Учреждение образования

«Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

«Основы защиты информации»

Выполнил:

Студент 2 курса 7 группы

Жуховцов Владислав Сергеевич

Принял:

Барковский Евгений Валерьевич

Минск 2022

**Практическое занятие №4**

Тема «Настройка Брандмауэра Windows »

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

**Теоретическое введение**

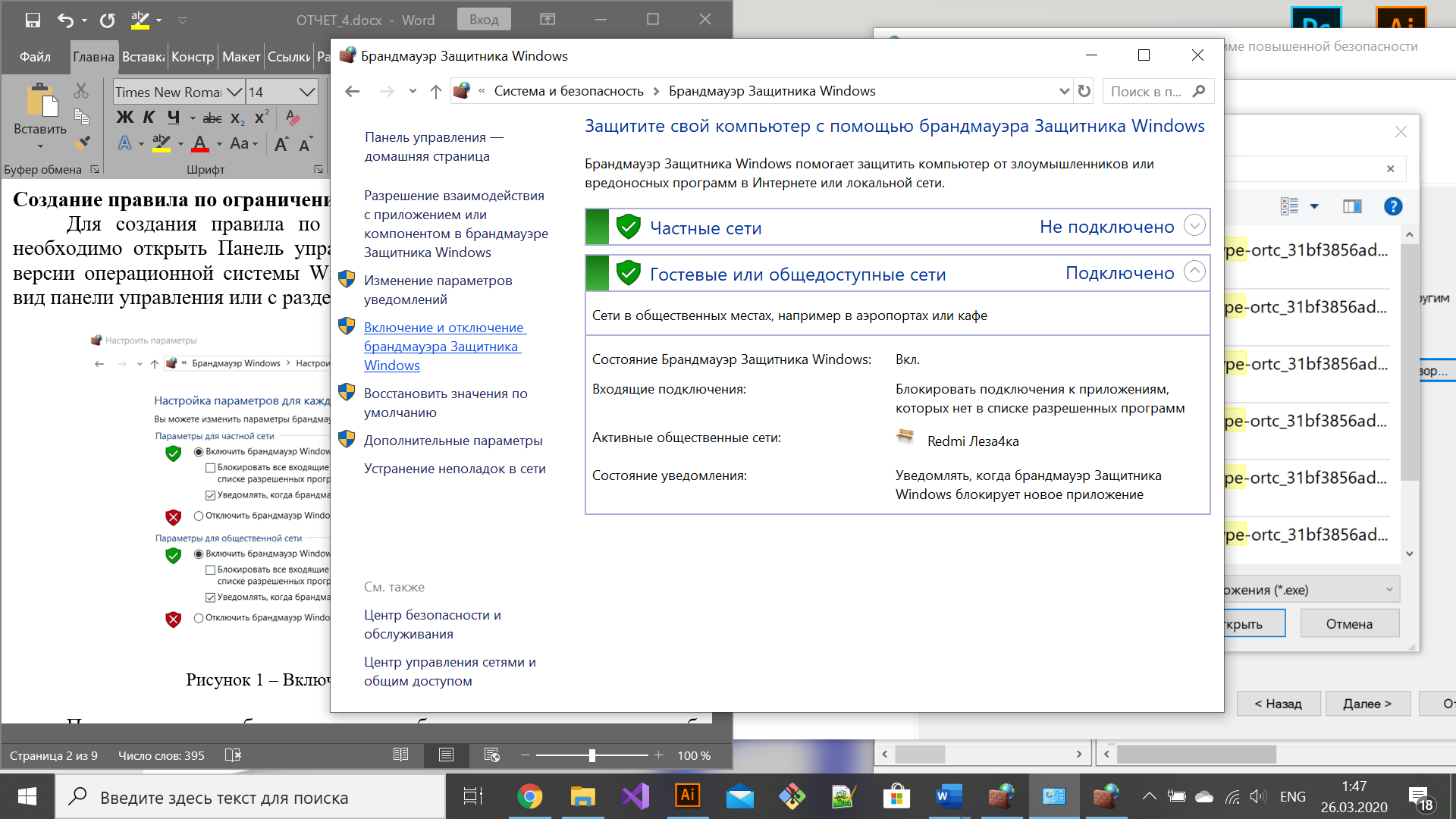
Брандмауэр (Межсетевой экран) - это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные

**Задания к выполнению**

1. Создать правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий):
   1. Для 1 программы (по выбору) на блокировку подключения;
   2. Для 1 программы (по выбору) на разрешение подключения;

**Создание правила по ограничению доступа программ к сети**

Для создания правила по ограничению доступа программ к сети необходимо открыть Панель управления в меню Пуск. В зависимости от версии операционной системы Windows может отображаться классический вид панели управления или с разделениям по категориям.



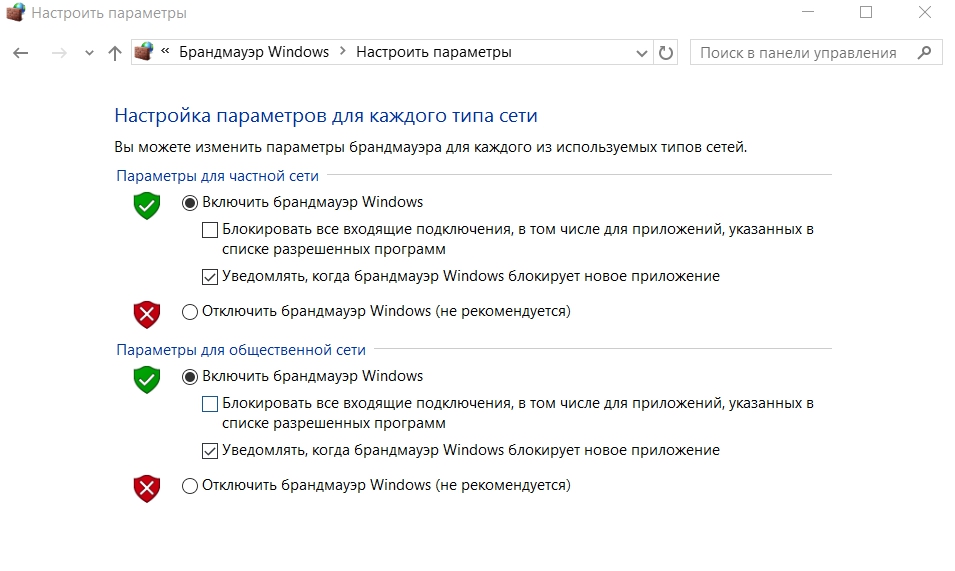


Рисунок 1 ­– Включение брандмауэра Windows

Первым этапом необходимо включить брандмауэр, в случае, если он был ранее выключен. Необходимо выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows» (Рис.1)

Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого во вкладке «Дополнительные параметры» (рис. 2).

