Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

**Отчет по лабораторной работе №6**

**“Межсетевое экранирование”**

Выполнил:

Студент гр. 221701 Телица И.Д.

Проверил: Захаров В.В.

Минск 2024

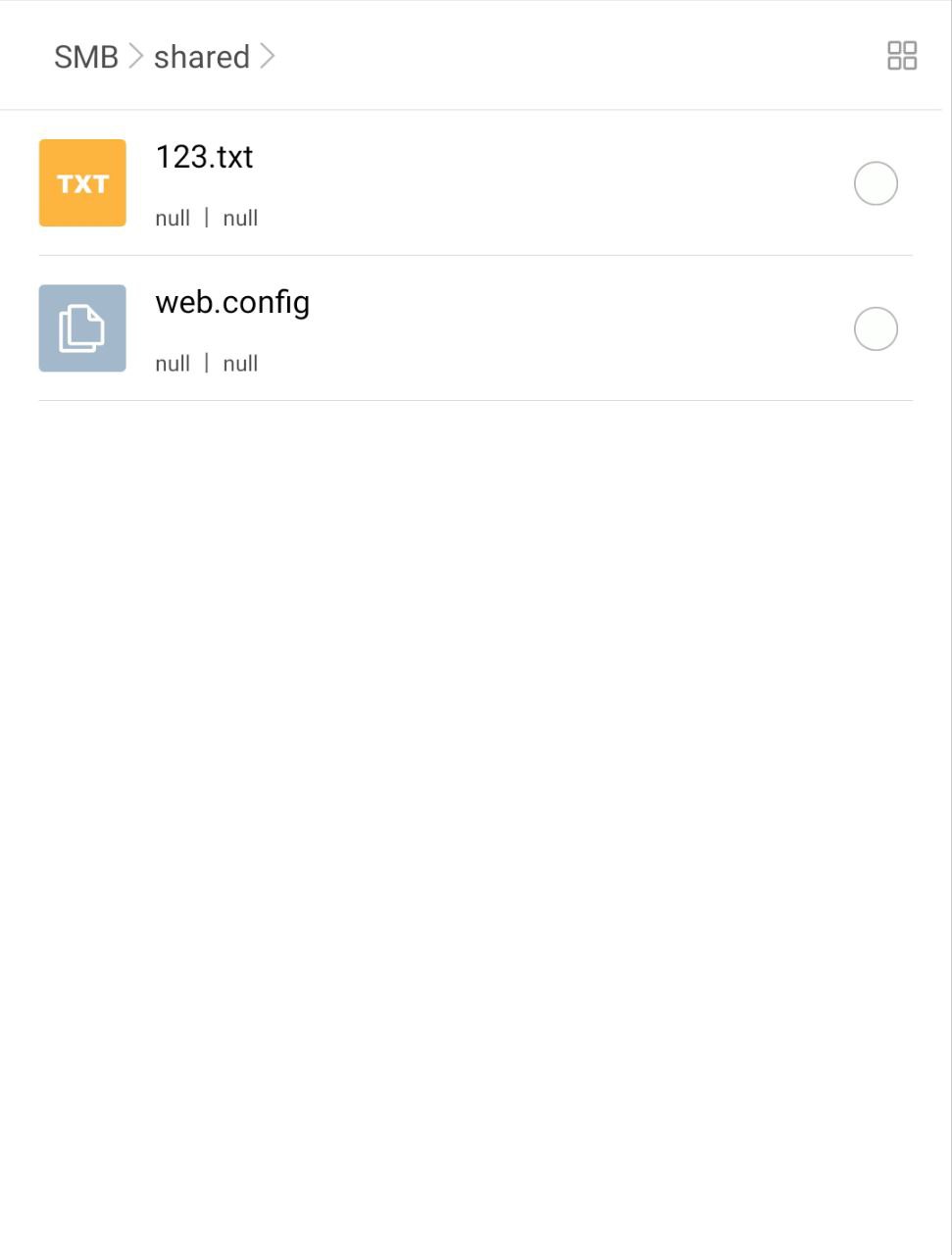
#### **Цель**:

