МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет  
информационных технологий, механики и оптики»

Лабораторная работа №4

Выполнил студенты группы М3204:  
Наскальнюк Никита Андреевич

САНКТ-ПЕТЕРБУРГ  
2018

Исследование основных способов обеспечения безопасности в сетях связи

1 Назначение

Приобретение знаний и умений по решению основных задач обеспечения безопасности, возникающих в сетях связи.

2 Цель работы

Формирование навыков по использованию основных инструментов фильтрации трафика в сетях связи – брандмауэров и iptables.

3 Перечень используемого оборудования и ПО

1. Персональный компьютер с установленной ОС Windows, или ОС Linux или ОС Mac
2. Брандмауэр Windows в ОС Windows или сетевая утилита Iptables в ОС Linux и ОС Maс

4 Порядок выполнения работы

4.1 Работа с брандмауэром Windows

4.1.1 Включение брандмауэра Windows (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Включение и отключение брандмауэра Windows*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Включение Брандмауэра»

4.1.2 Настройка брандмауэра Windows (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Брандмауэр Windows в режиме повышенной безопасности*). **Определить активный профиль**. Сделать скриншот и сохранить его. Формат названия файла скриншота «Профили Брандмауэра Windows»

Настроить активный профиль в параметры по умолчанию (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Брандмауэр Windows в режиме повышенной безопасности 🡪 Свойства брандмауэра Windows*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Настройка активного профиля»

4.1.3 Настройка входящих подключений (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Правила для входящих подключений*). **Настроить отображение правил только активного профиля** (*Фильтровать по профилю*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Активные правила входящих подключений»

4.1.4 Создать правила для входящих подключений.

1) Правило блокирующее программу для активного профиля (выбрать самостоятельно из программ, установленных на ПК. Например, Skype). Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка программы <название программы>»

Проверить отработку правила

-запуском программы. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. блокировка приложения <название приложения>.Проверка1»

-просмотром активных соединений в netstat с отображением приложения, инициализирующего подключение «Входящее подключение. Блокировка приложения <название приложения>.Проверка2»

2) Правило блокирующее 22 порт (ssh) по протоколу TCP для активного профиля. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка порта <номер порта>».

Проверить отработку правила попыткой подключения с другого компьютера через putty по ssh. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка порта <номер порта>.Проверка»

3) Правило блокирующее сетевой адрес с локальной сети. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка сетевого адреса <сетевой адрес>»

Проверить отработку правила с помощью сетевой утилиты ping со второго компьютера. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка сетевого адреса <сетевой адрес>.Проверка»

4.1.5 Настройка исходящих подключений (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Правила для исходящих подключений*). **Настроить отображение правил только активного профиля** (*Фильтровать по профилю*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Активные правила исходящих подключений»

4.1.6 Создать правила для исходящих подключений.

1) Правило блокирующее программу для активного профиля (выбрать самостоятельно из программ, установленных на ПК. Например, putty). Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка приложения <название приложения>»

Проверить отработку правила

-запуском программы. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. блокировка приложения <название приложения>.проверка1»

-просмотром активных соединений в netstat с отображением приложения, инициализирующего подключение «Исходящее подключение. Блокировка приложения <название приложения>.проверка2»

2) Правило блокирующее 80,443 порт (http, https) по протоколу TCP для активного профиля. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка портов <номер портов>».

Проверить отработку правила путем перехода на произвольный url адрес. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка портов <номер портов>.Проверка»

3) Правило блокирующее сетевой адрес с локальной сети. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение.Блокировка сетевого адреса <сетевой адрес>».

Проверить отработку правила с помощью сетевой утилиты ping. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка сетевого адреса <сетевой адрес>.Проверка»

5. Порядок обработки результатов

Windows:

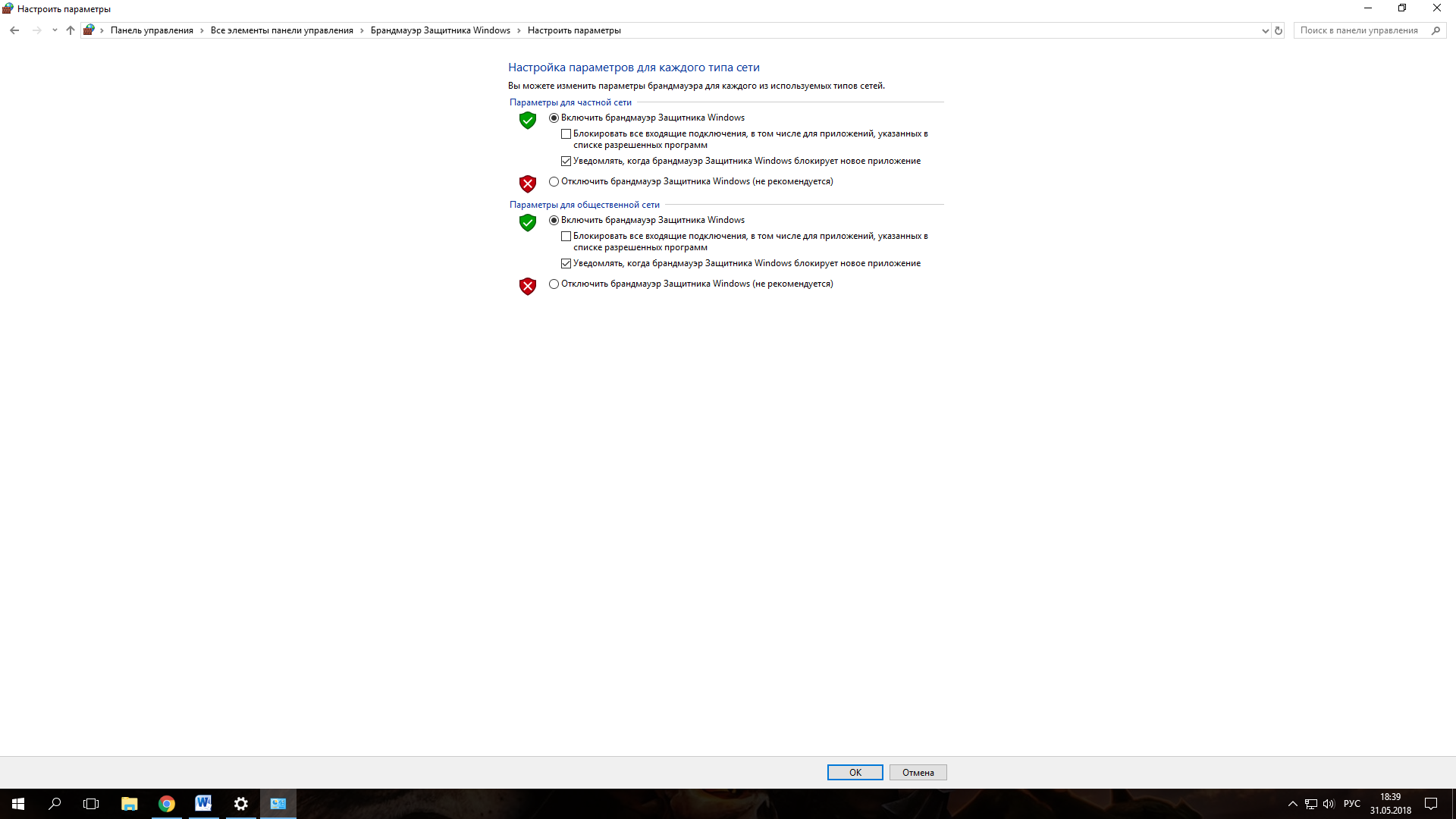


Рис. 1 - «Включения межсетевого экрана»