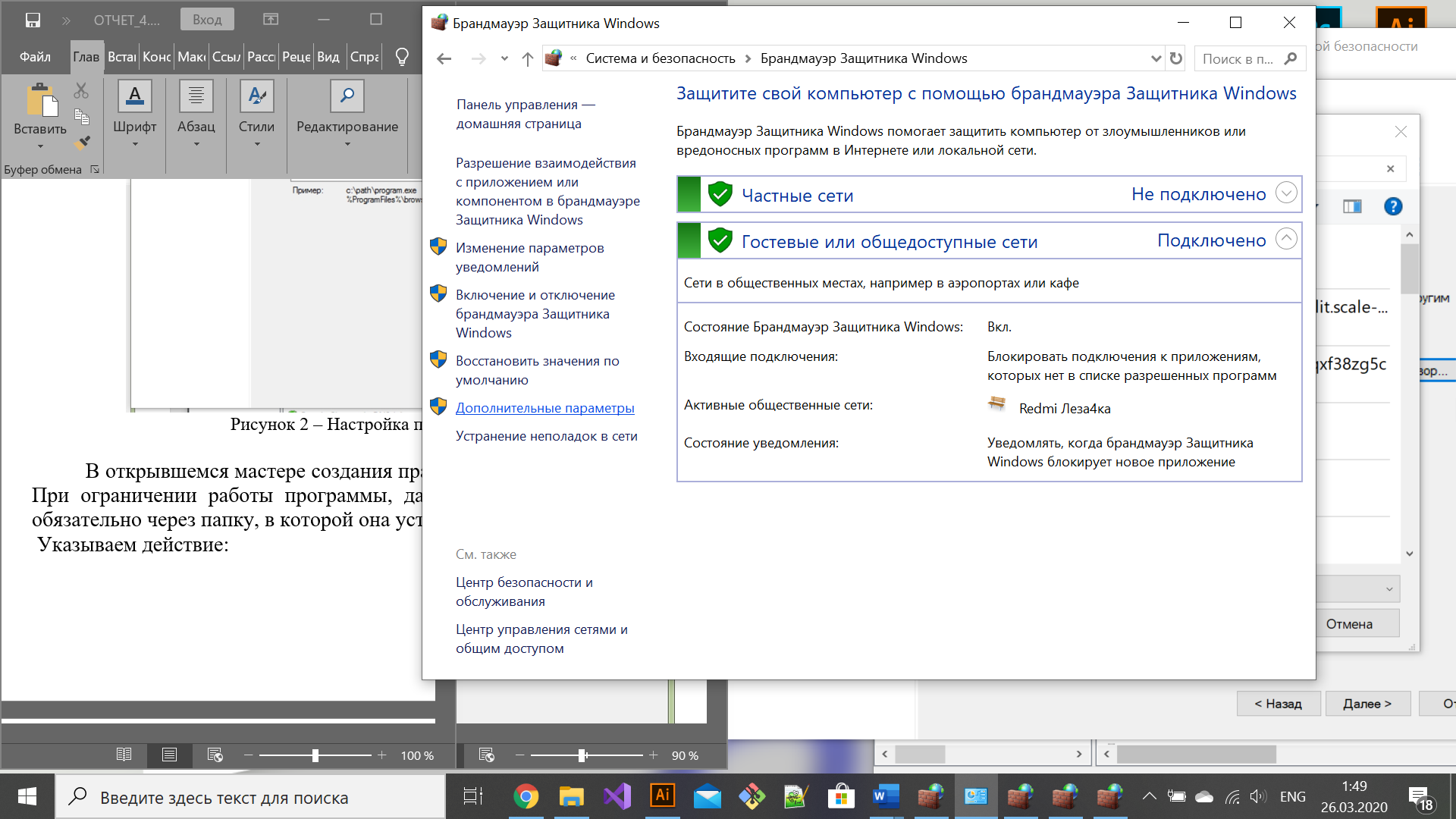


Рисунок 2 – Дополнительные параметры

В открывшемся окне выбираем в левой панели правила для входящих подключений, затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели (рис. 3).

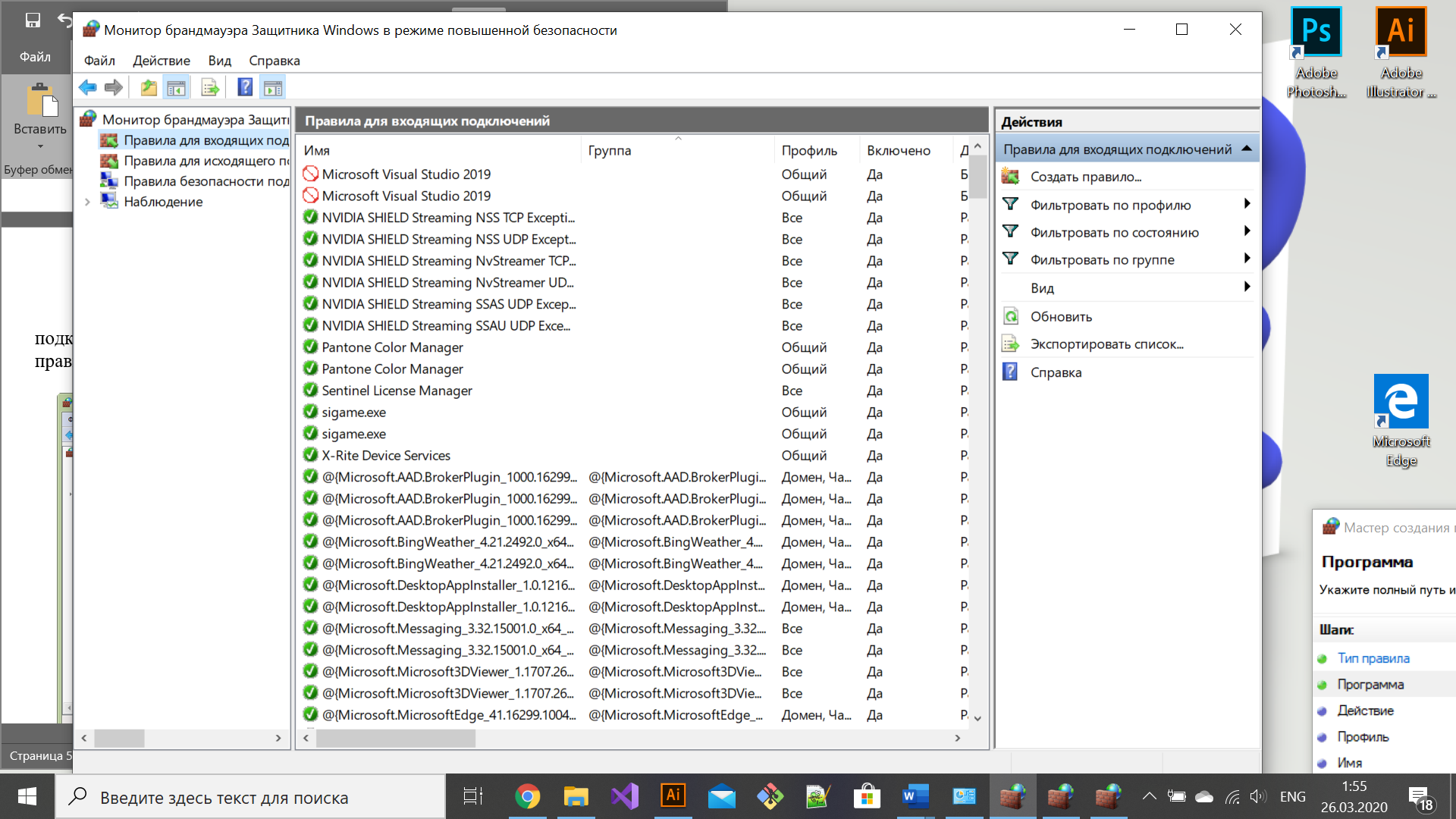
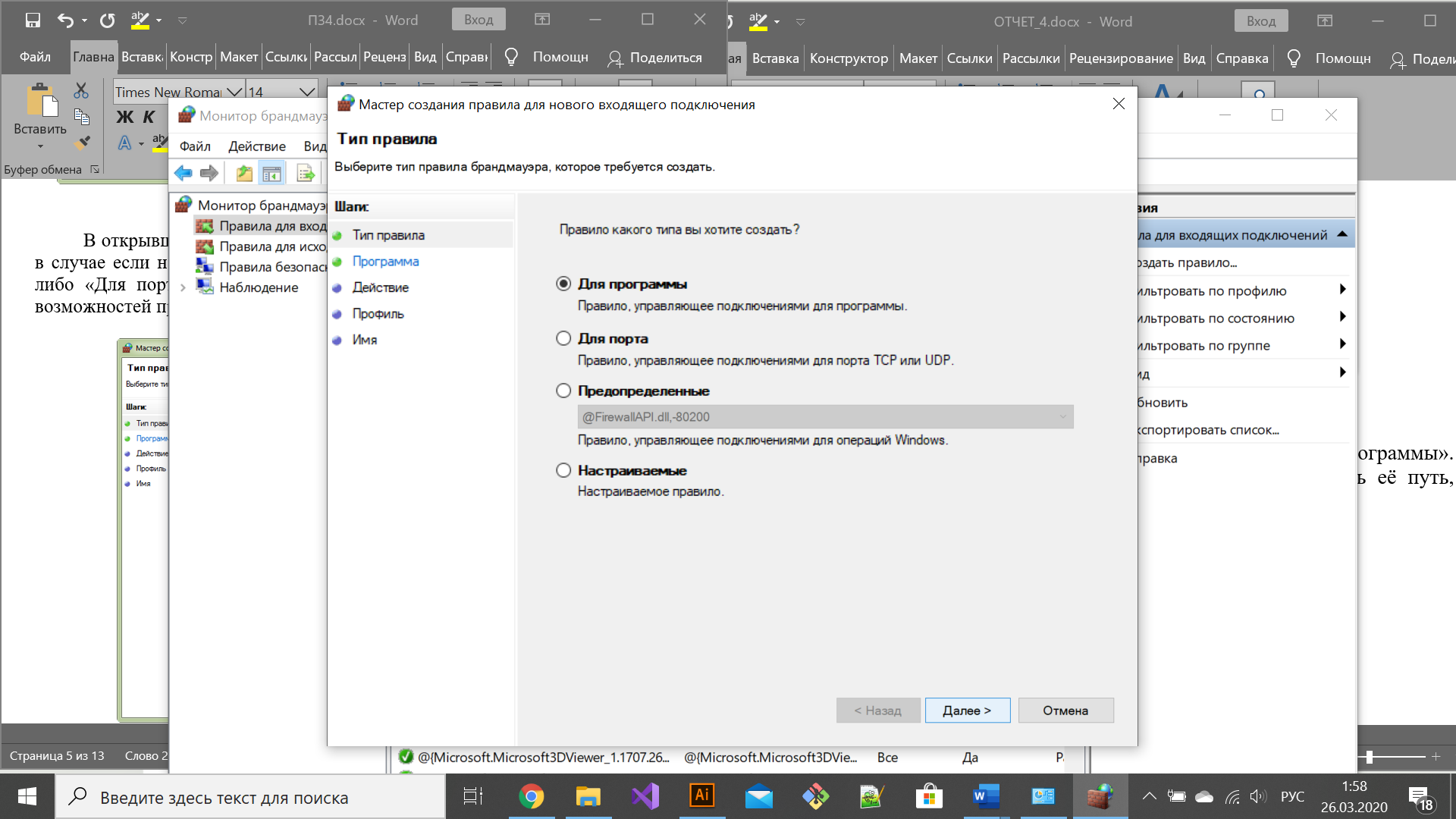


