

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ №2**

# **В РАМКАХ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»**

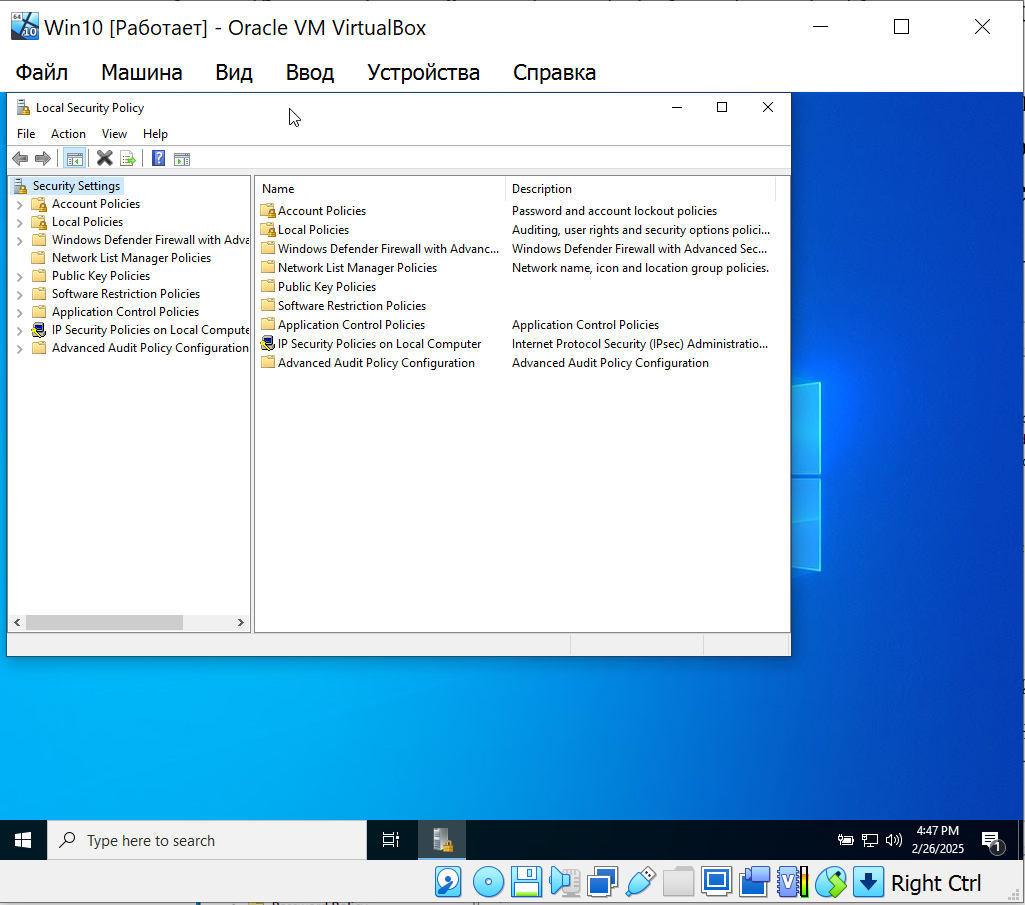
Выполнил:

Студент 3-ого курса

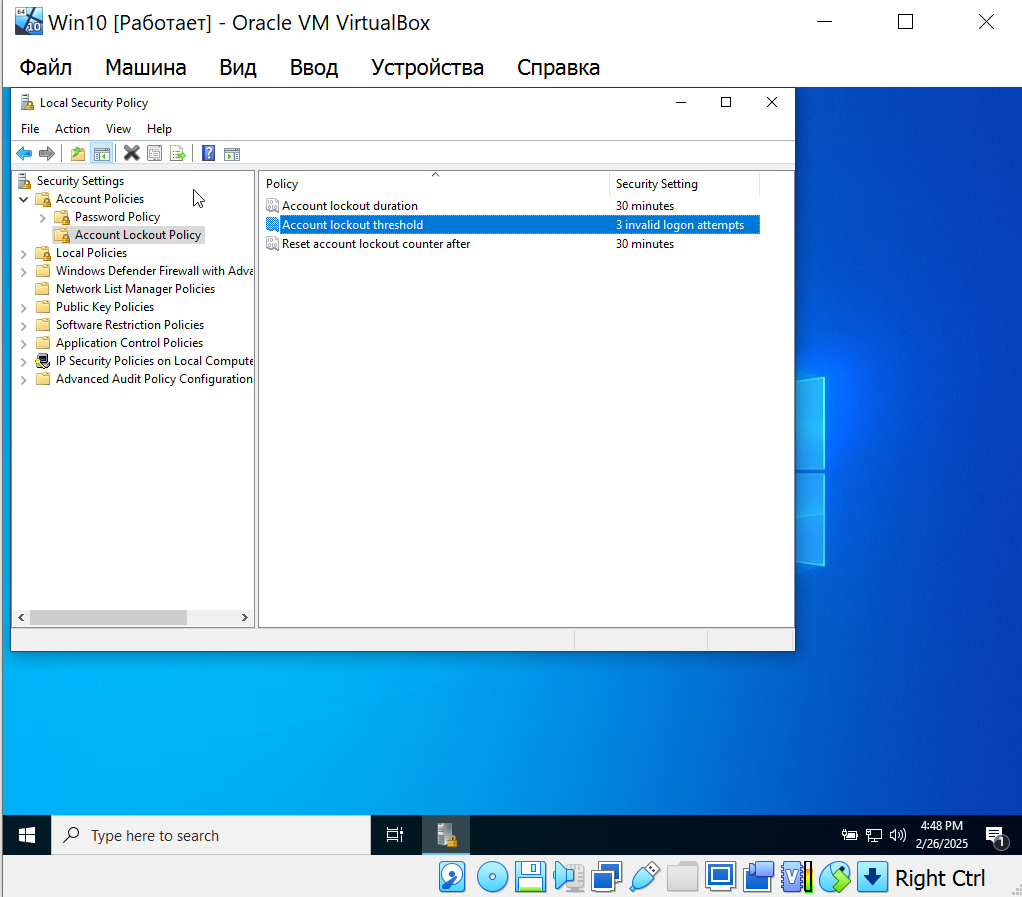
Учебной группы БИСО-02-22

Зубарев В.С.

