МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования

«Белорусский государственный технологический университет»

Отчет по дисциплине «Основы защиты информации»

Тема «Настройка Брандмауэра Windows»

Сдала: Керезь Екатерина, 2 курс, 4 группа

Принял: Буснюк Николай Николаевич

г. Минск, 2020

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. 4.1).

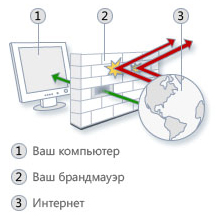


Рисунок 4.1 – Принцип действия Брандмауэра

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. Отметим, что большая часть проблем с информационной безопасностью сетей связана с "прародительской" зависимостью коммуникационных решений от ОС UNIX – особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов (Transmission Control Protocol/Internet Protocol — TCP/IP) имеет "бреши" в защите.

К числу таких 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.

Настройки межсетевого экрана, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах – запрещать всё, что не разрешено в явной форме, и разрешать всё, что не запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жёстко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как она предоставляет пользователям больше возможностей "обойти" межсетевой экран и использовать запрещенные сервисы через нестандартные порты (User Data Protocol – UDP), которые не запрещены политикой безопасности.

**Задание 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;
2. 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;
3. Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.
4. Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).

**Ход работы**

Открываем Монитор брандмауэра Защитника Windows в режиме повышенной безопасности.

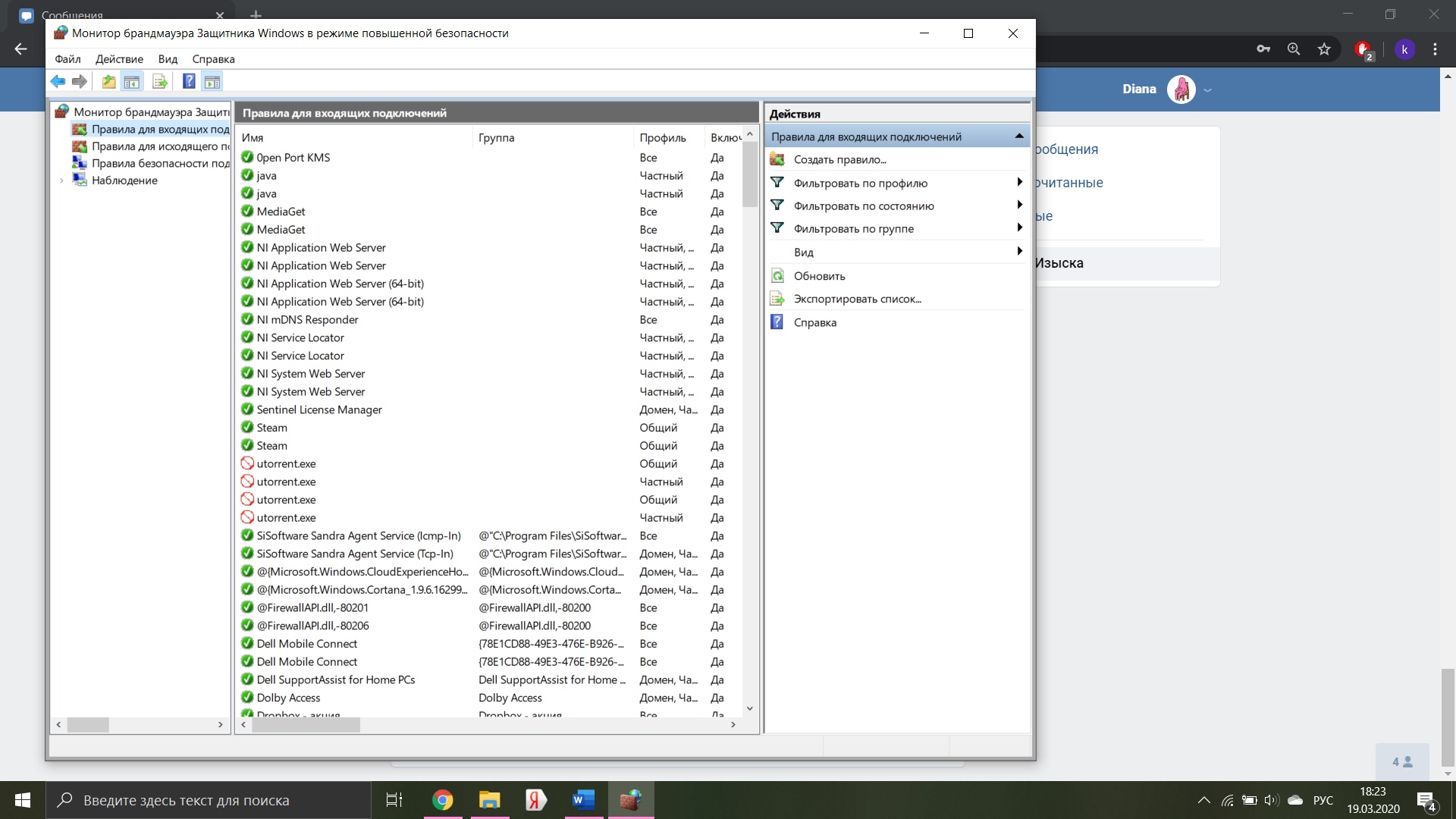


Рисунок 4.2

Открываем список правил для входящих подключений и в меню «Действия» выбираем пункт «Создать правило…» (рис. 4.2).



Рисунок 4.3

В Мастере создания правила для нового входящего подключения выбираем тип правила. В нашем случае, мы создаем правило, управляющее подключениями для программы (рис. 4.3).