Рисунок 3 – Создание правила



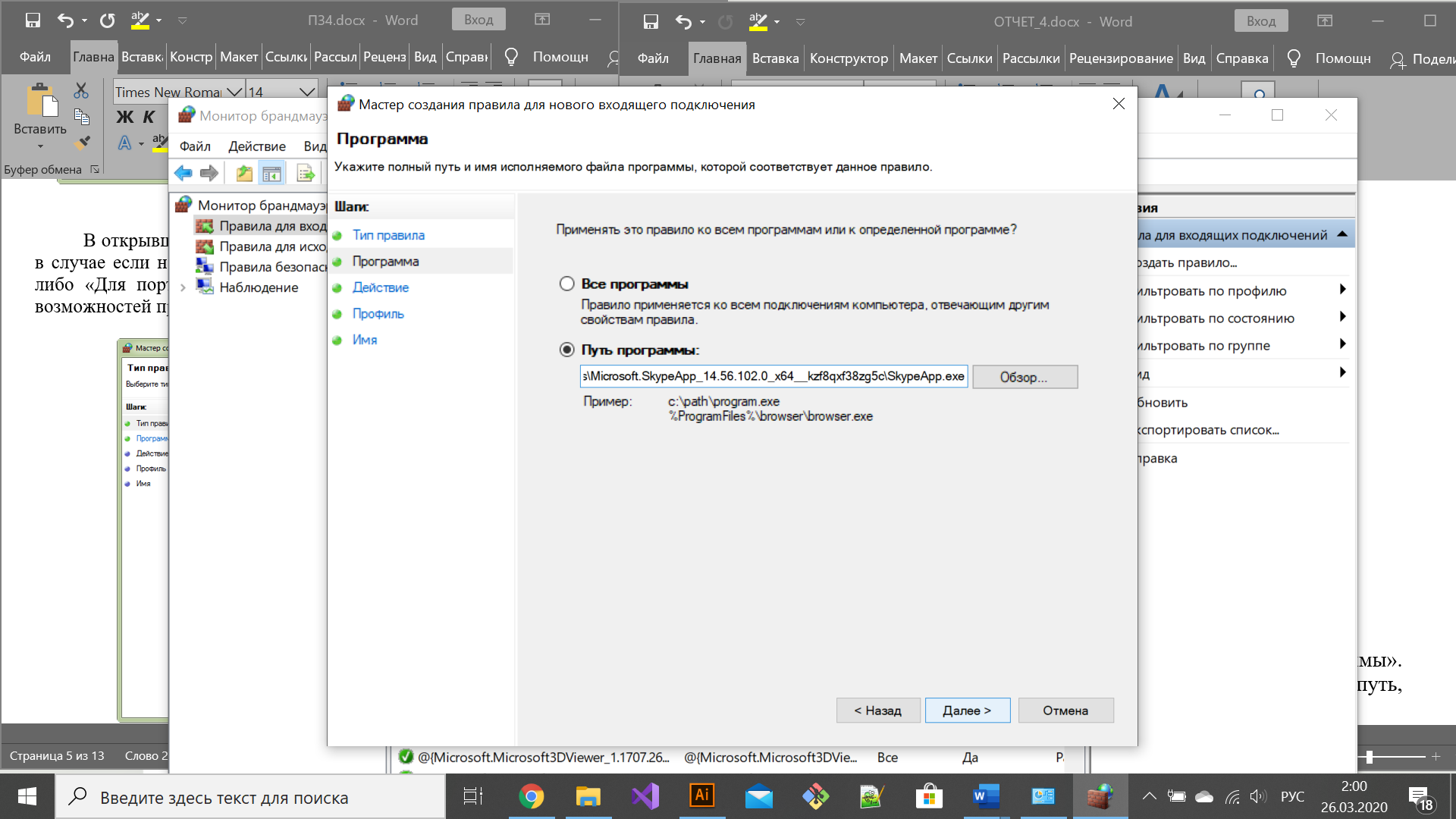


Рисунок 4 – Настройка пути программы

В открывшемся мастере создания правила выбираем «Для программы». При ограничении работы программы, далее необходимо указать её путь, обязательно через папку, в которой она установлена (Рис.4).