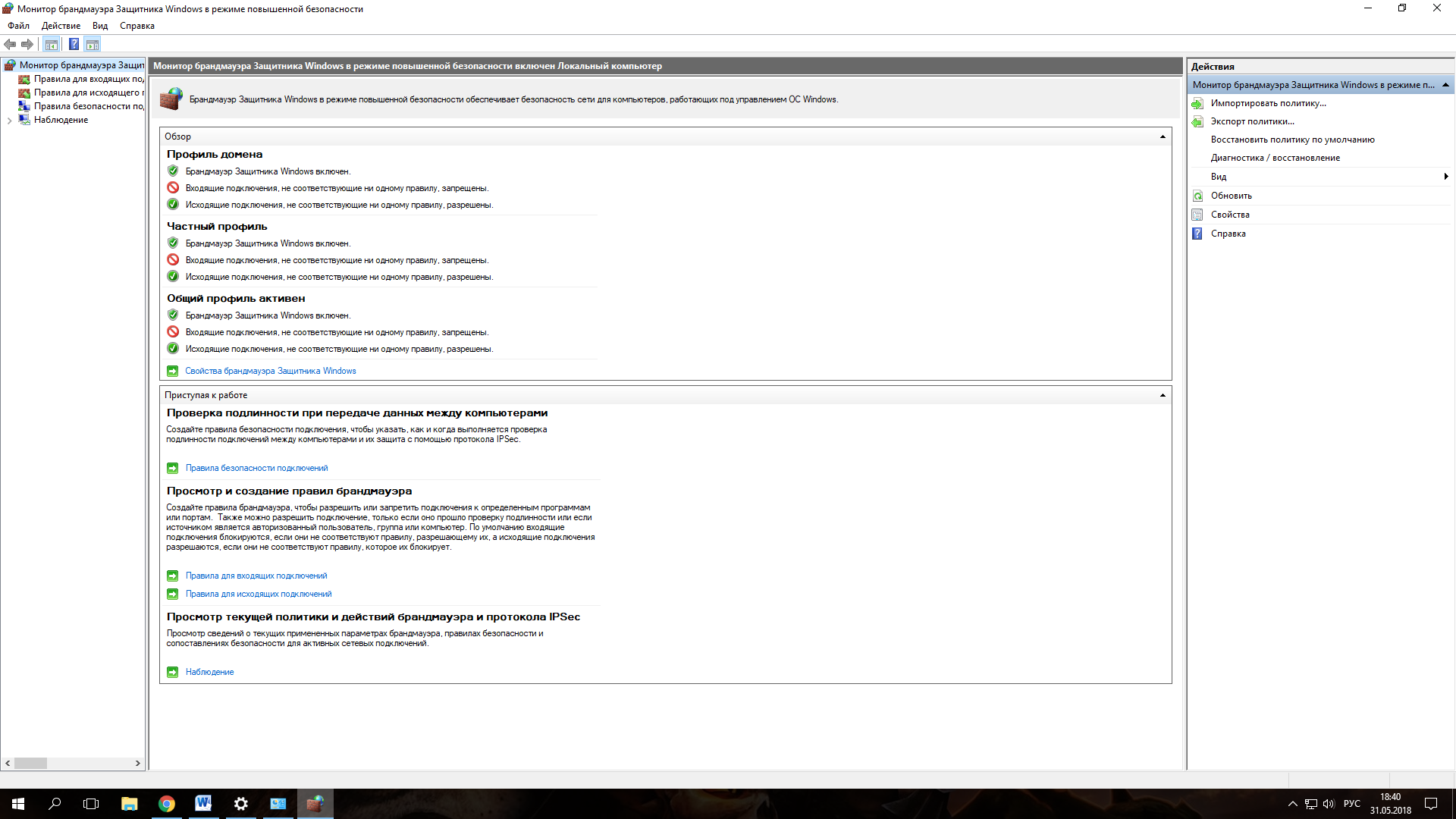


Рис. 2 - «Профили по умолчанию межсетевого экрана»

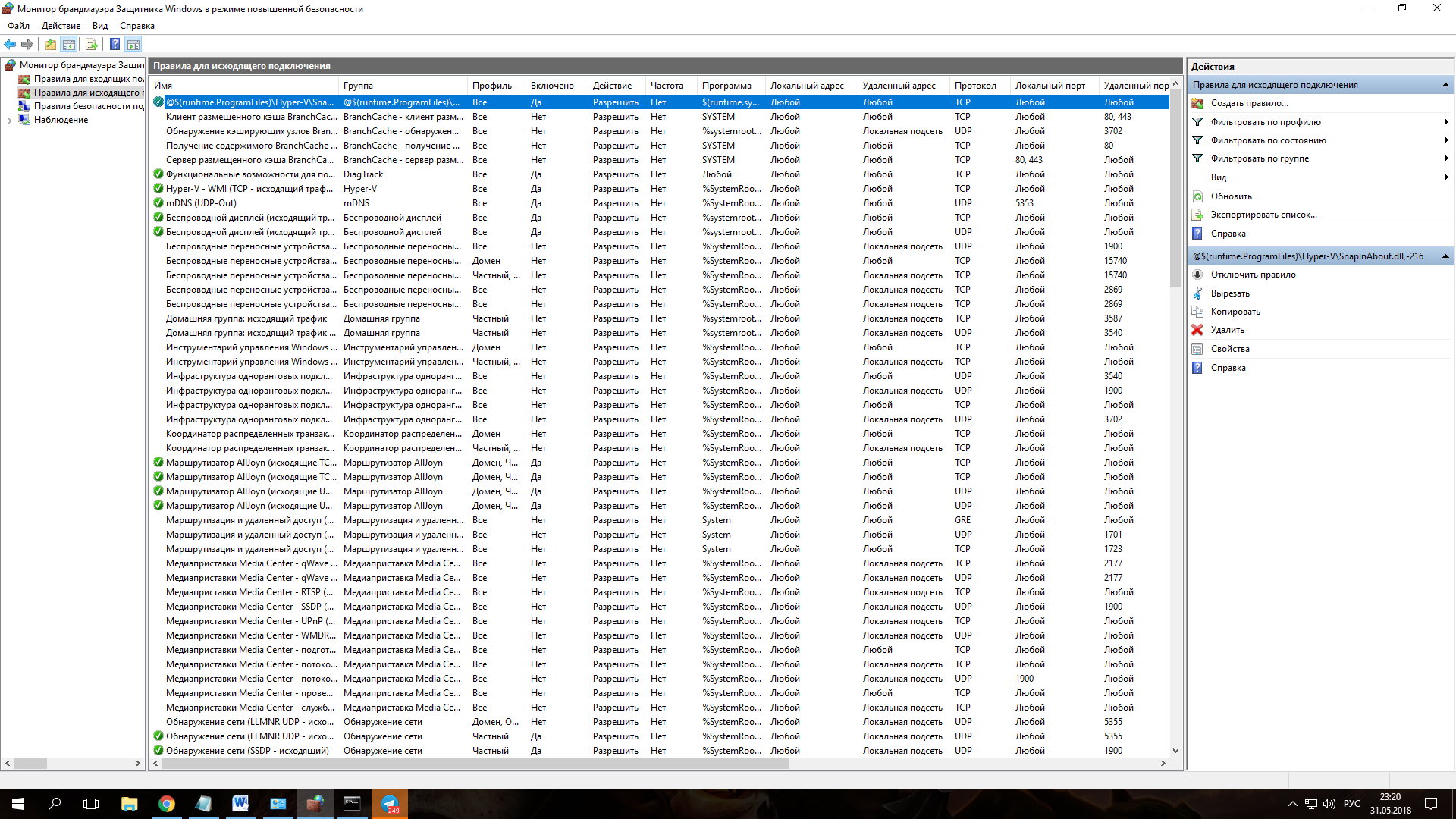
Исходящее подключение. 