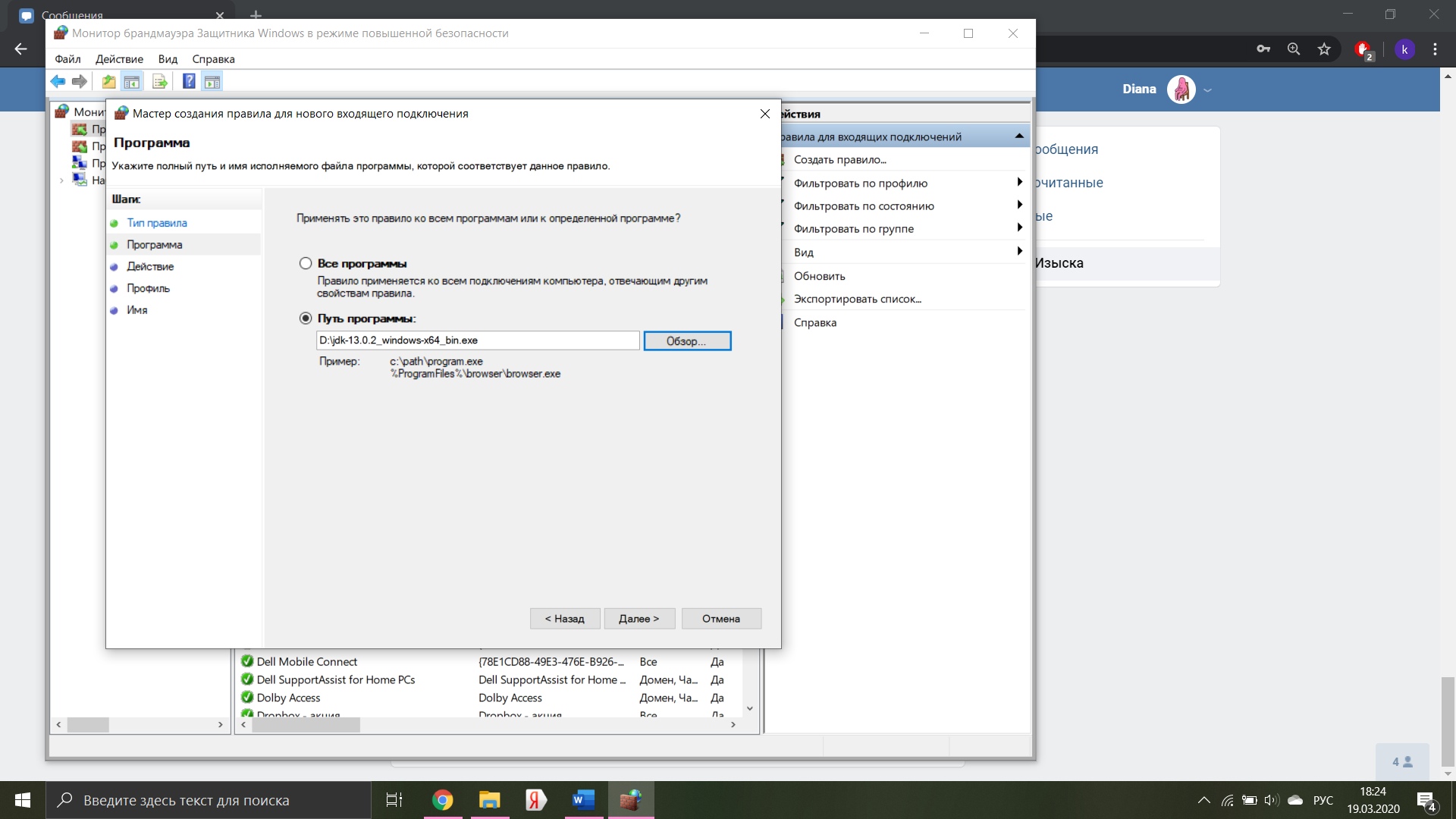


Рисунок 4.4

На шаге Программа указываем полный путь и имя исполняемого файла программы, которой соответствует данное правило (рис. 4.4).

