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: Гладков Артемий Ильич

Дисциплина/Профессиональный модуль: Инфокоммуникационные системы и сети

Группы: 3ПКС-120

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2023г.**

**Цель работы:** Ознакомиться с программным обеспечением для удаленного доступа к машине. RDP – Разобрать

**Ход работы:**

**История создания RDP**

Протокол Remote Desktop – детище разработчика софта Microsoft. Он изначально был практически единственным способом удаленного доступа к удаленным хостам или к рабочим местам с ПК администратора. Было еще одно предназначение: подключение к ресурсам более мощного сервера со слабых локальных машин (например, для сложных вычислений). Сегодня протокол RDP – это скорее инструмент для организации удаленных рабочих мест.

Подробнее об истории развития системы:

1. Впервые протокол стали применять в 1998 году, соответствующую утилиту интегрировали в Windows NT 4.0 Terminal Server.
2. Программное обеспечение для поддержки RDP Майкрософт продолжает использоваться во всех серверных и настольных системах вплоть до Windows 11/22 Server.
3. Протокол RDP, несмотря наличие других технологий вроде VNC, остается в Виндовс базовым вариантом доступа к удаленным хостам.

Клиенты существуют практически для всех операционных систем - Linux, FreeBSD, macOS, iOS, Android, Symbian. На сегодняшний день существует версия RDP 10, хотя существующий софт поддерживает и предыдущие релизы. В новых появляются дополнительные функции, например, AutoSize масштабирование, улучшения сжатия графики с использованием кодека H.264/AVC.

Общие характеристики протокола:

1. Поддерживаются 32 битные цвета и ниже (8, 15, 16, 24 бита).
2. Защита данных осуществляется со 128-битных шифрованием (алгоритм RC4).
3. Перенаправление звука, файловой системы, принтера, портов.
4. Поддержка функции буфера обмена между удаленным и локальным компьютером.

Большую роль в появлении и развитии Remote Desktop сыграл бренд Citrix Systems. Он уже в начале 90-х гг. имел специализацию в сфере методов удаленного доступа к многопользовательским системам. Специалисты этой фирмы создали сетевую систему WinFrame, основанную на Windows NT 3.51. Для этого понадобилось выкупить права на исходный код. Результат – Microsoft уже в 1997 г. заключила контакт с Citrix Systems.

Его основная часть включала использование технологий в обновленном релизе Windows NT 4.0. Попутно компании договорились о том, что Citrix не будет распространять свои продукты, а переключится на создание модулей для платформ Майкрософт. Также проговорили разграничение прав на протоколы. За Citrix сохранился ICA (Independent Computing Architecture), а за Microsoft – RDP, построенный на базе ITU T.120.

Конкуренция между Citrix и Microsoft продолжается. Первая позиционирует себя как разработчик высокопроизводительных систем, хотя в линейке продуктов есть и «облегченные» решения. Вторая со своим Terminal Services вышла вперед на рынке однотипных конфигураций на серверах средней и малой мощности. Но постоянно работает над расширением функционала системы, чтобы охватить еще и сегмент, традиционно занятый такими компаниями, как Citrix.

Преимущества Terminal Services:

* Простая установка приложений со стороны клиента.
* Обслуживание пользовательских сессий с одного рабочего места.
* Работоспособность при активной лицензии Terminal Services.

Продукты Citrix выделяет простое развертывание, доступное управление, понятная политика изменения доступа.

**Что такое RDP?**

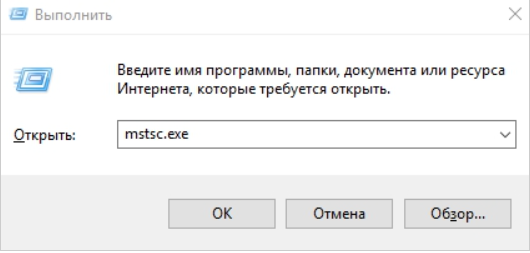
RDP (Remote Desktop Protocol) — протокол удаленного рабочего стола, предназначен для подключения и работы пользователя с удаленным сервером. На операционных системах Windows — RDP доступен из коробки.

Клиенты для подключения по RDP существуют для большинства версий Microsoft Windows (включая Windows Mobile), Linux, Unix, macOS, iOS, Android и других операционных систем. RDP-серверы встроены в операционные системы Windows; RDP-сервер для Unix и OS X также существует. По умолчанию сервер прослушивает TCP-порт 3389 и UDP-порт 3389.