Окно локальных политик безопасностей



Настройка локальных политик блокировки аккаунтов

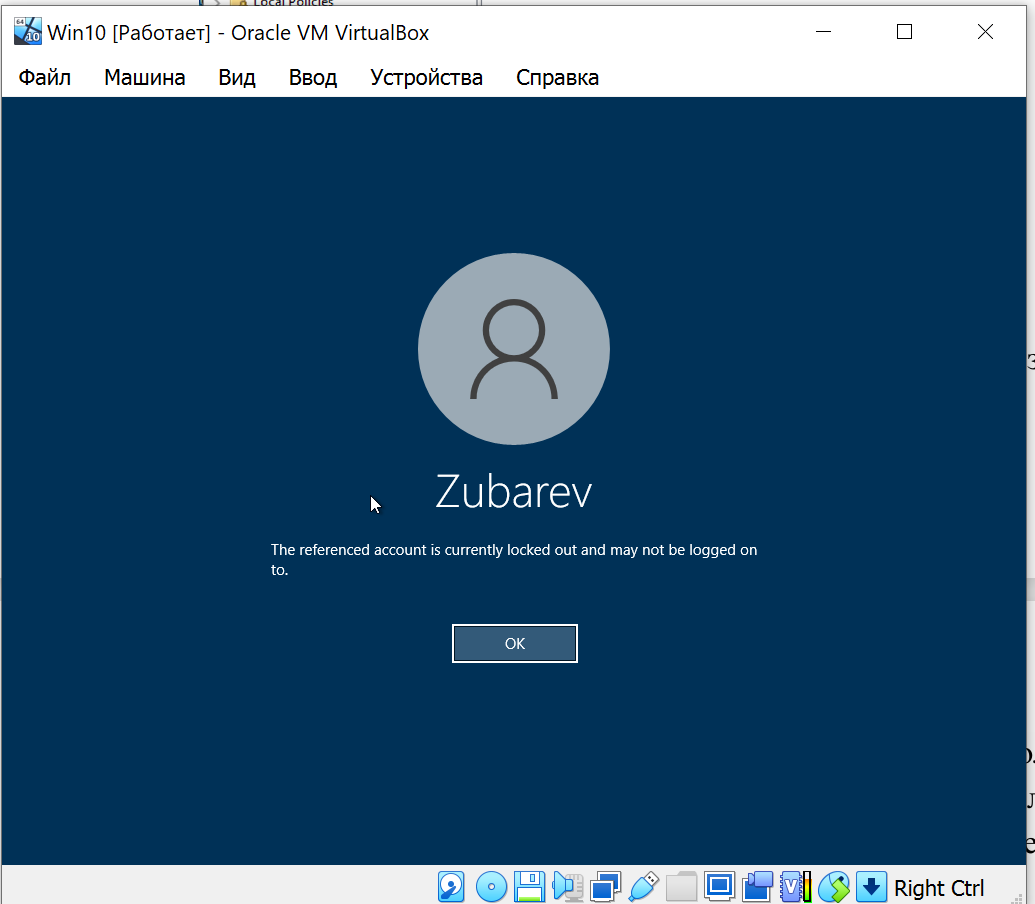


**Запишите в отчет, что означают данные параметры.**Account lockout duration -длительность в минутах блокировки аккаунта прежде, чем он будет заблокирован

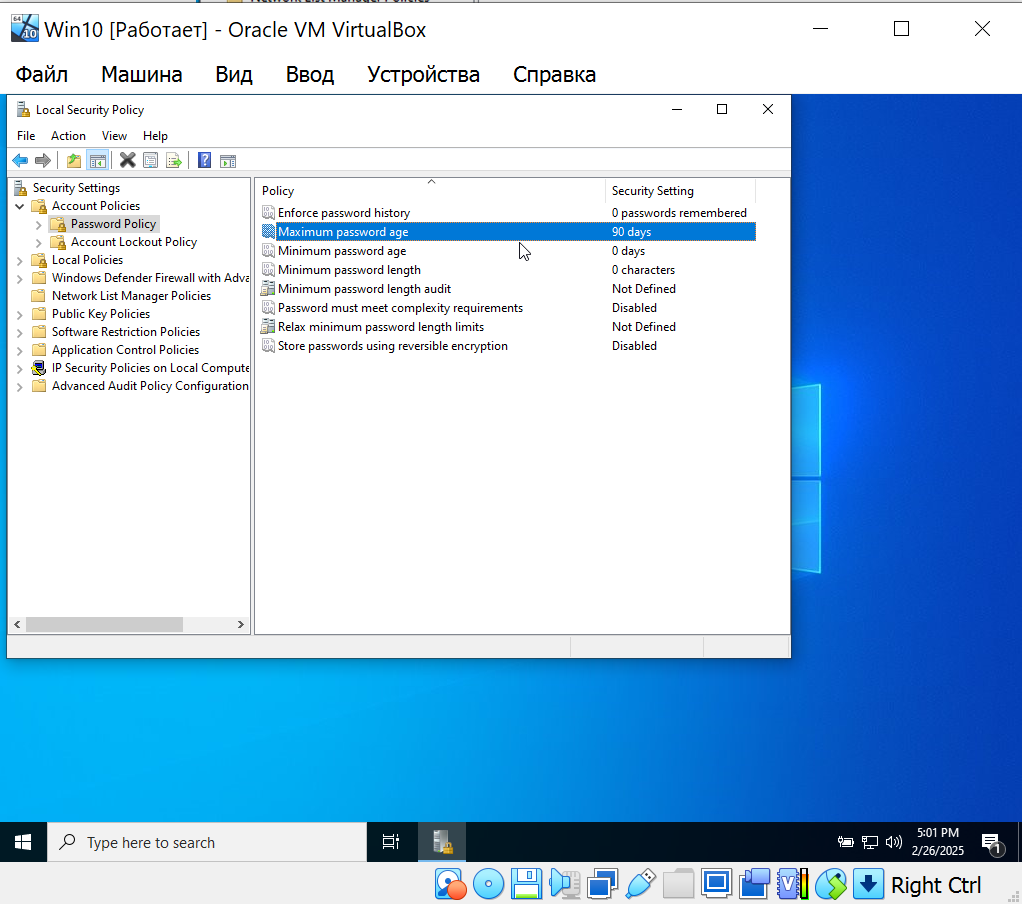
Account lockout threshold – количество неверных попыток (подряд) ввода пароля, для блокировки аккаунта

