|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |

**Институт кибербезопасности и цифровых технологий**

**Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»**

**ОТЧЁТ ПО ПРАКТИЧЕСКОМУ ЗАНЯТИЮ №2**

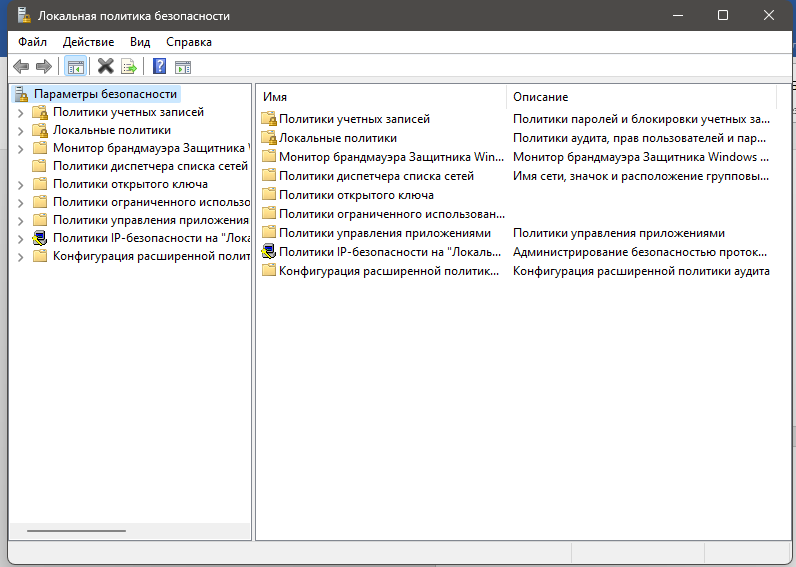
**по дисциплине «Безопасность операционных систем»**

|  |  |  |  |
| --- | --- | --- | --- |
| Отчет представлен к  рассмотрению:  Студент группы БББО-01-22 | «16» февраля 2024 г. | (подпись) | Сокол Д.М. |
|  |  |  |  |
| Преподаватель | «16» февраля 2024 г | (подпись) | Абрамов Д.П. |

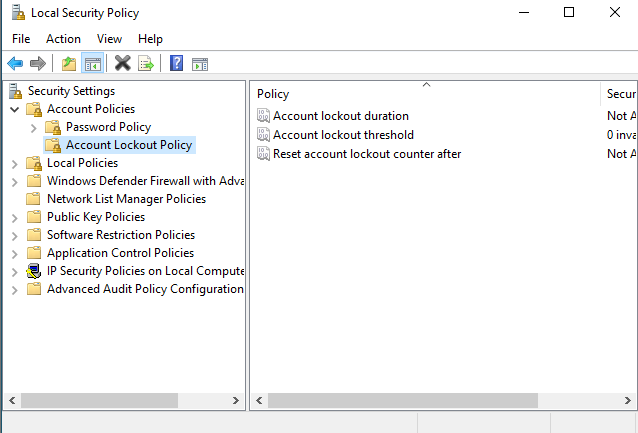
Москва, 2024 г.

**2.1. Политики безопасности Windows**

Для открытия оснастки управления политиками безопасности в окне поиска windows (внизу рабочего стола иконка с лупой) или в окне выполнения команд (Win + r) введите secpol.msc, должно открыться окно как на рисунке 1.

