Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Основы защиты информации»

Отчёт по практическому занятию №4

Студент: Миневич К.В.

ФИТ 2 курс 4 группа

Преподаватель: Барковский Е.В.

Минск 2022 г.

**Практическое занятие 4**

**«Настройка Брандмауэра Windows»**

Цель: овладение навыками настройки и использования Брандмауэра Windows.

**Теоретическое введение**

**Брандмауэр (Межсетевой экран)** - это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные (рис. 1).

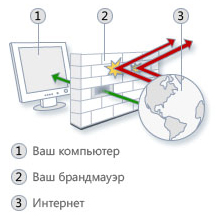


Рисунок 1 – *Принцип действия Брандмауэра*

Межсетевой экран является одним из основных компонентов защиты сетей. Наряду с Internet-протоколом межсетевого обмена (Internet Security Protocol — IPSec). Межсетевой экран является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от несанкционированного доступа.

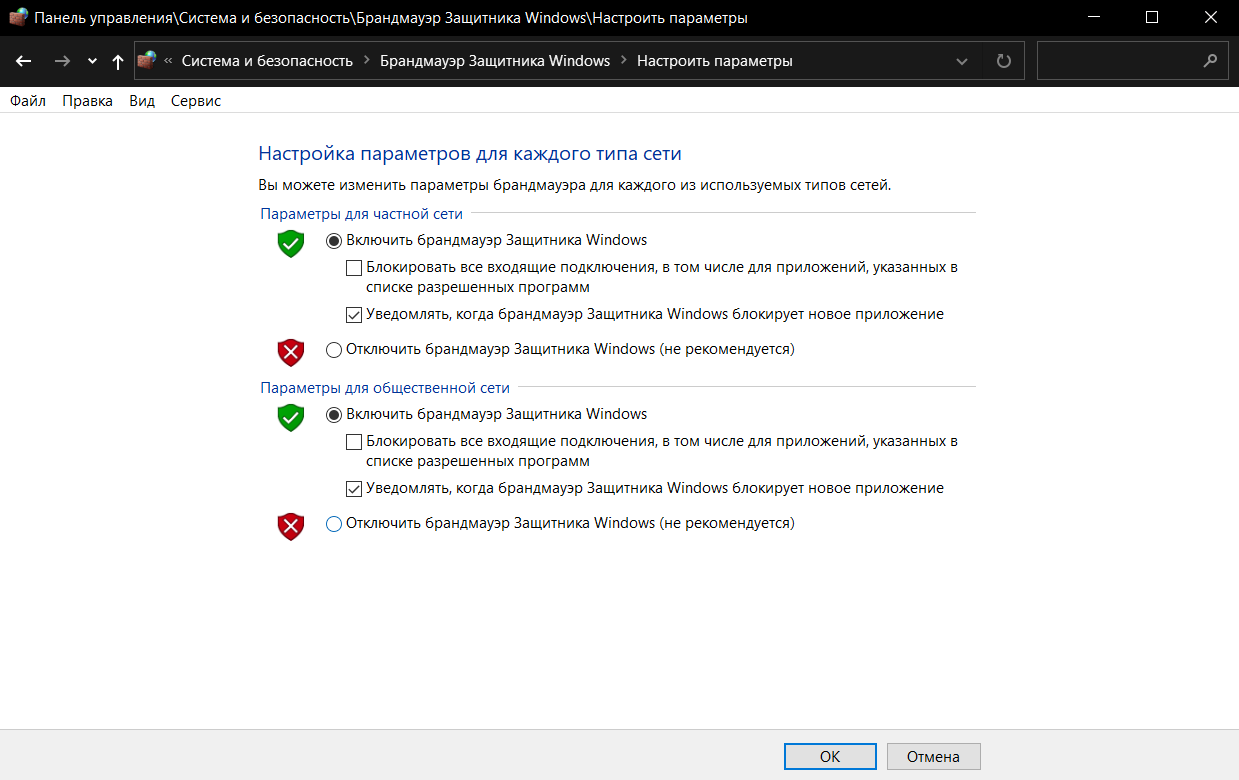
К числу служб и протоколов относятся:

* служба сетевых имен (Domain Name Server — DNS);
* доступ к всемирной паутине WWW;
* программа электронной почты Send Mail;
* служба эмуляции удаленного терминала Telnet;
* простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP);
* протокол передачи файлов (File Transfer Protocol);
* графическая оконная система X Windows.

**Задание для выполнения.**

1. **Включение брандмауэра**

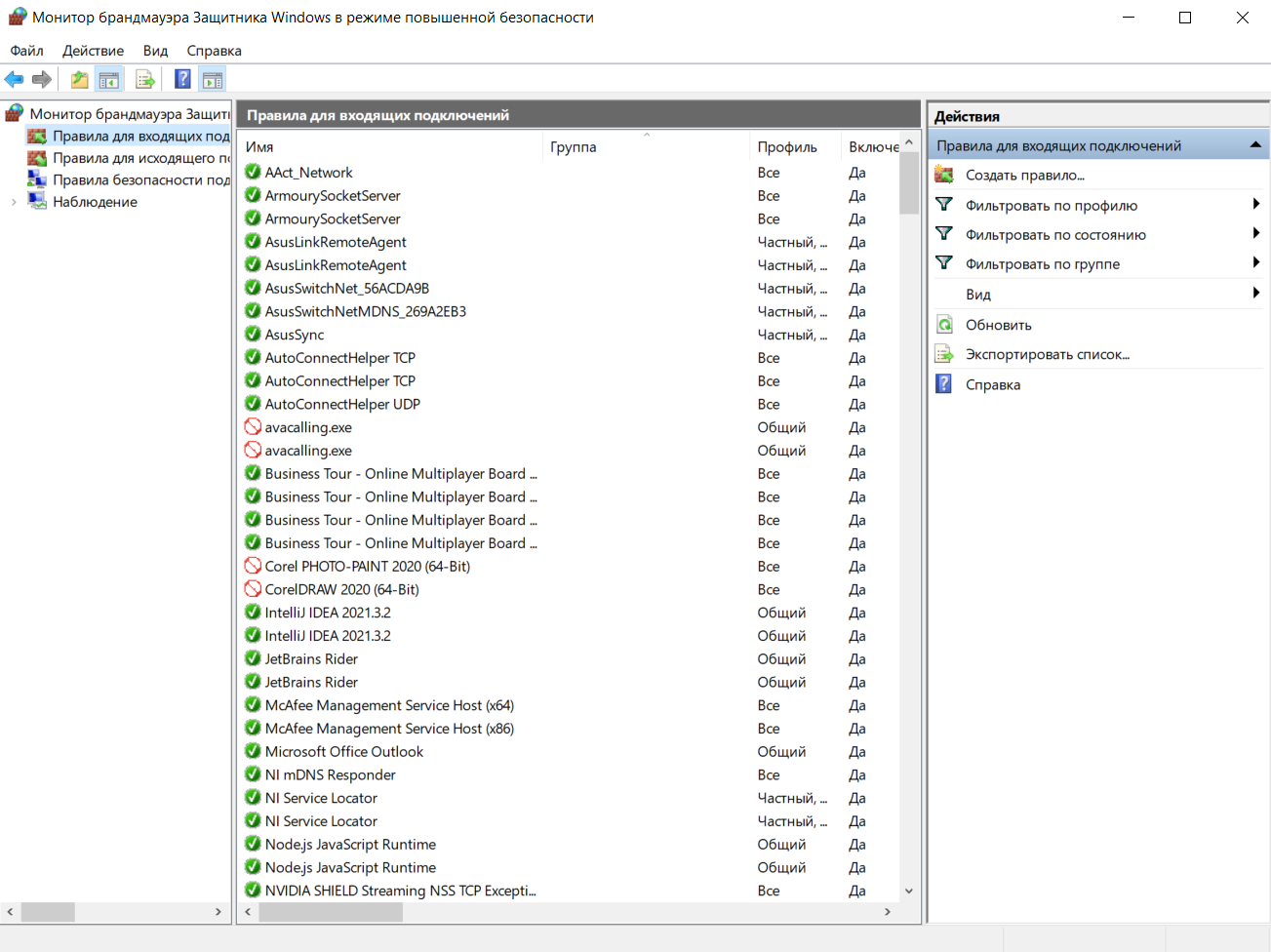
Чтобы проверить состояние брандмауэра необходимо войти: Панель управления -> Система и безопасность -> Брандмауэр Защитника Windows -> Изменение параметров уведомлений.