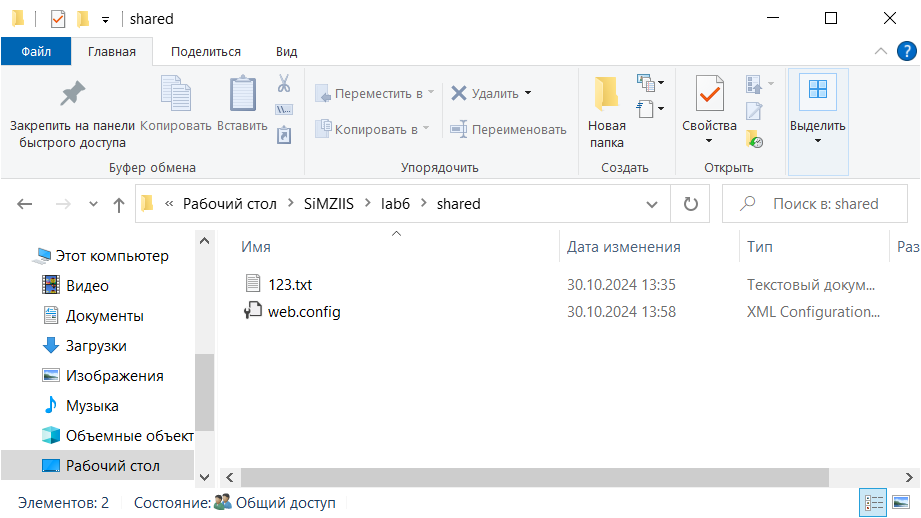
Изучить существующие классы межсетевых экранов. Приобрести

навыки выбора подходящей политики и схемы межсетевого взаимодействия, настройки брандмауэра.

