Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

Студент: Городилов М. П.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

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).

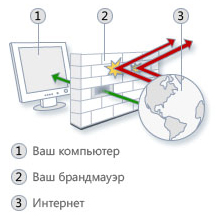


Рисунок 4.1 – Принцип действия Брандмауэра

Межсетевой экран является одним из основных компонентов защиты сетей. 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 имеет "бреши" в защите.

К числу таких служб и протоколов относятся:

* доступ к всемирной паутине WWW;
* программа электронной почты Send Mail;
* 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, которые не запрещены политикой безопасности.

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).

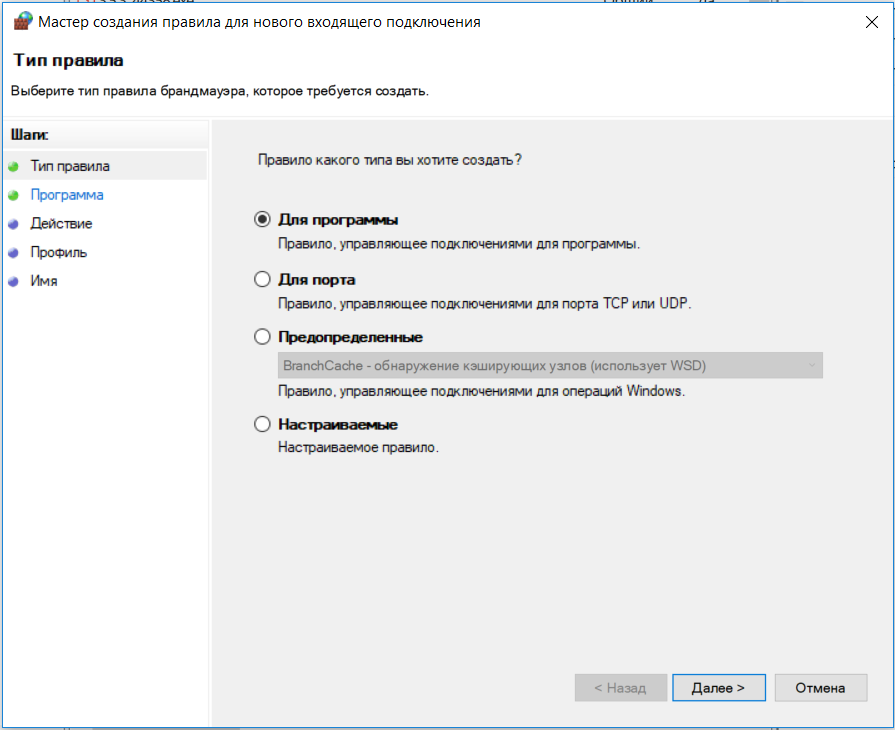
Открываем Мастер создания правила для входящего подключения(Рисунок 4.2).

Рисунок 4.2 – Выбор типа правила

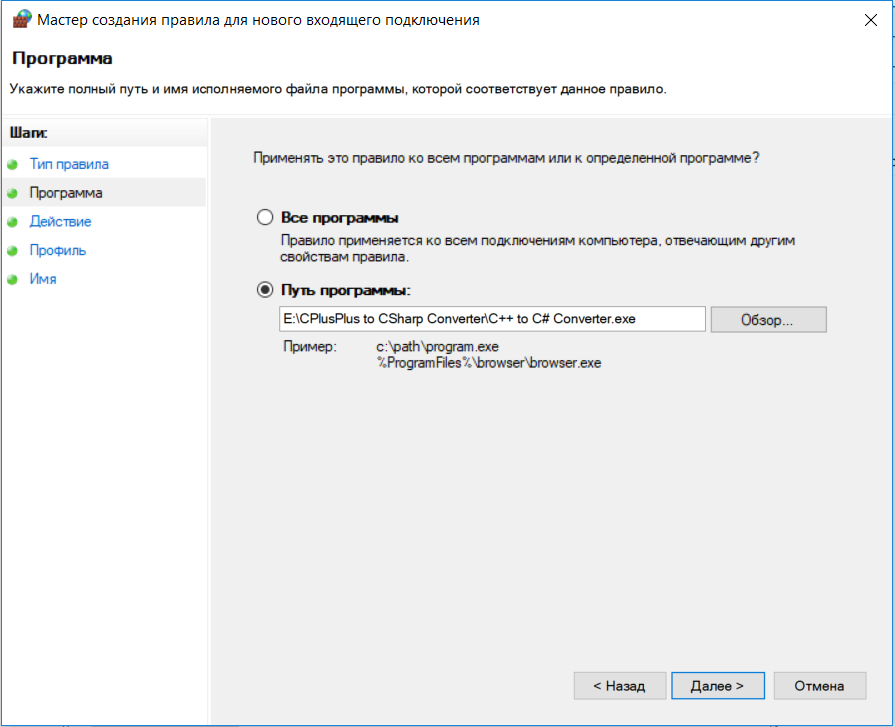
Указываем путь к программе(Рисунок 4.3) . 