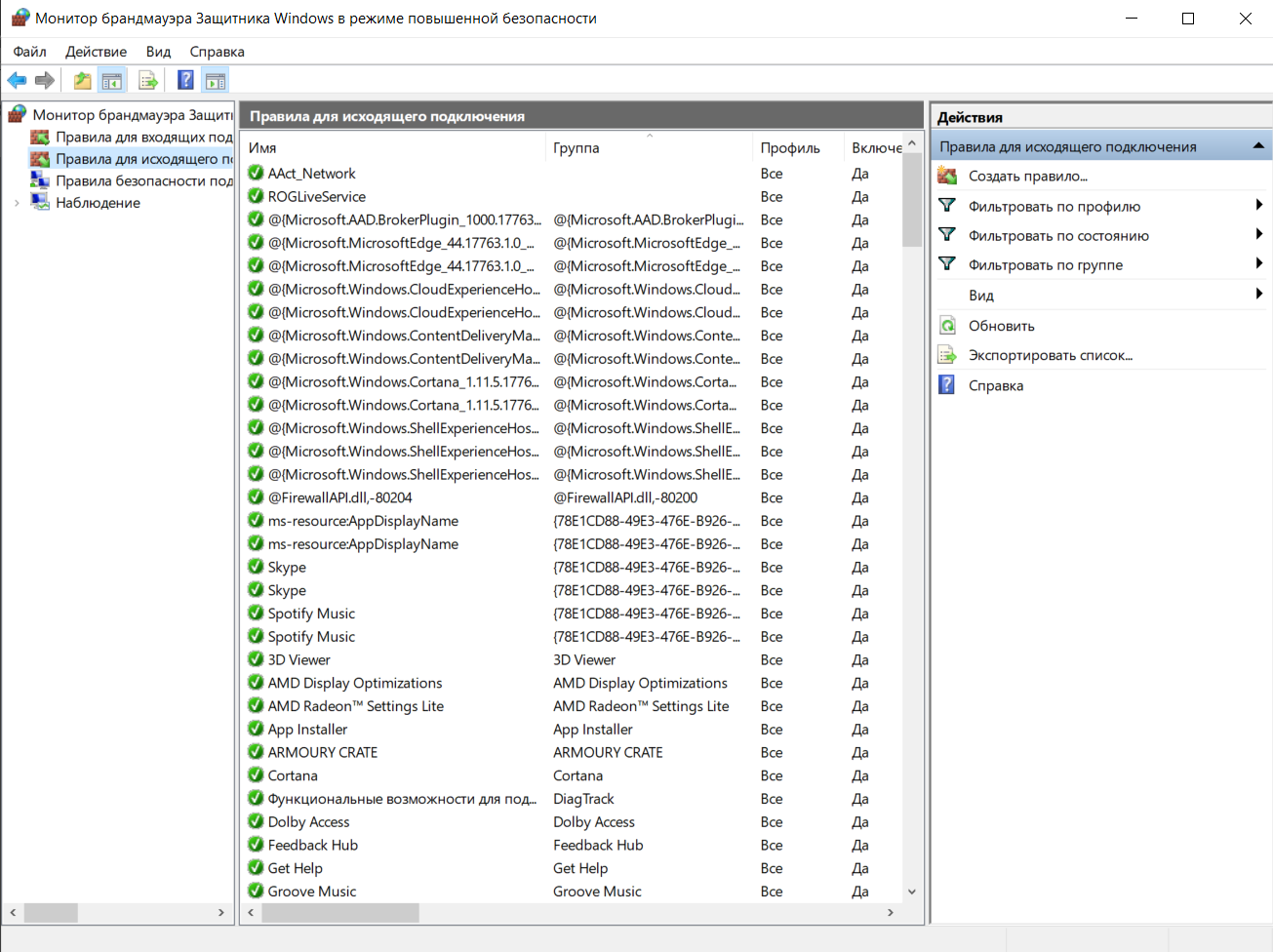
*Рисунок 4.1 – Включение брандмауэра*

1. **Настройка входящих и исходящих подключений**

Для настройки заходим в Панель управления -> Система и безопасность -> Брандмауэр Защитника Windows -> Дополнительные параметры.