****

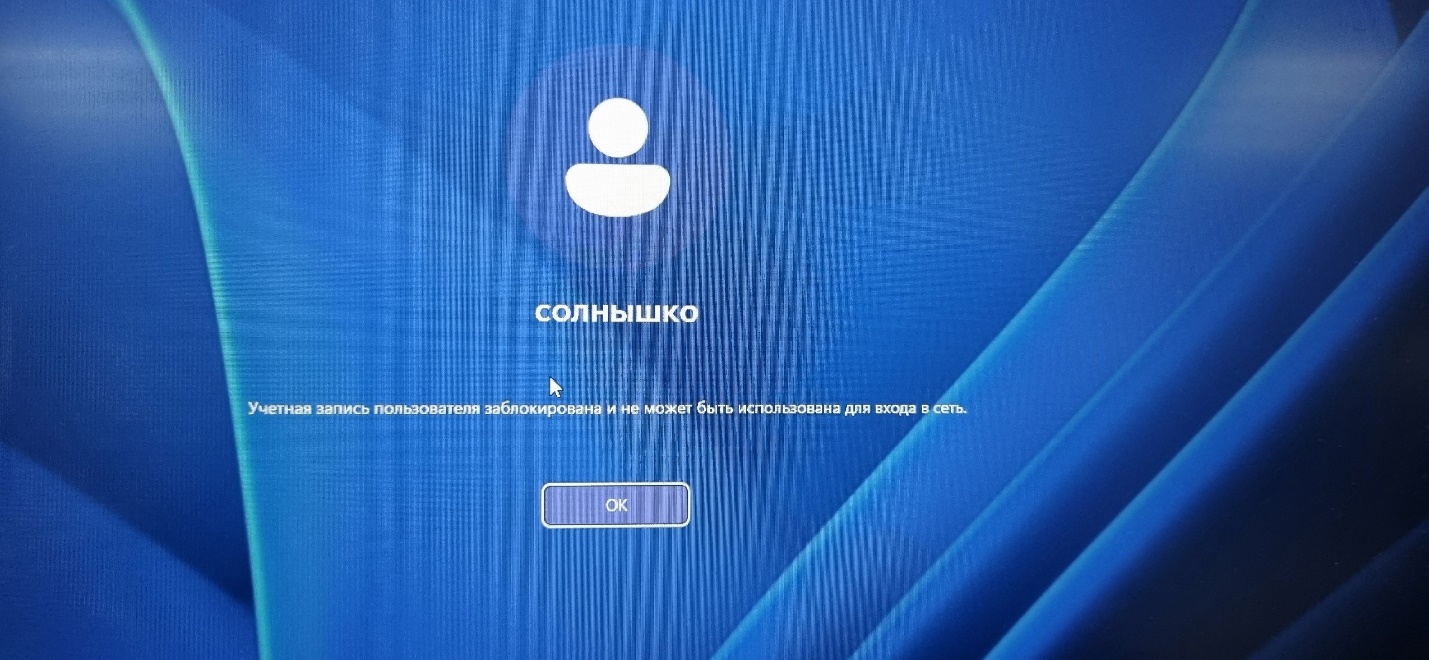
Теперь перейдем в Account Policies -> Account Lockout Policies и выполним настройку параметров блокировки пользователя, как показано на рисунке 2.

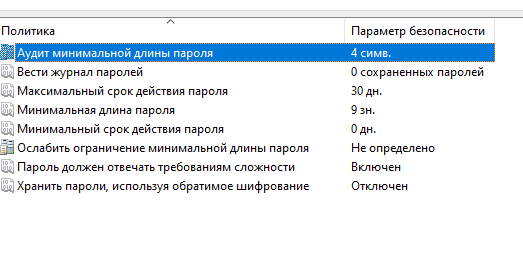
****

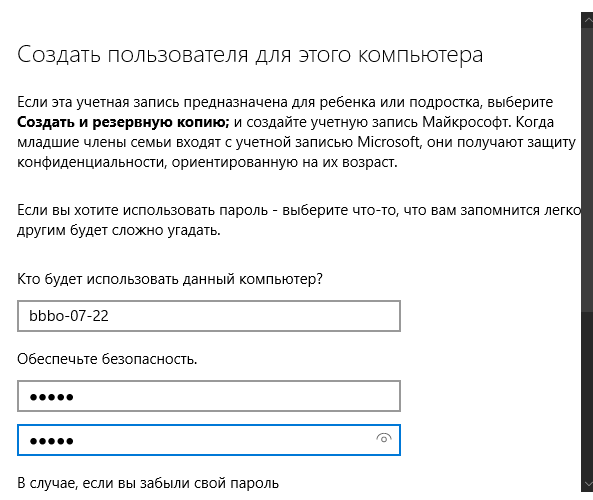
**account lockout duration -** Параметр политики длительности блокировки учетной записи определяет количество минут, в течение которых заблокированная учетная запись остается заблокированной, прежде чем она будет автоматически разблокирована.

**account lockout threshold -** Это пороговое значение означает, что при превышении указанного максимального числа неудачных попыток входа устройство аннулирует предохранитель доверенного платформенного модуля (TPM) и любой другой предохранитель, кроме пароля восстановления из 48 цифр, а затем перезагрузится

**Reset account lockout counter after -** Счетчик сброса блокировки учетной записи после параметра политики определяет количество минут, которое должно пройти с момента, когда пользователь не сможет войти в систему до сброса счетчика неудачной попытки входа до 0