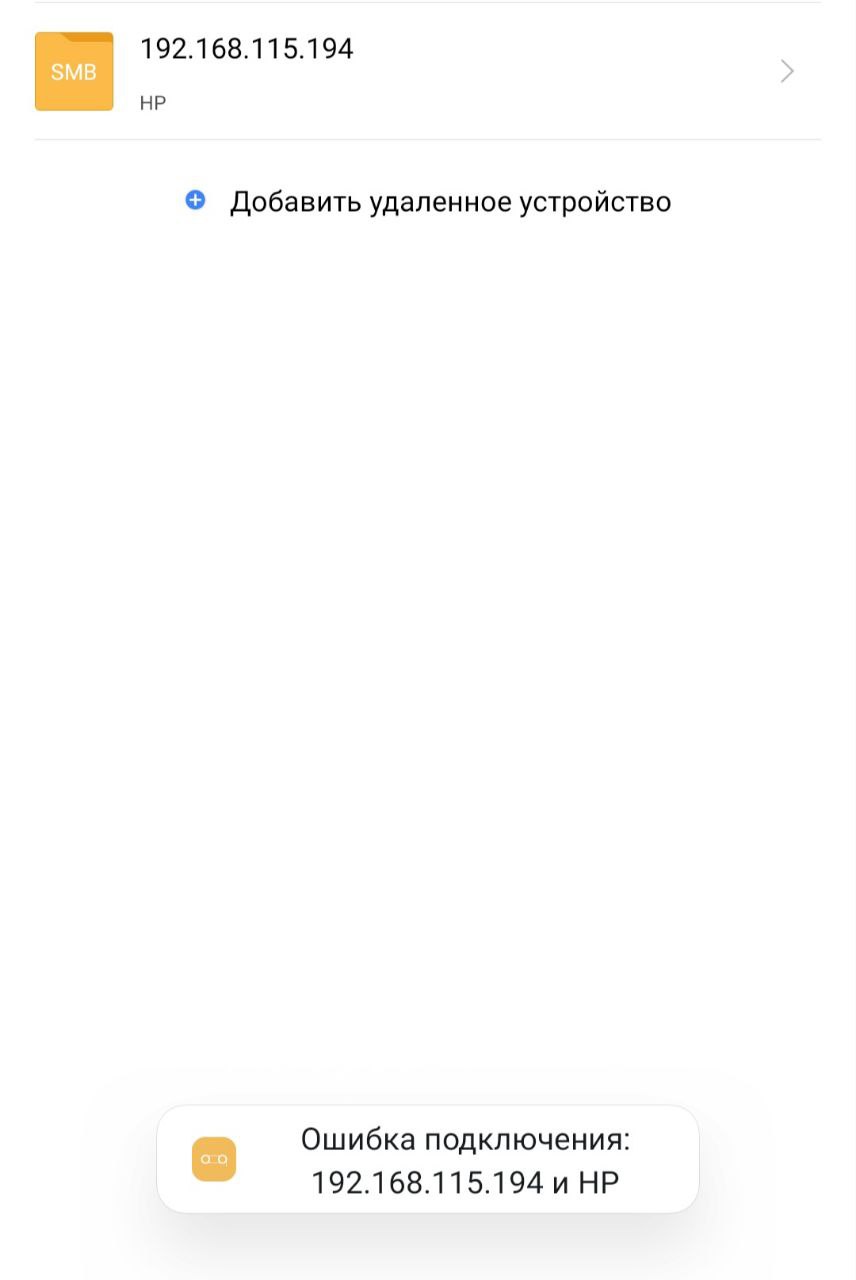
#### **Задание:**

1. Создать папку с общим доступом

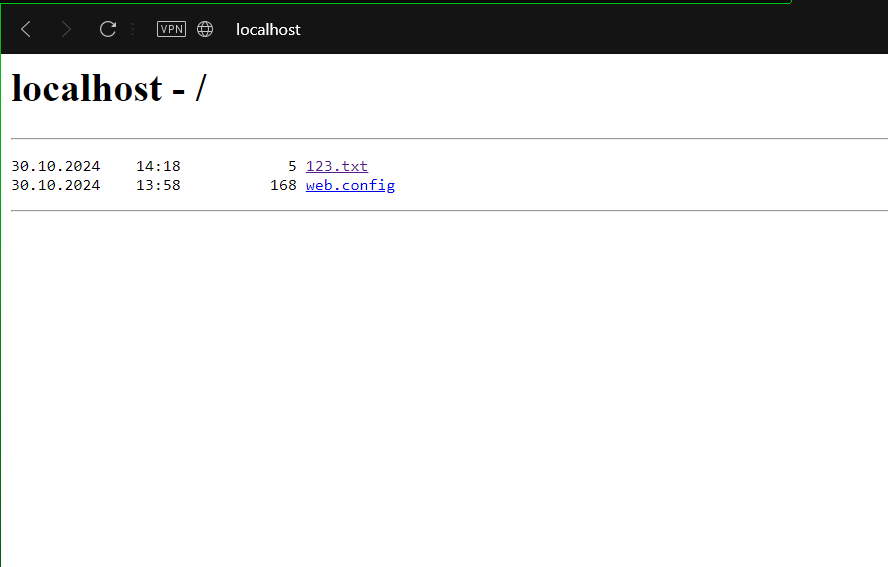