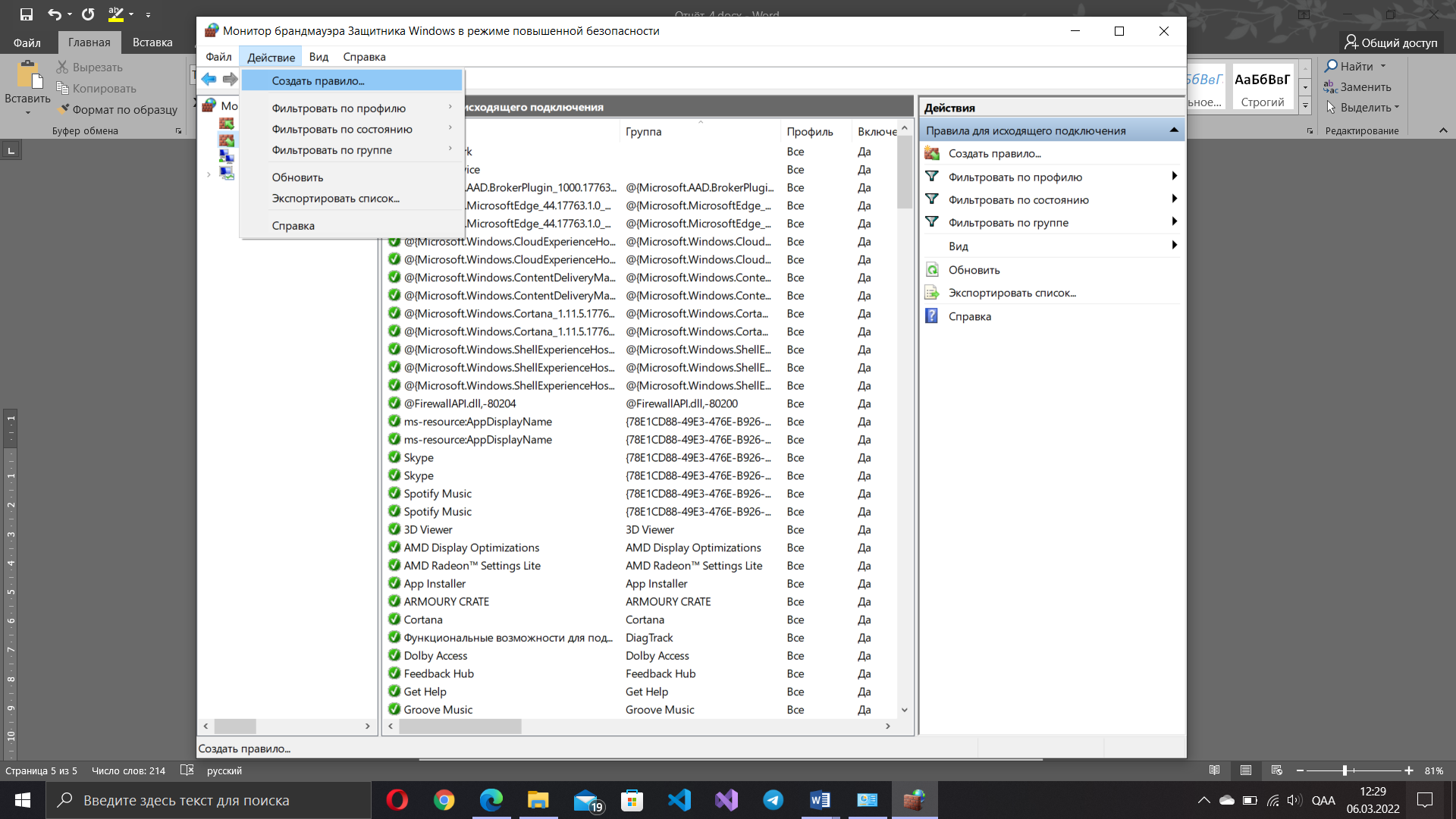


*Рисунок 4.2 – Правила для входящих подключений*



*Рисунок 4.3 – Правила для исходящих подключений*

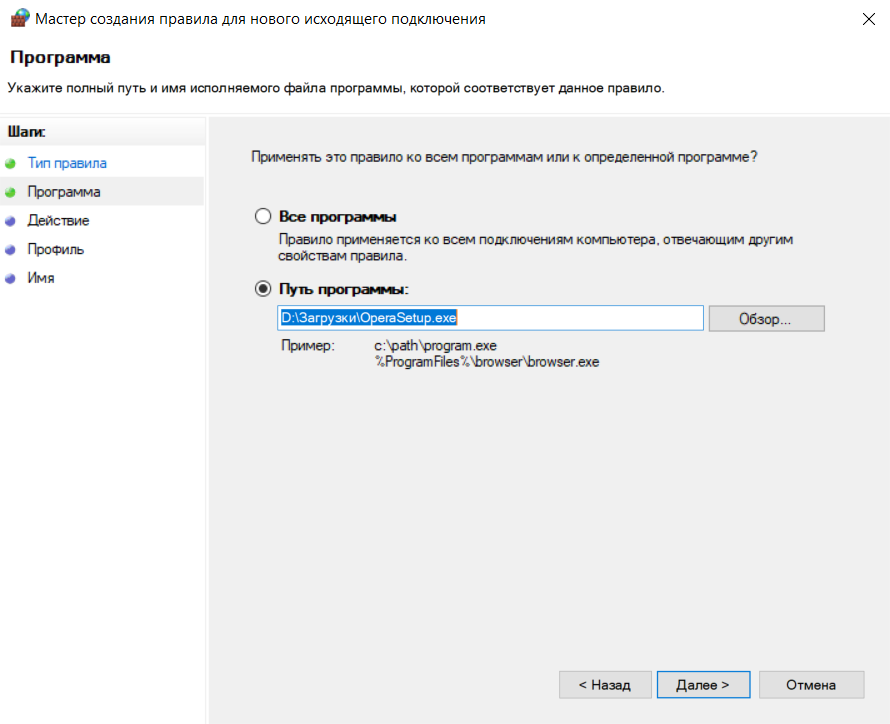
Для создания нового правила подключения нажимаем Действие -> Создать правило…



*Рисунок 4.4 - Мастер создания правил*

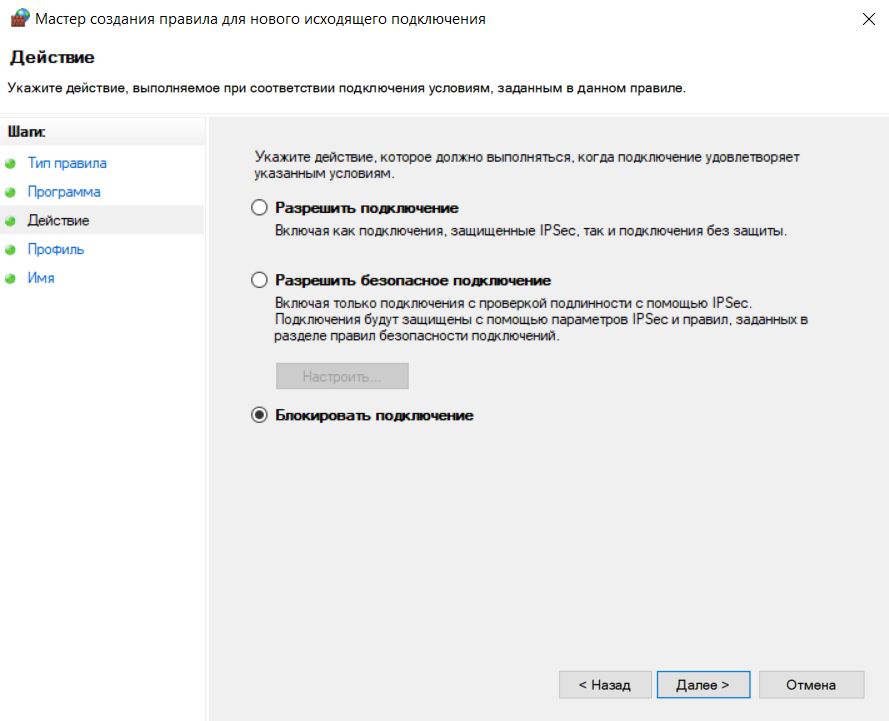
# **3. Установка пути к приложению (SIGame.Setup.exe) и далее блокировка подключений.**

Устанавливаем тип правила и указываем путь к нашему файлу.