Reset account lockout counter after – время, в минутах, после которого счетчик неправильных вводов пароля сбросится до 0

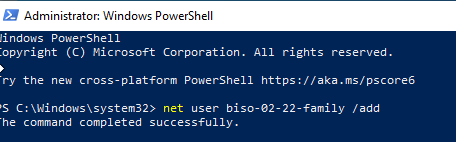
**Добейтесь блокировки пользователя (screenshot).**



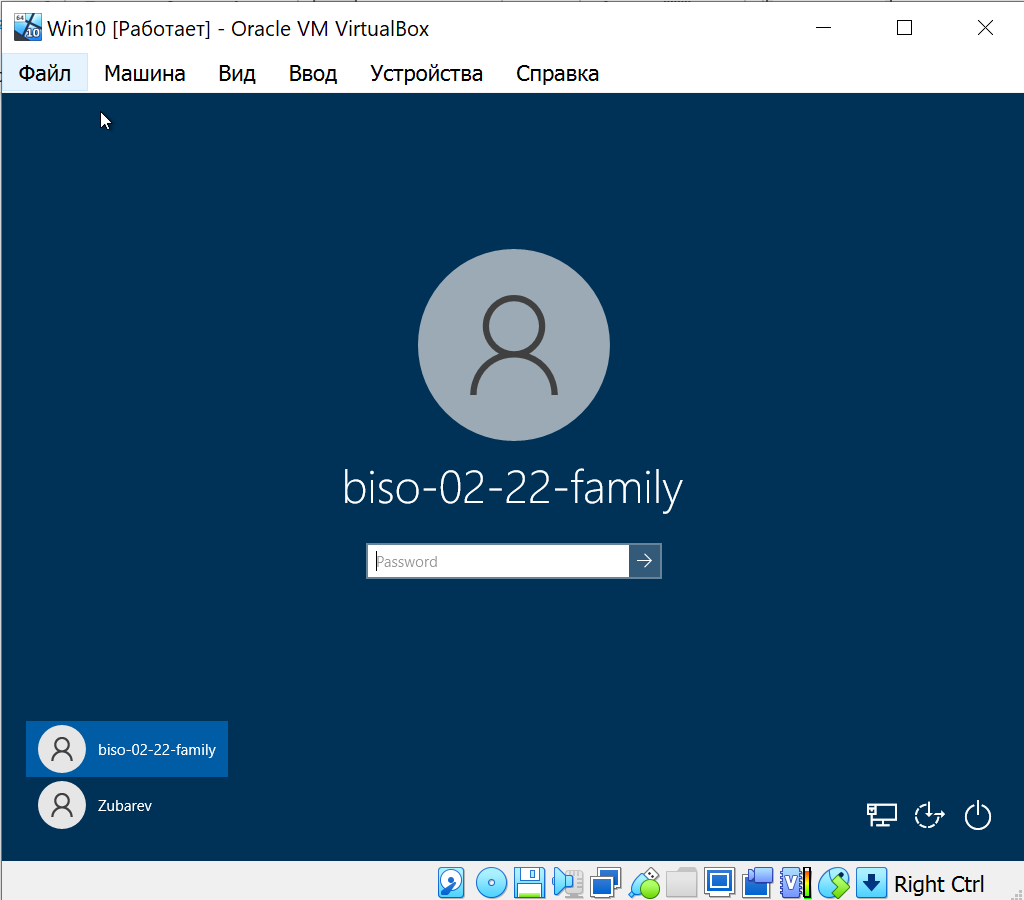
**Выполните настройку политики паролей (screenshot).**