Рис. 3 - «Правила для Исходящих подключения»

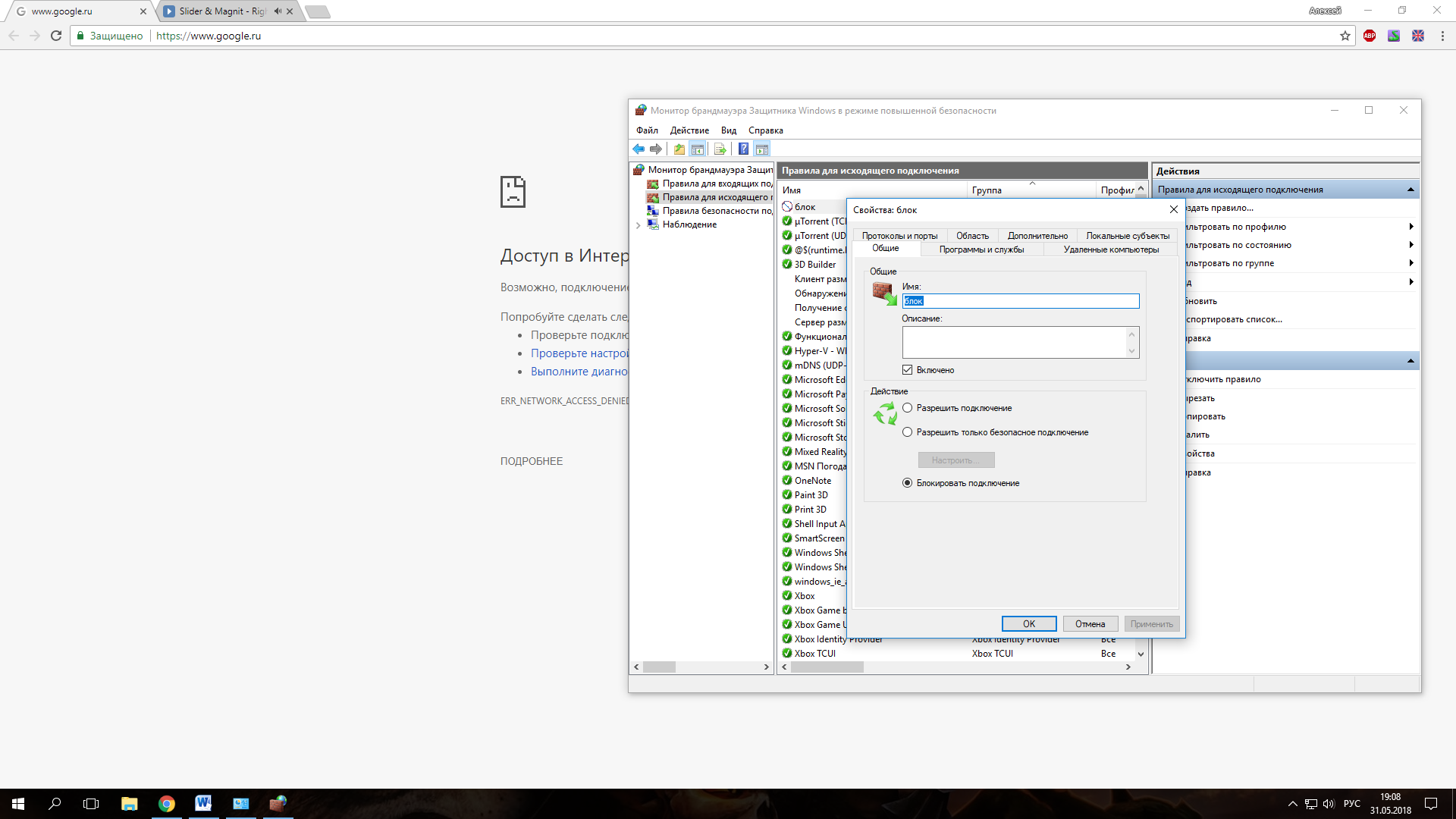


Рис. 4 - «Блокировка приложения Google Chrome»