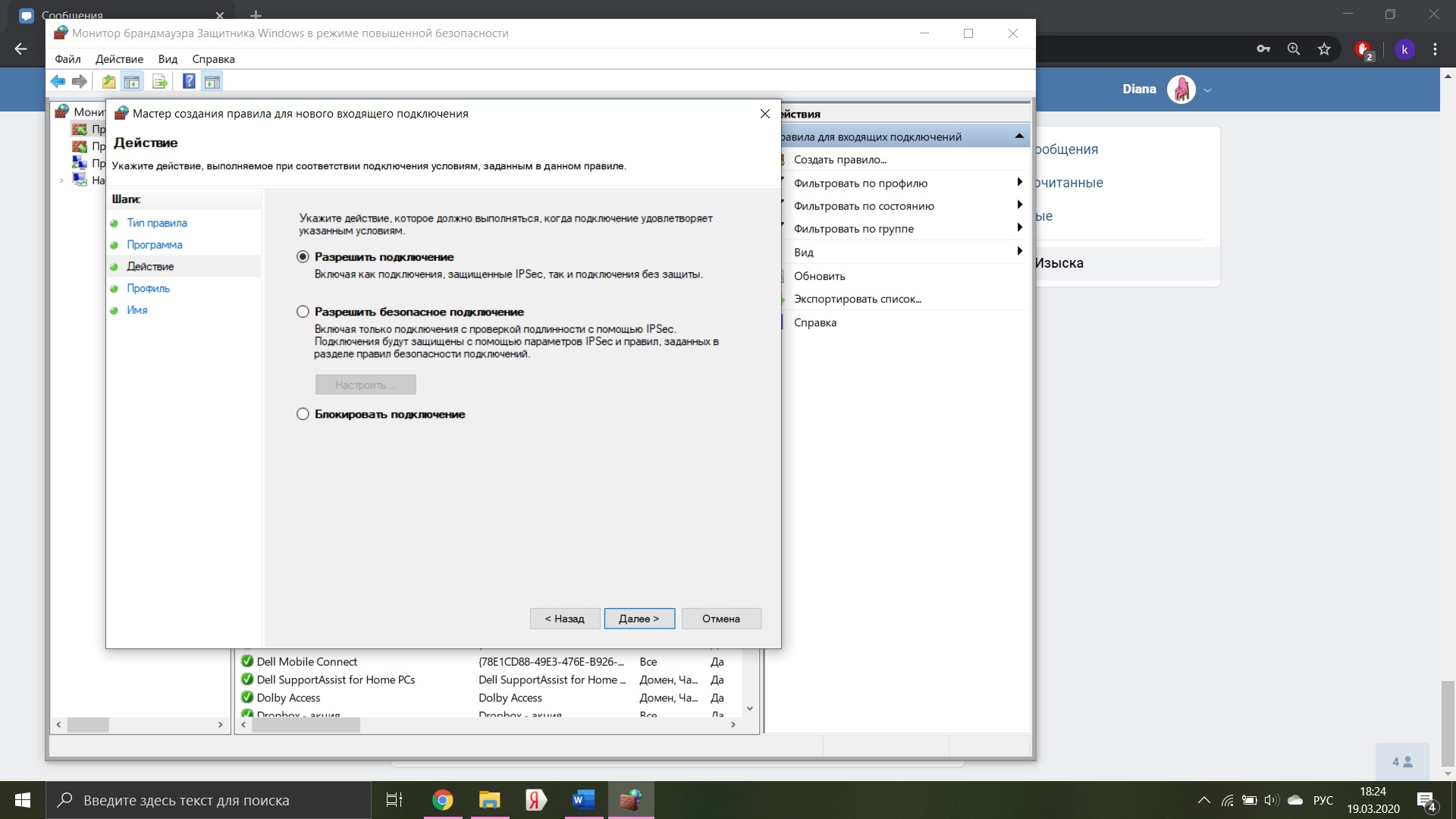


Рисунок 4.5

Далее указываем действие, выполняемое при соответствии подключения условиям, заданным в данном проекте (рис. 4.5).

В демонстрации создания этого правила мы разрешаем подключение. Блокировка подключения при создании правила для нового входящего подключения производится аналогичным способом.

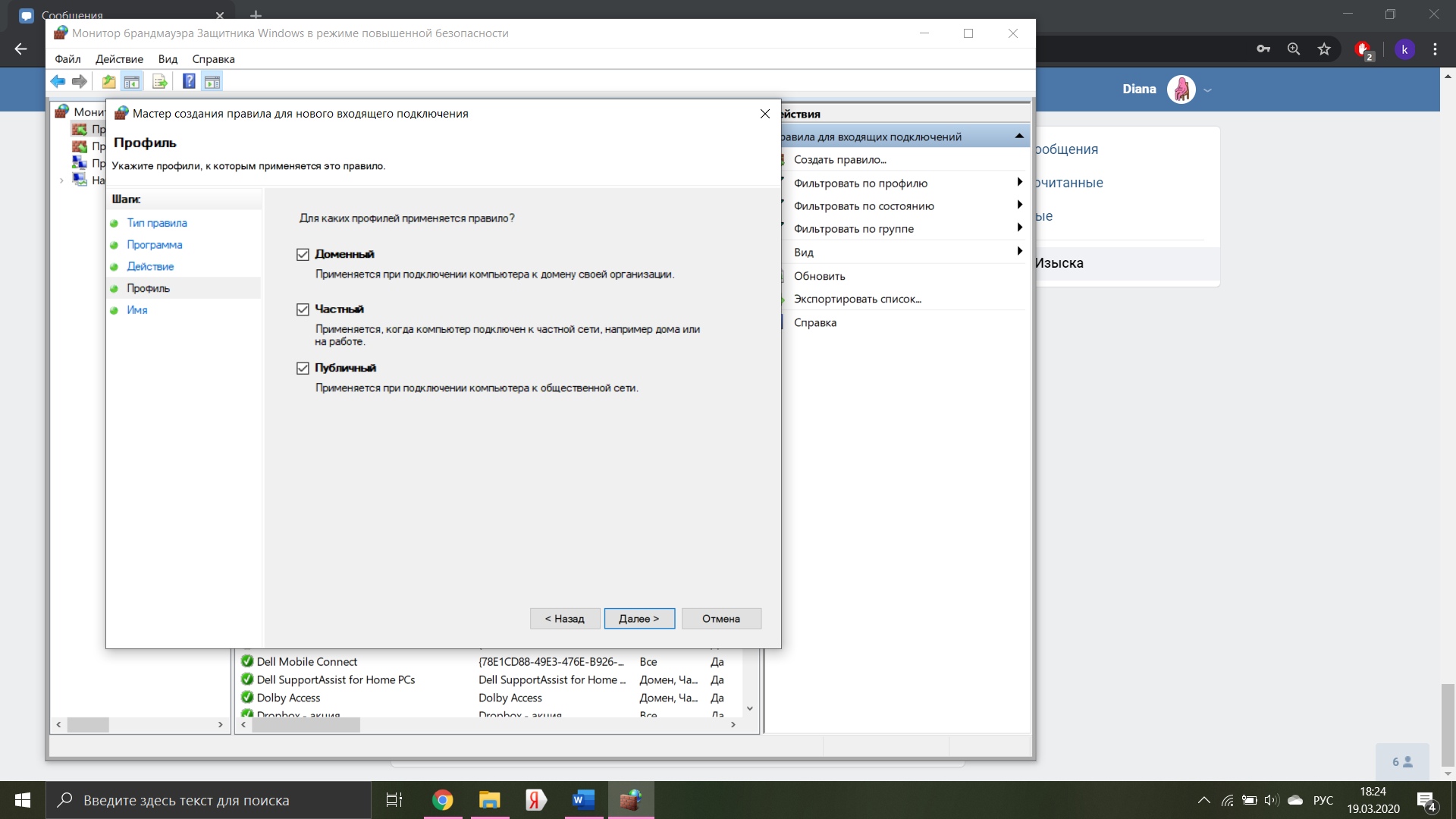


Рисунок 4.6

Так же мы можем указать профили, к которым применяется это правило (рис. 4.6).