****

****

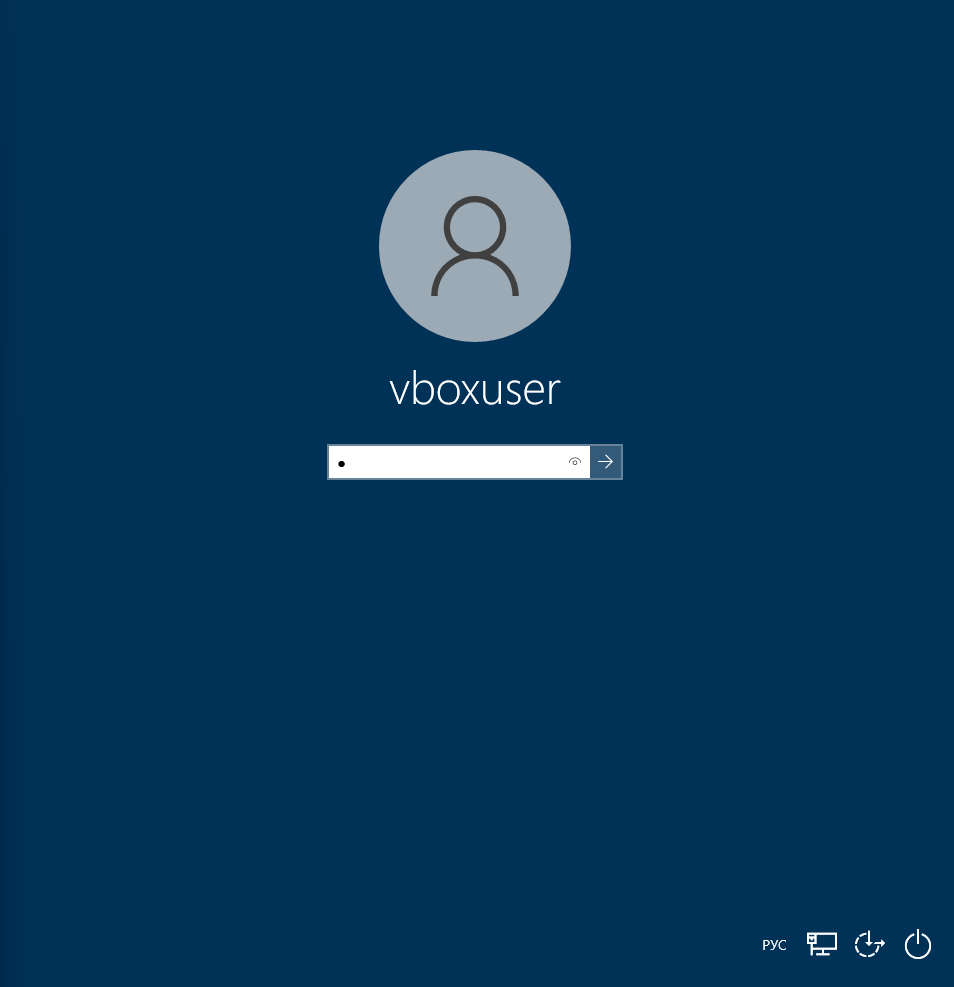
****

Рисунок 3. Окно авторизации Windows

