МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

Отчет о выполнении практического задания

по дисциплине «МДК.01.05 Эксплуатация компьютерных сетей»

на тему «Установка и настройка сетевых протоколов. Изучение сетевых настроек ОС Windows»

Практическое задание № 4

Специальность – 10.05.02 Обеспечение информационной безопасности автоматизированных систем

Выполнил студент:

_____ Маркаров М. О.

Группа: ИБ-32

Руководитель:

_____ Герасин В. Ю.

Работа защищена с оценкой _____

Дата защиты _____

Москва

2024

Практическая работа №4

Цель: Освоить принципы настройки сетевых параметров ОС Windows.

Задачи:

1. Ознакомиться с теоретической частью;

2. Освоить принципы настройки сетевых параметров ОС Windows;

3. Оформить отчет о выполнении практической работы.

8. Ответить на контрольные вопросы;

9. Оформить отчет. Отчет должен быть оформлен в текстовом редакторе и содержать:

— наименование работы;

— цель работы;

— задание;

— последовательность выполнения работы;

— ответы на контрольные вопросы;

— вывод о проделанной работе. Контрольные вопросы:

1. Какие сетевые протоколы Вы знаете? 18

2. Какие транспортные протоколы Вы знаете?

3. Объяснить основные настройки TCP/IP;

4. Функции DHCP;

5. Что такое шлюз?

6. Назначение маски подсети?

7. Какие параметры сети могут назначаться сервером DHCP;

8. Назначение файлов hosts и lmhosts.sam;

9. Что такое MAC–адрес;

10. Что позволяет выполнять команда ipconfig?

Ход работы:

Задание 1.

```
C:\Windows\system32>netstat -an

Активные подключения

  Имя     Локальный адрес         Внешний адрес           Состояние
  TCP     0.0.0.0:135             0.0.0.0:0               LISTENING
  TCP     0.0.0.0:445             0.0.0.0:0               LISTENING
  TCP     0.0.0.0:1462            0.0.0.0:0               LISTENING
  TCP     0.0.0.0:5040            0.0.0.0:0               LISTENING
  TCP     0.0.0.0:5357            0.0.0.0:0               LISTENING
  TCP     0.0.0.0:45769           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:49664           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:49665           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:49666           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:49667           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:52653           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:59757           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:59758           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:59759           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:59760           0.0.0.0:0               LISTENING
  TCP     0.0.0.0:64248           0.0.0.0:0               LISTENING
  TCP     26.124.139.185:139      0.0.0.0:0               LISTENING
  TCP     127.0.0.1:6463          0.0.0.0:0               LISTENING
  TCP     127.0.0.1:14622         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:14622         127.0.0.1:54763         ESTABLISHED
  TCP     127.0.0.1:26822         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:27060         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:32683         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:54763         127.0.0.1:14622         ESTABLISHED
  TCP     127.0.0.1:56219         127.0.0.1:56220         ESTABLISHED
  TCP     127.0.0.1:56220         127.0.0.1:56219         ESTABLISHED
  TCP     127.0.0.1:59549         127.0.0.1:59550         ESTABLISHED
  TCP     127.0.0.1:59550         127.0.0.1:59549         ESTABLISHED
  TCP     127.0.0.1:59561         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:59561         127.0.0.1:59580         ESTABLISHED
  TCP     127.0.0.1:59580         127.0.0.1:59561         ESTABLISHED
  TCP     127.0.0.1:59658         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:59658         127.0.0.1:59685         ESTABLISHED
  TCP     127.0.0.1:59662         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:59662         127.0.0.1:59684         ESTABLISHED
  TCP     127.0.0.1:59684         127.0.0.1:59662         ESTABLISHED
  TCP     127.0.0.1:59685         127.0.0.1:59658         ESTABLISHED
  TCP     127.0.0.1:59746         127.0.0.1:65001         ESTABLISHED
  TCP     127.0.0.1:65001         0.0.0.0:0               LISTENING
  TCP     127.0.0.1:65001         127.0.0.1:59746         ESTABLISHED
  TCP     192.168.0.141:139       0.0.0.0:0               LISTENING
  TCP     192.168.0.141:57098     149.154.167.41:443      ESTABLISHED
  TCP     192.168.0.141:57998     77.88.44.55:443         ESTABLISHED
  TCP     192.168.0.141:58005     87.250.250.90:443       ESTABLISHED
  TCP     192.168.0.141:58006     77.88.44.55:443         ESTABLISHED
  TCP     192.168.0.141:58009     96.16.49.209:443        ESTABLISHED
  TCP     192.168.0.141:58010     87.245.209.201:443      ESTABLISHED
  TCP     192.168.0.141:58011     52.98.151.66:443        ESTABLISHED
  TCP     192.168.0.141:58012     20.42.65.84:443         ESTABLISHED
  TCP     192.168.0.141:58016     20.191.45.158:443       ESTABLISHED
  TCP     192.168.0.141:58017     13.107.213.254:443      ESTABLISHED
  TCP     192.168.0.141:58018     52.108.9.254:443        ESTABLISHED
  TCP     192.168.0.141:58019     13.107.246.254:443      ESTABLISHED
  TCP     192.168.0.141:58020     162.159.133.234:443     FIN_WAIT_1
  TCP     192.168.0.141:58021     204.79.197.222:443      ESTABLISHED
  TCP     192.168.0.141:58022     45.9.25.86:443          ESTABLISHED
  TCP     192.168.0.141:58023     45.9.25.86:443          ESTABLISHED
  TCP     192.168.0.141:58024     3.234.18.99:443         ESTABLISHED
  TCP     192.168.0.141:58025     20.54.232.160:443       ESTABLISHED
  TCP     192.168.0.141:58026     104.192.108.127:80      SYN_SENT
  TCP     192.168.0.141:58343     20.54.37.73:443         ESTABLISHED
  TCP     192.168.0.141:58344     20.54.37.73:443         ESTABLISHED
  TCP     192.168.0.141:58346     20.238.236.234:443      ESTABLISHED
  TCP     192.168.0.141:58347     64.233.164.188:5228     ESTABLISHED
```