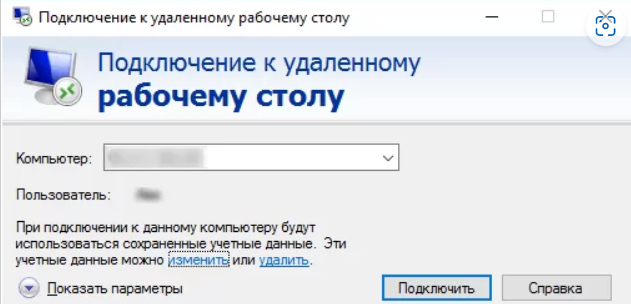
В настоящее время Microsoft называет своё официальное клиентское программное обеспечение RDP «Подключение к удалённому рабочему столу» (Remote Desktop Connection), которое ранее называлось «Клиент служб терминалов» (Terminal Services Client).

**Пример подключения к серверу по RDP**

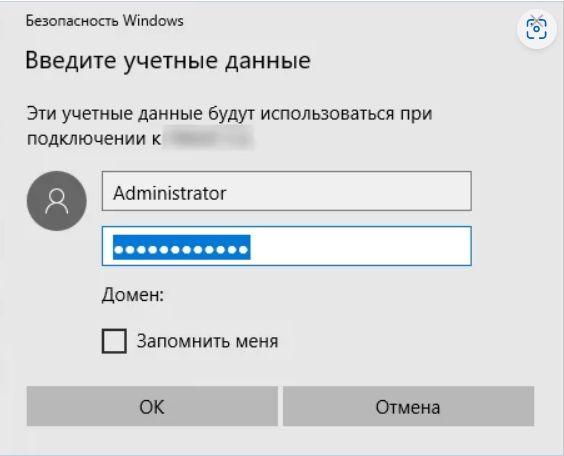
1. Для подключения необходимо знать IP-адрес и данные доступа администратора (логин/пароль) сервера, к которому мы будем подключаться.
2. Используем стандартную программу от Windows «Подключение к удаленному рабочему столу», набираем сочетание клавиш «Win+R» и вводим в поле команду «mstsc», затем нажимаем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



1. В открывшемся окне вводим IP-адрес сервера.



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



**Принцип работы RDP**

Система RDP – прикладной протокол TCP. Сначала компьютеры инициируют подключение. На транспортном уровне после подтверждения коннекта система инициализирует сессию RDP. После удачного завершения процедуры сервер терминалов включает трансляцию изображения рабочего стола и ввод с клавиатуры или мышки. Отображение возможно в виде картинки или отрисовкой графических примитивов.

Система поддерживает одновременную работу нескольких виртуальных каналов внутри одного физического соединения. Это необходимо, чтобы обеспечить работу следующих блоков:

1. Печать на принтере или обмен данными по последовательному порту.
2. Работа буфера обмена и иных операций с дисковой подсистемой.
3. Использование подсистемы воспроизведения-записи звука.

Параметры, каким должны соответствовать создаваемые виртуальные каналы, задаются в начале, еще не этапе установления коннекта с хостом. При инициировании подключения применяют два варианта организации безопасности. Это интегрированная Standard RDP Security и подключаемая Enhanced RDP Security. Рассмотрим их функционал подробнее и разберемся, какими особенностями обладает каждая.

**Standard RDP Security**

Подход к защите передаваемой информации предполагает аутентификацию, шифрация данных и мониторинг целостности за счет модулей, интегрированных в RDP. В кодировании применяют алгоритм RC4 со сложностью ключа 40-168 бит (зависит от релиза Windows). При создании коннекта система генерирует пару ключей – для шифрации информации, переданной клиентом и сервером.

Процесс аутентификации выглядит так:

1. Сначала система генерирует пару RSA-ключей.
2. Затем создает сертификат открытого ключа (Proprietary Certificate).
3. Его подписывают RSA-ключом, «зашитым» в Windows.
4. Клиенту передают Proprietary Certificate для доступа к серверу терминалов.
5. После проверки сертификата передается открытый ключ сервера.