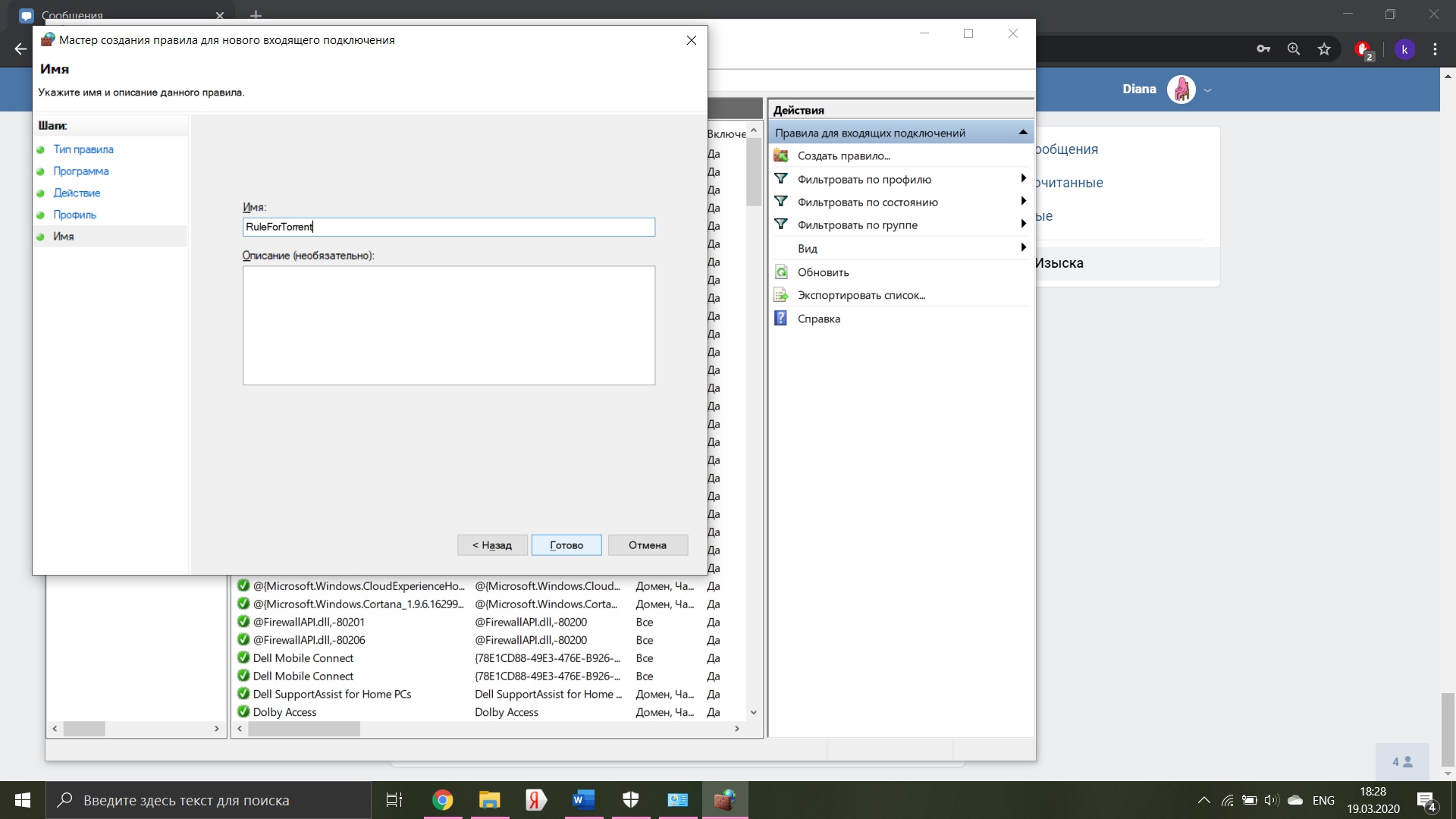


Рисунок 4.7

На финальном шаге мы указываем имя и описание данного правила (рис. 4.7).

Создание правила для нового исходящего подключения производится аналогичным образом.

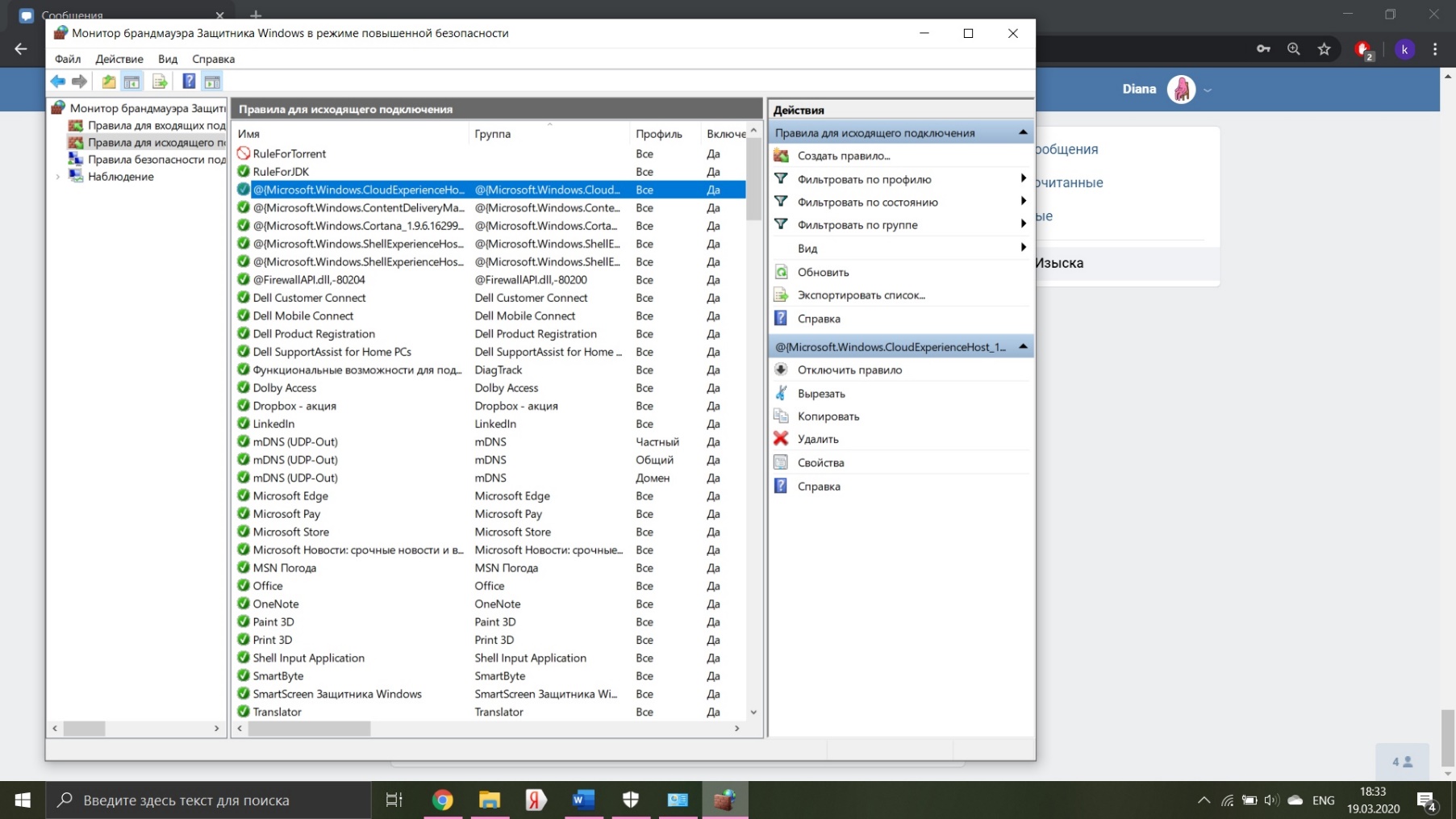


Рисунок 4.8

Открываем список правил для исходящих подключений и в меню «Действия» выбираем пункт «Создать правило…» (рис. 4.8).