Рисунок 4.3 – Путь к программе

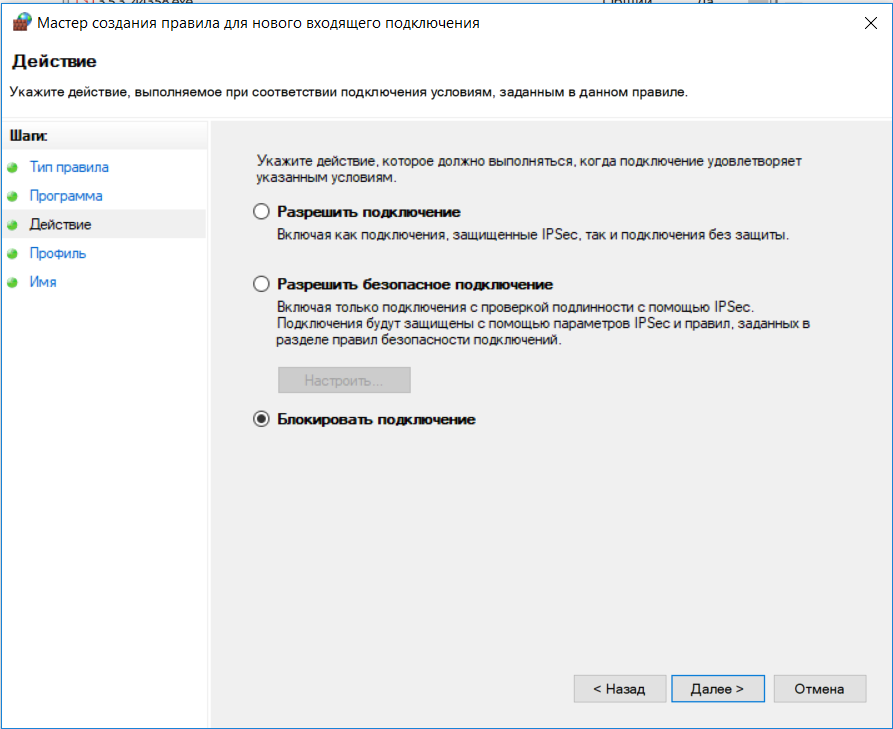
Далее выбираем блокировку подключения (Рисунок 4.4)

Рисунок 4.4 – Блокировка подключения

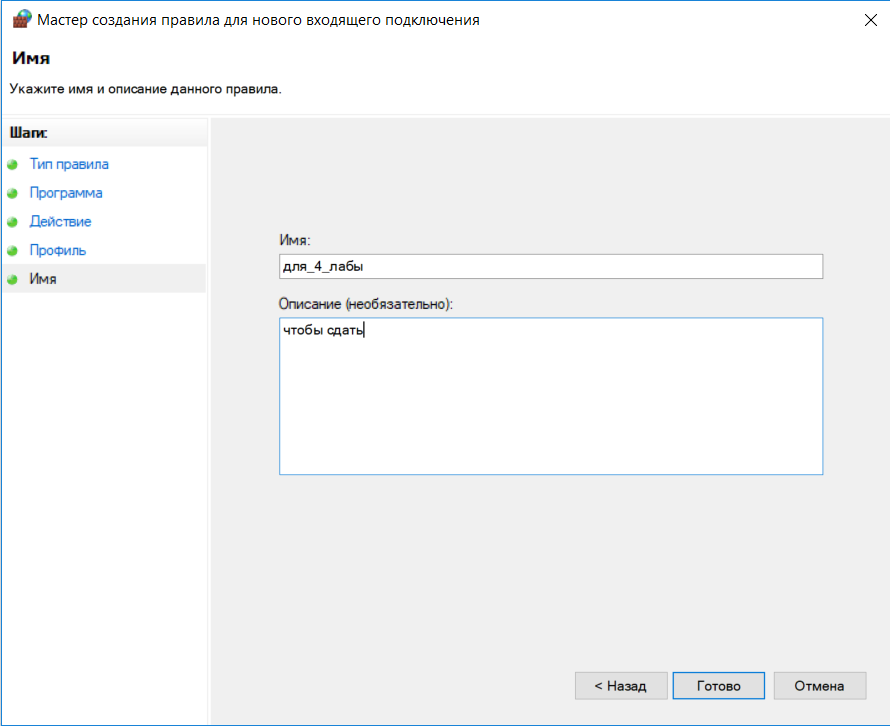
В Следующем окне указывается имя правила (Рисунок 4.5)