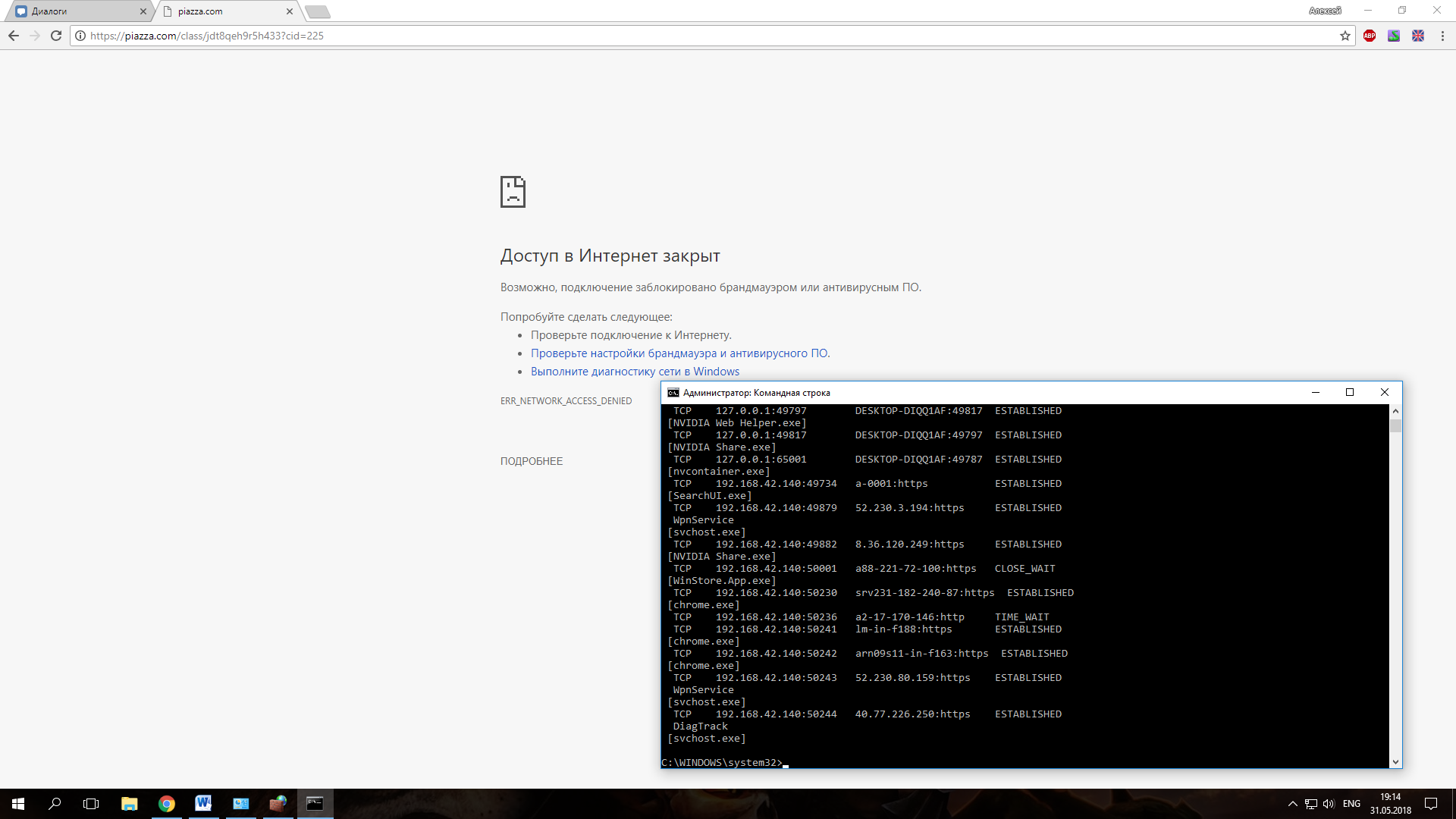
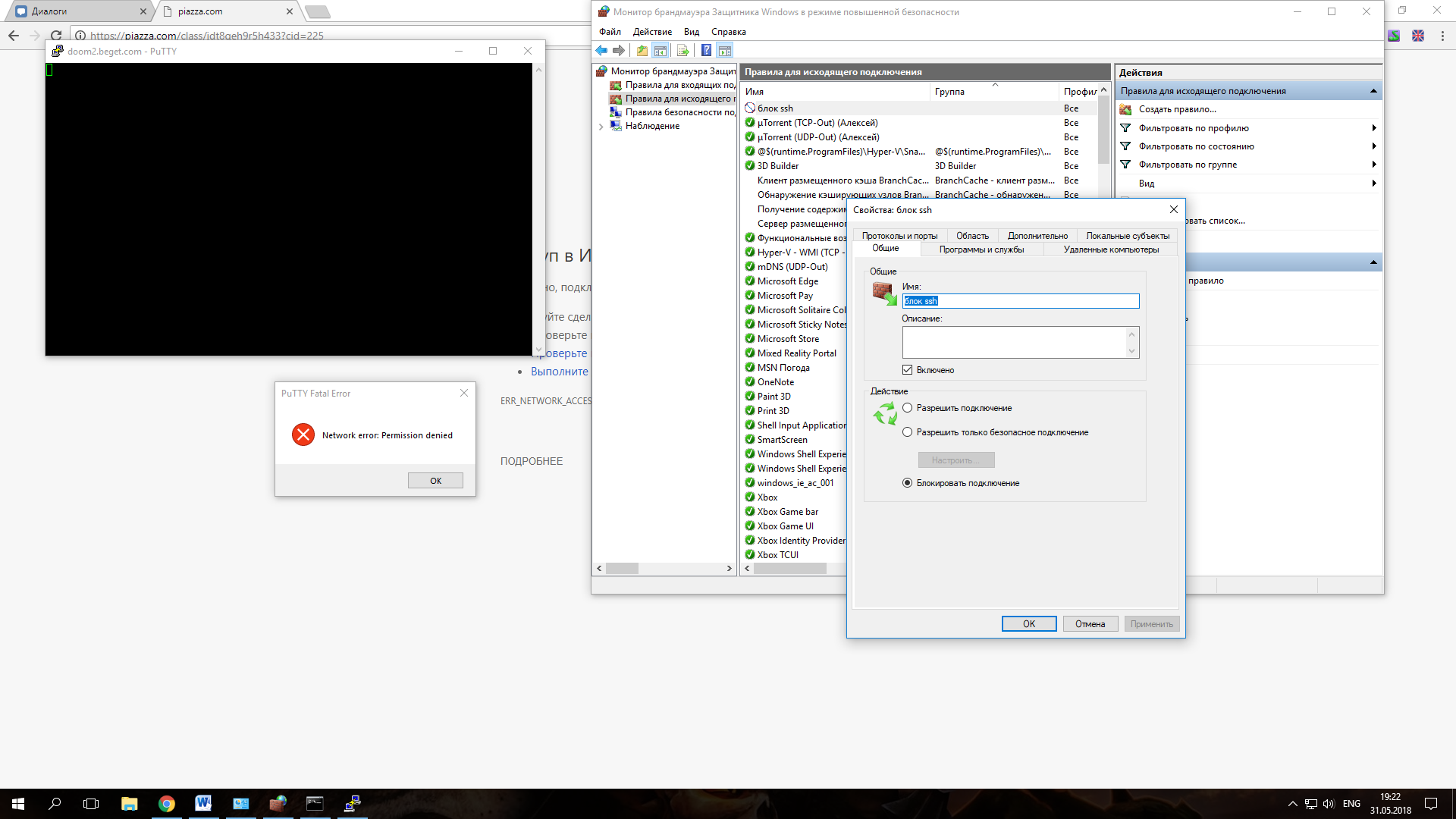


Рис. 5 «Блокировка приложения Google Chrome.Проверка2»

Рис. Рис. 6 - «Блокировка порта ssh»