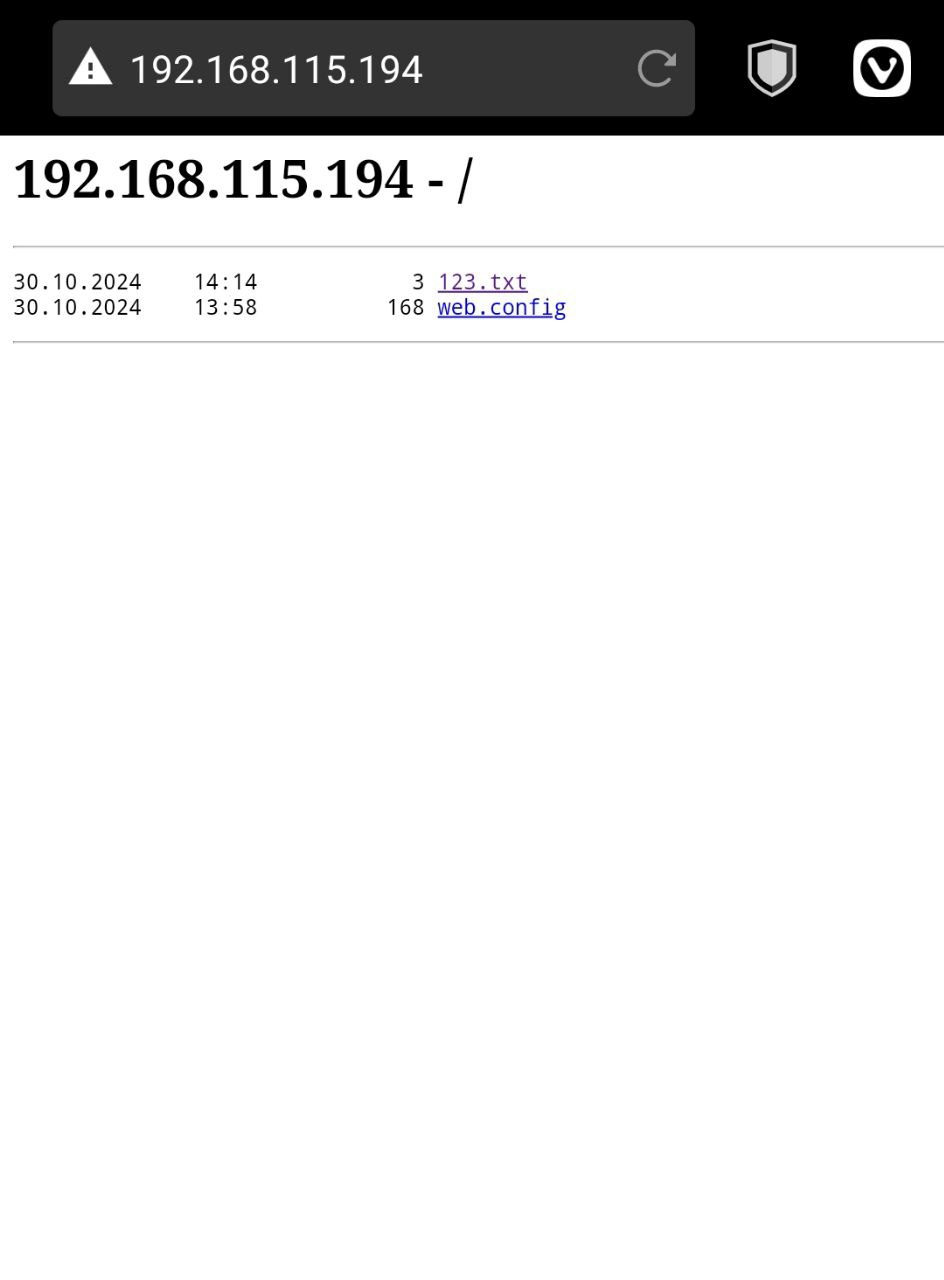


1. Настроить брандмауэр, применив разные политики:
   1. доступ к разделяемому ресурсу разрешен только компьютеру с данным IP-адресом;