Рисунок 4.5 – Описание правила

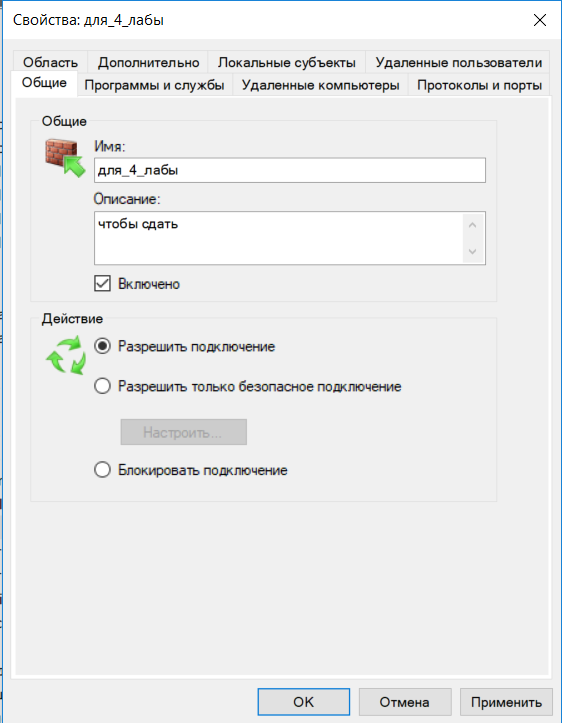
Разрешить подключение (Рисунок 4.6).

Рисунок 4.6 – Свойство правила

Встроенный брандмауэр Windows предоставляет возможность создавать мощные правила. Вы можете блокировать программам доступ к сети Интернет, ограничивать трафик на определенные порты и IP-адреса, а также многое другое не устанавливая файрвол от стороннего производителя.

Таким же образом создаются и правила для исходящих подключений.

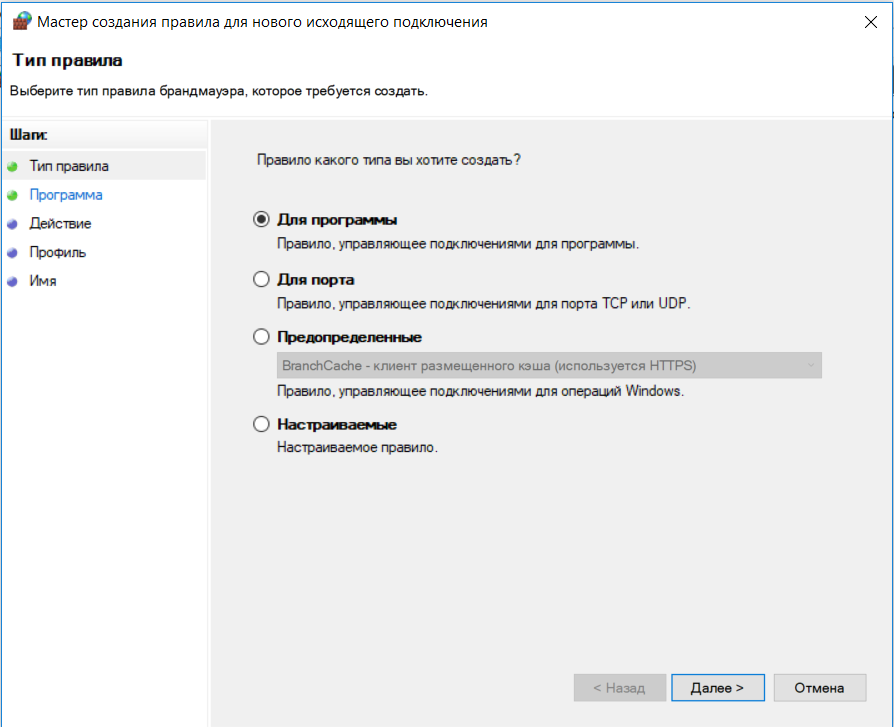
Открываем Мастер создания правила для входящего подключения(Рисунок 4.7)