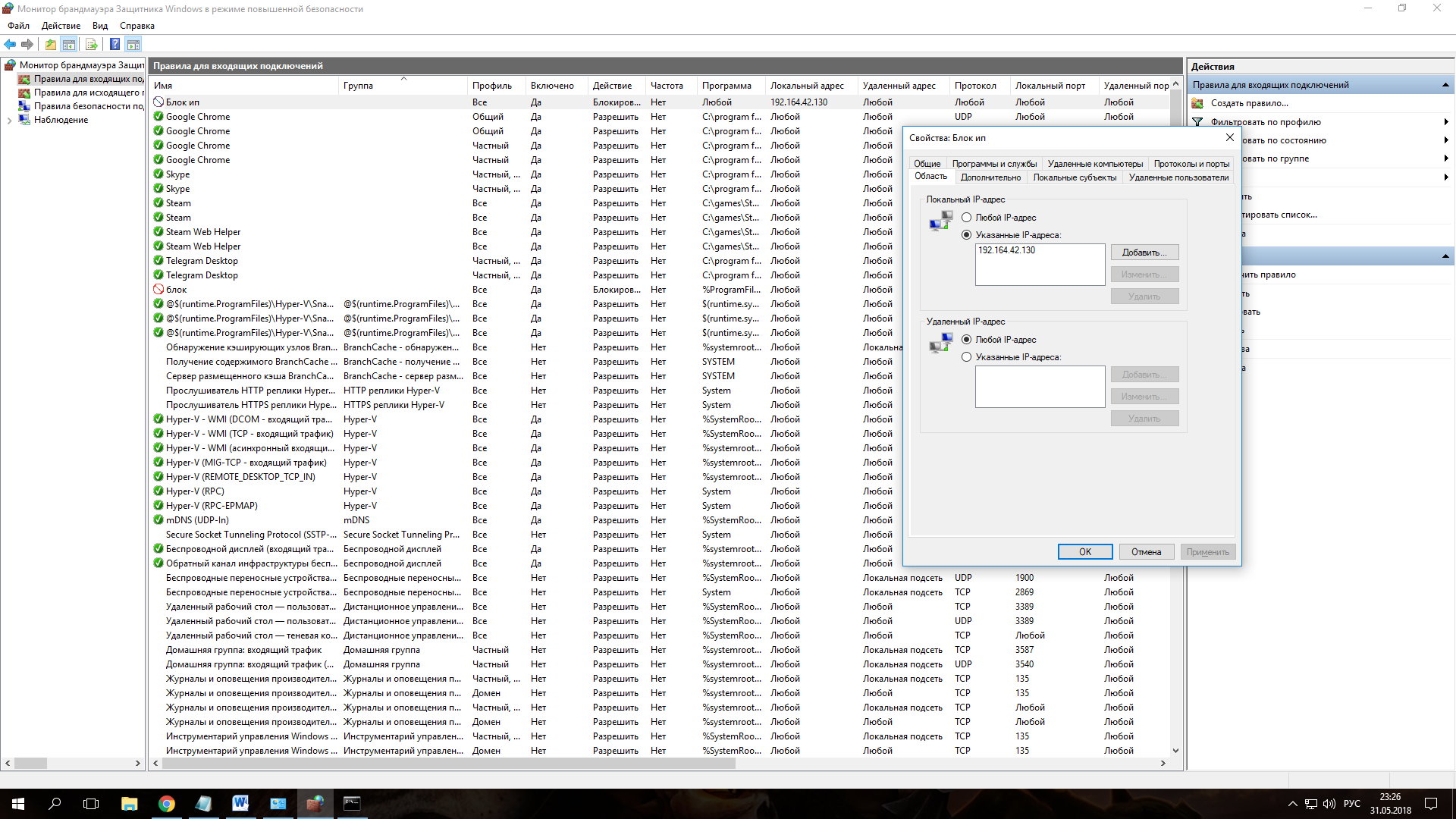


Рис. 9 - «Блокировка сетевого адреса»



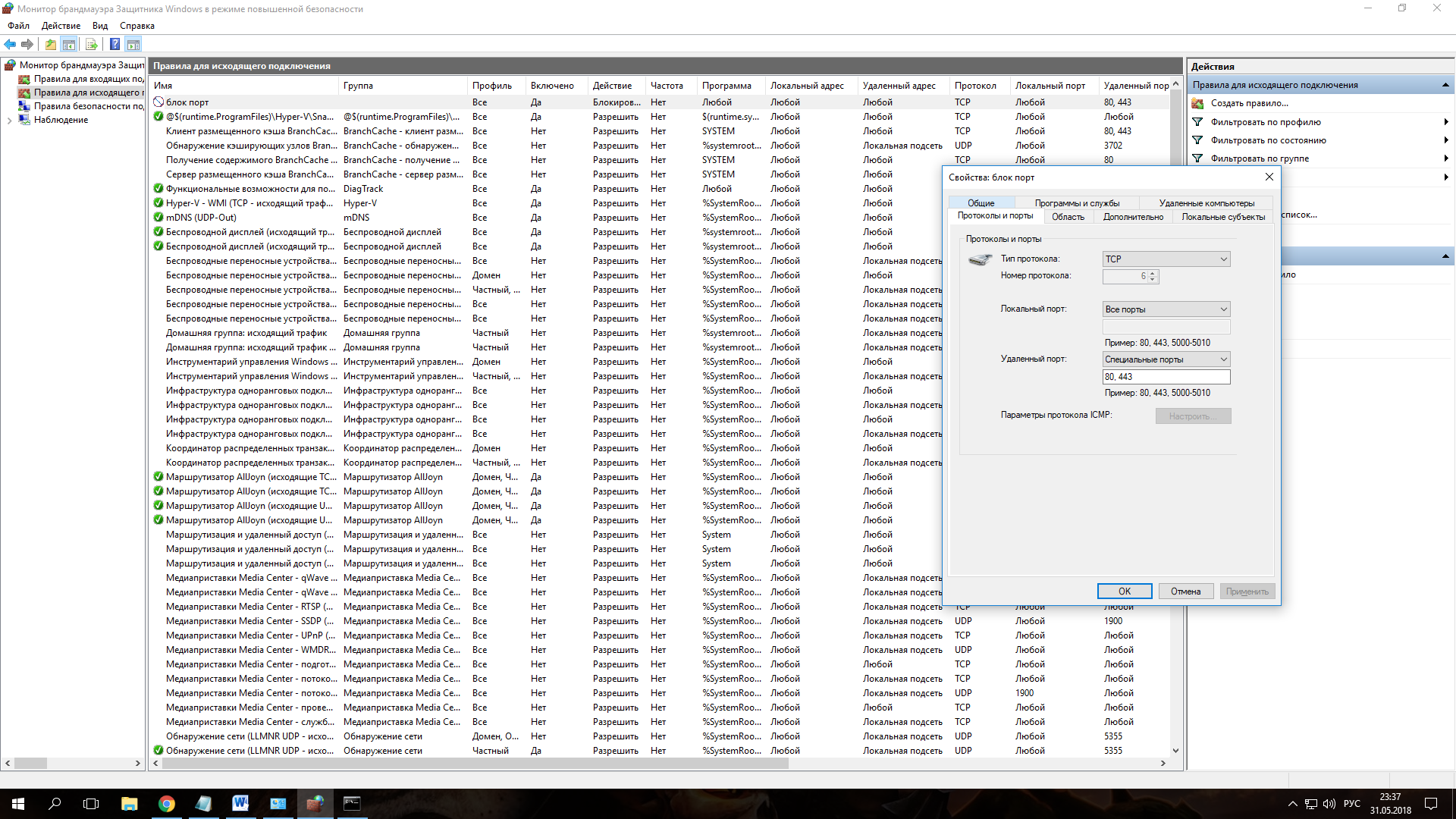
Рис. 10 - «Блокировка сетевого адреса. Проверка» 