Рисунок 1 использование команды netstat -an

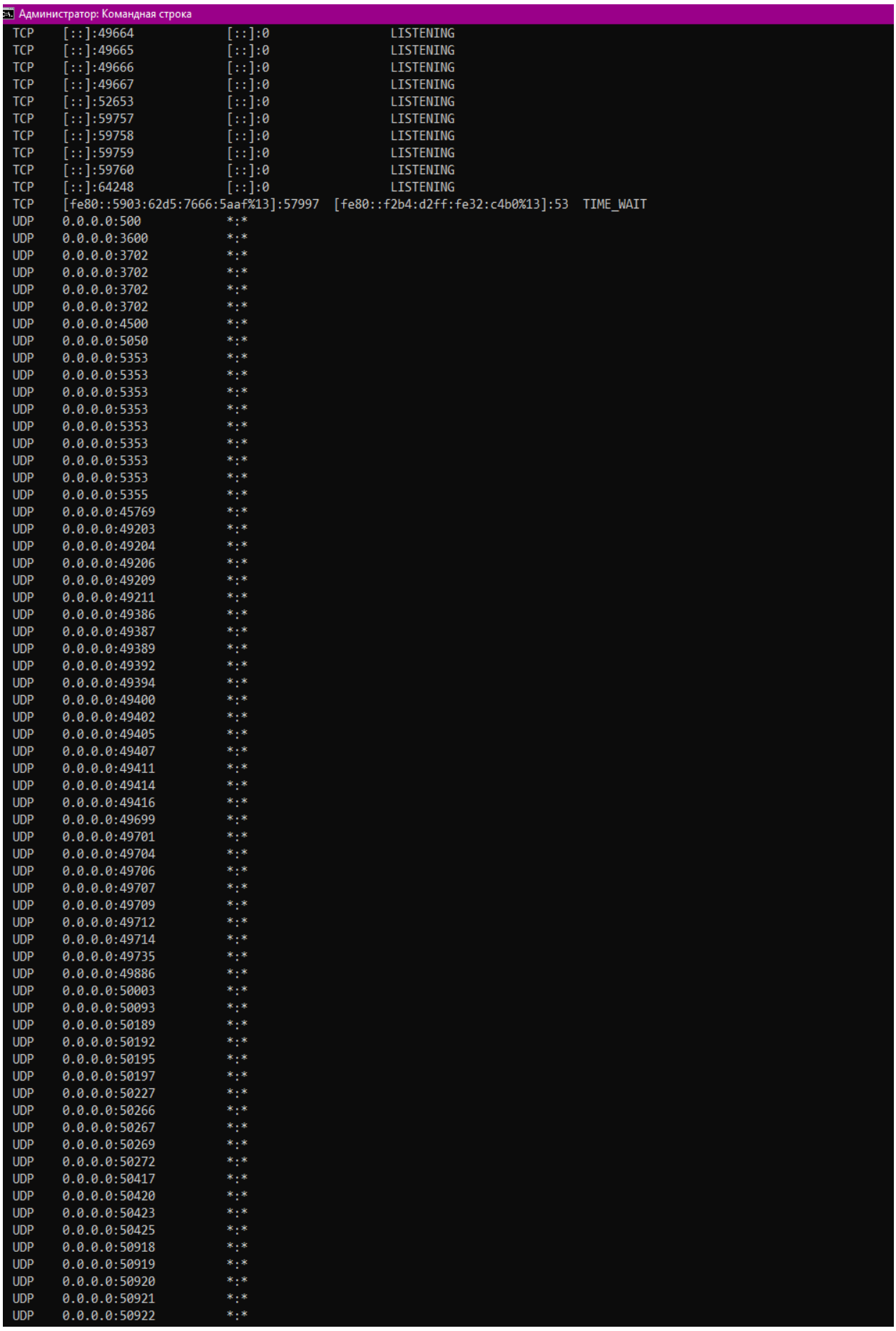

Рисунок 2Использование команды netstat -an продолжение

Задание 2.

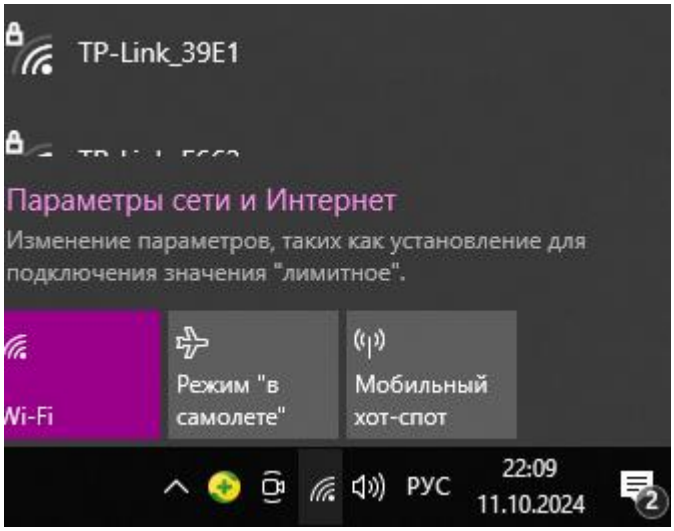

Рисунок 3 Параметры сети и Интернет

1. На рабочем столе правой кнопкой мыши нажимаем на значок интернета где будет параметры сети и интернет как показано на рисунке 3.

2. Выбираем «параметры сети и интернет» далее «Центр управления сетями и общим доступом»

3. В центре управления сетями и общим доступом выбираем «Создание и настройка нового подключения или сети»

4. Откроется окно с предложением как выполнить подключение. Выбираем «Использовать моё подключение к Интернет»

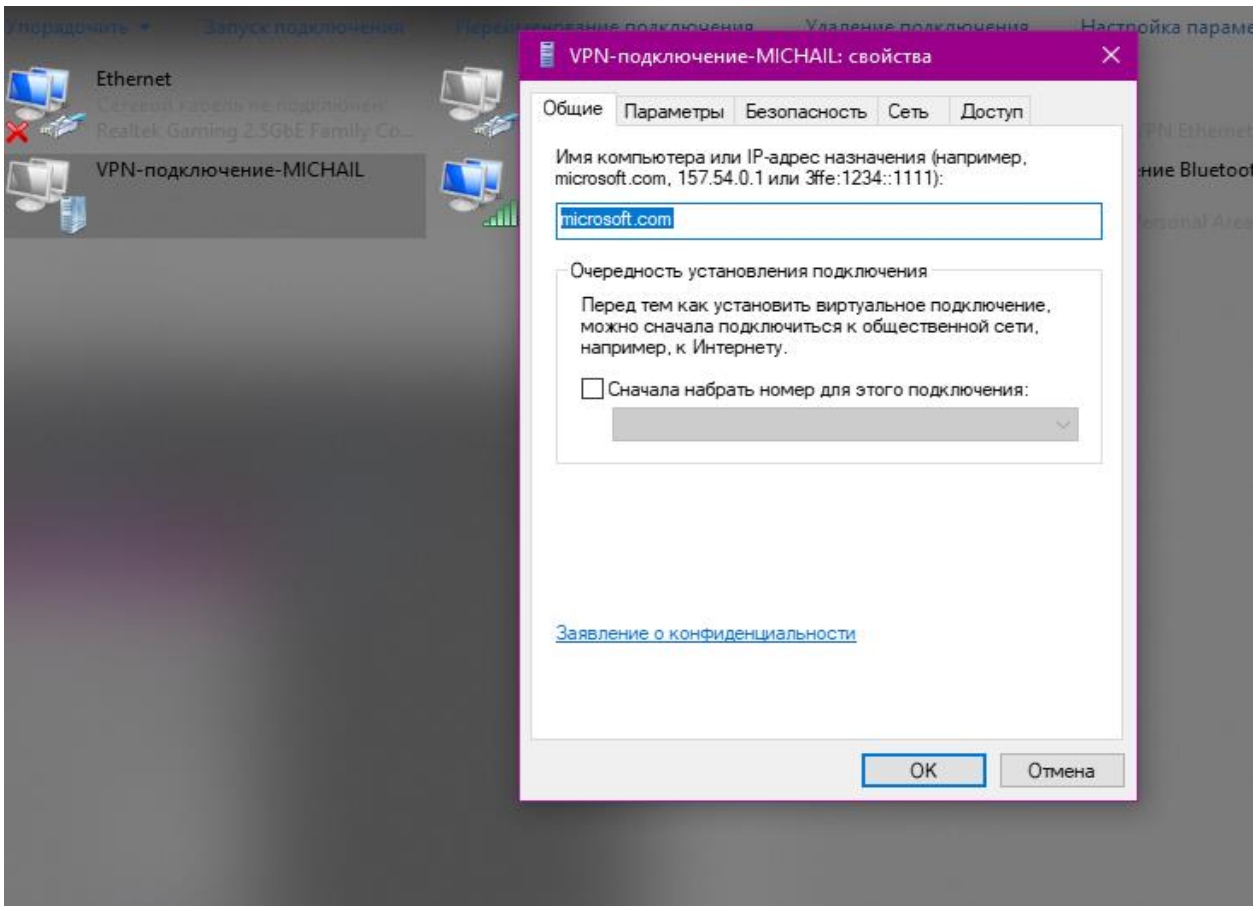

Рисунок41 VPN "Общие"