Указываем действие:

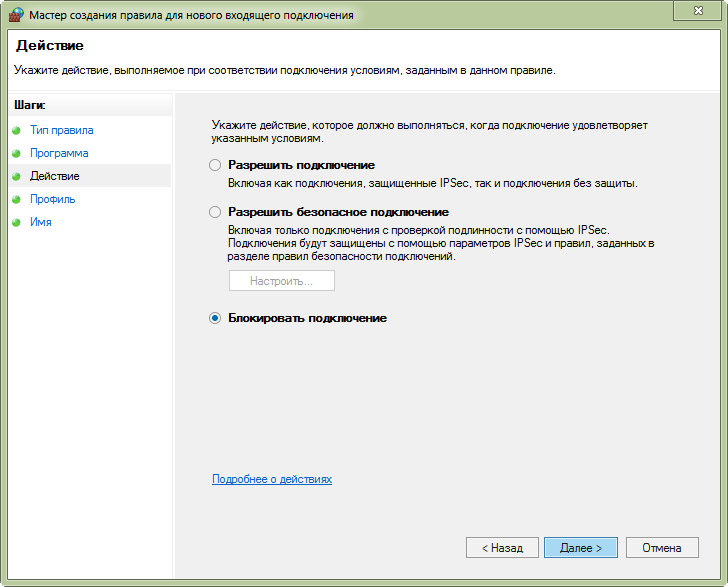


Рисунок 5 – Выбор действия

Указывается какое именно действие нужно применить. В данном случае необходимо блокировать подключение (Рис.5).

В следующем окне указывается имя правила (рис. 6).

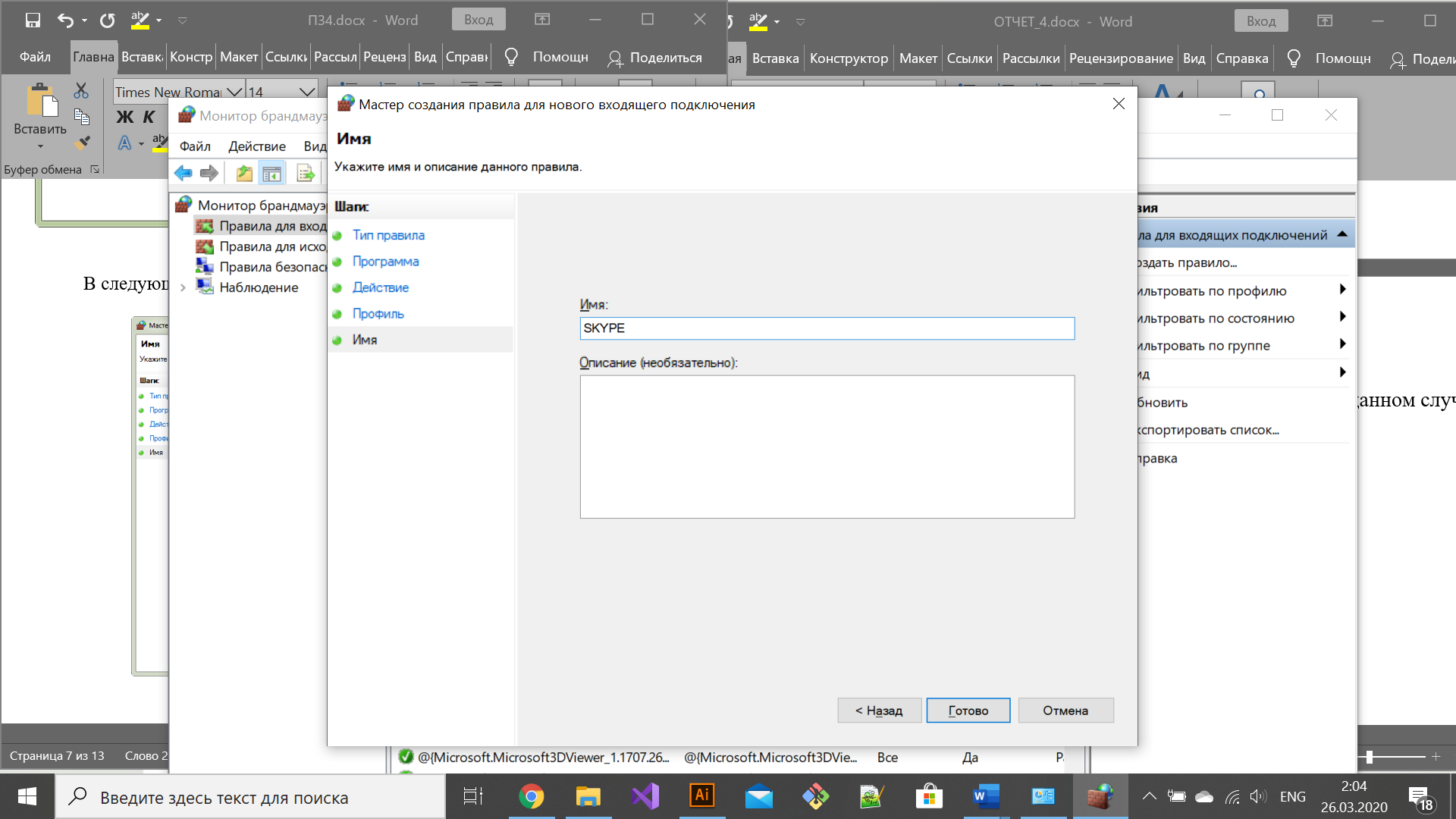


Рисунок 6 – Окно ввода имени

Проверка списка правил:

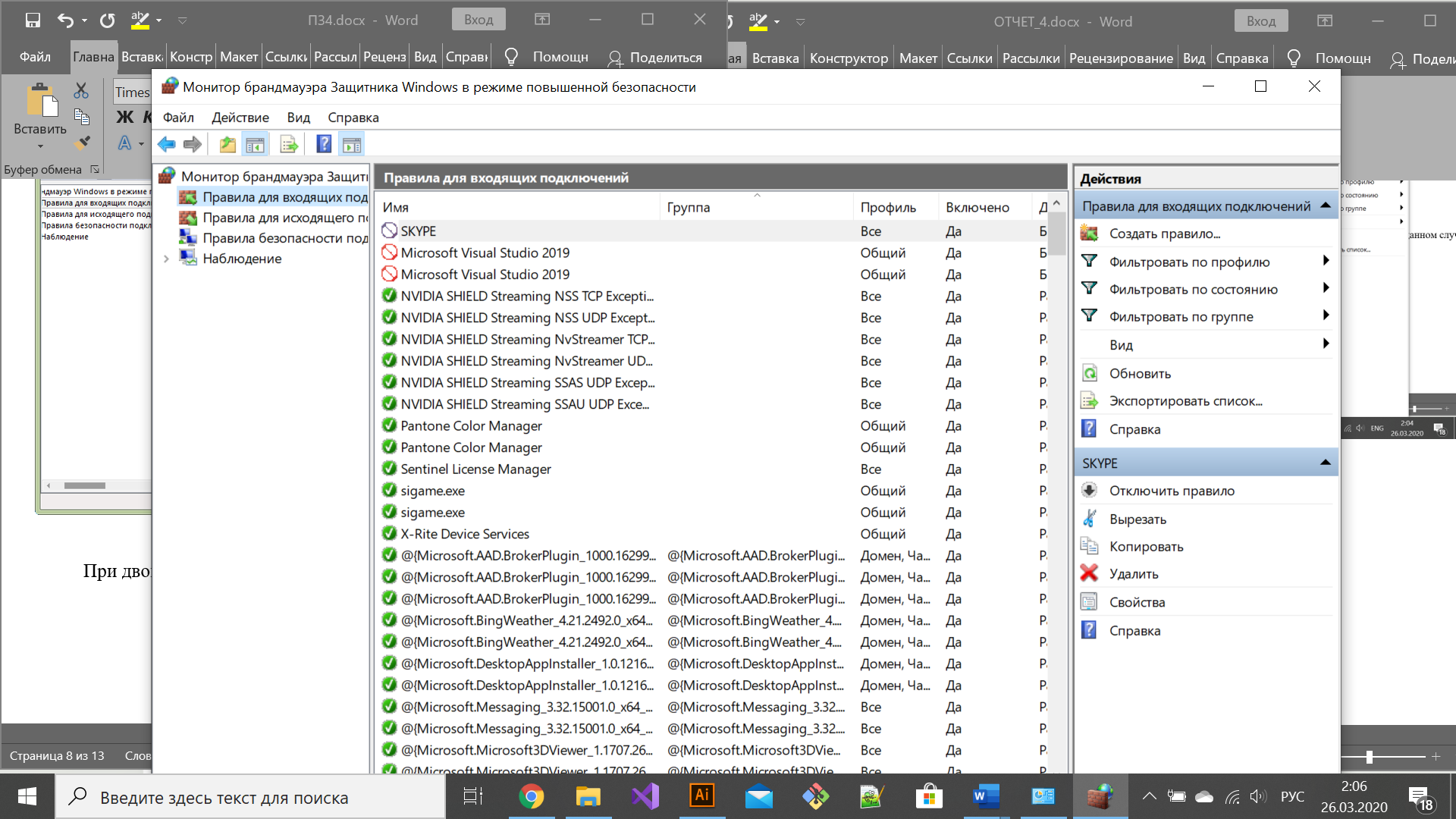


Рисунок 7 – Созданное правило

В общем списке появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели (Рис.7).

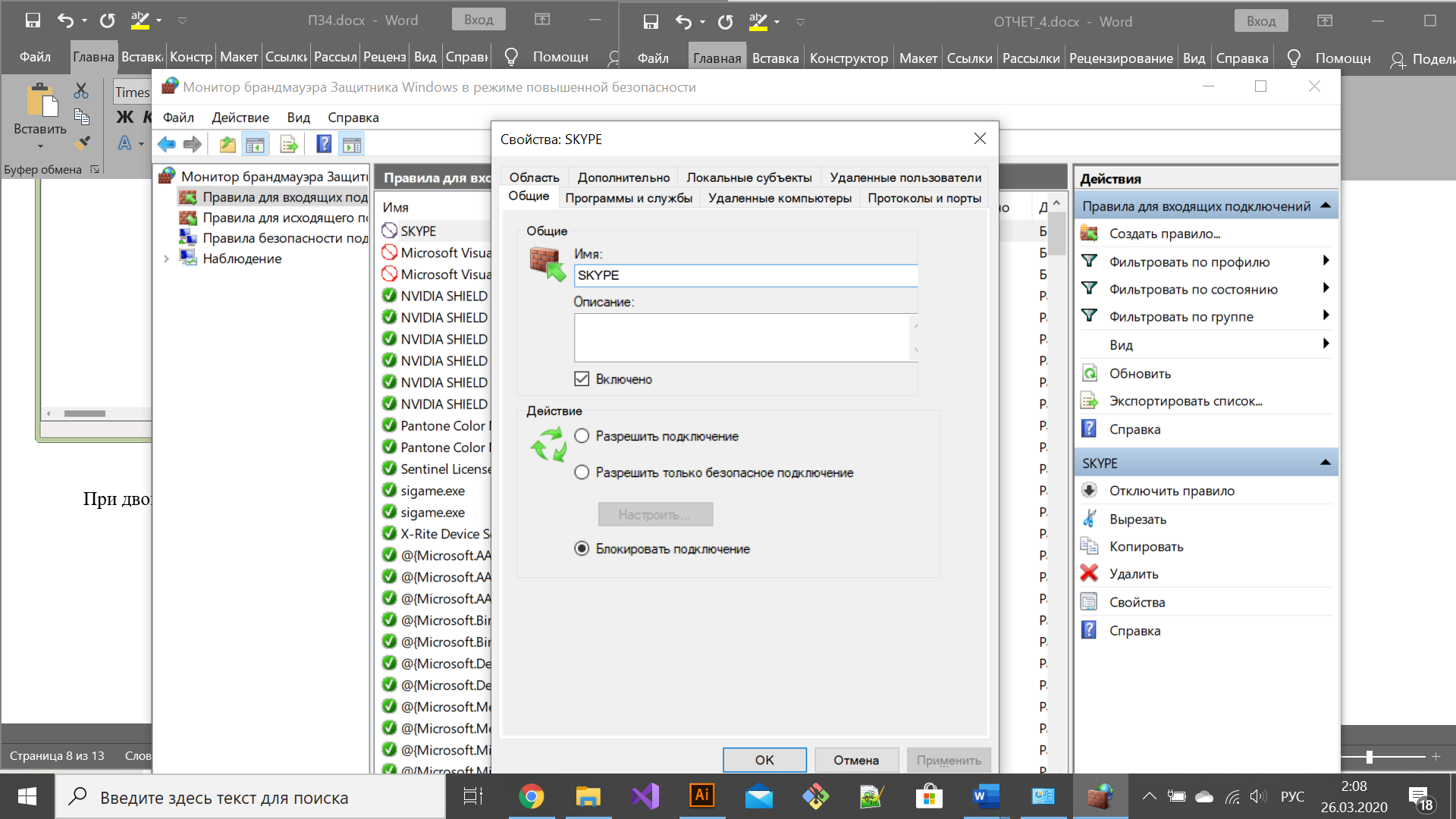


Рисунок 8 – Свойства правила

Проверяем свойства правила (Рис.8).

1. Создать правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий):
   1. Для 1 программы (по выбору) на блокировку подключения;
   2. Для 1 программы (по выбору) на разрешение подключения