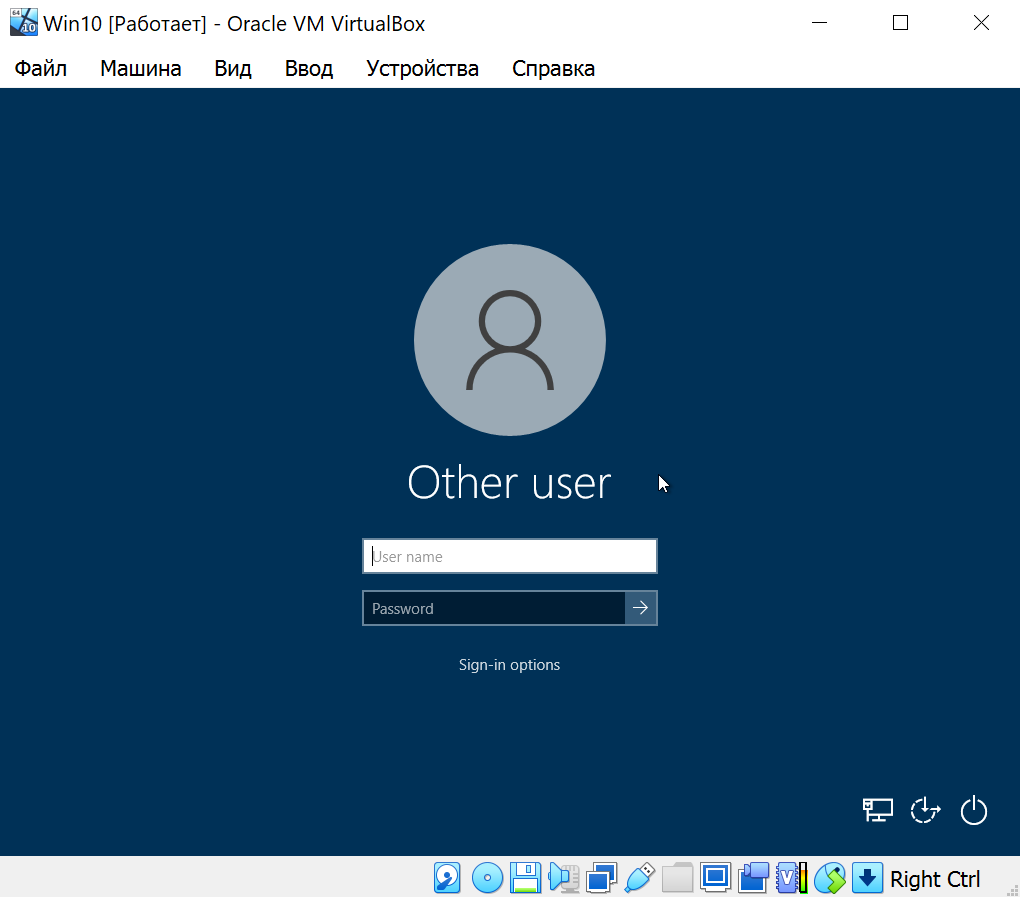
**Создайте нового пользователя с именем biso-0\*-22-family, задайте ему пароль (screenshot).**