5. В строке Адрес в Интернете вводим адрес VPN сервера с соотвествием как показанно на рисунке 4

если вы используете **служебную учетную запись**, необходимо указать сервер **microsoft**

если вы используете **личную учетную запись**, необходимо указать сервер **microsoft.com**

6. VPN соединение создано, теперь надо настроить. Для этого в «центре управления сетями и общим доступом» открываем пункт «Изменение параметров адаптера»

7. Выбираем созданное VPN подключение, выбираем свойства

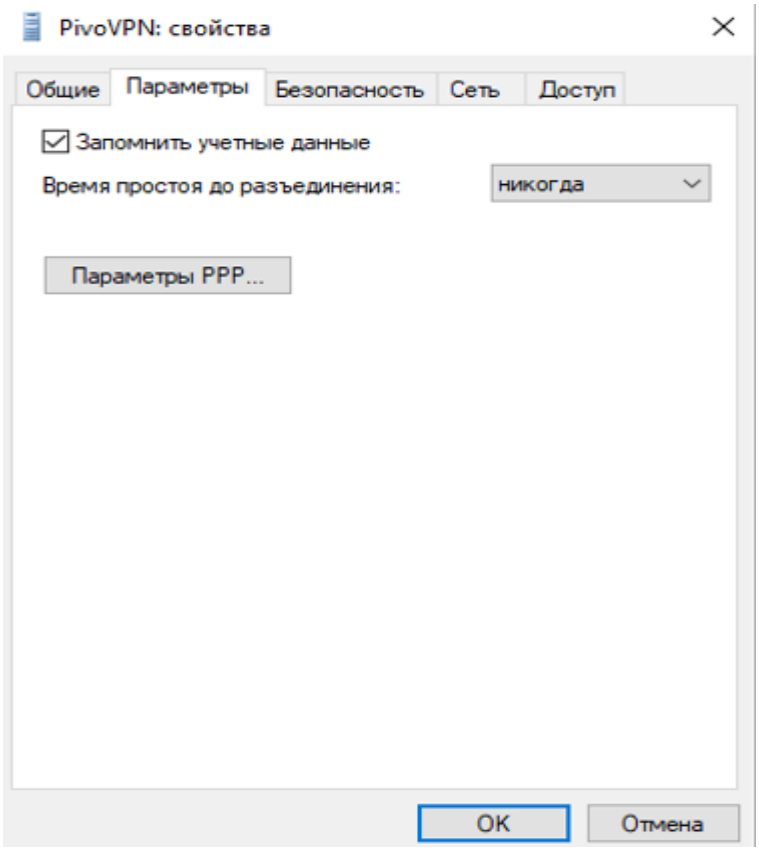

Рисунок 5"Параметры"

8. Открываем через свойства «Параметры» как показанно на рисунке 5 ставим или нет галочку, для того чтобы windows запомнила логин и пароль для VPN подключения или наоборот не запоминала выбираем «Безопасность». В выпадающем списке «Шифрование данных» выбираем «необязательное (подключится даже без шифрования)».

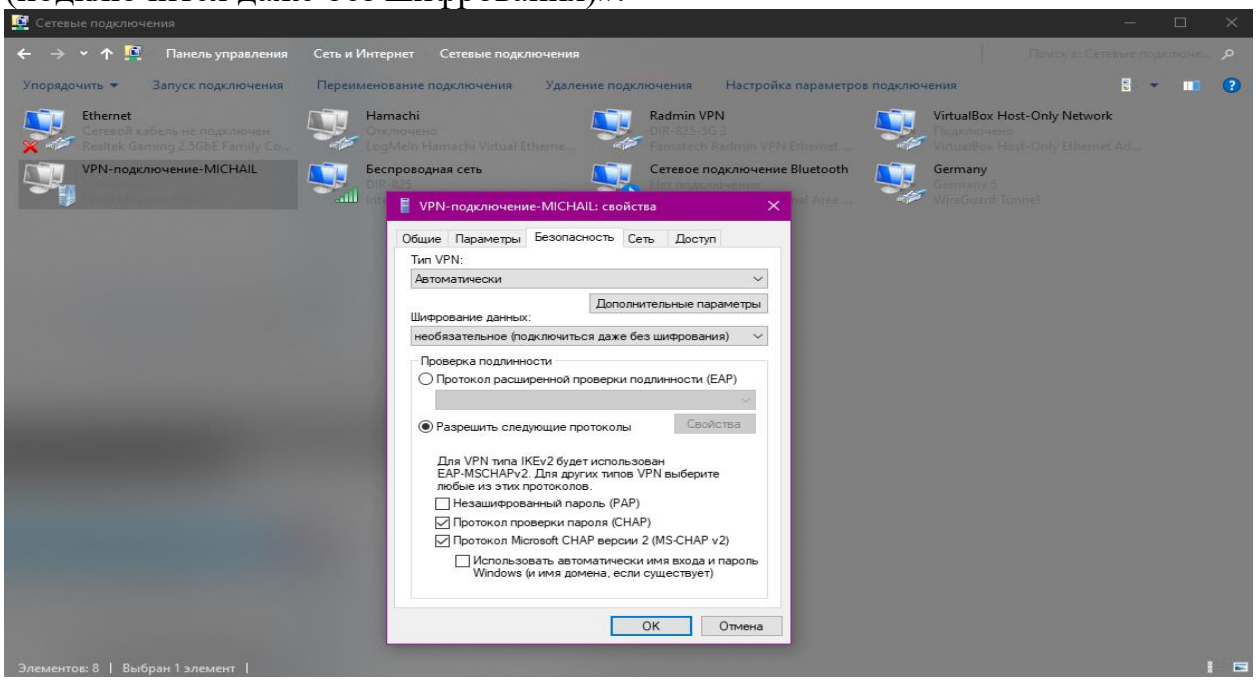

Рисунок 6 "Безопасность"

9. Выбираем раздел «Безопасность» как на рисунке 6. В списке «Шифрование данных» выбираем «необязательное (подключится даже без шифрования)». «Проверка подлинности» выделяем «Разрешить следующие протоколы» и ставим галочки напротив «Протокол проверки пароля (CHAP)» и «Протокол Microsoft CHAP версии 2 MS-CHAP v2».