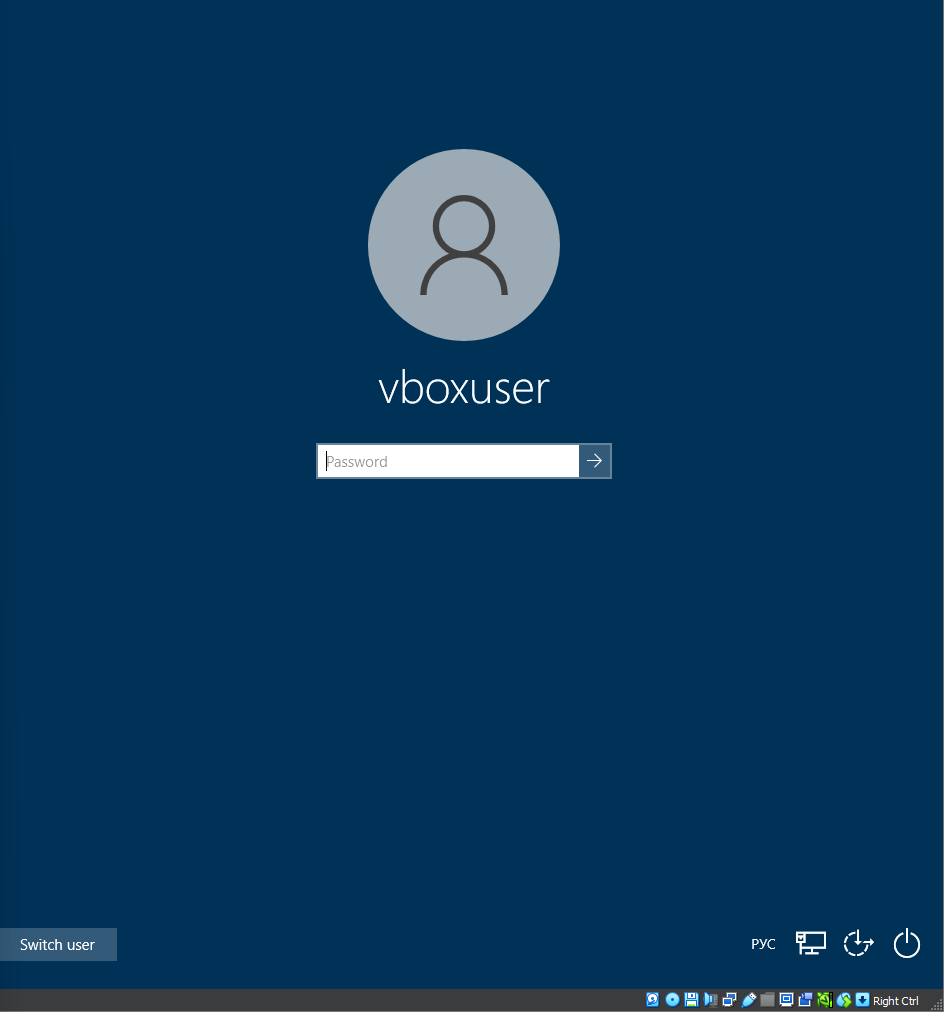
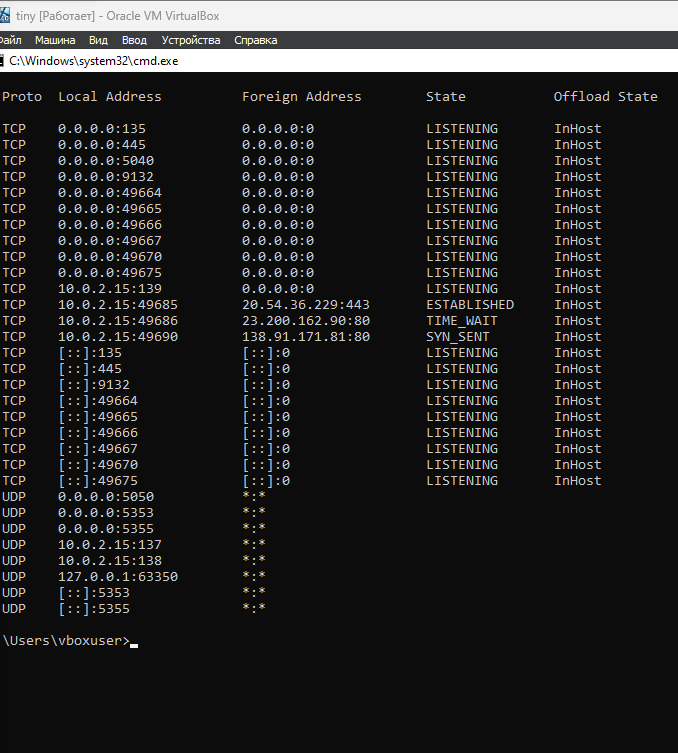