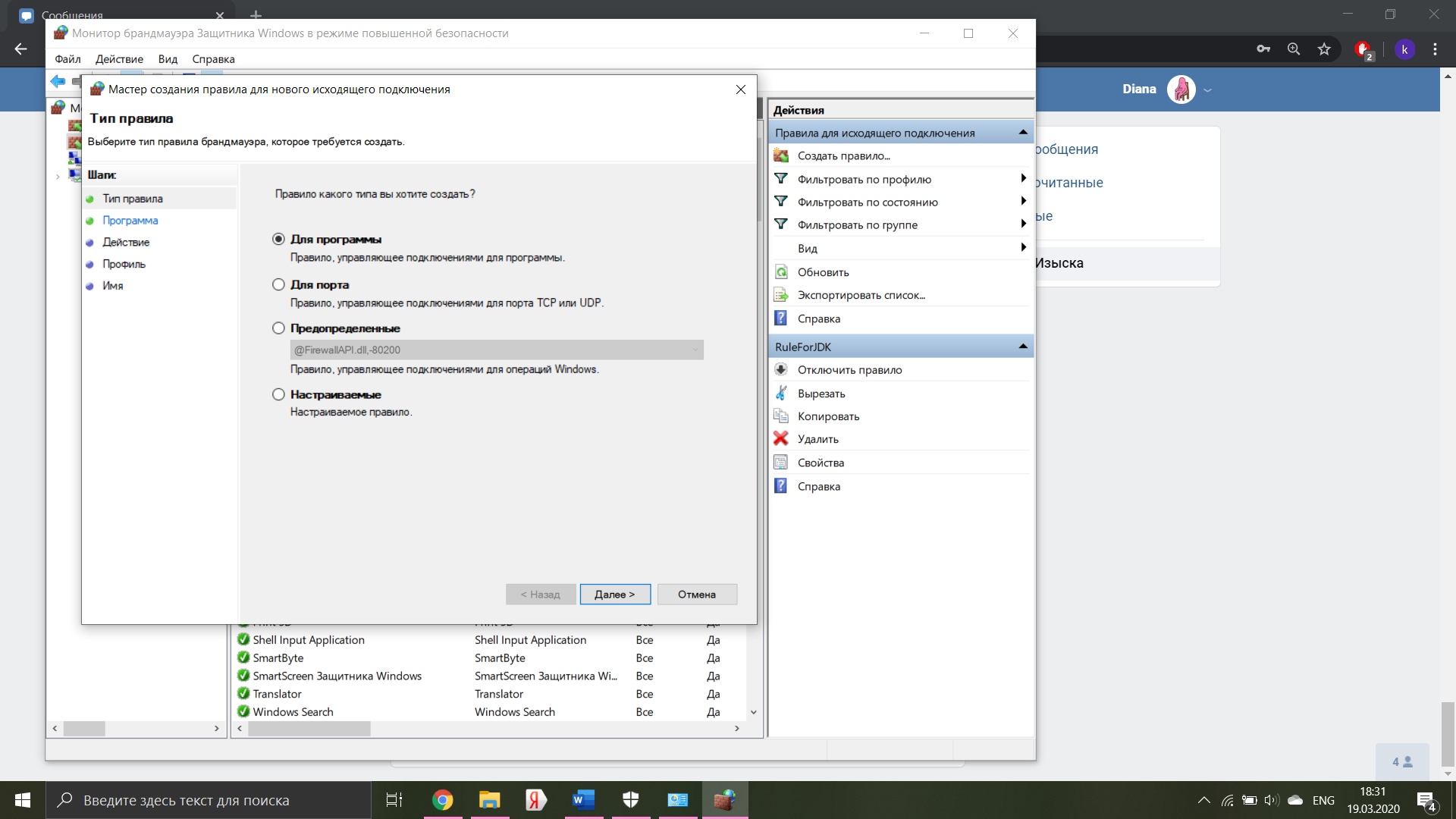


Рисунок 4.9

В Мастере создания правила для нового исходящего подключения выбираем тип правила. В нашем случае, мы создаем правило, управляющее подключениями для программы (рис. 4.9).