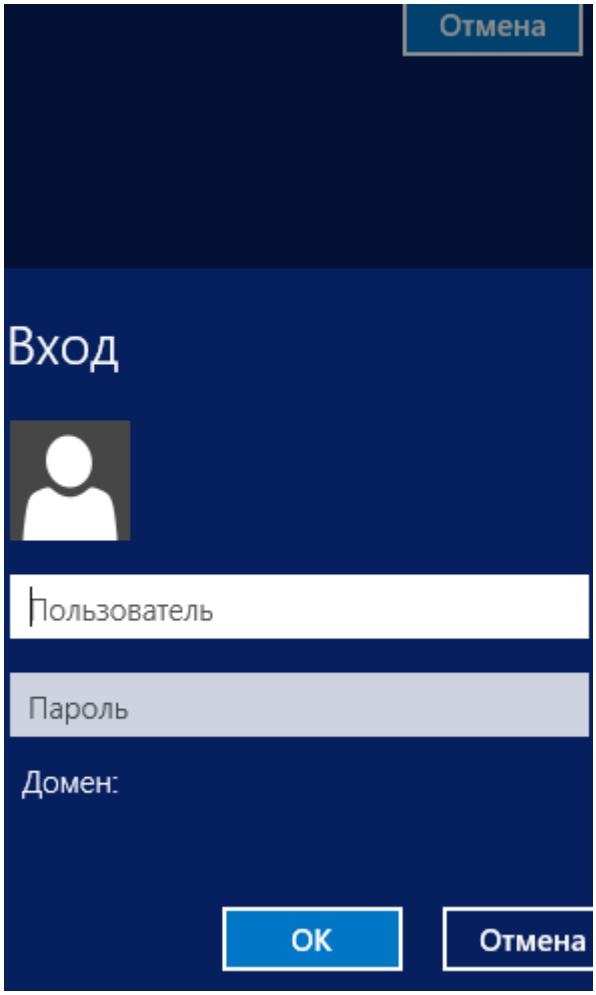

Рисунок 7 Конечный результат после подключения к VPN

После изменения настроек нажима ем кнопку «OK» в низу появляется меню как показанно на рисунке 7 .

Нужно выбрать «VPN-подключение» ввести логин, пароль и дождаться установки соединения с VPN сервером.

Задание 3.

Одним из ключевых аспектов работы с удалённым рабочим столом является настройка экрана. В разделе «Экран» пользователь может выбрать разрешение, которое будет использоваться при подключении.

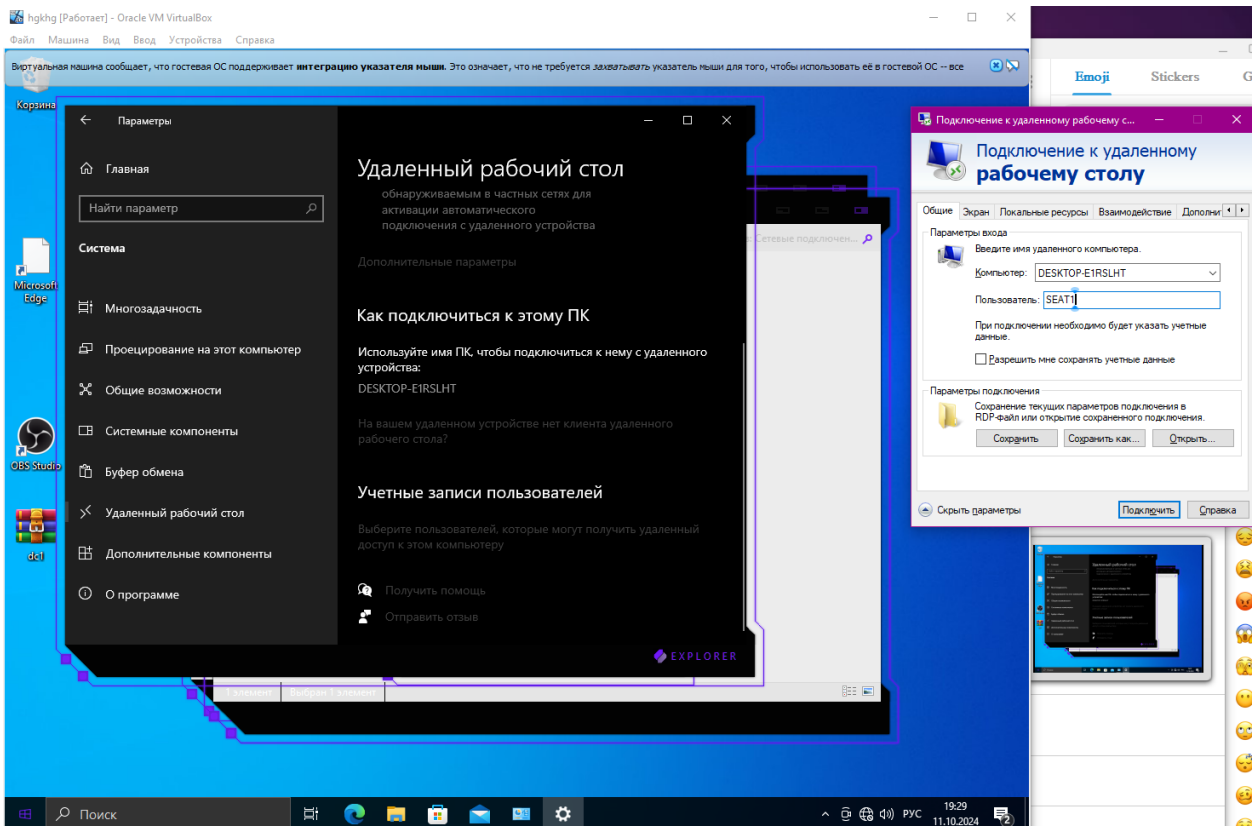

Рисунок 8 Нахождение в параметрах Windows пользователя/IP-V4

В ходе выполнения работы я решил выбрать название ПК в разделе удалённый рабочий стол для того чтобы заполнить поле “компьютер” как показано на рисунке 8.

В строке пользователь нужно написать “Пользователя” который будет подключаться к ПК