Рисунок 4. Окно авторизации Windows, пользователи скрыты



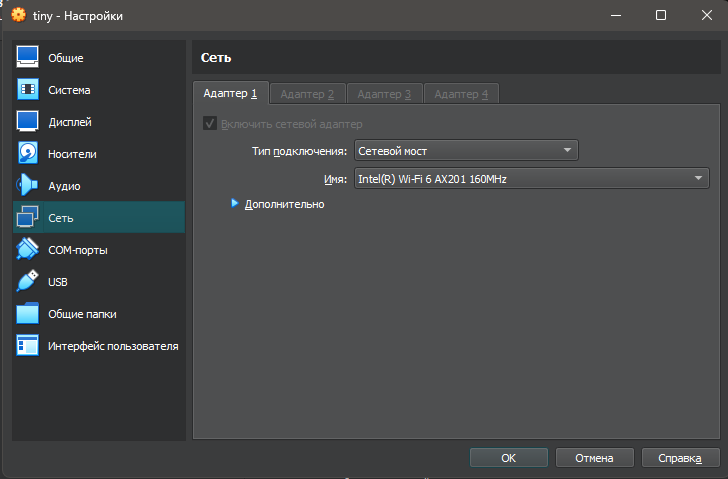


Рисунок 5. Настройки сетевого адаптера ВМ

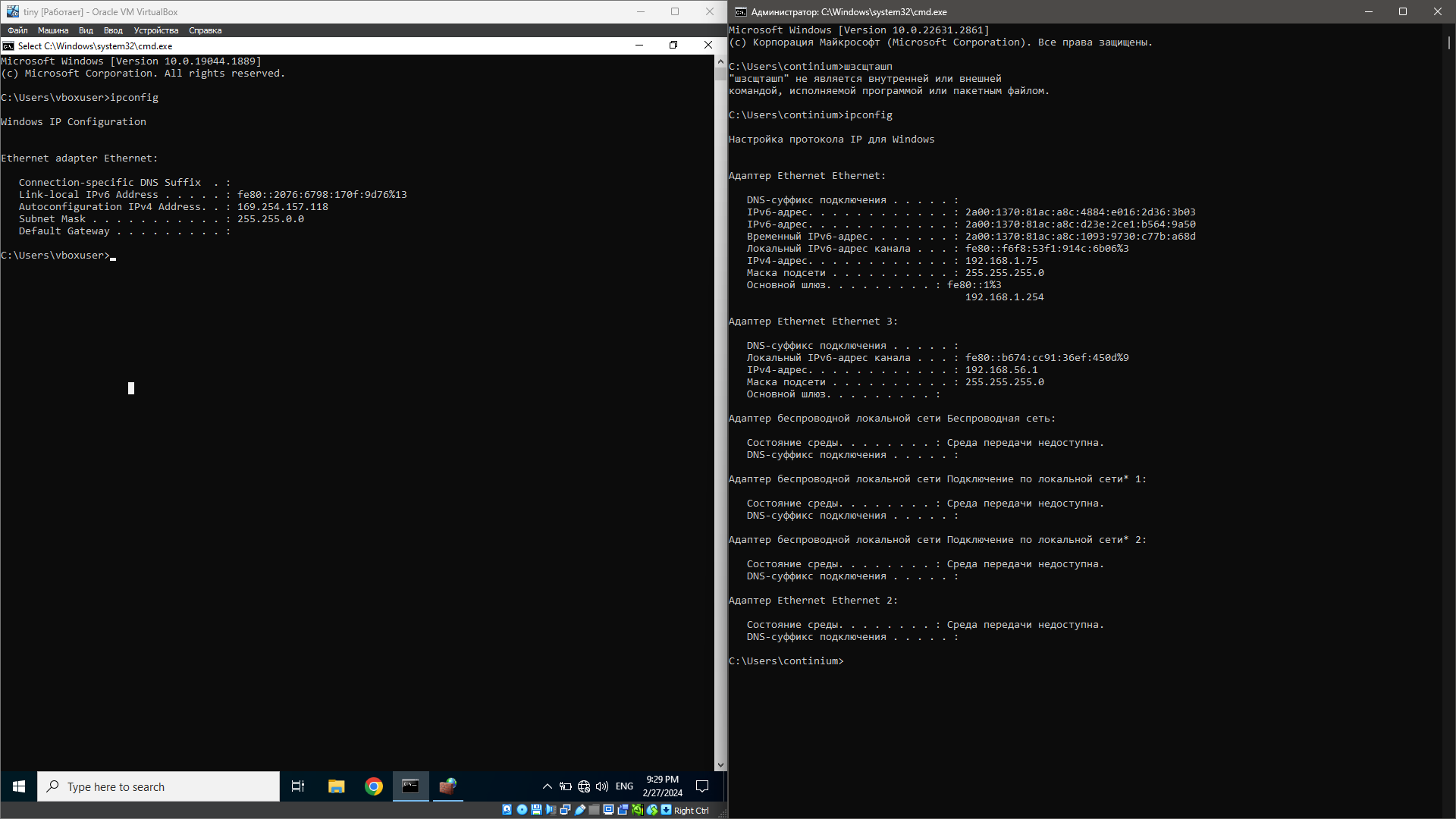


Рисунок 6. Результат команды ipconfig

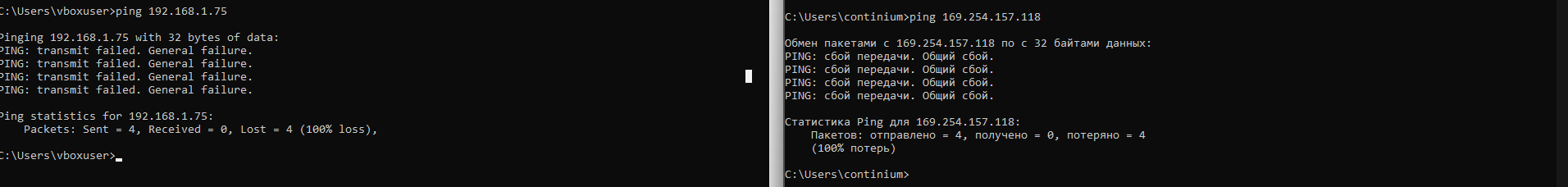
****

Рисунок 7. Результат команды ping

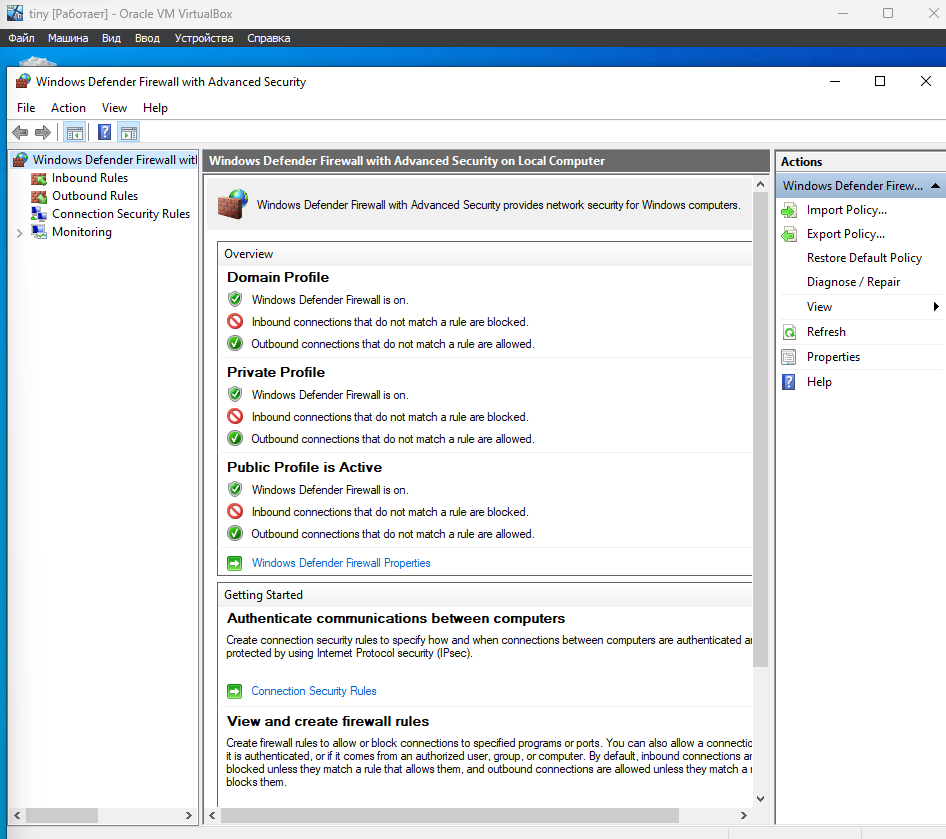