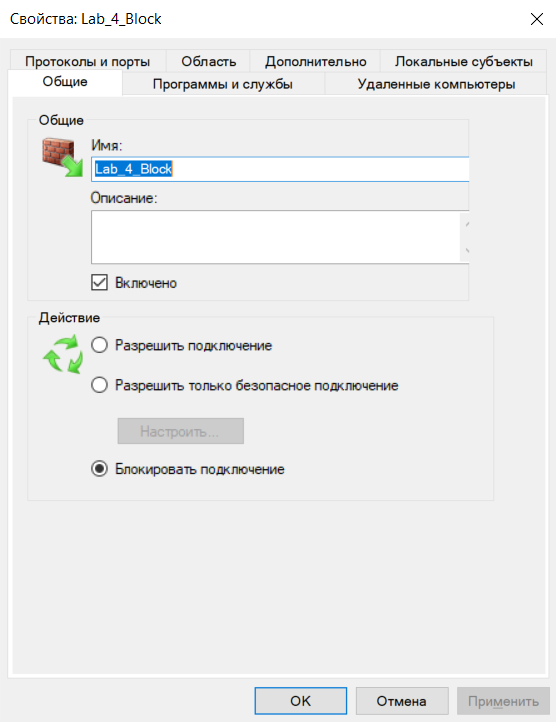
*Рисунок 4.5 - Мастер создания правил, выбор пути*

Далее указываем действия, которые будут выполняться, когда когда подключение удовлетворяет условиям.



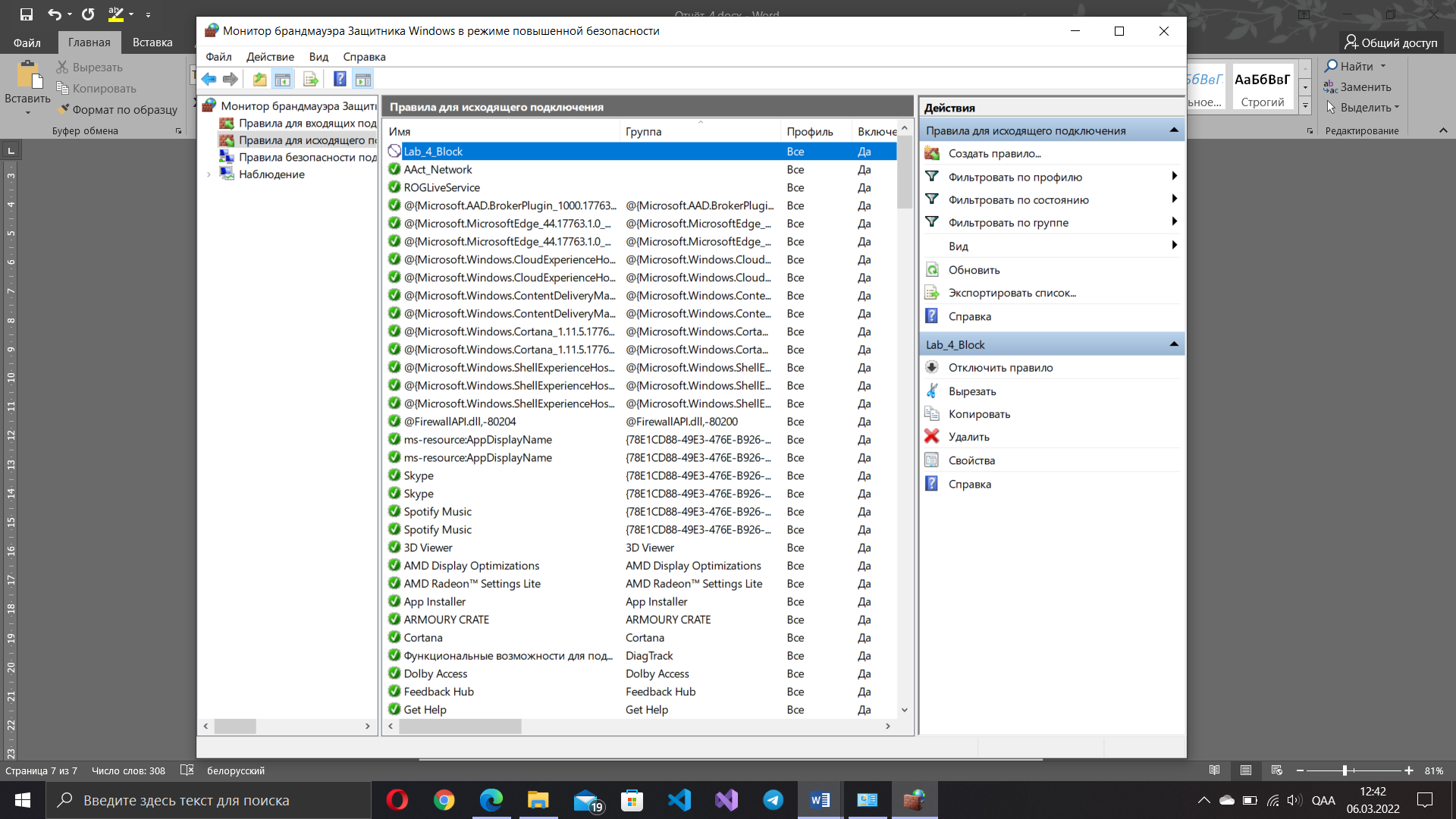
*Рисунок 4.6 - Блокировка/разрешение подключения*

Указываем имя нашего правила. Просматриваем свойства полученного правила.