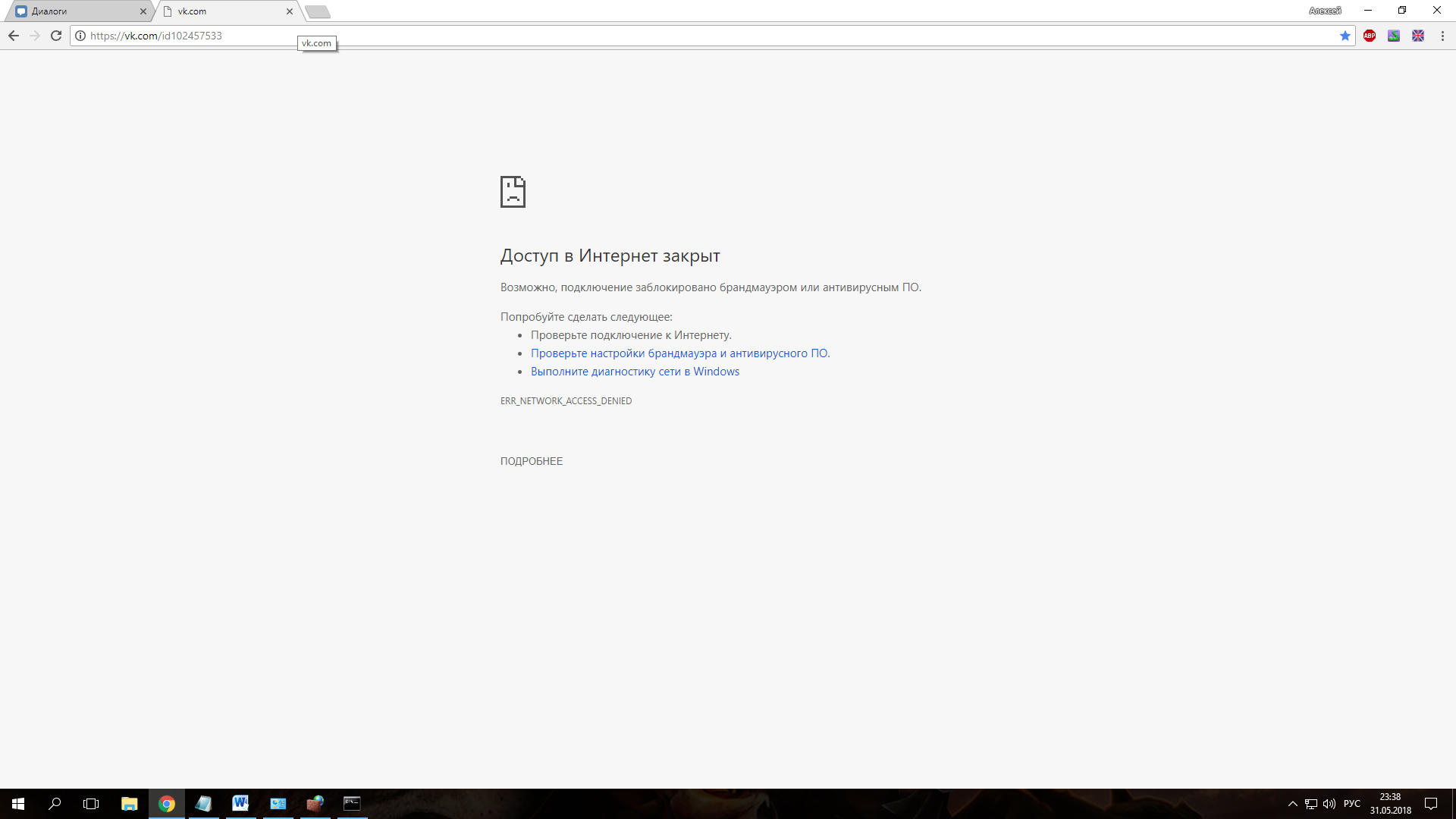
Рис. 11 - «Блокировка порта 80, 443» 

Рис. 16 - «Блокировка порта 80, 443.Проверка»

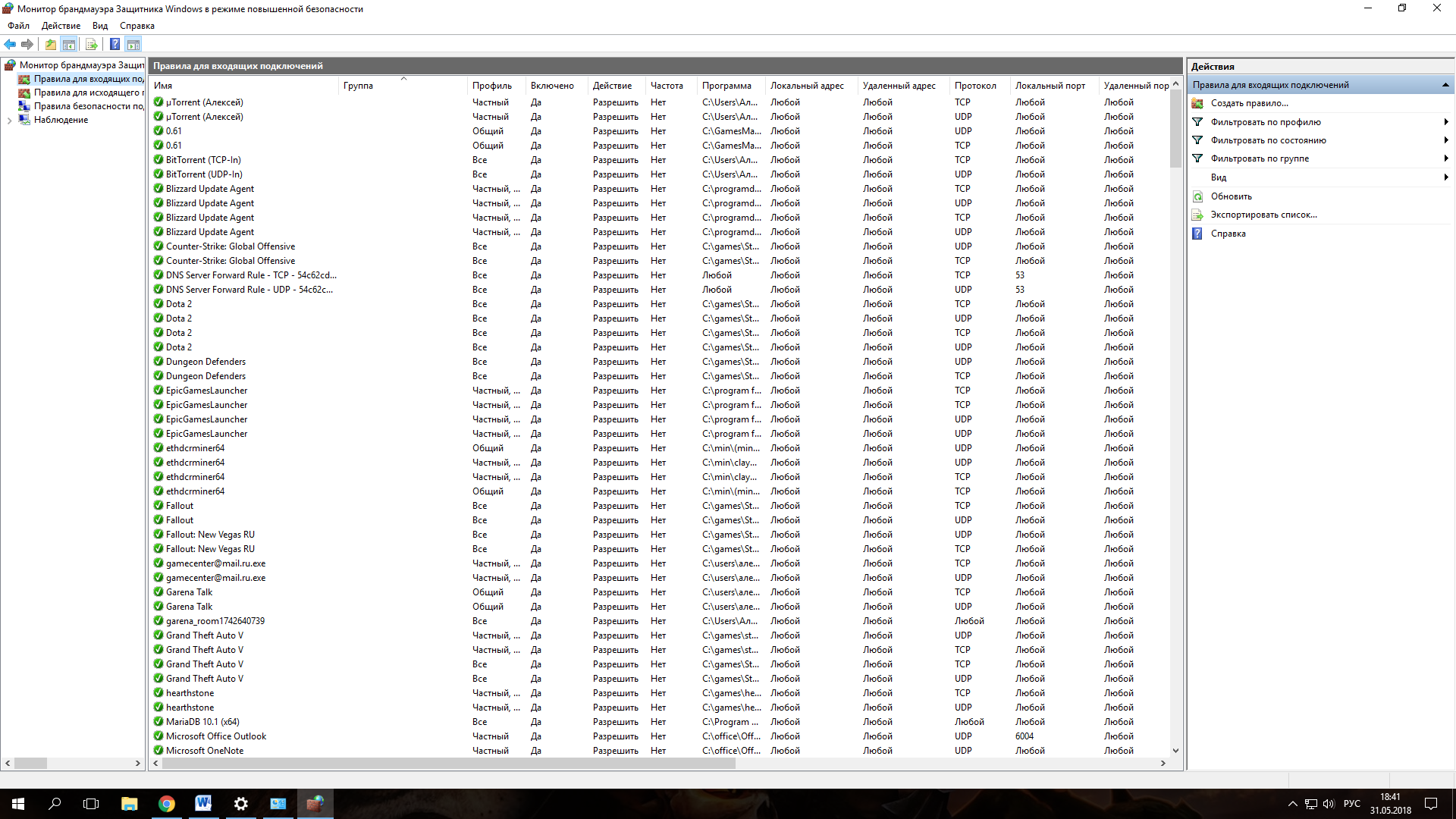
Входящие подключения. 