Рисунок 8. Оснастка управления брандмауэром

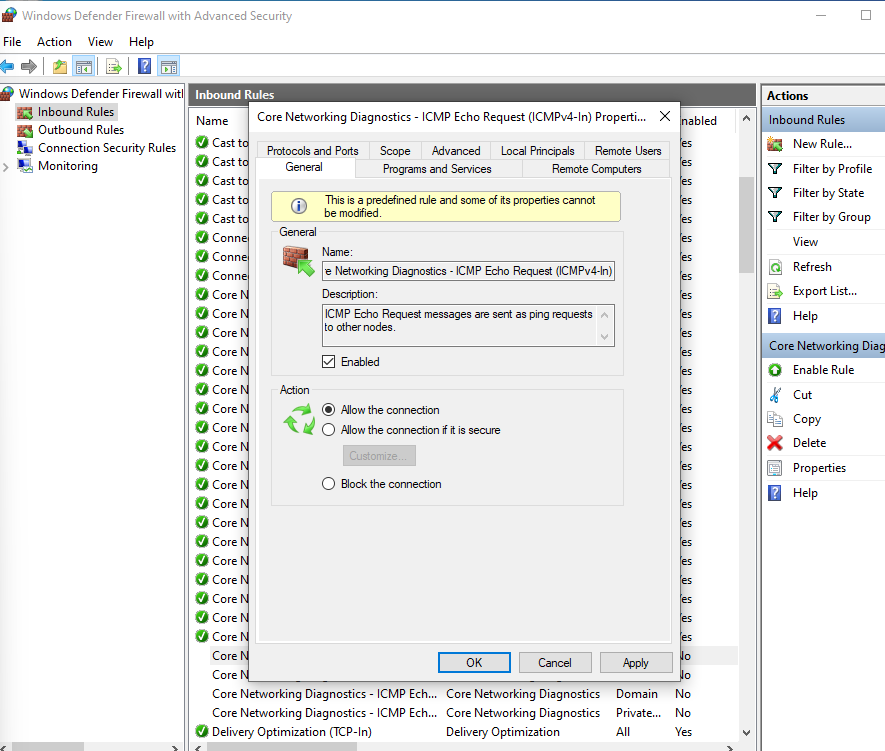
****

Рисунок 9. Включение параметра брандмауэра

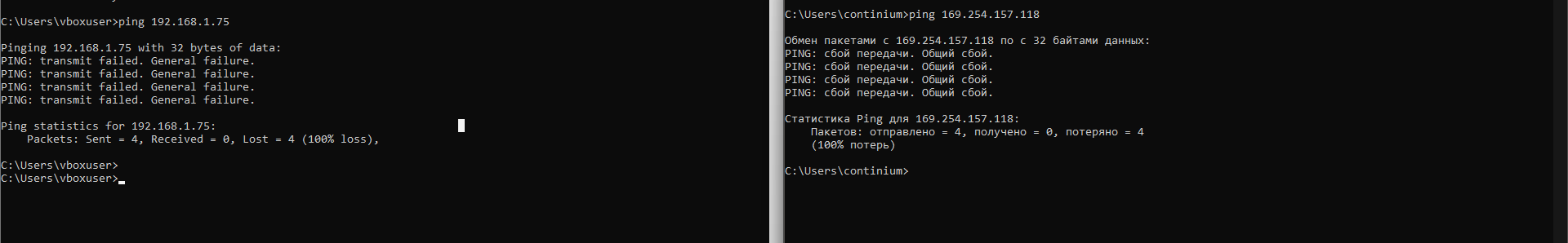
****

Рисунок 10. Результат команды ping

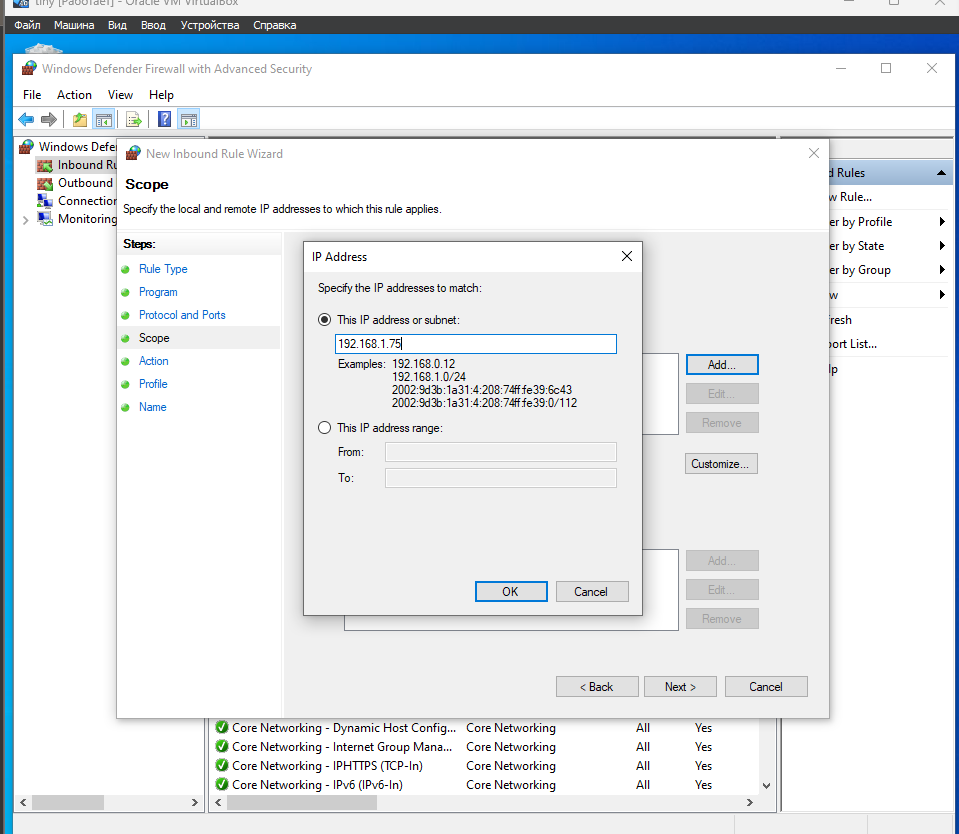
1)Объясните, почему получен результат, показанный на рисунке 10:

На рисунке 10 отключили защиту брендмауэром

2) Какой протокол используется командой ping и на каком уровне модели OSI он работает?

Команда ping использует протокол ICMP (Internet Control Message Protocol) и работает на сетевом уровне модели OSI.

3) Создайте собственное правило брандмауэра для блокировки протокола, который использует команда ping, только для ip-адреса вашей хостовой системы (screenshot)