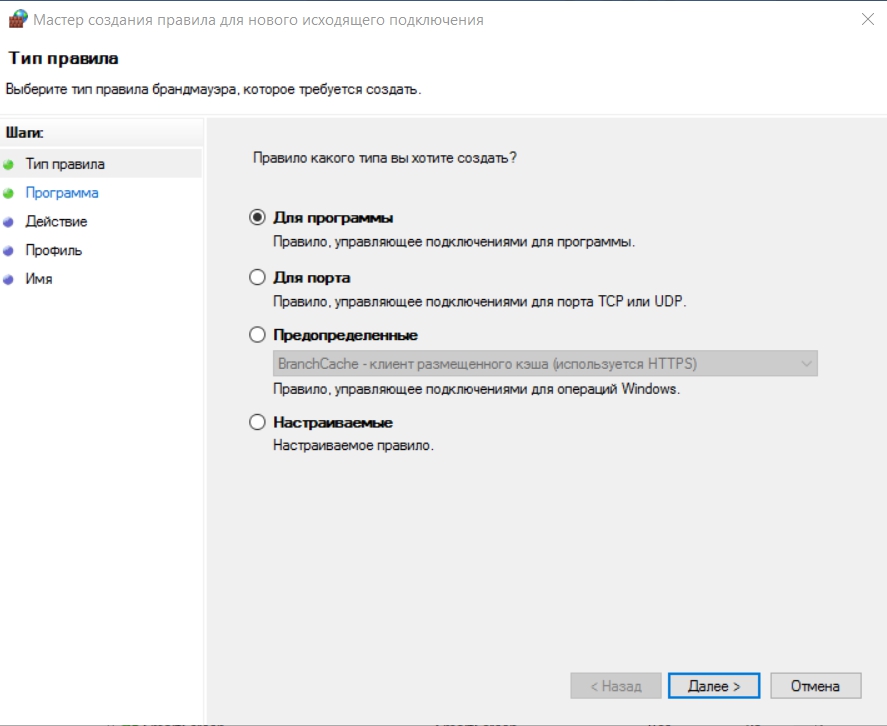


Рисунок 9 – Выбор типа для правила

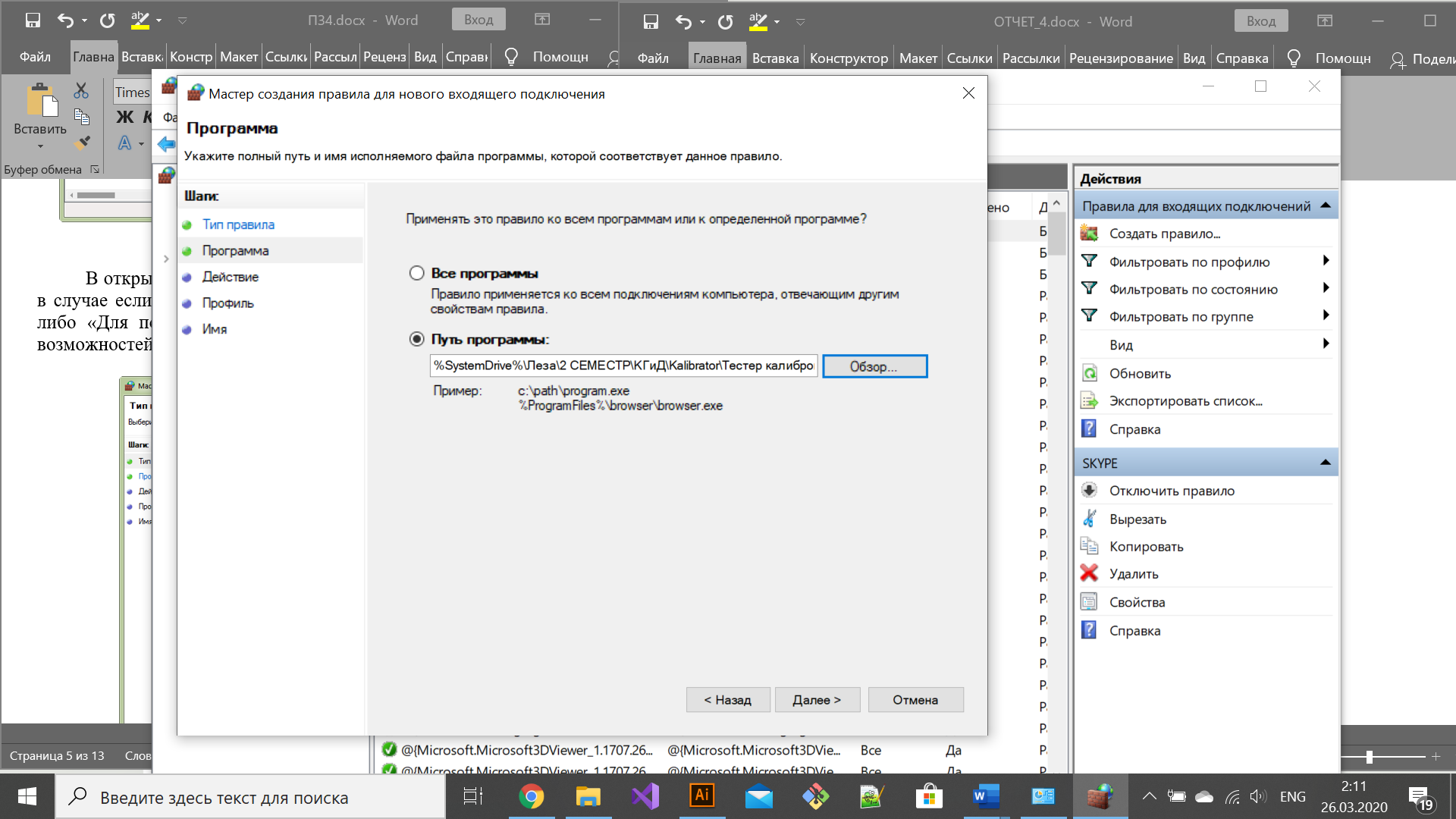


Рисунок 10 – Путь к программе

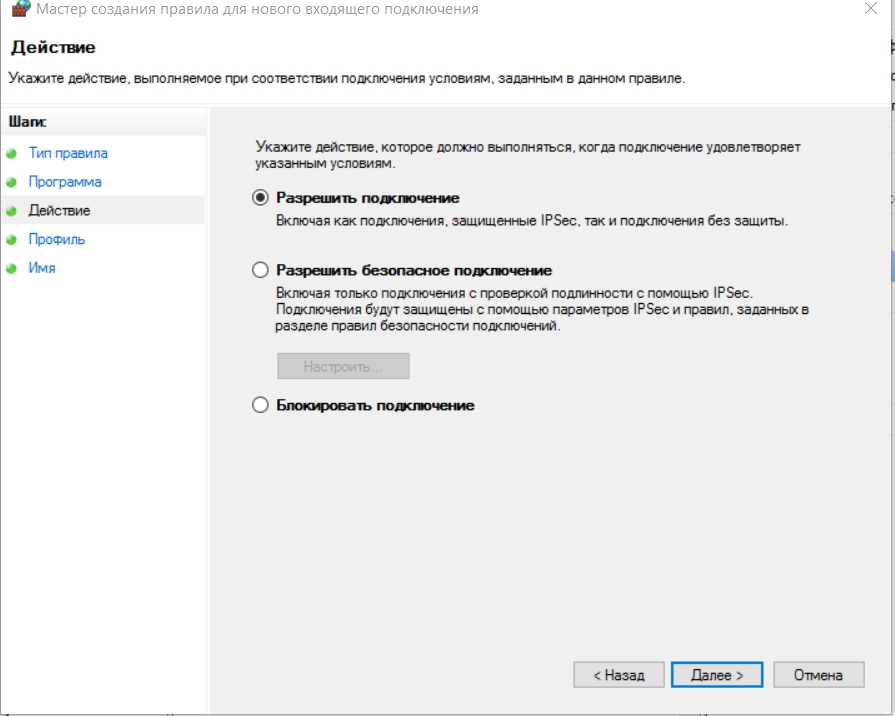


Рисунок 11 – Выбор действия