****

****

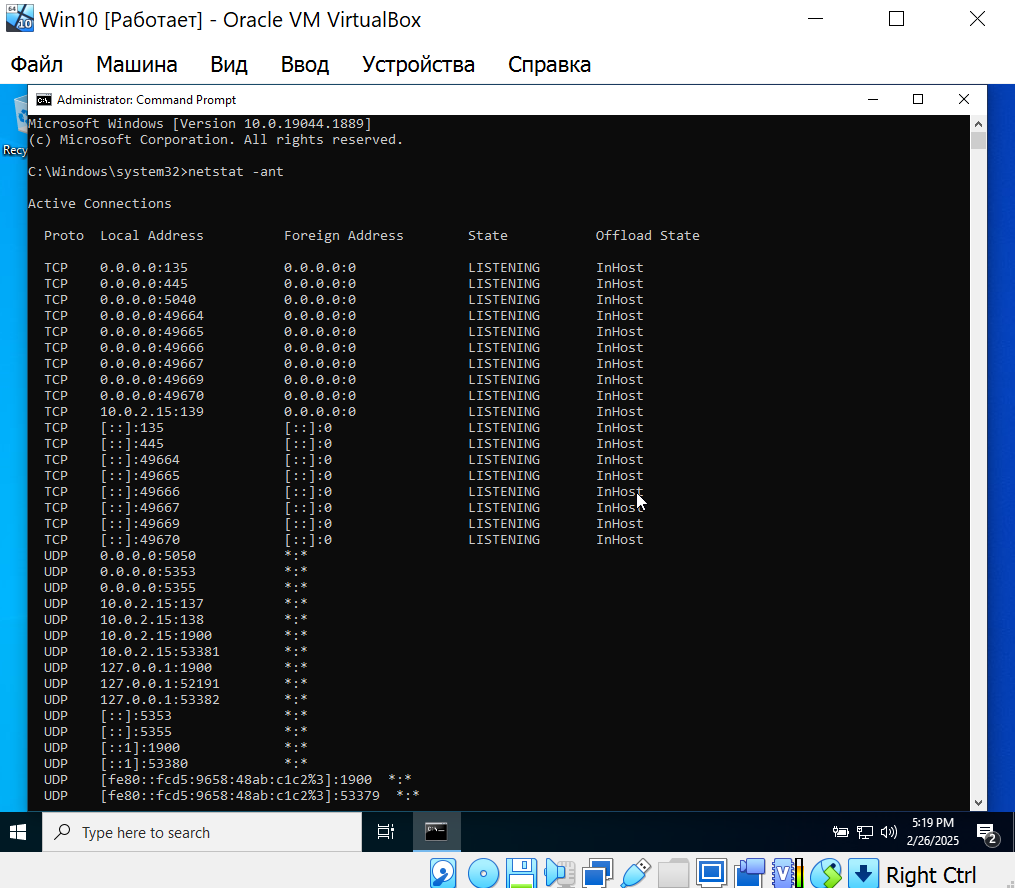
****

Вход после выполнения настроек сокрытия информации

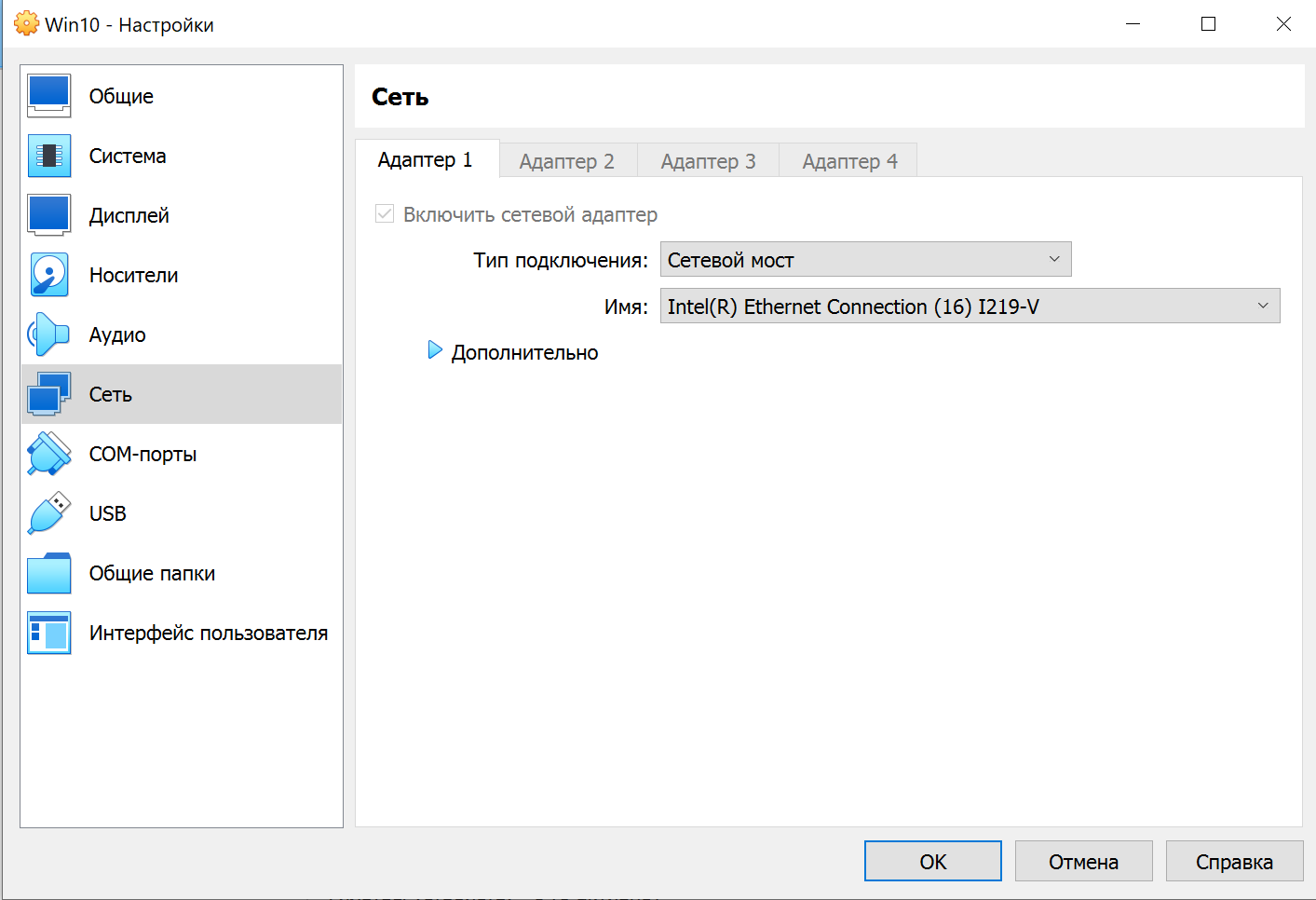