**2.3. Журналирование в Windows**

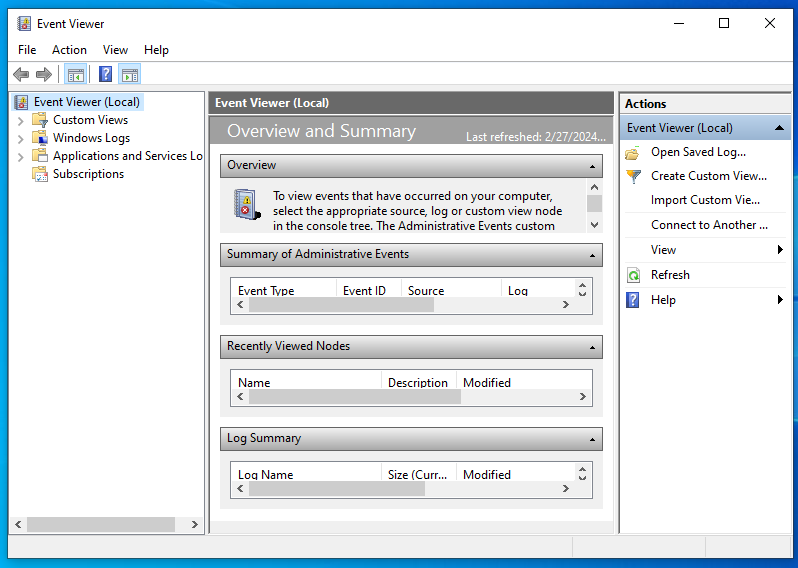


Рисунок 11 Окно оснастки журнала событий Windows

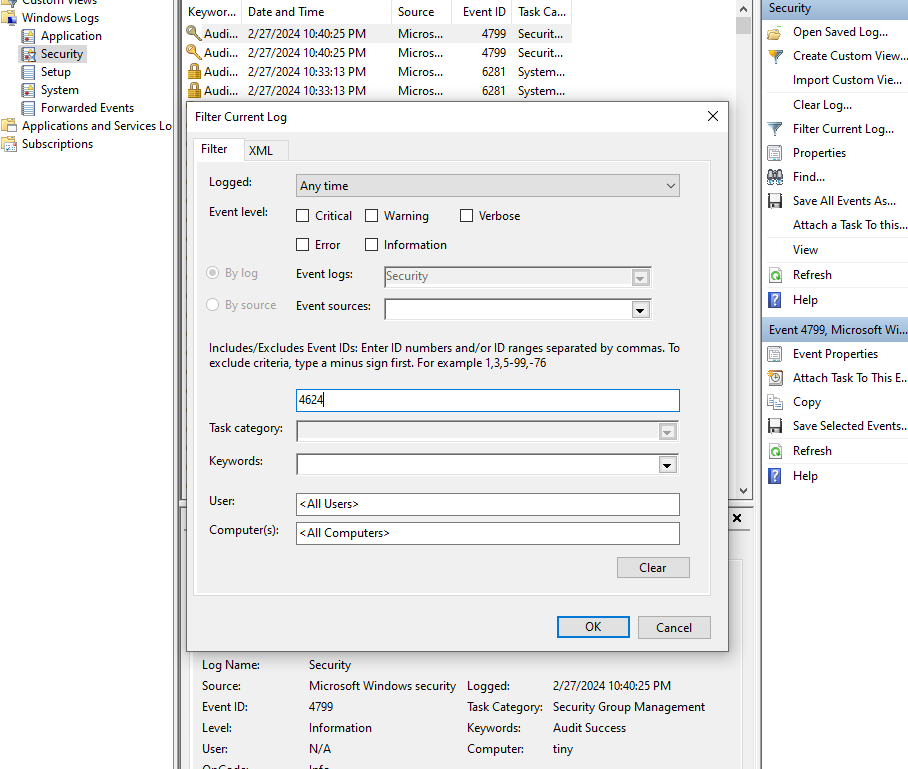
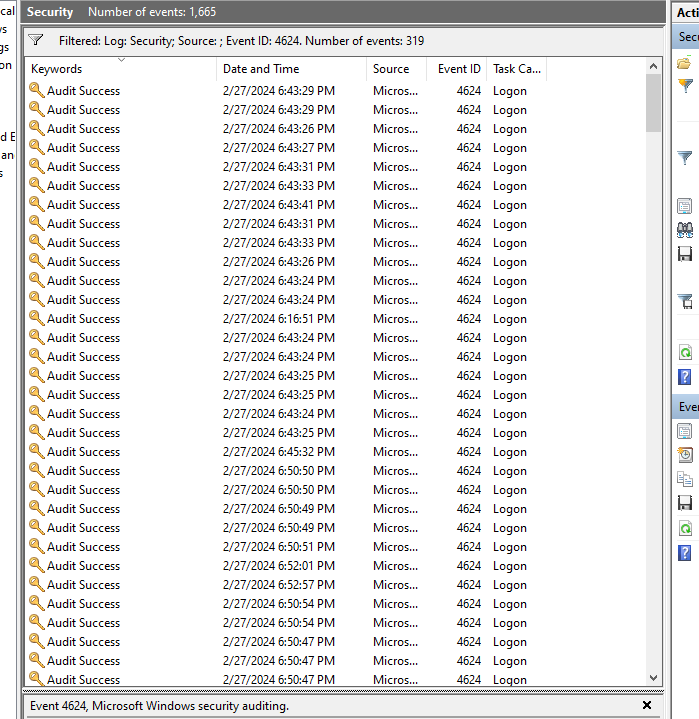
****

Рисунок 12 Фильтр журнала событий по коду

1)Найдите все события, связанные с неуспешным входом пользователя в систему (screenshot).



2)Напишите в каких случаях обращаются к журналам событий Windows.

Отслеживание ошибок и предупреждений

Мониторинг работы системы

Поиск причин сбоев и проблем

Анализ безопасности

Аудит и соответствие требованиям безопасности

3)Напишите ПО, которое применяется специалистами по ИБ для работы с журналами событий Windows

Splunk, SolarWinds Log & Event Manager, ManageEngine EventLog Analyzer, IBM QRadar, ELK Stack