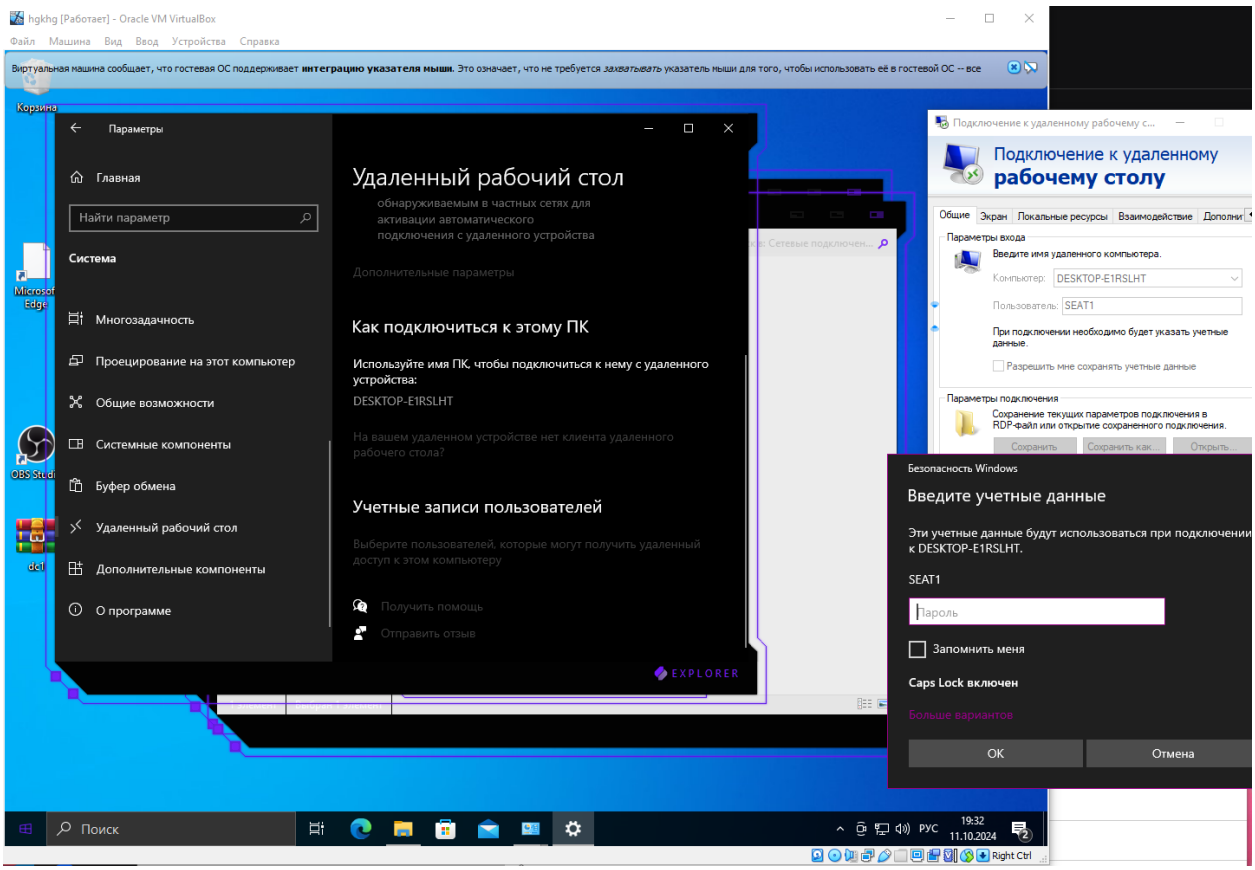

Рисунок 9 Конечный результат "ввод пароля ПК к которому подключаемся"

На рисунке 9 представлен результат после того как мы нажали кнопку “Подключить”. Соотвественно после ввода пароля ПК к которому нужно подключиться мы сможем к нему подключиться и будим иметь доступ к переименованиям файлов, управлять менеджером файлов и делать множество функций и операций которые могут делать обычные пользователи Windows 10 pro.

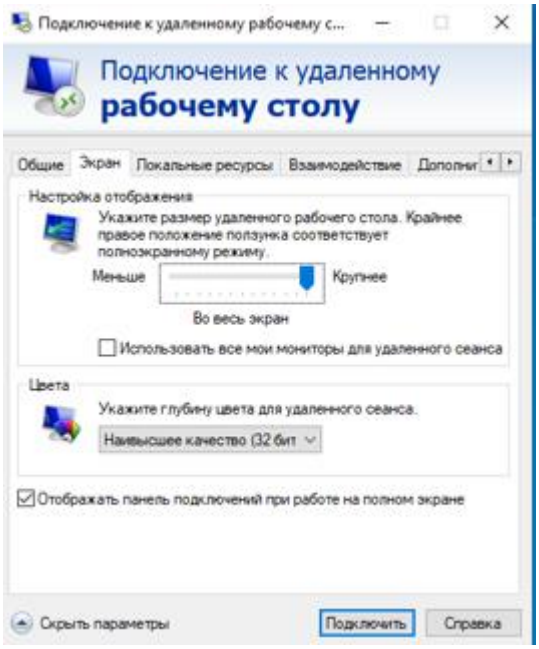

Рисунок 10 Настройка "Экрана для удобного пользования удалённого доступа для пользователя который подключается к другому монитору"

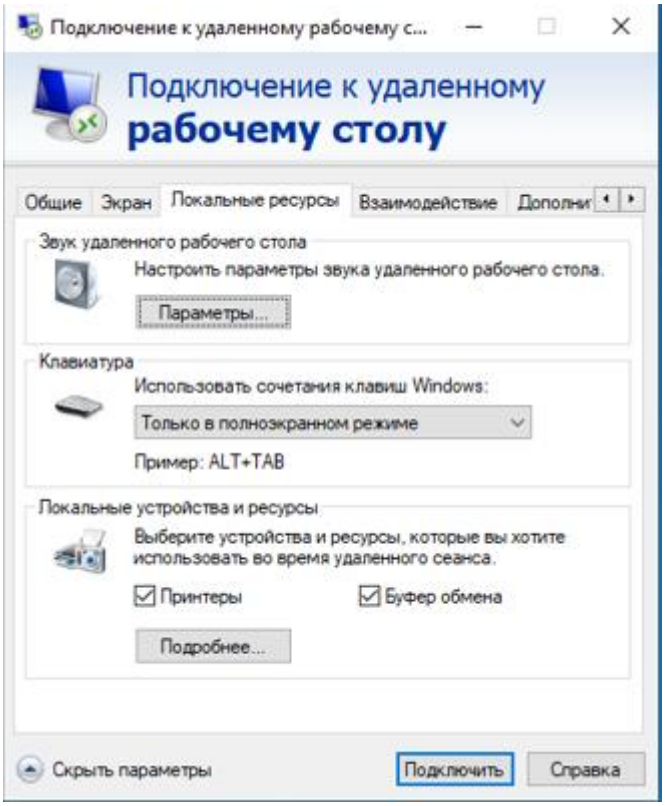

Рисунок 11 Это необходима для компьютера атакующего так как это "Локальные ресурсы"

С соответствии поставленной задачей подключиться удалённо к другому монитору данная опция позволяет делать пользователю множество операций а именно то что представлено на рисунке 10, 11.

Задание 4.