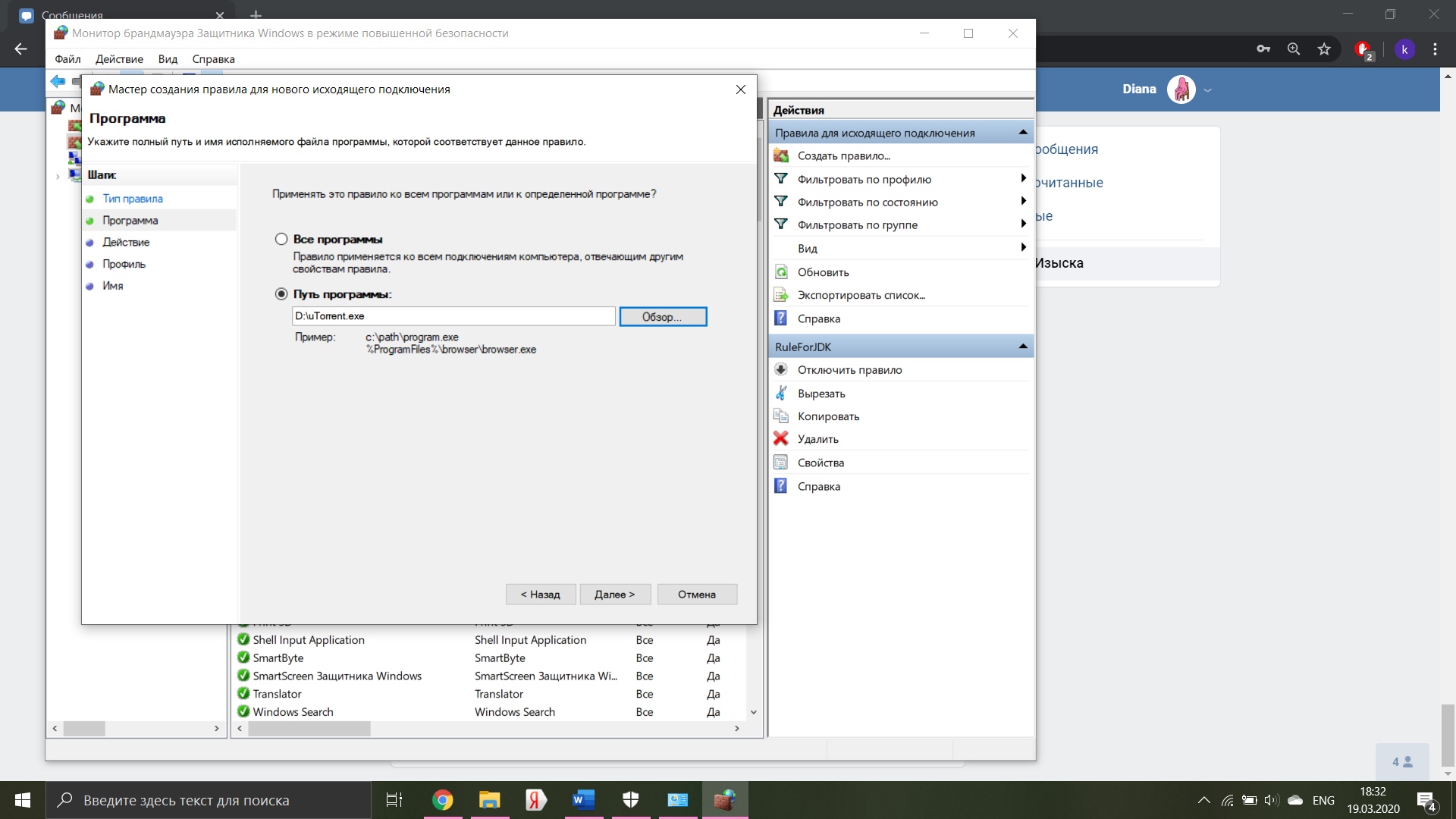


Рисунок 4.10

На шаге Программа указываем полный путь и имя исполняемого файла программы, которой соответствует данное правило (рис. 4.10).

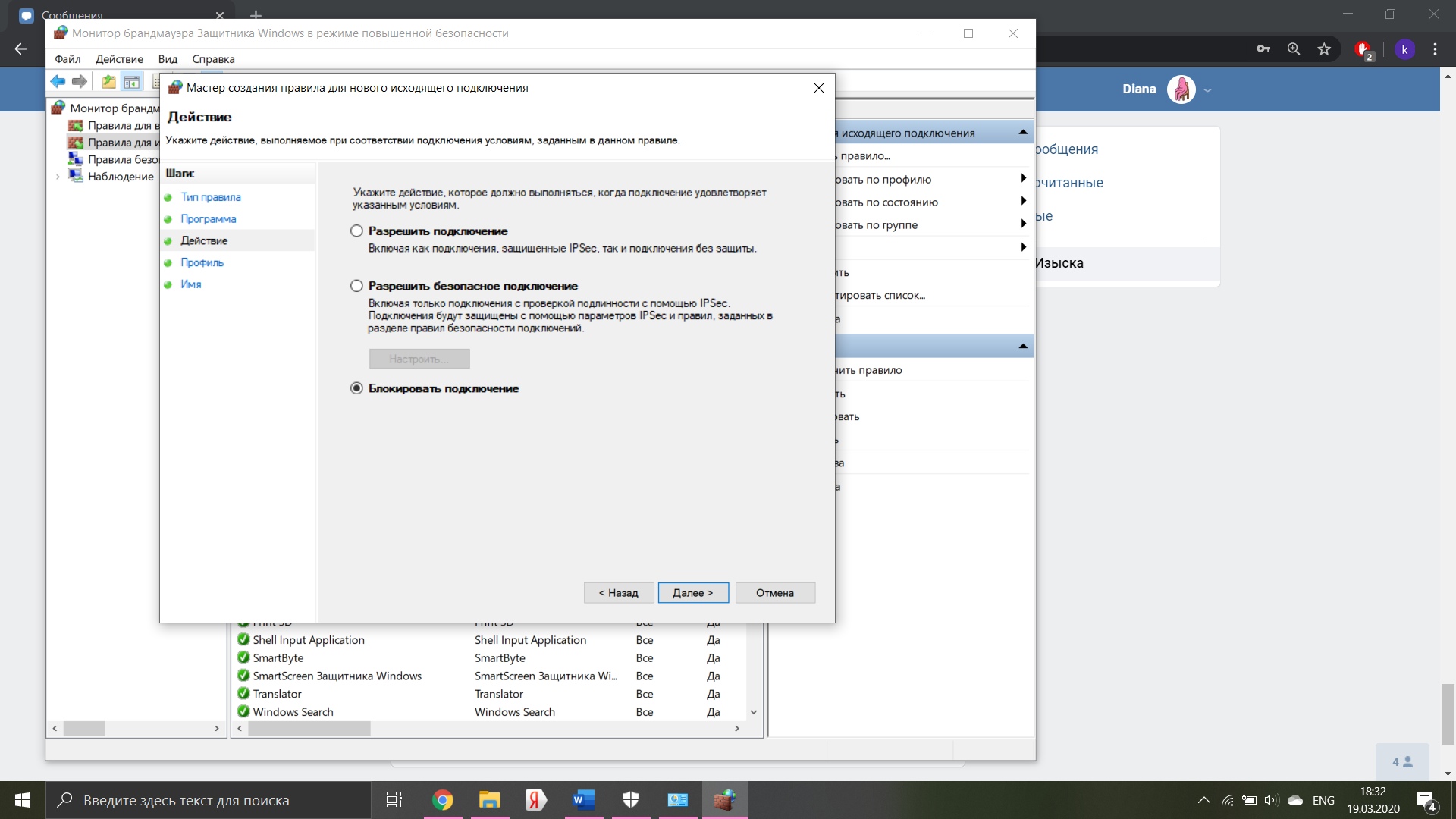


Рисунок 4.11

Далее указываем действие, выполняемое при соответствии подключения условиям, заданным в данном проекте (рис. 4.11).