*Рисунок 4.7 – Свойство созданного правила*

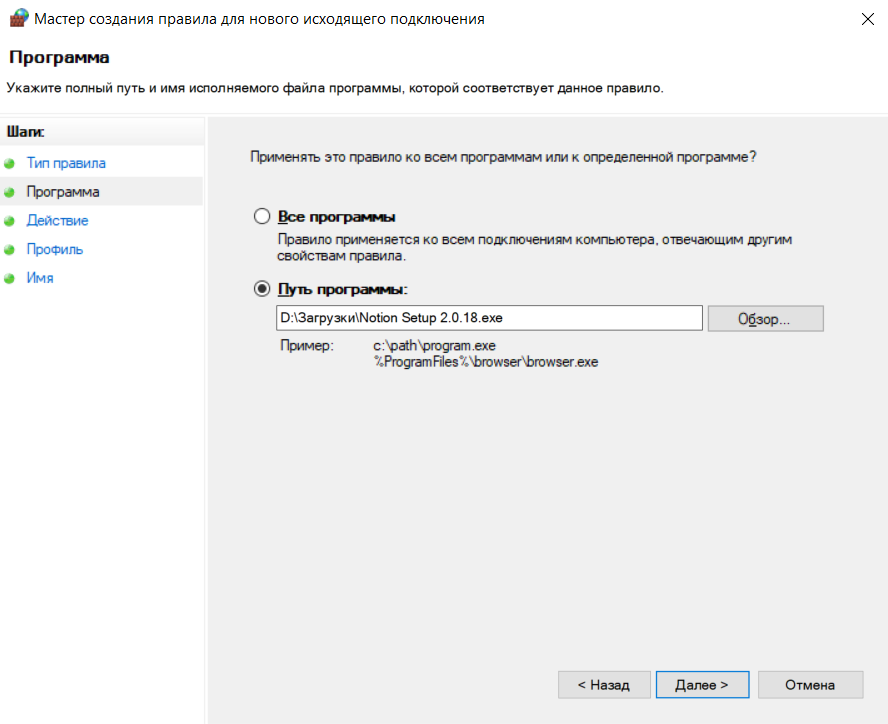
4. Наблюдаем правило в общем списке, а далее просматриваем его свойства.



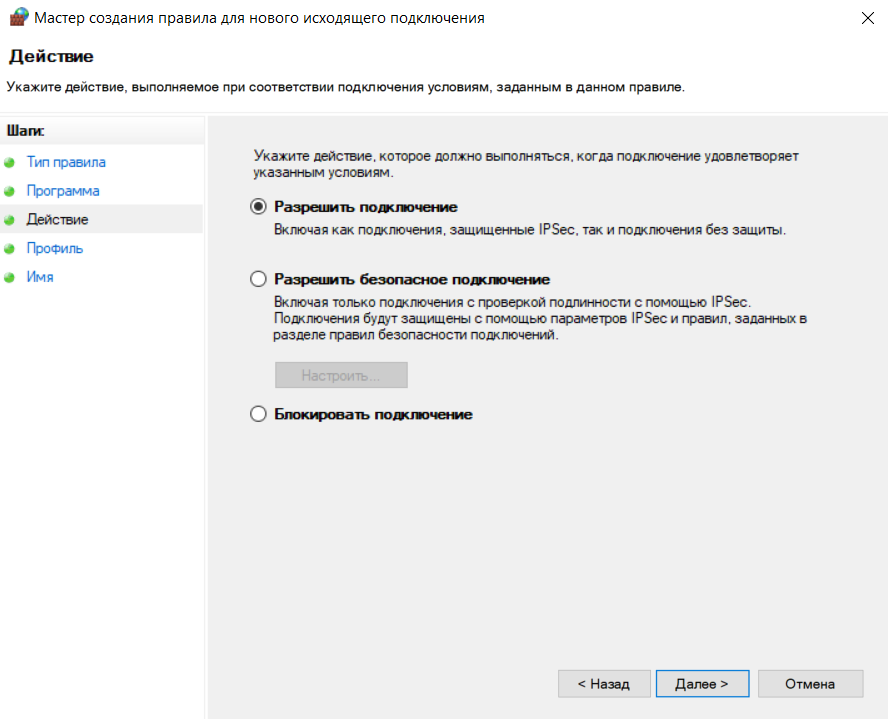
*Рисунок 4.8 - Активные правила в списке*

5. Проделываем такие же действия с входящими подключениями. Ниже представленные иллюстрации соответствуют рис. 4.4-4.8.

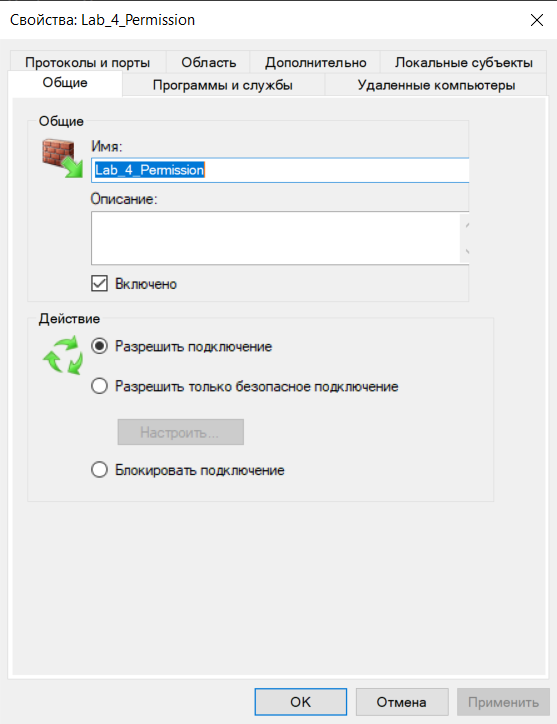
# **Создание разрешающего правила для исходящего подключения:**



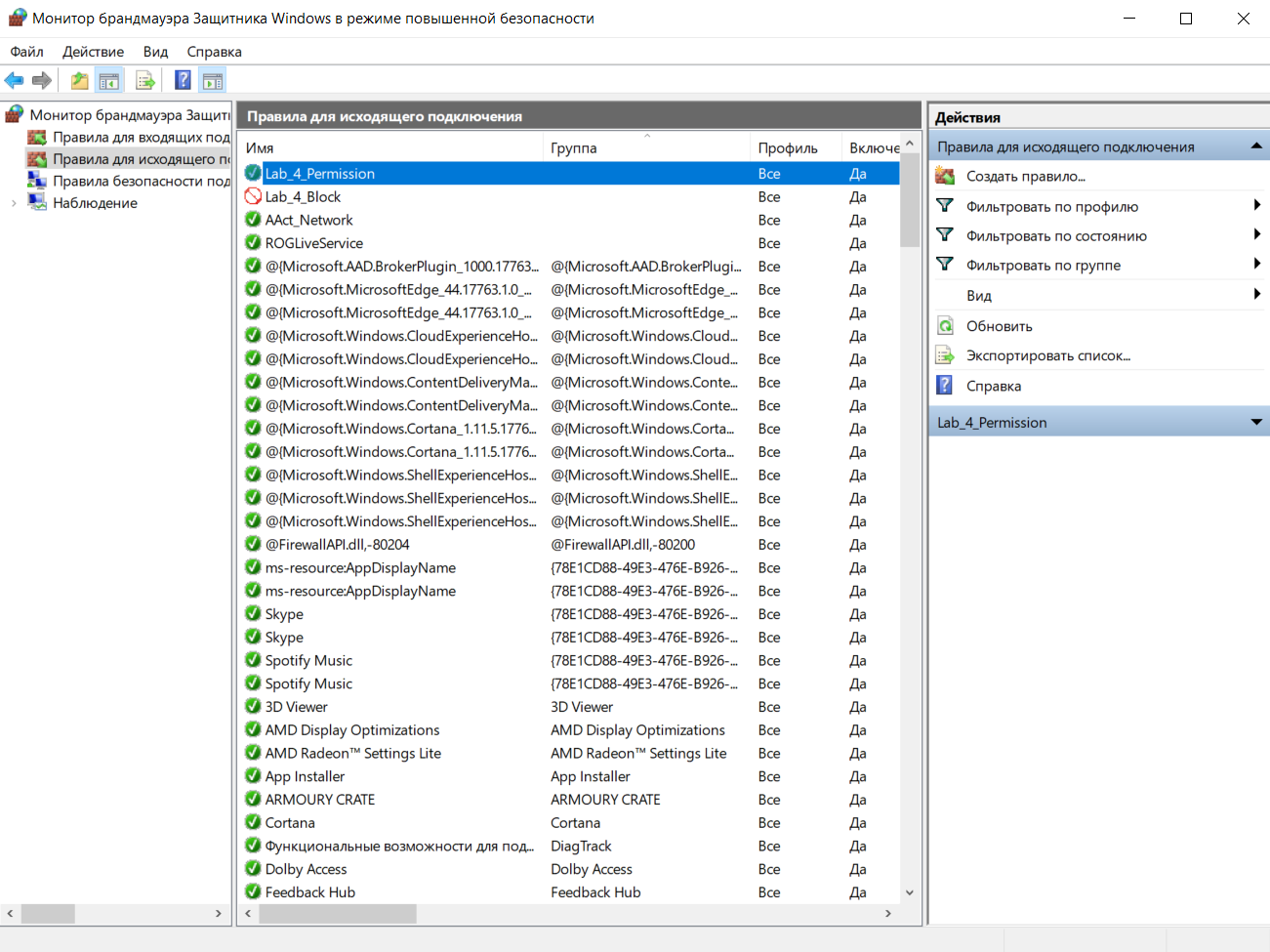
*Рисунок 4.9 - Мастер создания правил, выбор пути*