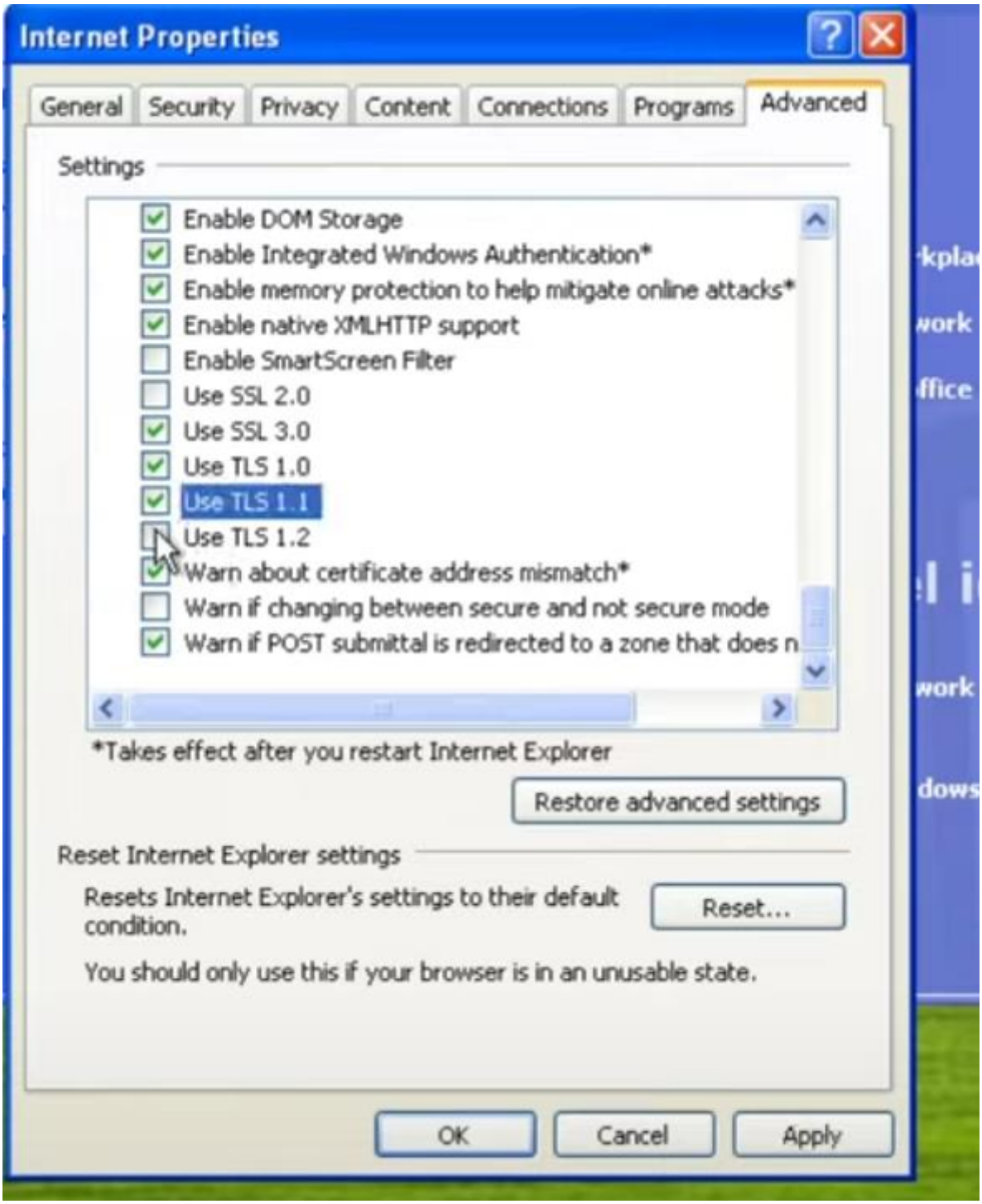

Рисунок 12 Добавление протокола защиты в интернете TLS.

В ходе выполнения работы мы смогли добавить протокол для Windows XP протокол TLS представленный на рисунке 12. TLS это криптографический

протокол, который обеспечивает защищённый обмен данными между устройствами внутри сети.

Задание 5.

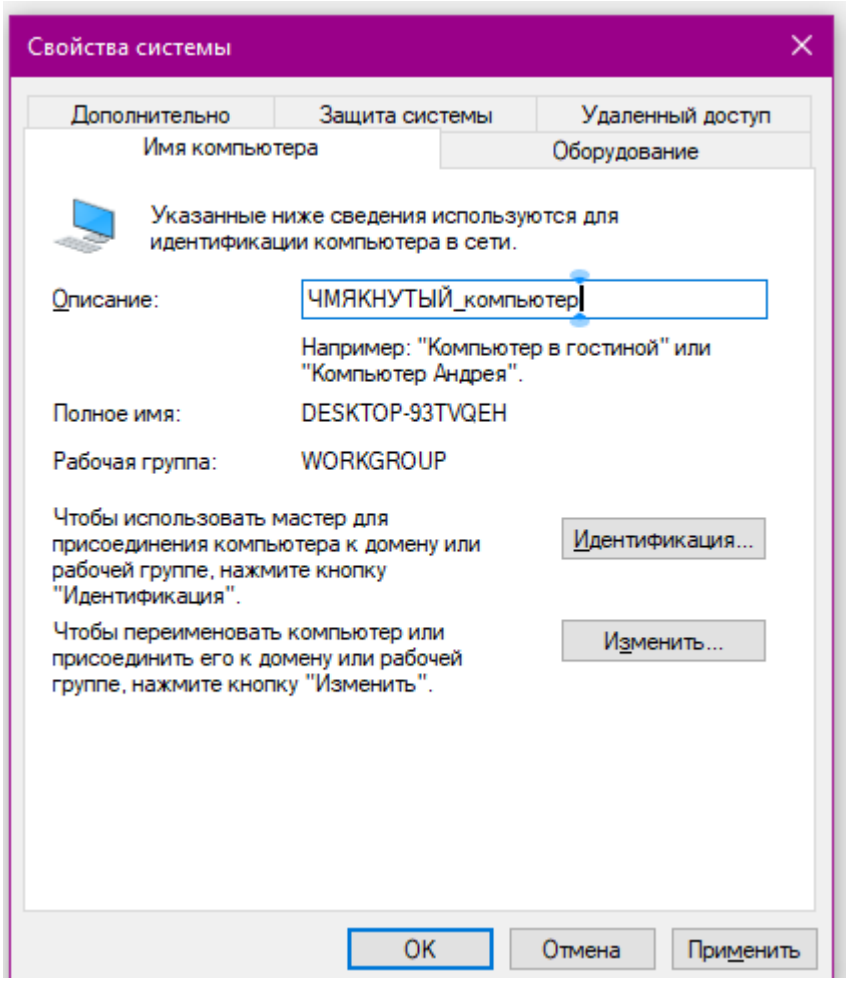

Рисунок 13 ЧМЯКНУТЫЙ_компьютер

Чтобы поменять описание ПК необходимо перейти в раздел из “параметров” в “свойства системы” потом нажимаем на “Имя компьютера” как показано на рисунке 13.

После того перехода на раздел будет возможность написать в описании всё что пожелает пользователь.

Задание 6.

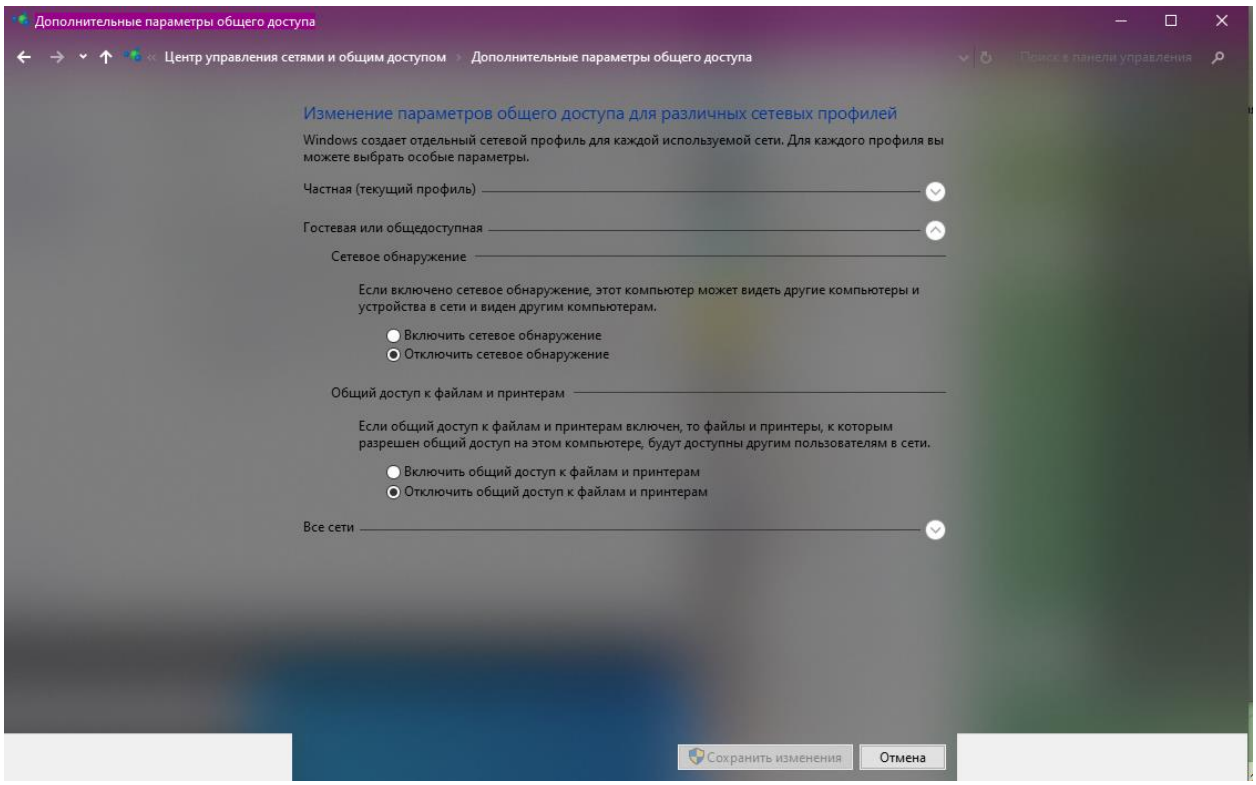

Рисунок 14 Отключение сетевых оборудований

На рисунке 14 продемонстрированно как включать/отключать возможность расшаркивания ресурсов.