Перечисленные действия активируются после указания аккаунта и его пароля, но только при подтверждении их корректности. Все передаваемые данные проходят проверку на целостность при помощи алгоритма MAC (Message Authentication Code). Он разработан на основе MD5 и SHA1. Есть возможность переключить систему на применение 3DES, ее поддержка появилась в Windows 2003 Server (необходима для соответствия стандарту FIPS).

**Enhanced RDP Security**

Второй вариант предполагает подключение внешних модулей – это TLS 1.0 и CredSSP. Протокол TLS появился в Windows Server с релиза 2003. Его используют, когда RDP поддерживает клиентская машина. Поэтому перед подключением желательно проверить утилиту – нужен релиз 6.0 или выше. Доступен выбор между генерацией собственного сертификата или использованием имеющегося в системе Windows.

Протокол CredSSP – это комбинированный продукт, совмещающий возможности TLS, Kerberos и NTLM. Преимущества решения:

1. Разрешение на вход проверяется до завершения коннекта по RDP, такой подход экономит мощности сервера при большом объеме запросов.
2. Шифрация и идентификация аккаунтов будет осуществляться по стандартам TLS.
3. Единовременный вход на хост работает на базе Kerberos или NTLM.

Выбрать CredSSP можно при помощи флажка Use Network Level Authentication, доступного во всех ОС начиная с Windows Vista/2008 Server.

**Порядок лицензирования Terminal Services**

Популярным способом доступа считается «тонкий клиент». Его особенность – это необходимость создания и активации сервера лицензий, без которого система функционировать не будет (возможно подключение через «толстого клиента» или к стандартному рабочему столу, но только в удаленном варианте).

Выдача лицензий осуществляется в двух режимах. Без активации пользователю дают временную лицензию на период текущей сессии или другое лимитированное время. После активации пользователю на сервере выдается «постоянная» лицензия. Процедура выглядит как предоставление цифрового сертификата, подтверждающего легитимность подключаемой рабочей машины.

Типы клиентских лицензий:

1. Temporary Terminal Server CAL – временная, ограниченная сроком функционирования.
2. Device Terminal Server CAL – с привязкой к конкретному устройству.
3. User Terminal Server CAL – привязанная к указанному в настройках пользователю.
4. External Terminal Server Connector – рассчитанная на внешние подключения.

**Подключение по RDP на macOS**

Под операционные системы macOS компания Microsoft выпустила утилиту Remote Desktop, она доступна для скачивания в магазине приложений App Store. Процесс подключения с ней такой же, как и в Windows - сначала вводится IP-адрес сервера или его домен, затем при запросе логин и пароль пользователя, которому предоставлен доступ для удаленного управления.

После запуска возможна выдача сообщения о недоверенном сертификате. Все, что требуется от пользователя, это кликнуть “Показать сертификат” и отметить опцию “Всегда доверять…” После этого система всегда будет осуществлять соединение без дополнительных вопросов.

**Подключение к удаленному рабочему столу в Ubuntu**

При подключении из Windows к удаленному хосту с установленной системой Ubuntu используют все ту же утилиту Remote Desktop. Единственное, нужно подготовить сервер — установить на него поддержку технологии:

sudo apt install xrdp

После инсталляции запустите сервис:

sudo systemctl status rdp

В обратной ситуации, когда локальная машина работает под управлением Linux, пригодится утилита Remmina. Только в ней надо поменять протокол VNC на RDP. Несмотря на разные системы пользователь работает как в «родной» среде. Также используют клиенты Linux – Gnome Connection, Vinagre, Xfreerdp, Rdesktop.

Процесс установки пакета Remmina:

sudo apt-add-repository ppa:remmina-ppa-team/remmina-next

sudo apt-get update

sudo apt-get install remmina remmina-plugin-rdp libfreerdp-plugins-standard

**Выводы**

Мы завершили рассмотрение протокола RDP, узнали, что это такое и как работает. Остается лишь добавить, что серверу лицензий можно задать одну из двух возможных ролей. Первая предполагает работу в рамках домена или рабочей группы (Domain or Workgroup License Server). Вторая – работу внутри организации (Entire Enterprise License Server).

Выбор влияет на методику сканирования сервера лицензий. В первом случае система ищет его по Active Directory, во втором – через широковещательный запрос NetBIOS (в обоих вариантах корректность будет проверяться через RPC-запрос).