**Пункт 2.2**

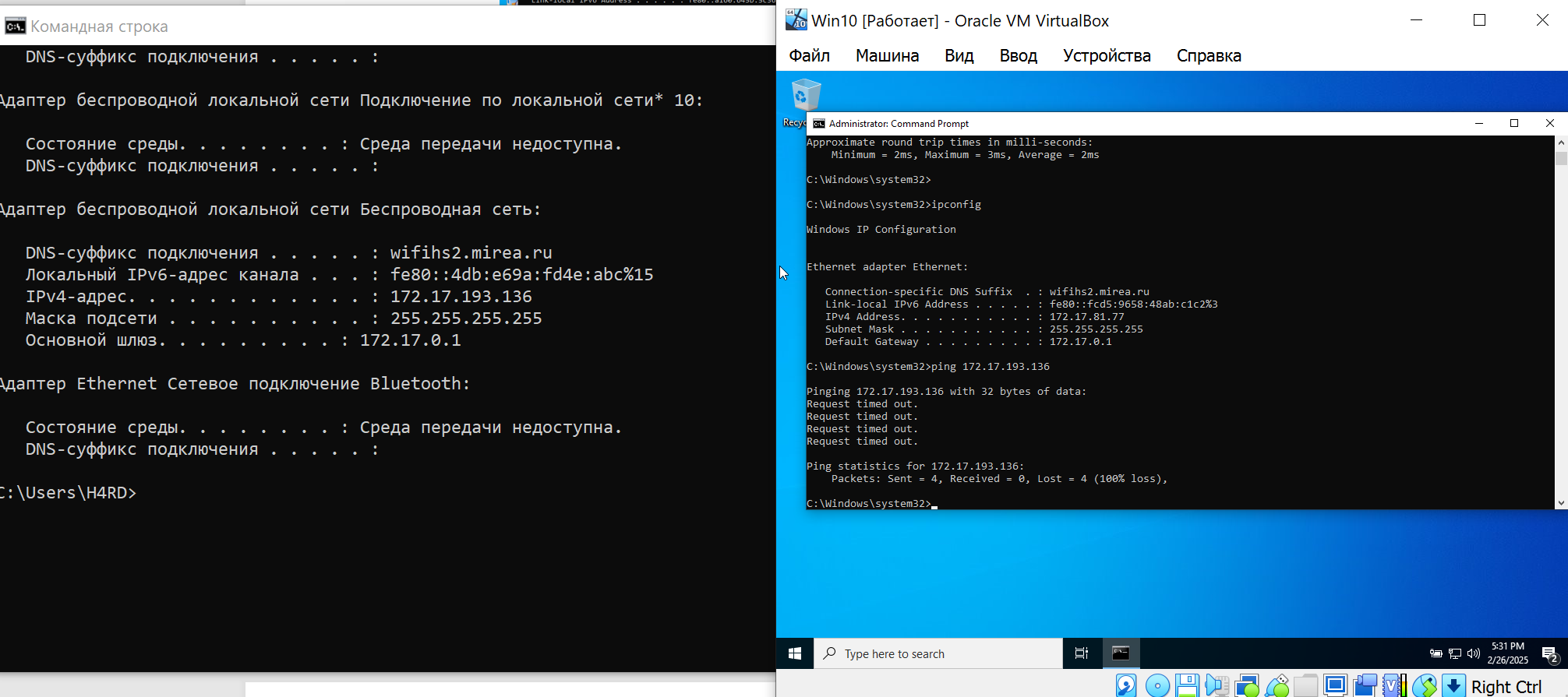
Выполнение netstat – ant



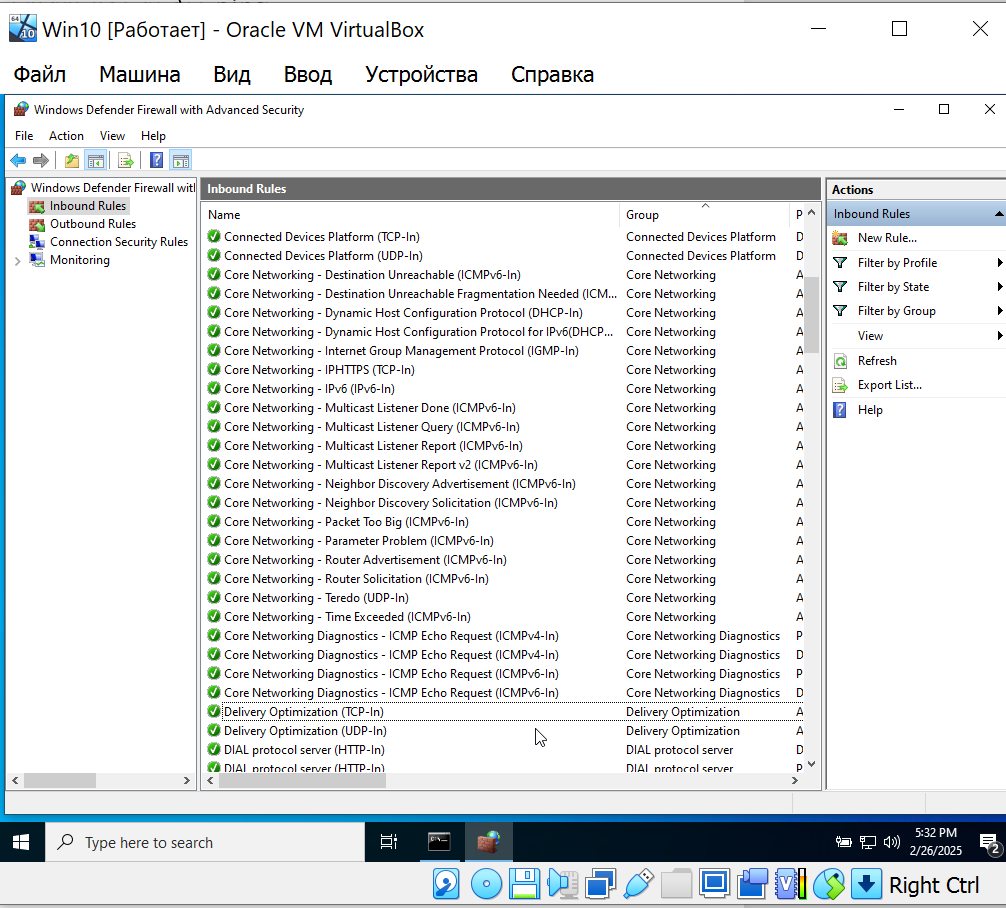
Изменения параметров адаптера на сетевой мост