Задание 7.

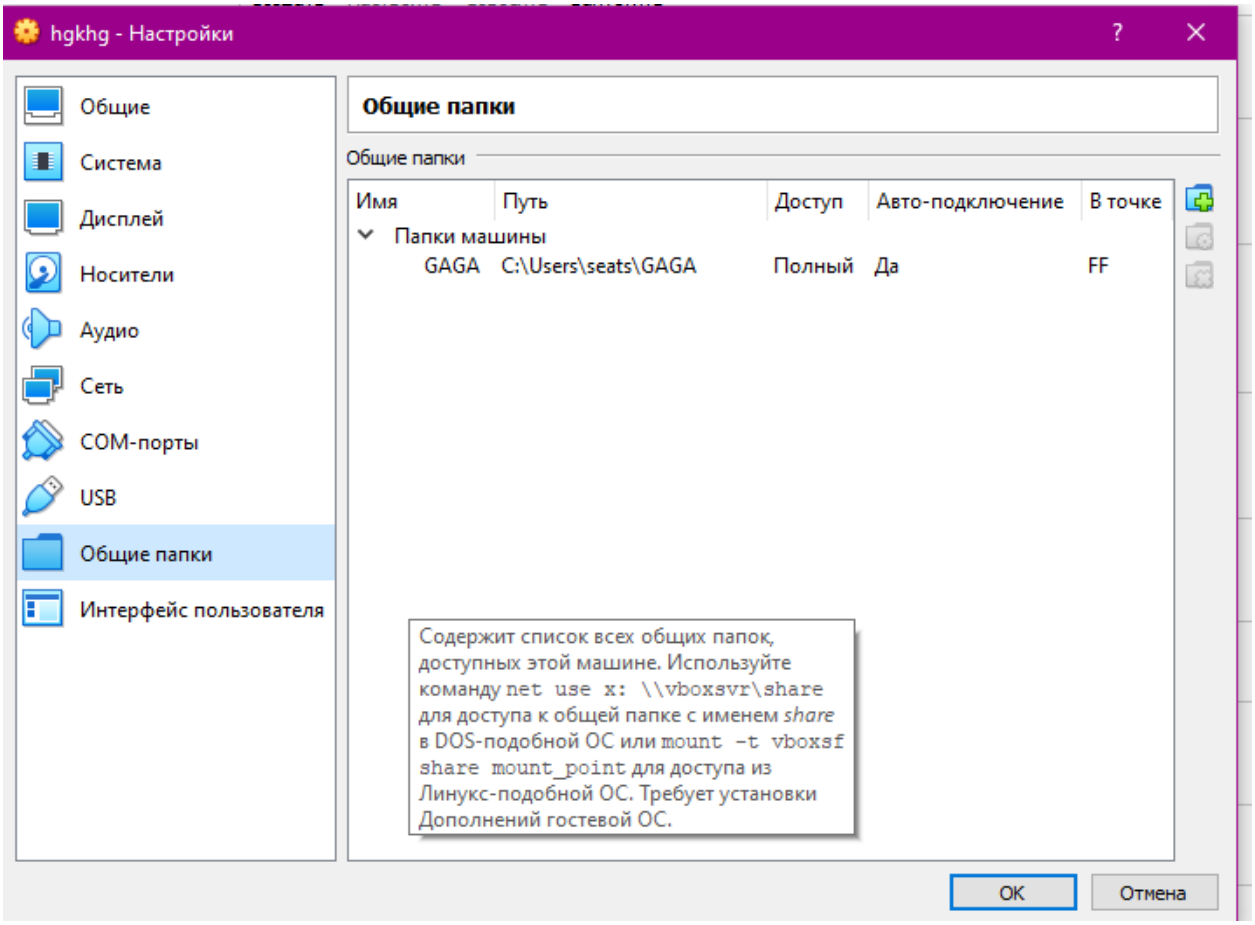

Рисунок 15 Параметры Virtual BOX

Для начала в Virtual BOX мы создаём в общих папках (пример папку с именем GAGA) как показанно на рисунке 15.

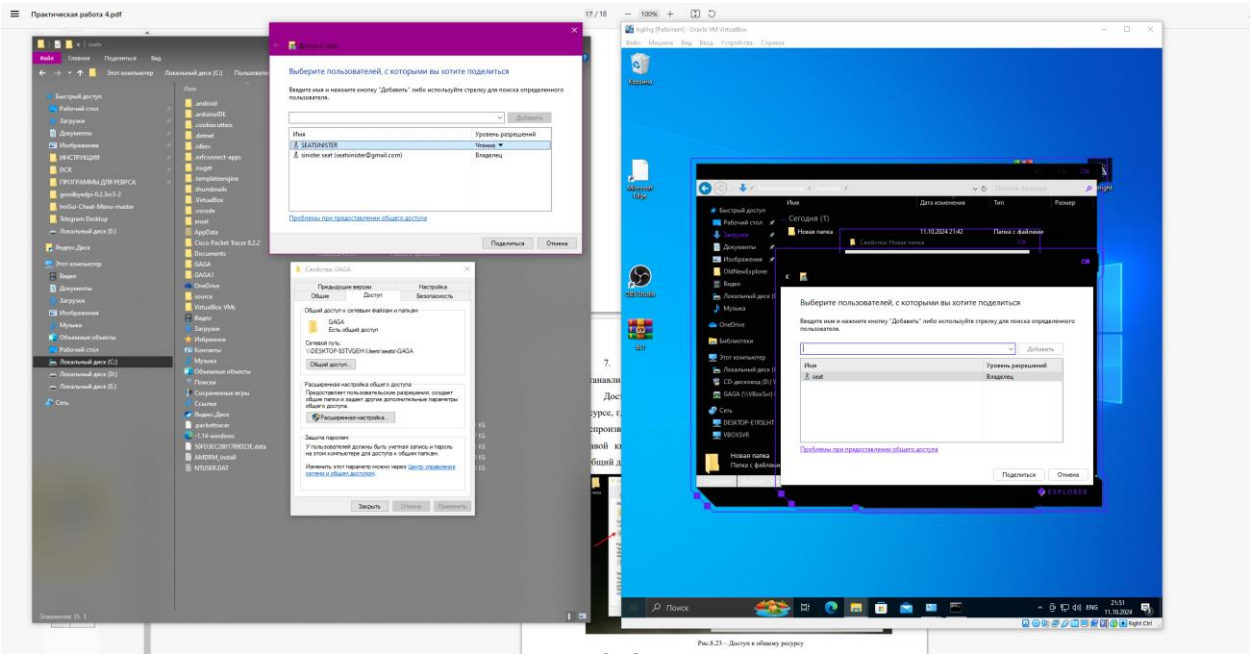

Рисунок 16 Процесс занесения юзеров для доступа к папке GAGA

После создании папки мы должны перейти в виртуальную машину найти папку и нажать на неё свойство и перейти в раздел “Доступ” где мы заносим администратора (seat sinister) и гостя (SEATSINISTER) как показано на рисунке 16.