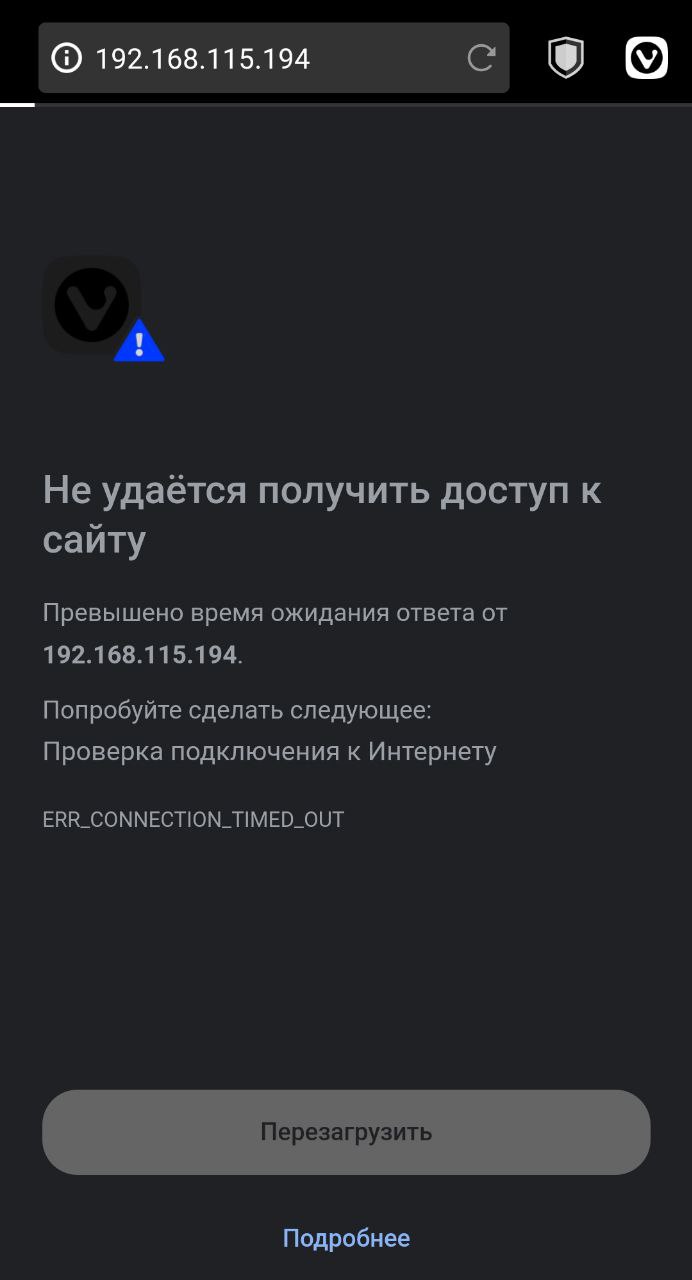


* 1. доступ к виртуальной машине разрешен только по заданным портам(например, www или ftp);





* 1. доступ к виртуальной машине разрешен только по заданным портам(например, www или ftp) и только компьютерам с данным IP-адресом (адресами);