В демонстрации создания этого правила мы разрешаем подключение. Разрешение подключения при создании правила для нового исходящего подключения производится аналогичным способом.

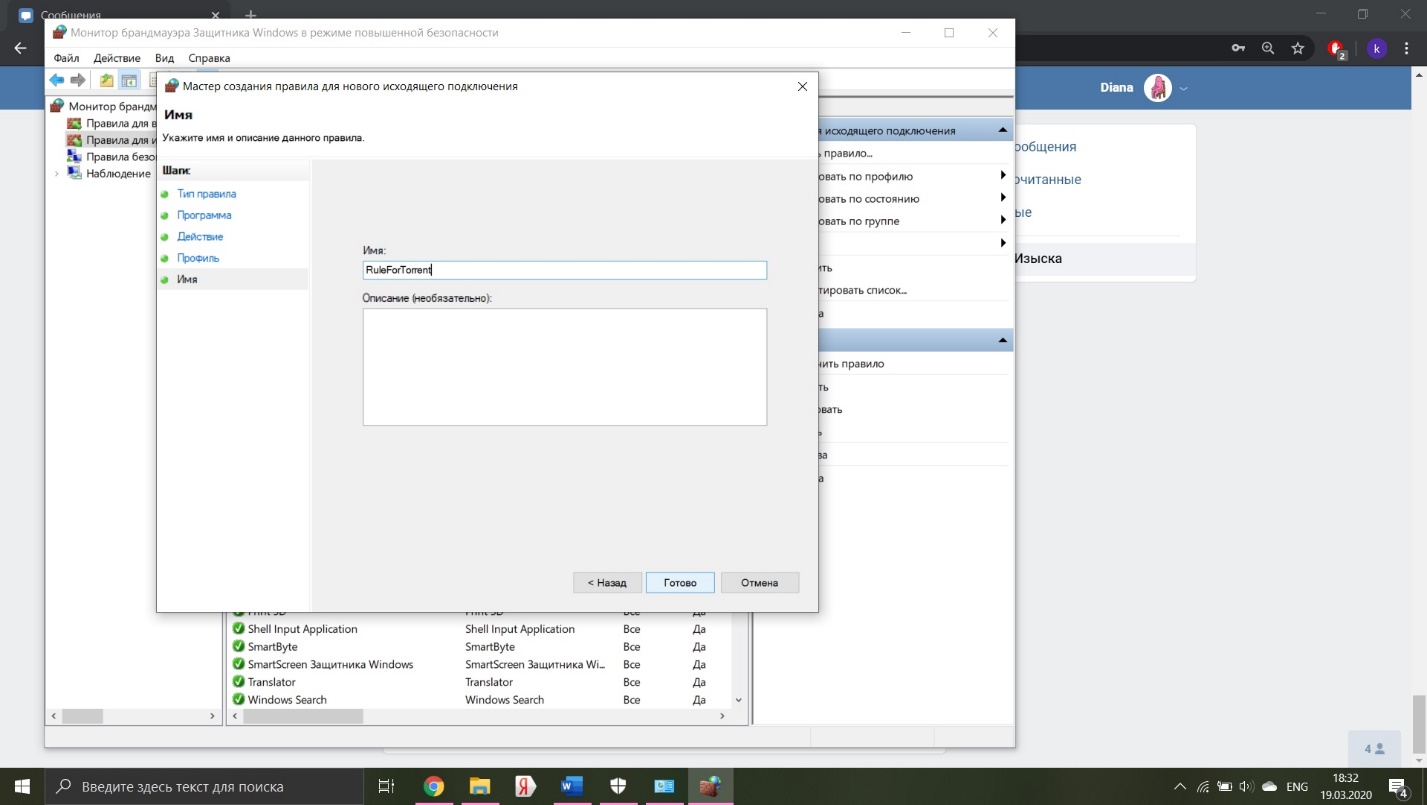


Рисунок 4.12

На финальном шаге мы указываем имя и описание данного правила (рис. 4.12).

Созданные правила можно просмотреть в списке правил для исходящего или входящего подключения (рис. 4.13).