*Рисунок 4.10 - Блокировка/разрешение подключения*

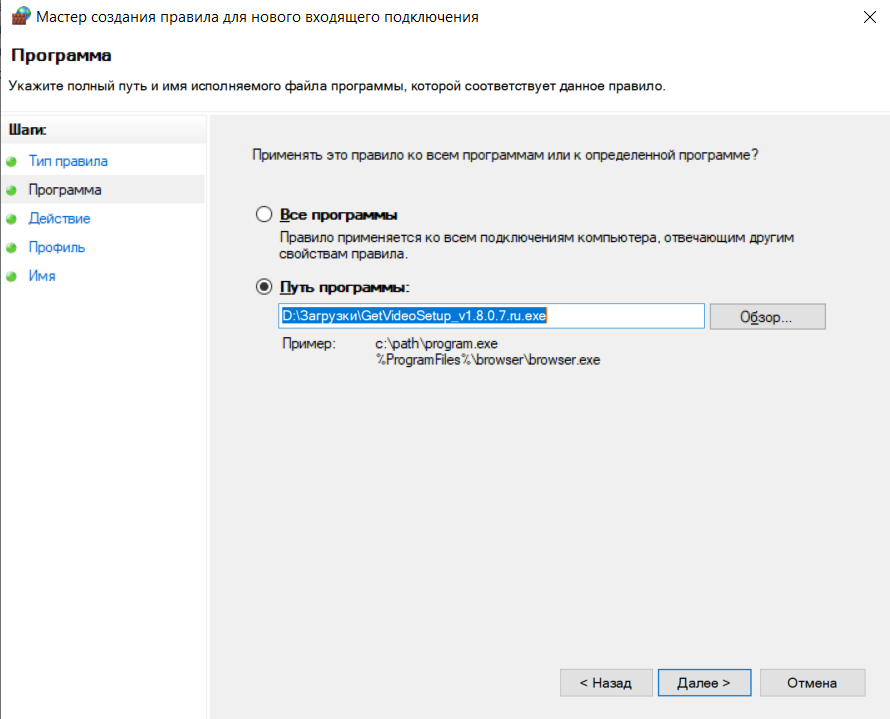


*Рисунок 4.11 – Свойство созданного правила*

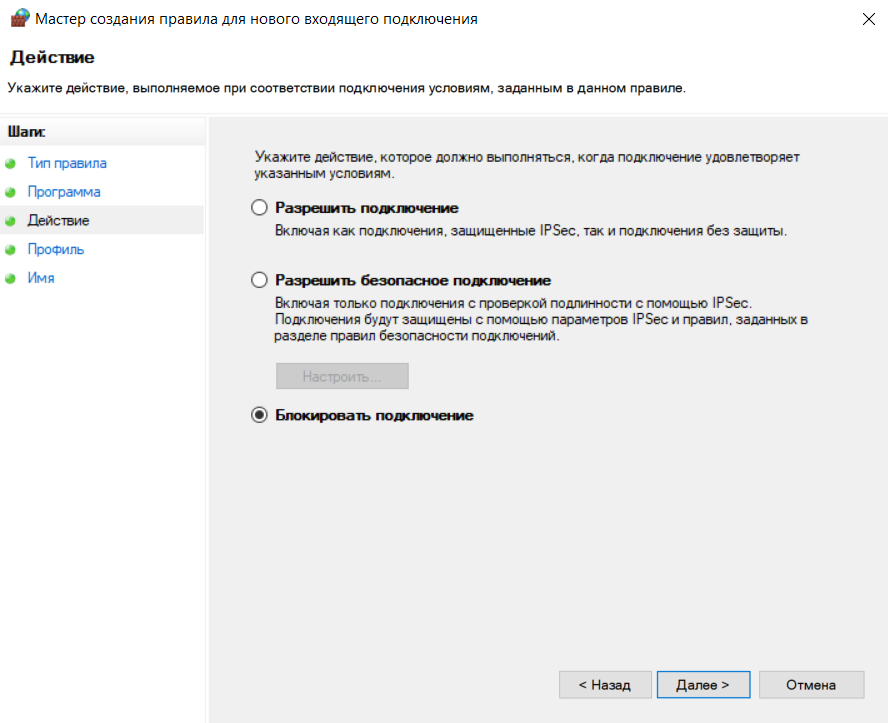


*Рисунок 4.12 - Активные правила в списке*

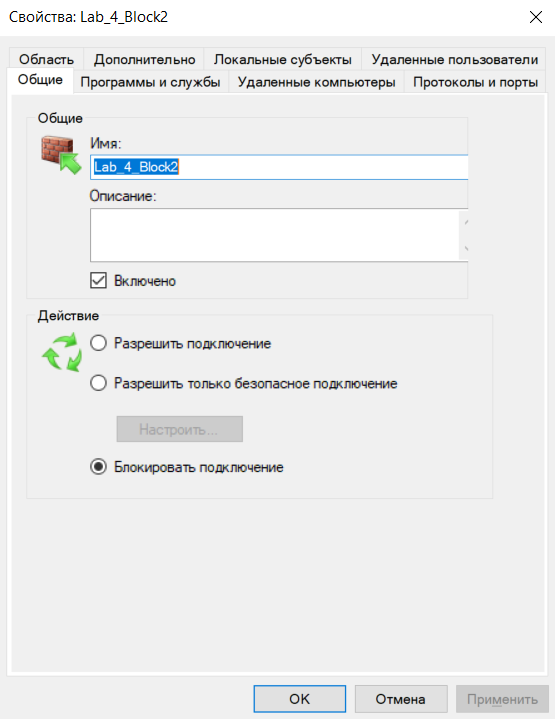
# **Создание блокирующего правила для входящего подключения:**