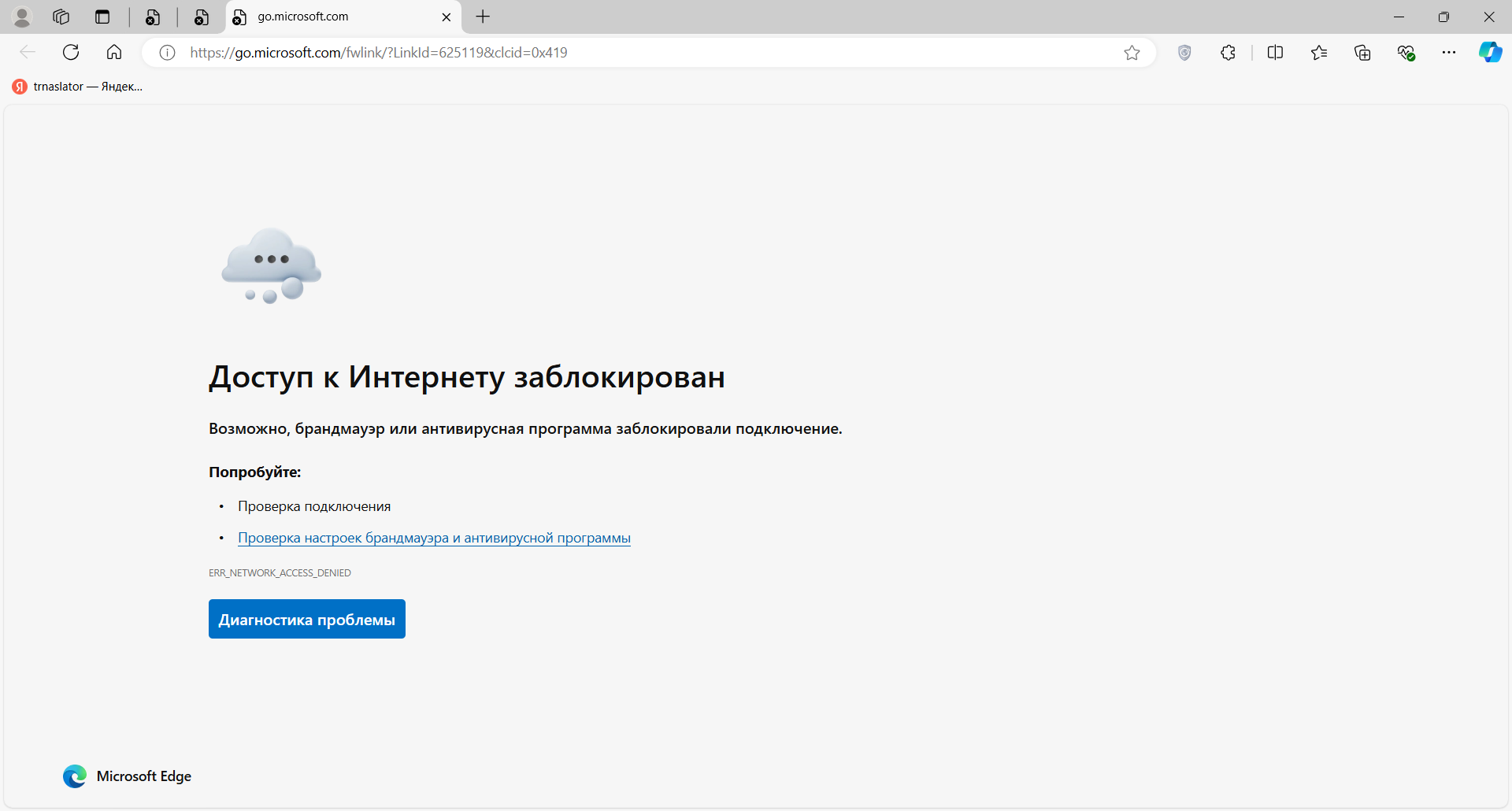


* 1. доступ к внешним ресурсам разрешен только конкретным программам;

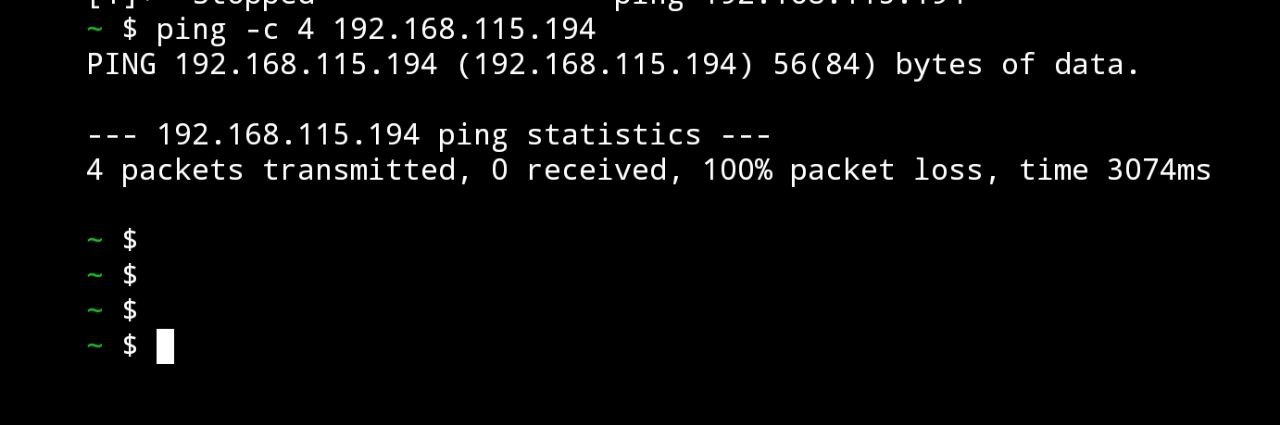
Opera имеет доступ:



Edge не имеет:



* 1. запретить запрос входящего эха (ICMP).



## **Вывод:**

В ходе лабораторной работы познакомились с межсетевым экраном с фильтрацией пакетов, который работает на уровне модели OSI, фильтруя входящие пакеты на основе проверки IP-адресов, типа протокола, номеров портов.

* Плюсы пакетных фильтров, в том что они оказывают минимальное влияние на производительность, дешевы и просты в использовании.
* Минусы:
  + пакетный фильтр анализирует только заголовок и не анализирует поле данных.
  + сложность настройки и администрирования, которое требует создания как минимум двух правил для каждого типа разрешённых взаимодействий.
  + слабая аутентификация трафика, выполняемая только на основе адреса отправителя.