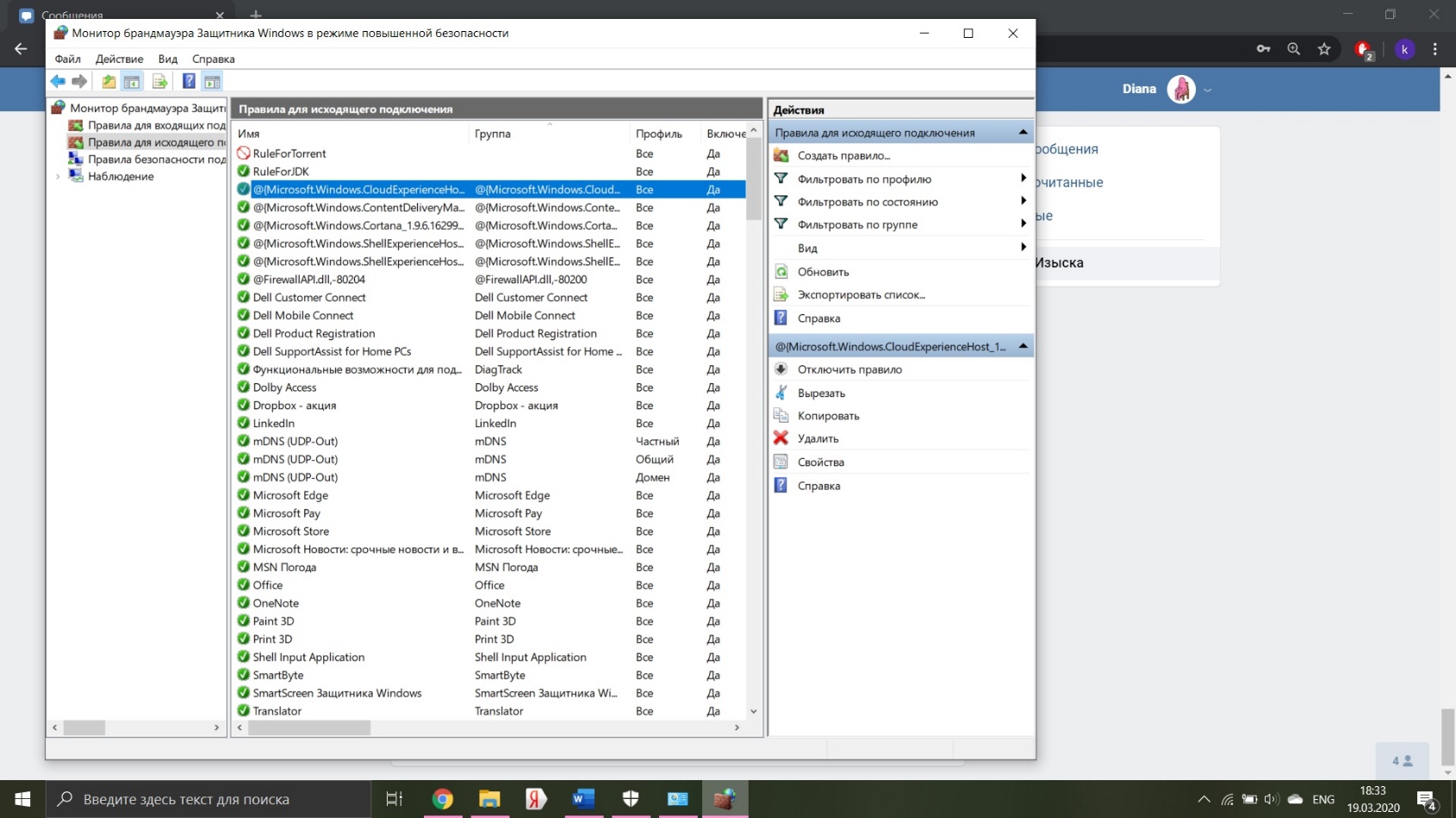


Рисунок 4.13

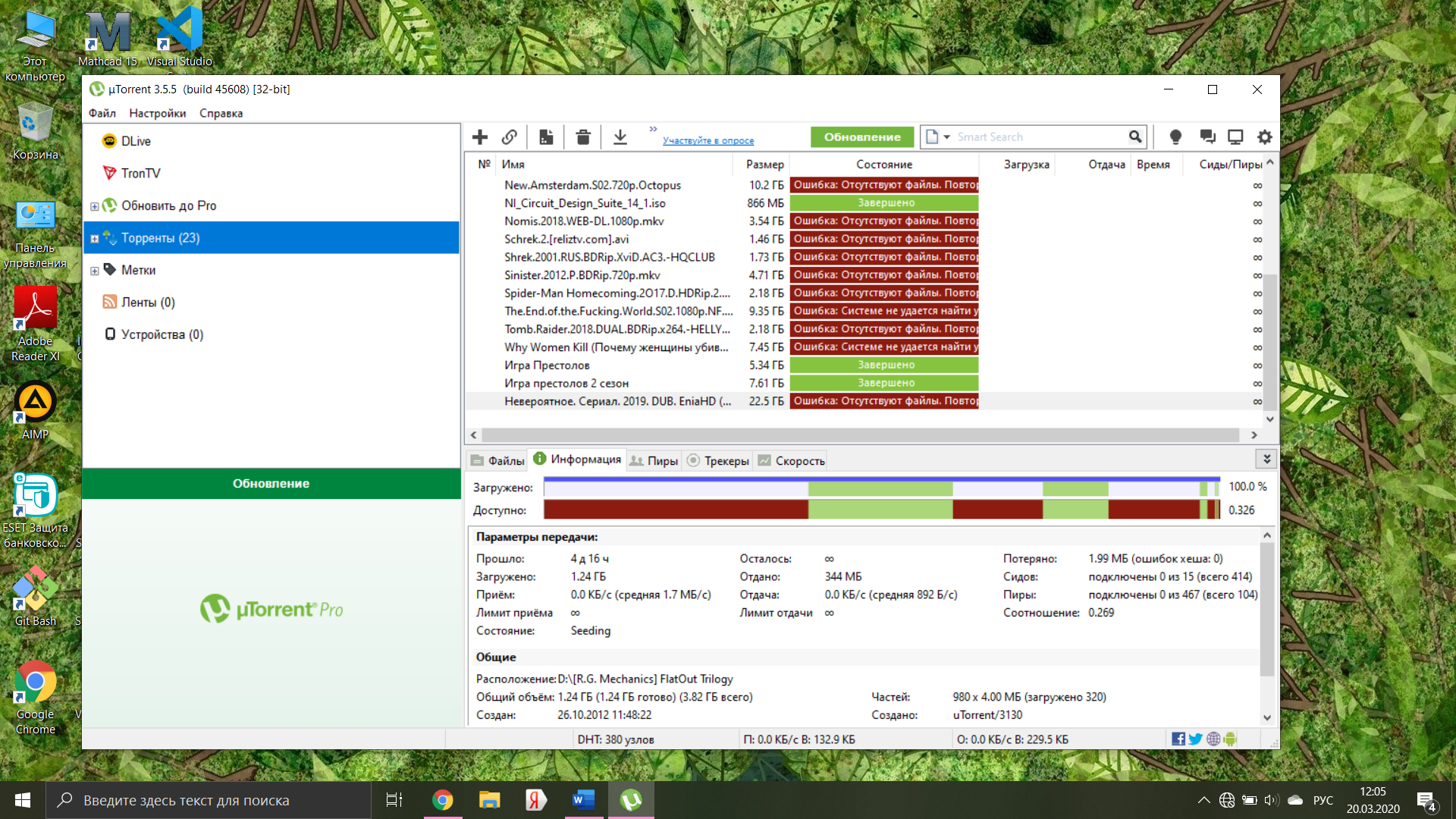


Рисунок 4.14

Проверка работоспособности программ (рис. 4.14).

**Вывод:** в процессе выполнения задания ознакомились с брандмауэром Windows, его функциями и попробовали в действии команды администратора.