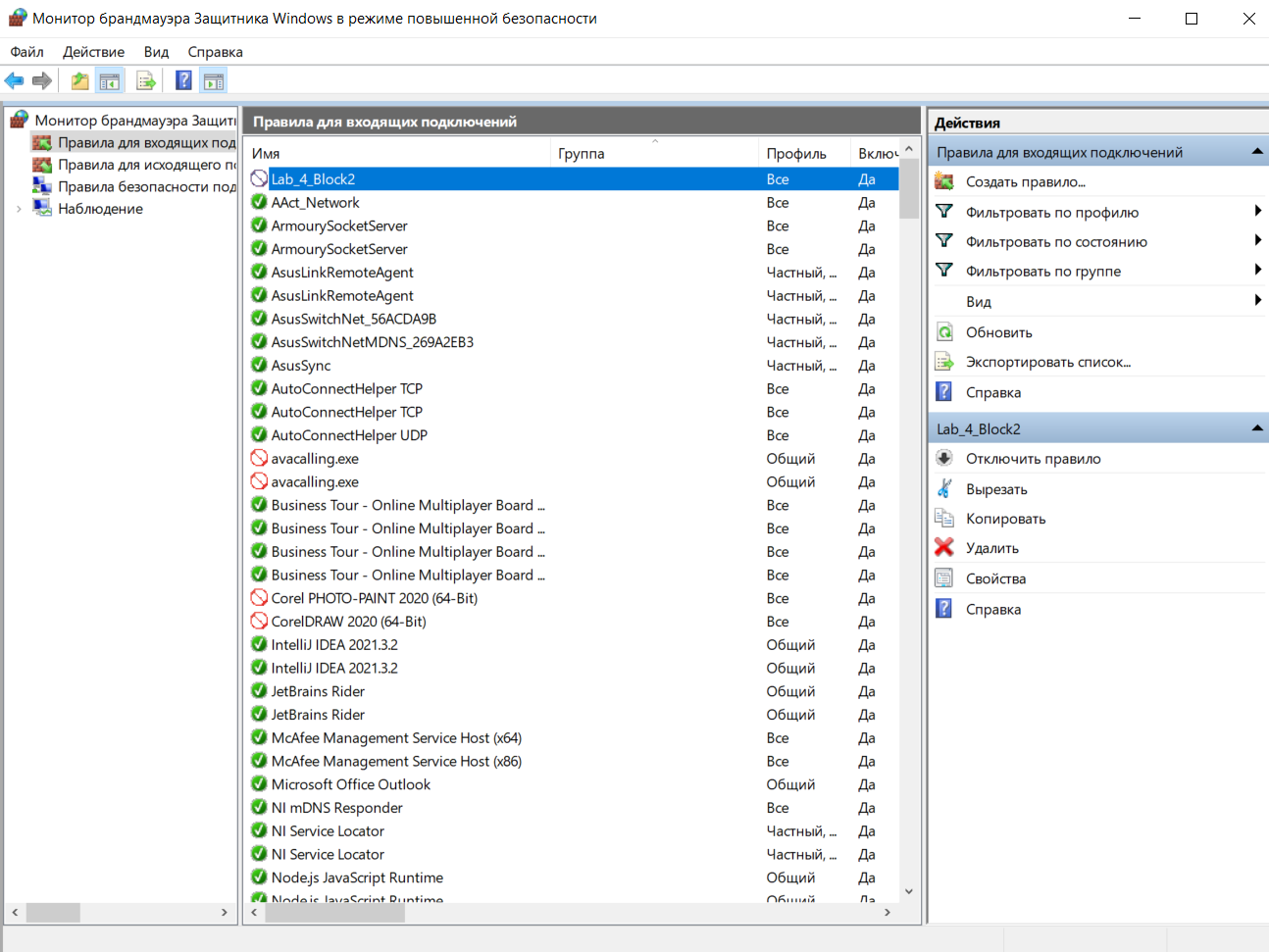
*Рисунок 4.13 - Мастер создания правил, выбор пути*



*Рисунок 4.14 - Блокировка/разрешение подключения*



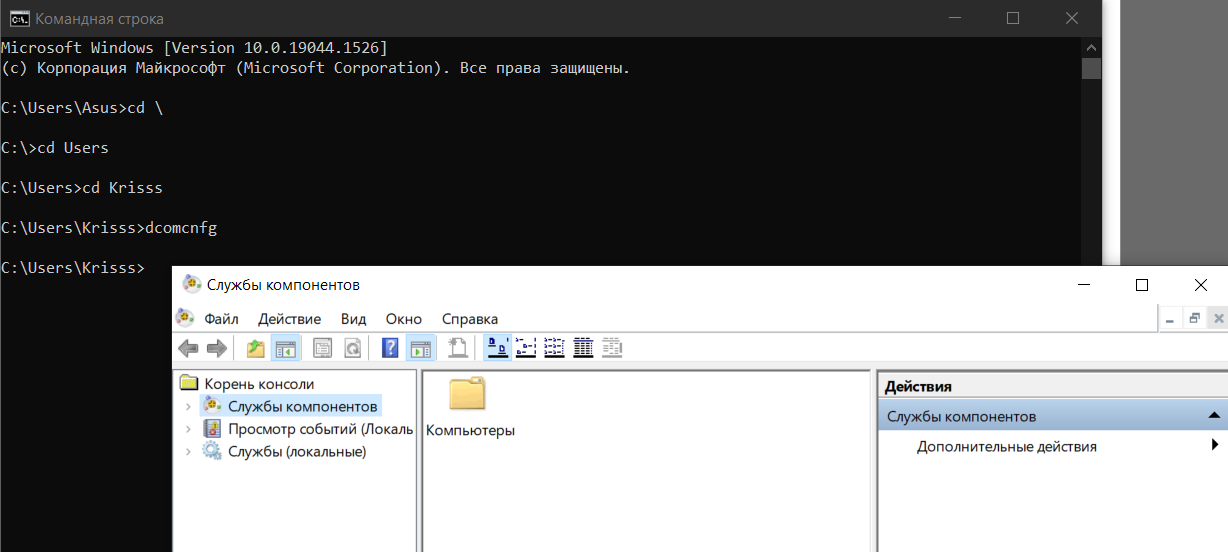
*Рисунок 4.15 – Свойство созданного правила*