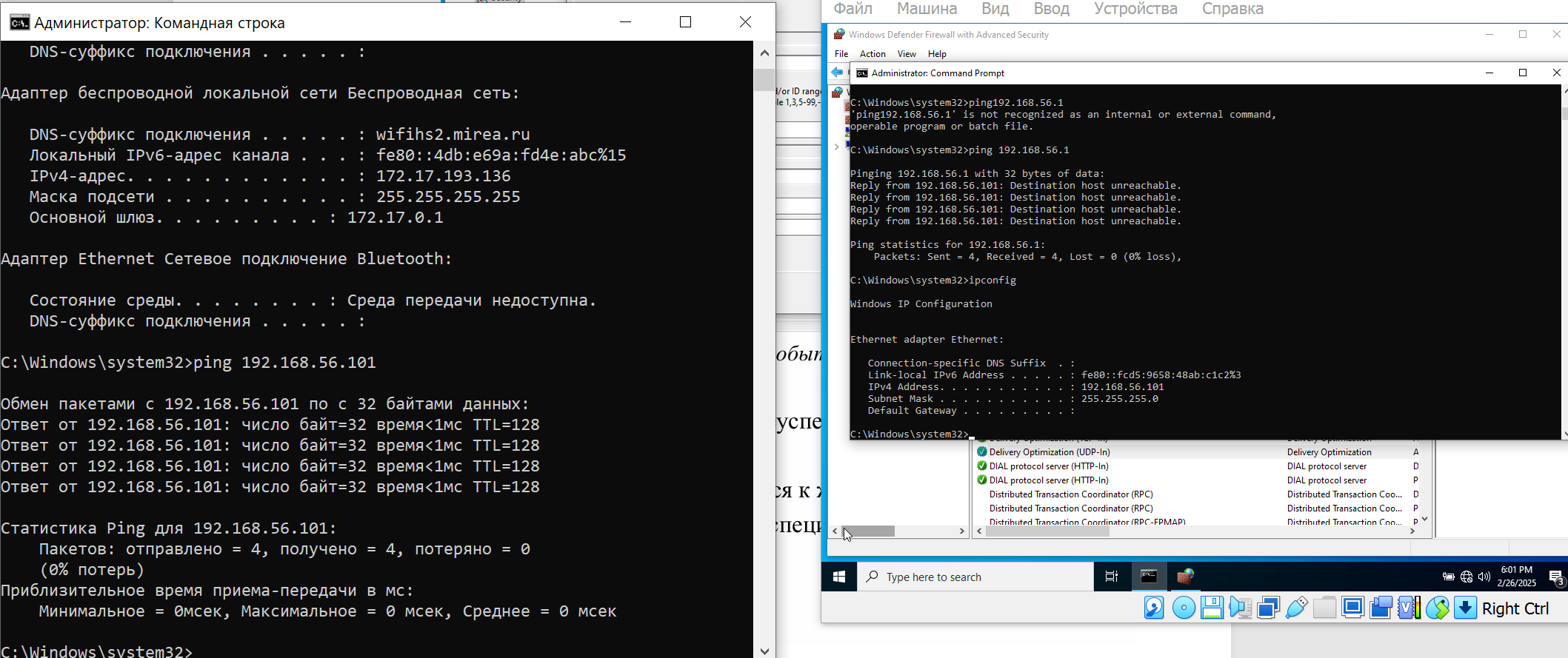


Пинг хоста



Отключение блокировки ICMP трафика



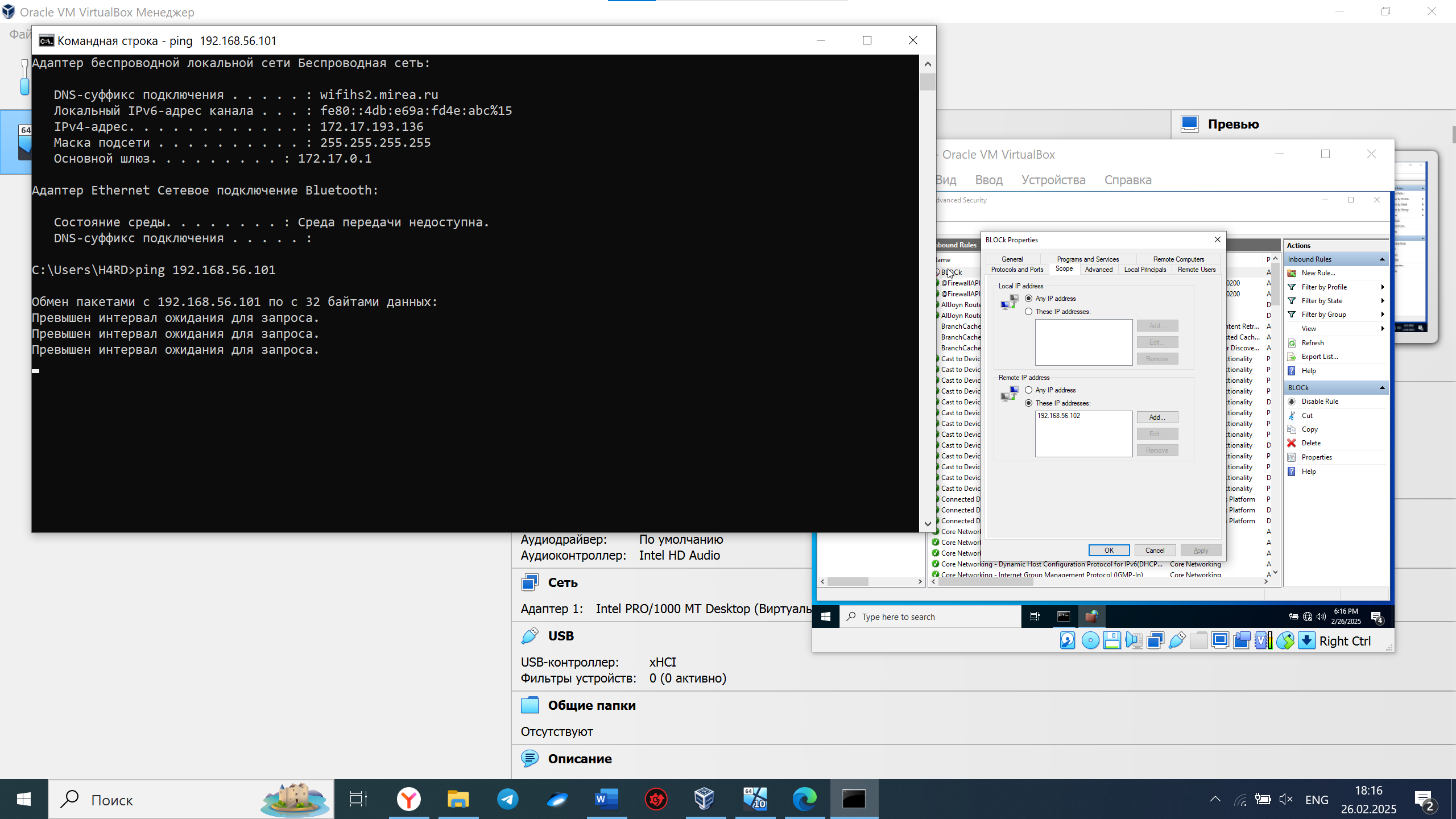
Пинг с хоста виртуальной машины

**Объясните, почему получен результат, показанный на рисунке 10.**

Мы разрешили принимать сетевой трафик icmpv4 на гостевой машине. До изменения параметров такой трафик блокировался.