Рис. 12 - «Правила для входящего подключения»

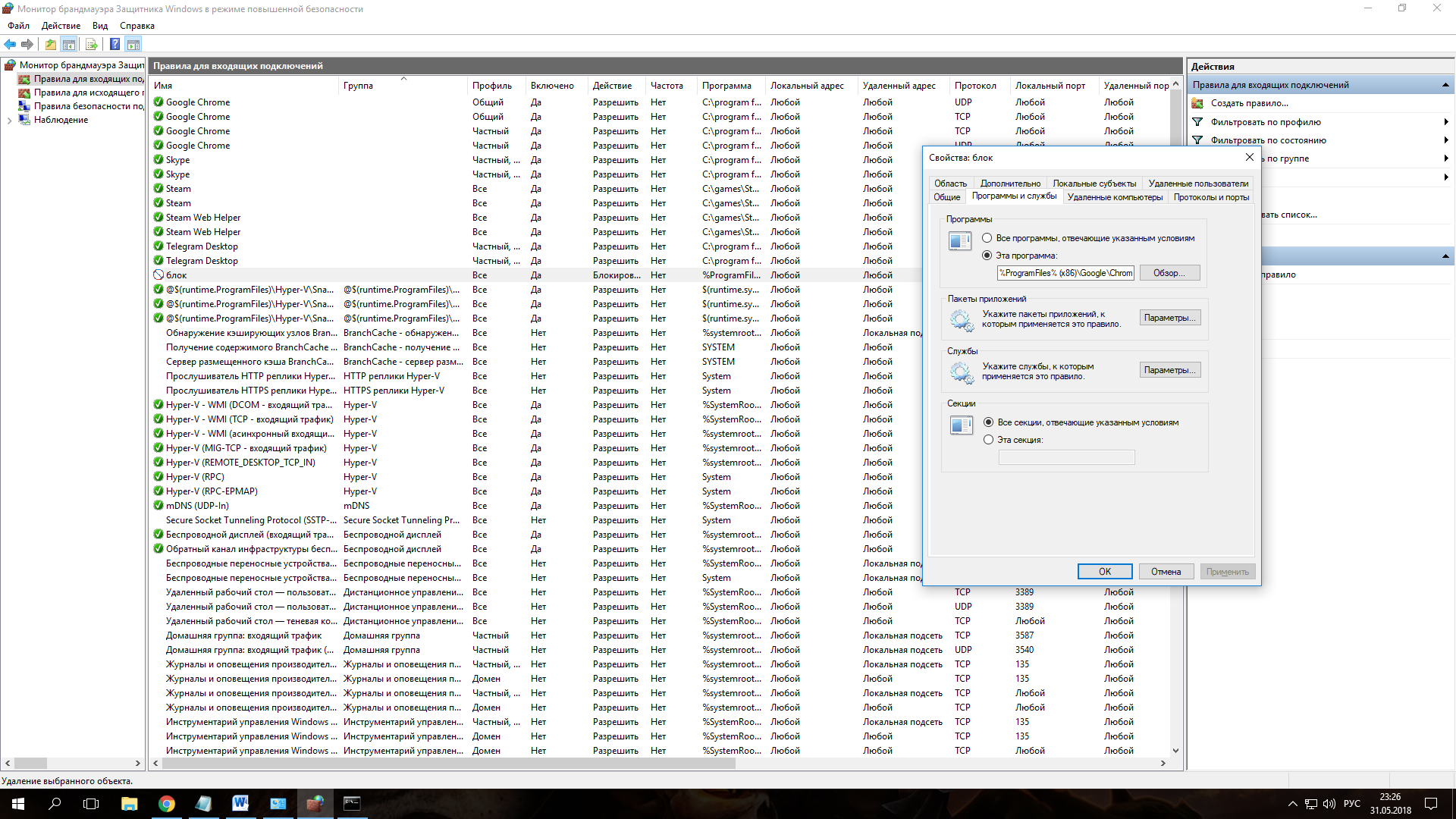


Рис. 13 - «Блокировка приложения Google Chrome»

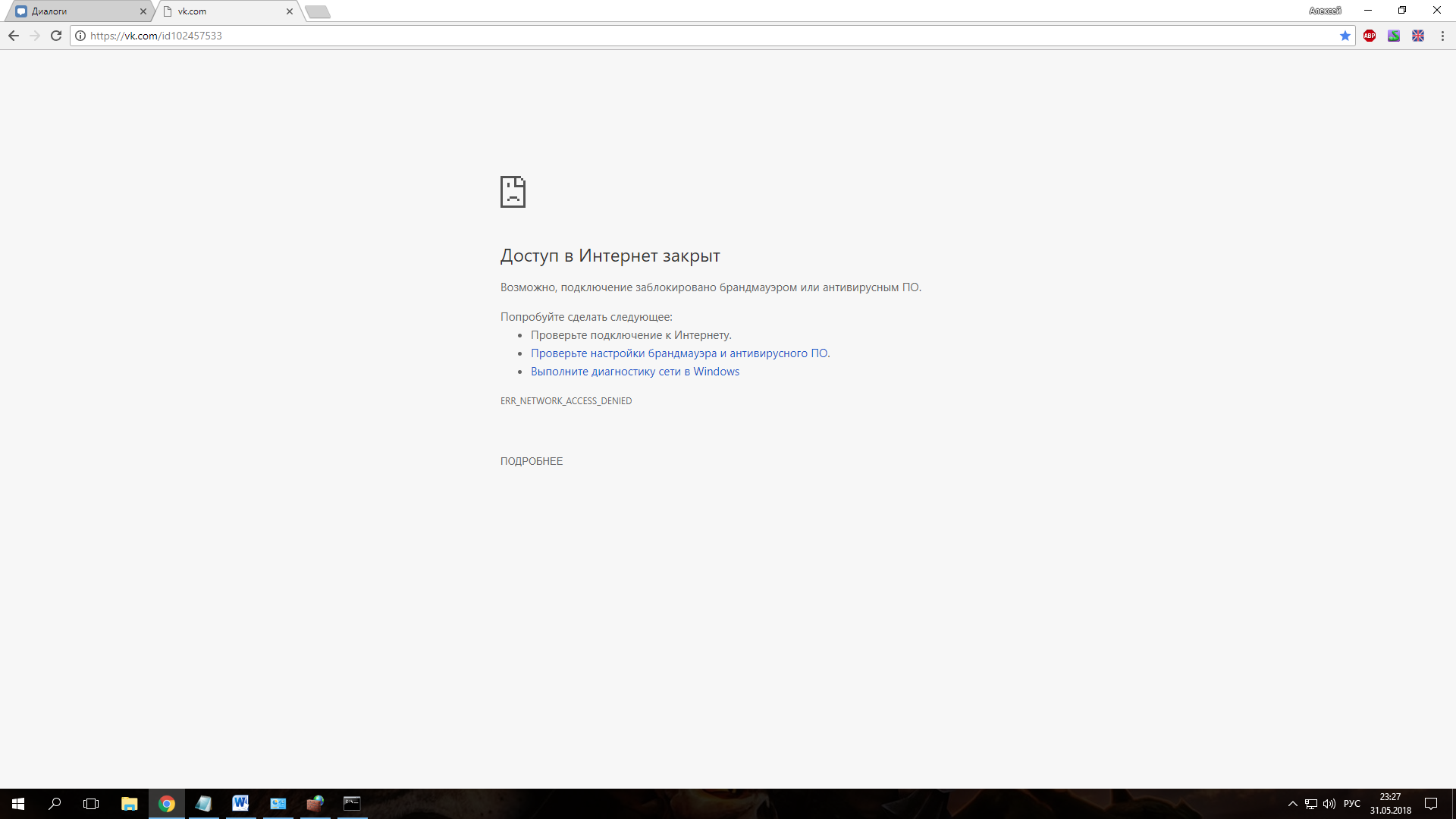


Рис. 14 - «Блокировка приложения Google Chrome.Проверка»