*Рисунок 4.16 - Активные правила в списке*

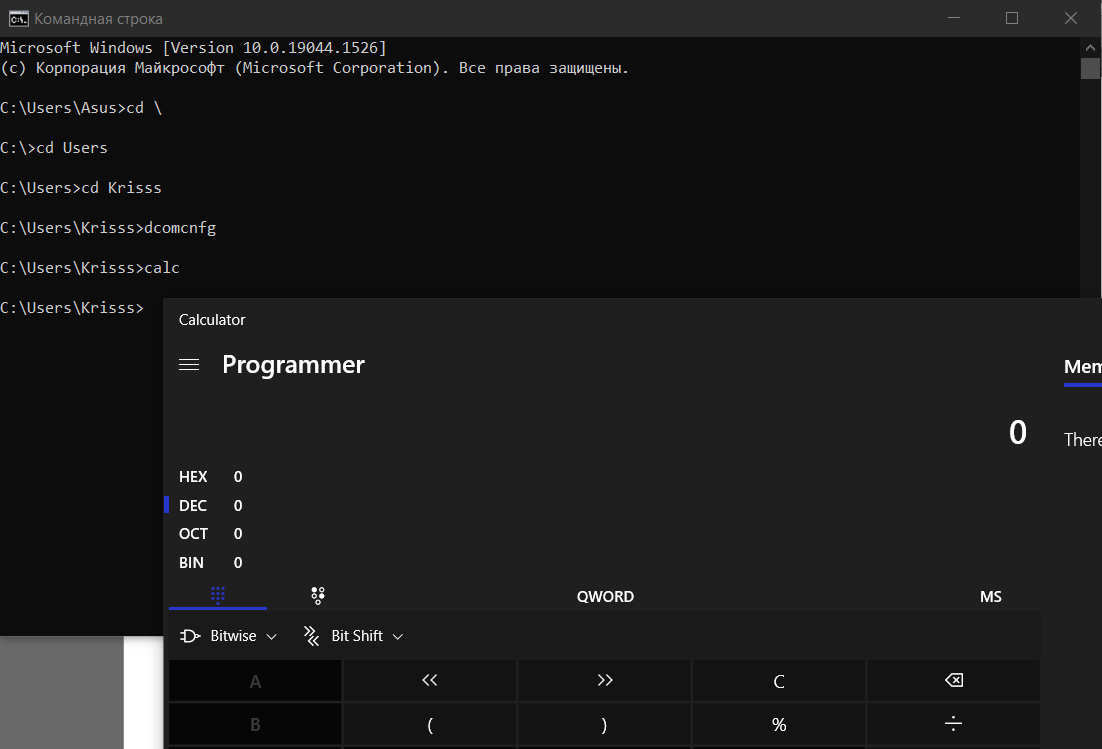
# **6. Опробовать действие нескольких команд "командной строки Windows"( Пуск -> cmd)**

1. Службы компонентов – dcomcnfg.



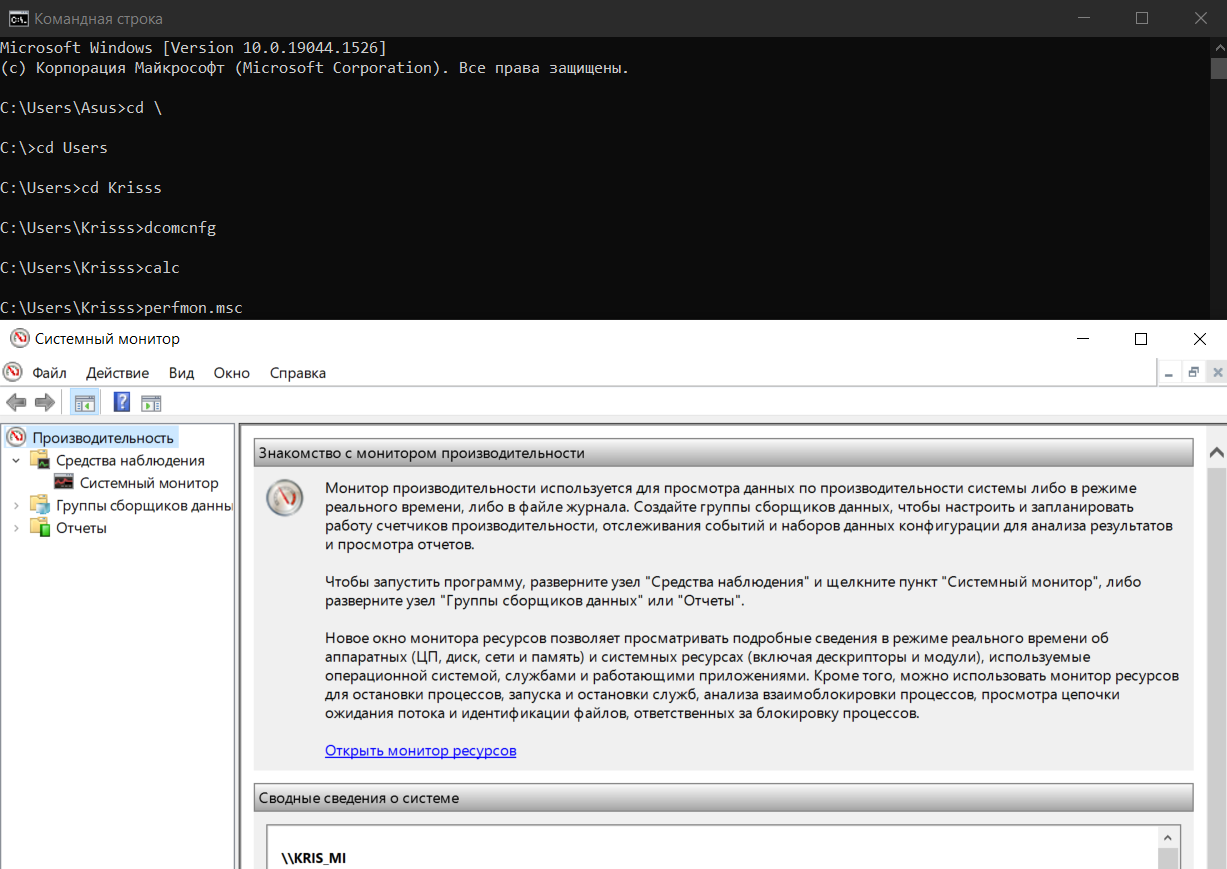
*Рисунок 4.17 – Результат команды dcomnfg.*

2. Калькулятор – calc.



*Рисунок 4.18 – Результат команды calc.*

3. Производительность - perfmon.msc



*Рисунок 4.19 – Результат команды perfmon.msc.*

**Вывод**: в ходе работы были получены навыки настройки и использования Брандмауэра Windows, создания правил для блокировки и разрешения входящих и исходящих подключений, опробованы действия нескольких команд "командной строки Windows".