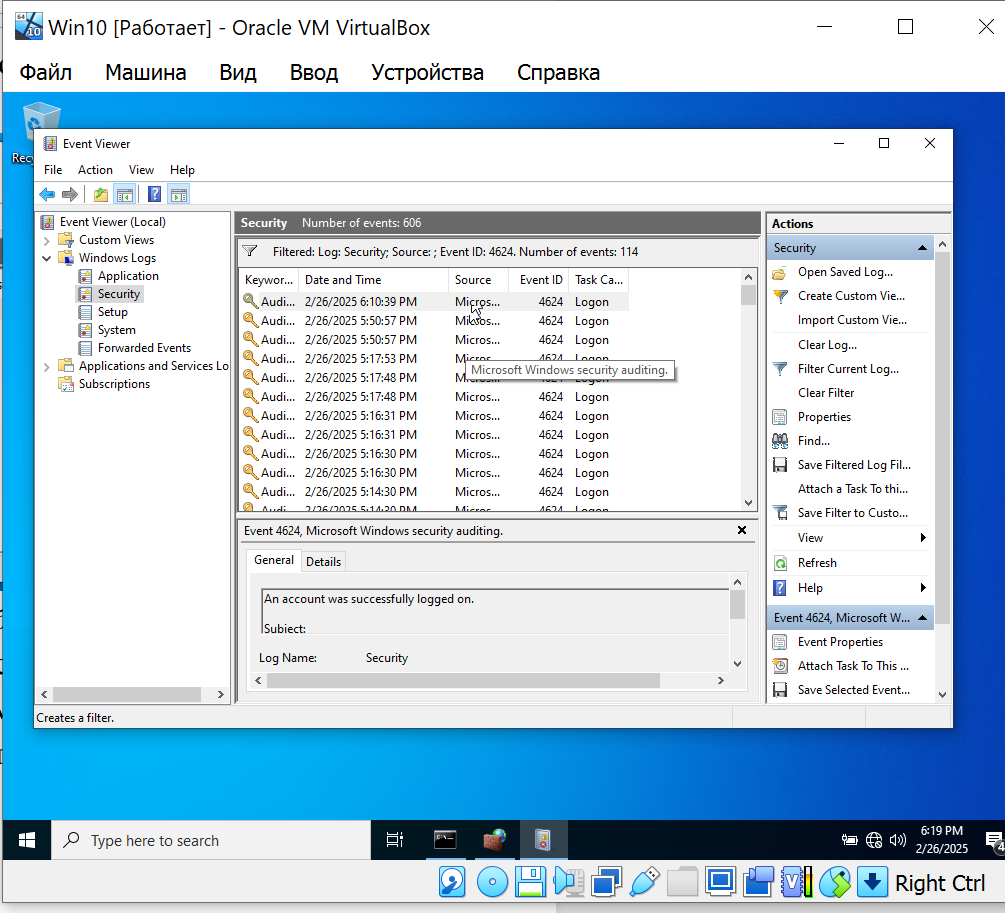
**Какой протокол используется командой ping и на каком уровне модели OSI он работает? (screenshot)**

Команда ping использует протокол ICMP. Уровень модели OSI, на котором работает ICMP, — третий.

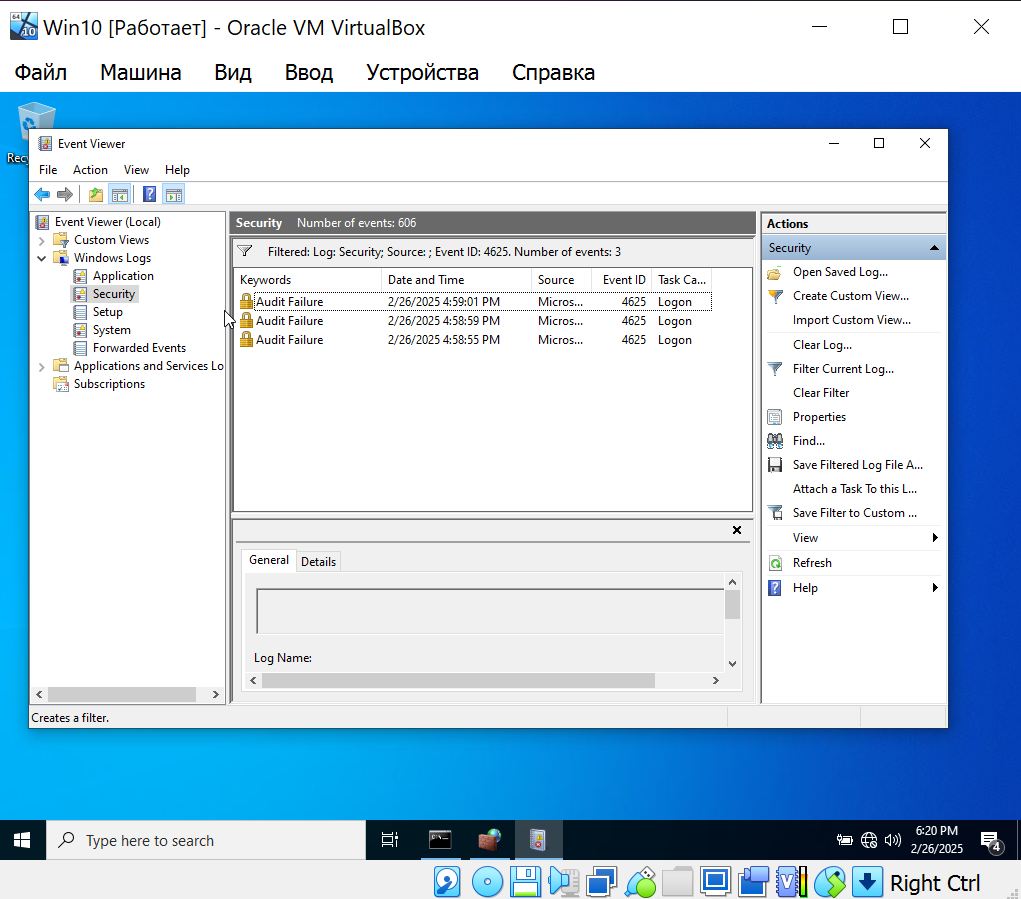


Задание 3.3

Отфильтрованный (по 4624) журнал безопасности



**Найдите все события, связанные с неуспешным входом пользователя в систему**



**Напишите в каких случаях обращаются к журналам событий Windows.**

Диагностика ошибок  
Расследования инцидентов ИБ

**Напишите ПО, которое применяется специалистами по ИБ для работы с журналами событий Windows.**

SolarWinLogsAnalyzer

EventLogExplorer

Sysmon