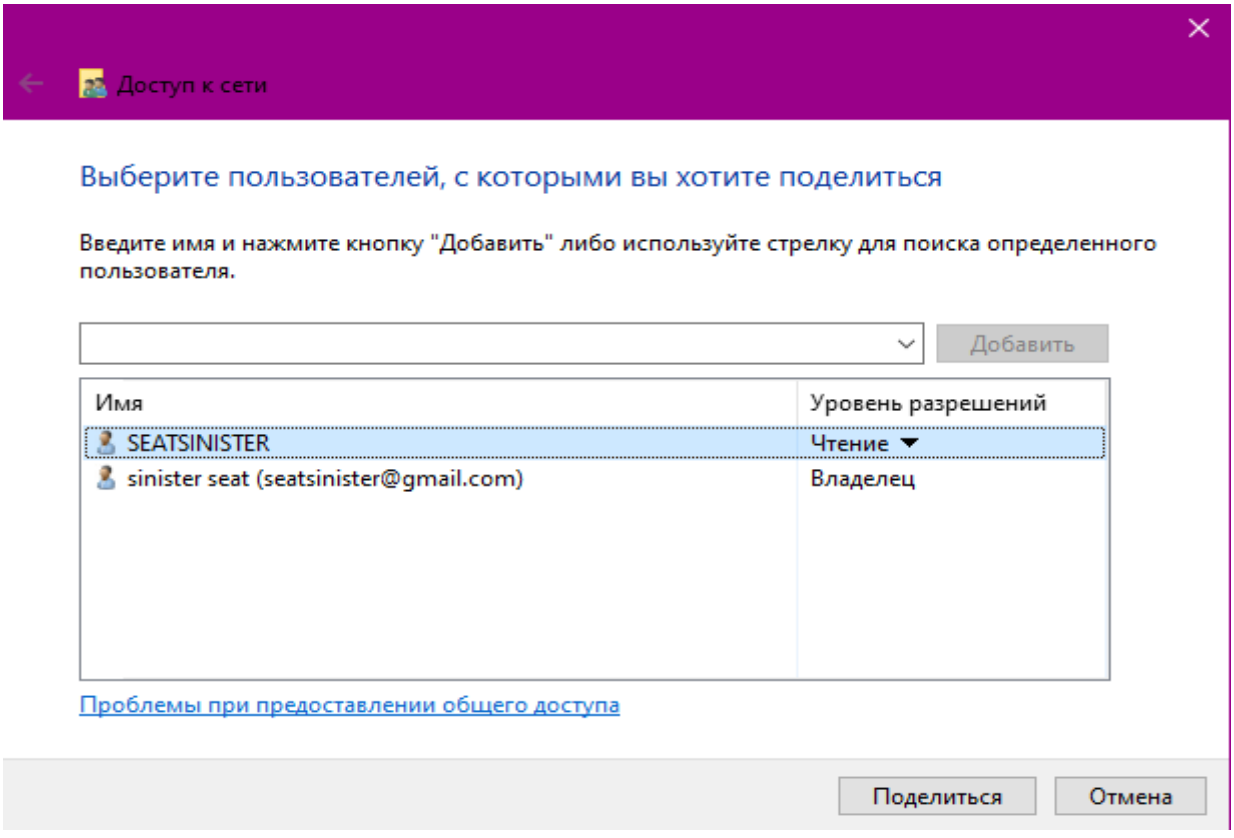

Рисунок 17 Конечный результат после занесения пользователей папки GAGA

После занесения всех юзеров надо мы получаем папку к которой имеют доступ только два пользователя как демонстрируется на рисунке 17.

Задание 8.

1 Сетевые протоколы включают в себя HTTP, DNS, DHCP. Эти протоколы определяют, как устройства обмениваются данными в компьютерной сети.

HTTP- это сетевой протокол прикладного уровня, который используется для передачи гипертекстовых документов между веб-серверами и браузерами. Он был разработан специально для работы с документами в формате HTML, но со временем стал использоваться для обмена данными между узлами в интернете и в изолированных веб-инфраструктурах. Протокол HTTP работает по принципу "клиент-сервер", где клиенты инициируют соединение и отправляют запросы, а серверы ждут подключения и обрабатывают запросы, возвращая ответы. Основным способом идентификации ресурсов в HTTP являются глобальные URI (Uniform Resource Identifiers). Протокол HTTP не поддерживает сохранение состояния между парами "запрос-ответ", однако компоненты, использующие его, могут самостоятельно сохранять информацию о состоянии. Протокол HTTP также предоставляет возможность указывать в запросах и ответах способы представления ресурсов, такие как формат, кодировка и язык.

DNS - это компьютерная распределенная система, предназначенная для получения информации о доменах. Основная функция DNS заключается в преобразовании доменных имен в IP-адреса. Это позволяет пользователям использовать легко запоминающиеся имена для доступа к ресурсам в интернете, а не сложные числовые IP-адреса. DNS также используется для получения информации о маршрутизации почты и обслуживающих узлах для протоколов в домене. Система DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу. Основой DNS является представление об иерархической структуре имени и зонах. Каждый сервер, отвечающий за имя, может передать ответственность за дальнейшую часть домена другому серверу. Таким образом, ответственность за актуальность информации возлагается на серверы различных организаций. DNS была разработана Полом Мокапетрисом в 1983 году и описаны в RFC 882 и RFC 883.

DHCP - это сетевой протокол, который позволяет сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP

2 Транспортные протоколыTCP (Transmission Control Protocol) и UDP (User Datagram Protocol). Они отвечают за доставку данных между приложениями и гарантируют целостность данных при передаче.

3 Основные настройки TCP/IP включают в себя IP-адреса, маску подсети, шлюз по умолчанию, DNS-серверы и WINS-серверы. Эти настройки позволяют устройству корректно взаимодействовать с другими устройствами в сети.

4 Функции DHCP включают в себя автоматическое назначение IP-адресов, масок подсетей,

5 Шлюз – это устройство или программный компонент, который используется для передачи данных между различными сетями. Он перенаправляет пакеты данных от одной сети к другой, используя различные протоколы и порты.

6 Маска подсети определяет, какие биты IP-адреса относятся к сети, а какие – к хосту

7 Сервер DHCP может назначать IP-адреса, маски подсетей, DNS-серверы.

8 Файл hosts содержит список IP-адресов и соответствующих им доменных имен. Этот файл используется операционной системой для быстрого разрешения имен доменов

9 MAC-адрес – это уникальный идентификатор, присваиваемый каждому сетевому интерфейсу (например, Ethernet-карте) производителем.

10 Команда ipconfig позволяет получить информацию о текущих сетевых настройках компьютера, включая IP-адрес, маску подсети, шлюз по умолчанию, DNS-серверы и другие параметры сети

Вывод в ходе выполнения работы мы научились администрировать windows а также сформировали представление сетей и протоколов для различных задач а также мы повторили протоколы и настройки прав пользователей.