Лабораторная работа №11**

**Описание протокола RDP**

**Цель работы:** ознакомиться с протоколом удаленного рабочего стола RDP.

**Задание:** дать описание протоколу и рассказать о его подключении

**Выполнение работы:**

Протокол Удаленный рабочий стол (Майкрософт) (RDP) предоставляет возможности удаленного отображения и ввода через сетевые подключения для приложений на основе Windows, работающих на сервере. Протокол RDP предназначен для поддержки различных типов сетевых топологий и нескольких протоколов локальной сети.

Протоколы RDP основаны на семействе протоколов ITU T.120. RDP — это протокол с поддержкой нескольких каналов, который позволяет использовать отдельные виртуальные каналы для передачи данных об обмене данными об устройстве и презентации с сервера, а также зашифрованных данных клиентской мыши и клавиатуры. RDP предоставляет расширяемую базу и поддерживает до 64 000 отдельных каналов для передачи данных и подготовки для многоточечных передач.

RDP многие считают небезопасным способом удаленного доступа по сравнению с использованием [специальных программ](https://www.comss.ru/list.php?c=remote_access), таких как [RAdmin](https://www.osp.ru/lan/2015/11/13047560/), TeamViewer, VNC и пр. Другой предрассудок – большой трафик RDP. Однако на сегодня RDP не менее безопасен, чем любое другое решение для удаленного доступа, а с помощью настроек можно добиться высокой скорости реакции и небольшой потребности в полосе пропускания.

**Защита RDP и настройка его производительности**

|  |  |
| --- | --- |
| Шифрование и безопасность | Нужно открыть gpedit.msc, в «Конфигурация компьютера — Административные шаблоны — Компоненты Windows — Службы удаленных рабочих столов — Безопасность» задать параметр «Требовать использования специального уровня безопасности для удаленных подключений по методу RDP» и в «Уровень безопасности» выбрать «SSL TLS». В «Установить уровень шифрования для клиентских подключений» выберите «Высокий». Чтобы включить использование FIPS 140-1, нужно зайти в «Конфигурация компьютера — Конфигурация Windows — Параметры безопасности — Локальные политики — Параметры безопасности» и выбрать «Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания». Параметр «Конфигурация компьютера — Параметры Windows — Параметры безопасности — Локальные политики — Параметры безопасности» параметр «Учетные записи: разрешать использование пустых паролей только при консольном входе» должен быть включен. Проверьте список пользователей, которые могут подключаться по RDP. |
| Оптимизация | Откройте «Конфигурация компьютера — Административные шаблоны — Компоненты Windows — Службы удаленных рабочих столов — Среда удаленных сеансов». В «Наибольшая глубина цвета» выберите 16 бит, этого достаточно. Снимите флажок «Принудительная отмена фонового рисунка удаленного рабочего стола». В «Задание алгоритма сжатия RDP» установите «Оптимизация использования полосы пропускания. В «Оптимизировать визуальные эффекты для сеансов служб удаленных рабочих столов» установите значение «Текст». Отключите «Сглаживание шрифтов». |

**Подключение к удаленному рабочему столу**

Для [подключения по RDP](http://www.dprotricks.com/remote-desktop-access-computer-remotely/) необходимо, на удаленном компьютере была учетная запись с паролем, в системе должны быть разрешены удаленные подключения, а чтобы не менять данные доступа при постоянно меняющемся динамическом IP-адресе, в [настройках сети](http://spvcomp.com/stat/rdp_nastroit_udaalennij_rabochij_stol.php) можно присвоить статический IP-адрес. Удаленный доступ возможен только на компьютерах с Windows Pro, Enterprise или Ultimate.

Для удаленного подключения к компьютеру нужно разрешить подключение в «Свойствах Системы» и задать пароль для текущего пользователя, либо создать для RDP нового пользователя. Пользователи обычных аккаунтов не имеют права самостоятельно предоставлять компьютер для удаленного управления. Такое право им может дать администратор. Препятствием использования протокола RDP может стать его блокировка антивирусами. В таком случае RDP нужно разрешить в настройках антивирусных программ.

При подключении к удаленному рабочему столу через командную строку (MSTSC) можно задать дополнительные параметры RDP:

|  |  |
| --- | --- |
| Параметр | Значение |
| /v:<сервер[: порт]> | Удаленный компьютер, к которому выполняется подключение. |
| /admin | Подключение к сеансу для администрирования сервера. |
| /edit | Редактирование RDP-файла. |
| /f | Запуск удаленного рабочего стола на полном экране. |
| /w:<ширина> | Ширина окна удаленного рабочего стола. |
| /h:<высота> | Высота окна удаленного рабочего стола. |
| /public | Запуск удаленного рабочего стола в общем режиме. |
| /span | Сопоставление ширины и высоты удаленного рабочего стола с локальным виртуальным рабочим столом и развертывание на несколько мониторов. |
| /multimon | Настраивает размещение мониторов сеанса RDP в соответствии с текущей конфигурацией на стороне клиента. |
| /migrate | Миграция файлов подключения прежних версий в новые RDP-файлы. |