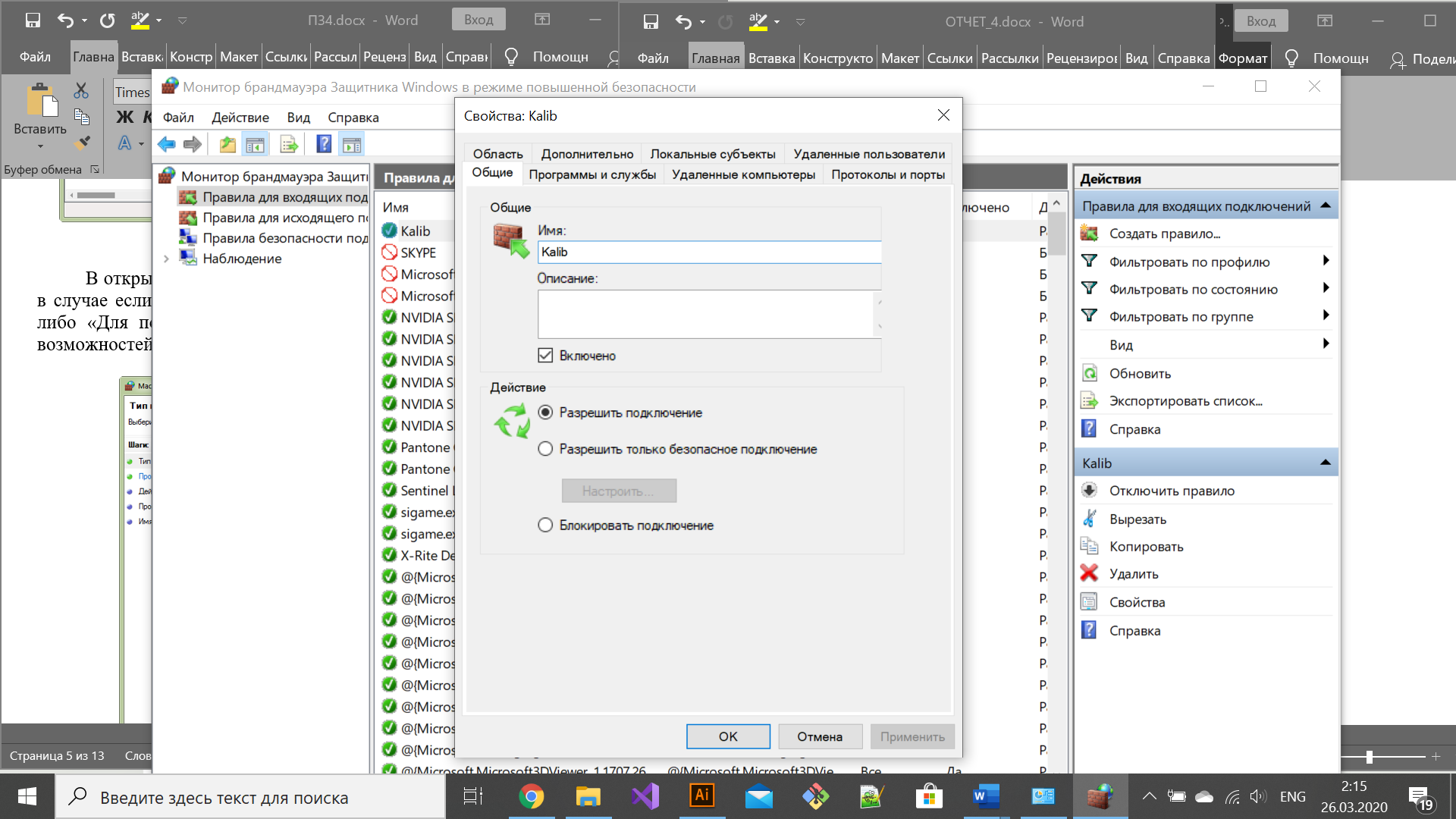


Рисунок 12 – Свойства

Проверка созданного правила(Рис.13):

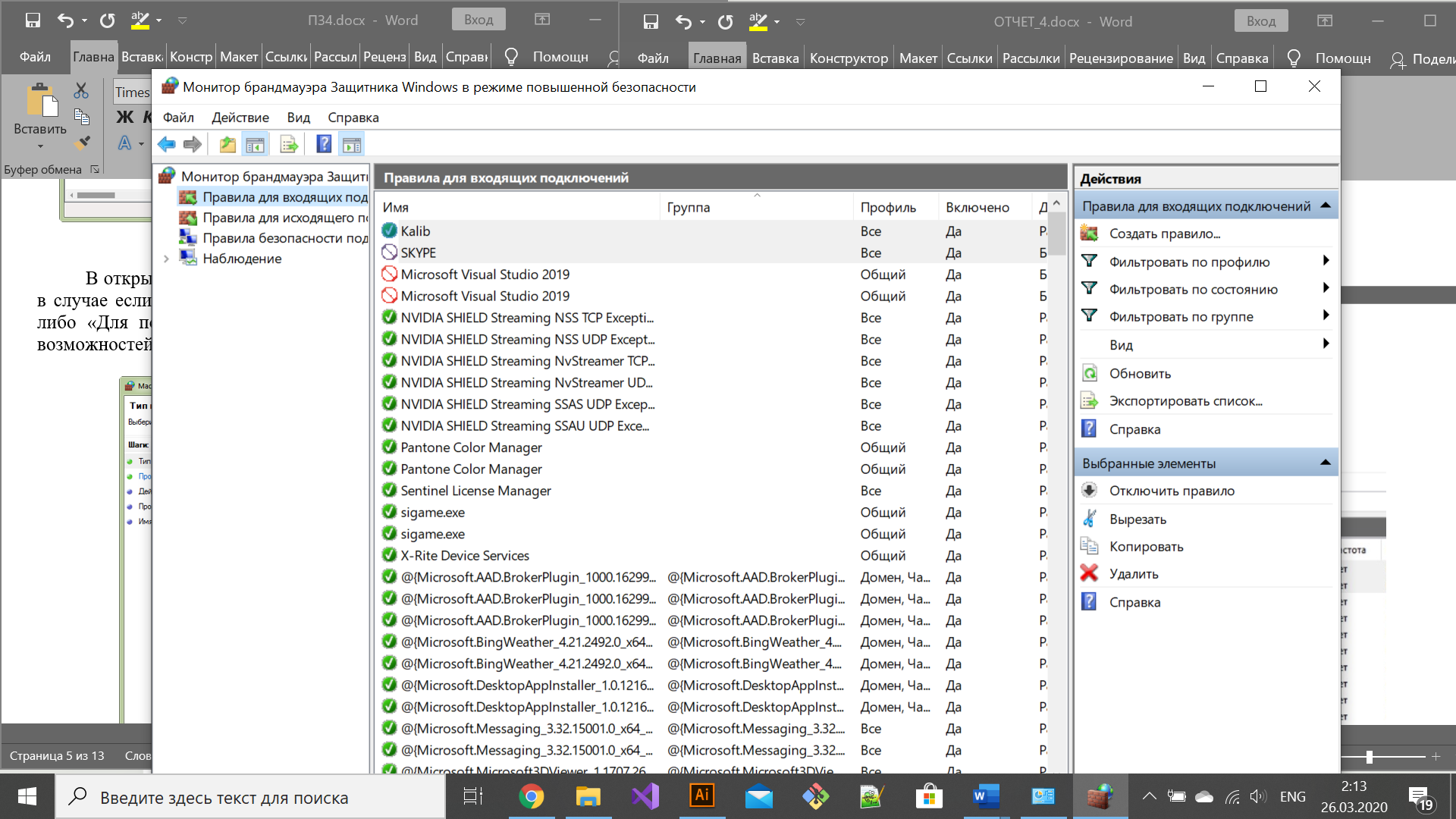


Рисунок 13 – Созданное правило

Для блокировки исходящего подключения (Рис.14):