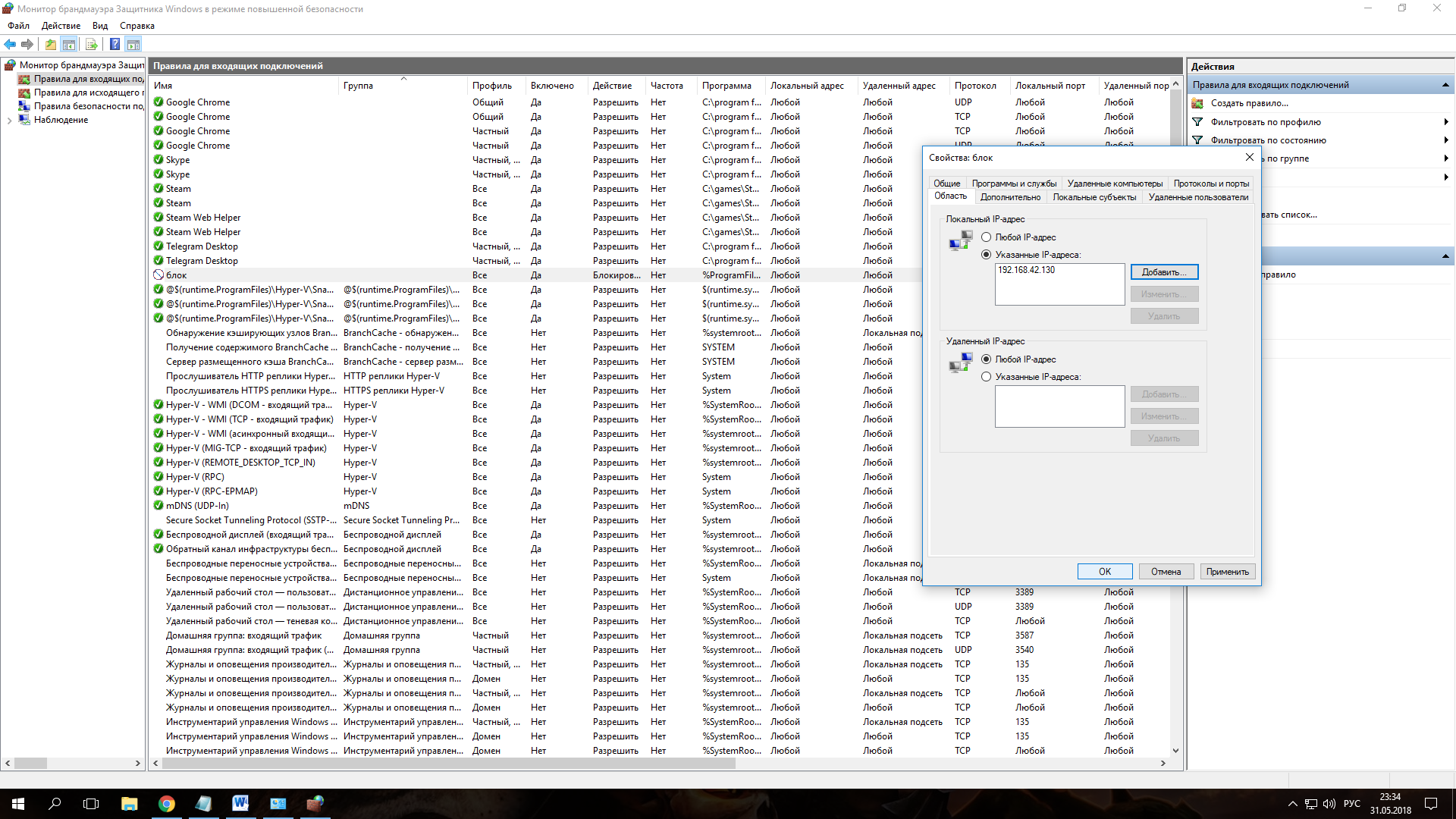


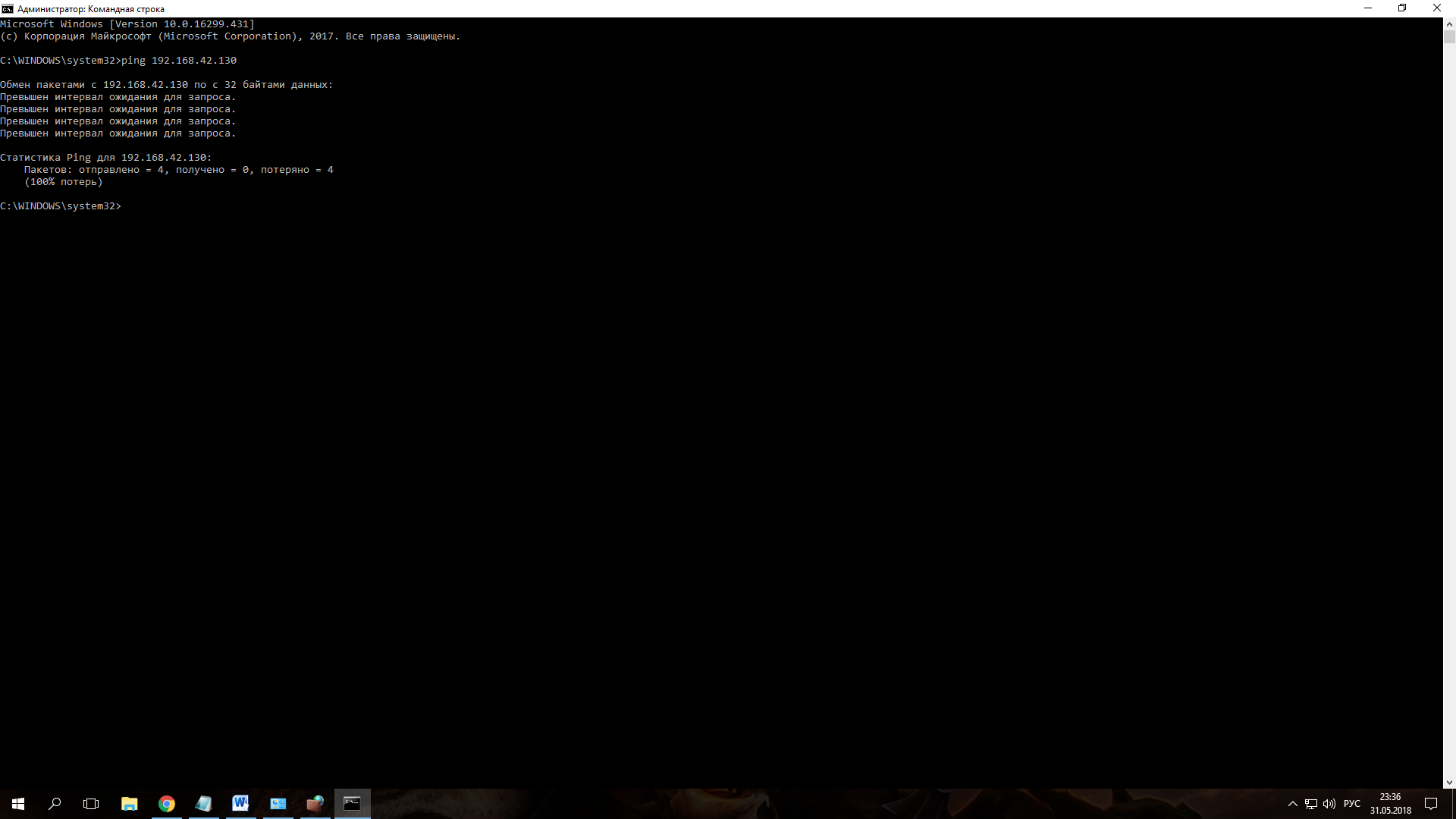
Рис. 17 - «Блокировка сетевого адреса» 

Рис. 18 - «Блокировка сетевого адреса. Проверка»