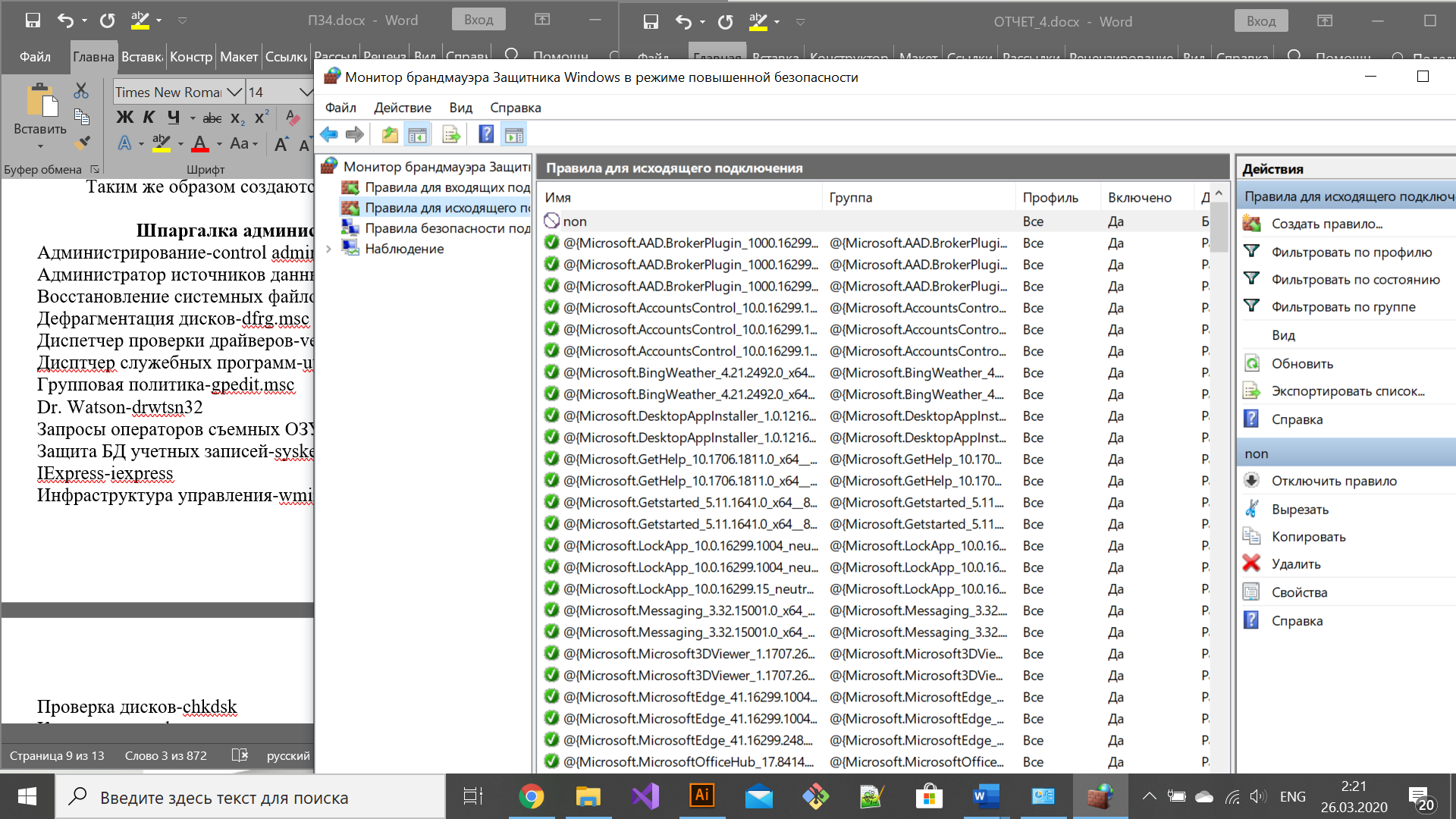


Рисунок 14 – Созданное правило

1. Опробовать действие нескольких.

Проверка использования команды *control admintools* (Рис.15):

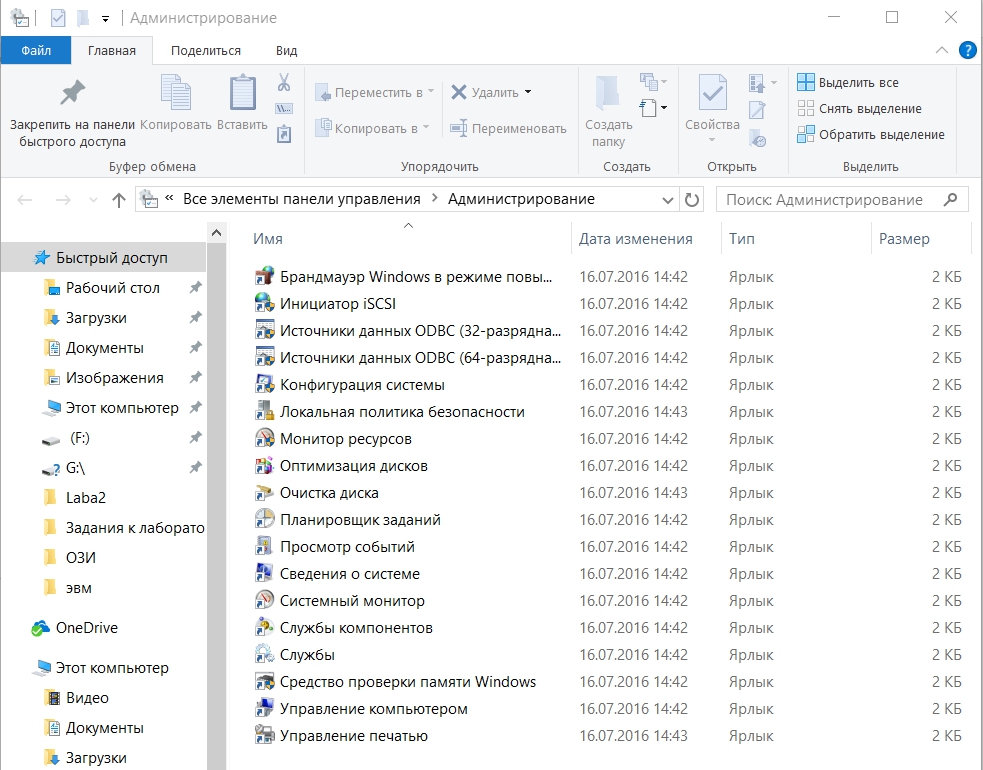


Рисунок 15 – control admintools

Проверка использования команды *perfmon.msc* (Рис.16):

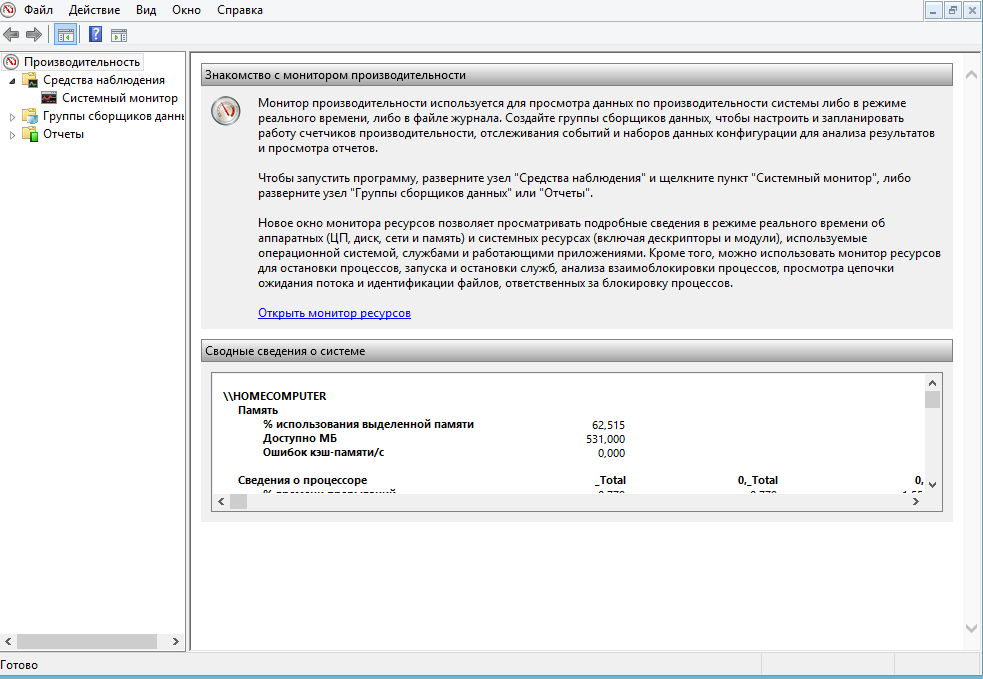


Рисунок 16 – perfmon.msc

**Вывод**: В ходе выполнения данной работы мы изучили работу брандмауэра Windows, научились включать и отключать запреты на подключения для программ. Так же изучили команды, необходимые для работы администратора.