Рисунок 4.7 – Выбор типа правила

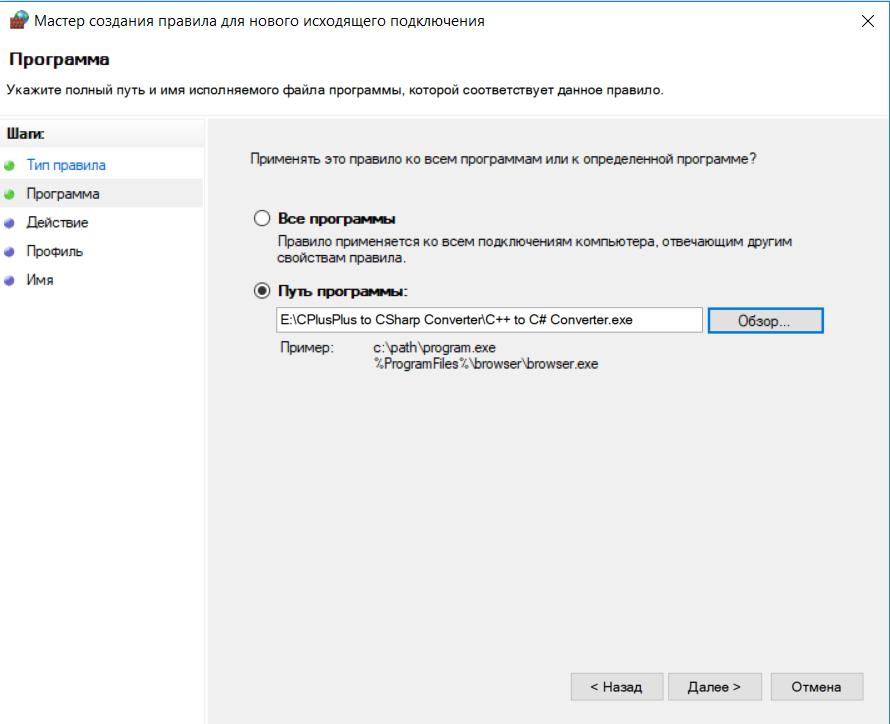
Указываем путь к программе(Рисунок 4.8)

Рисунок 4.8 – Путь к программе

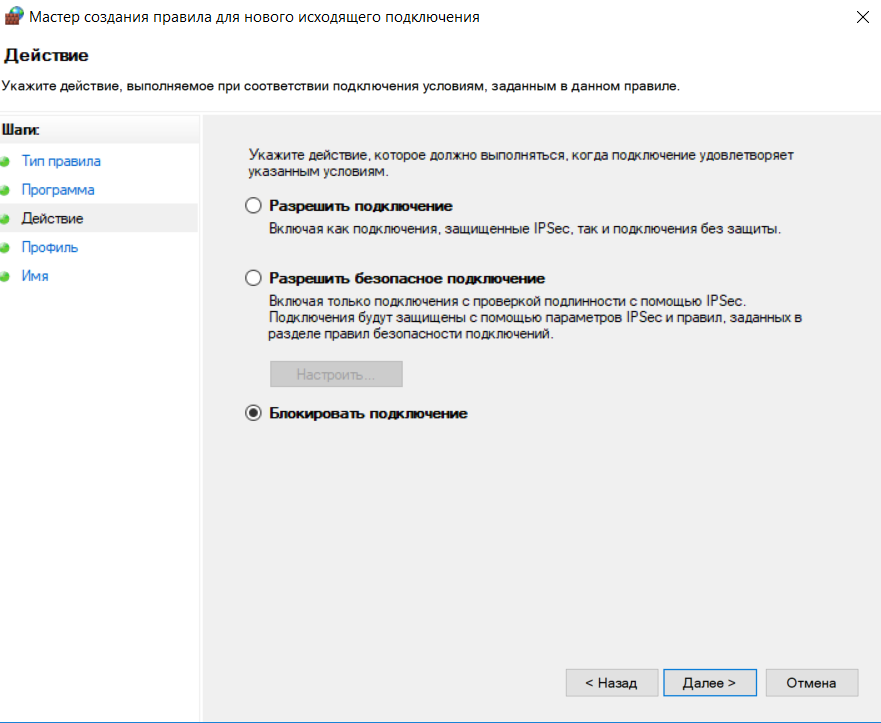
Далее выбираем блокировку подключения (Рисунок 4.9)

Рисунок 4.9 – Блокировка подключения

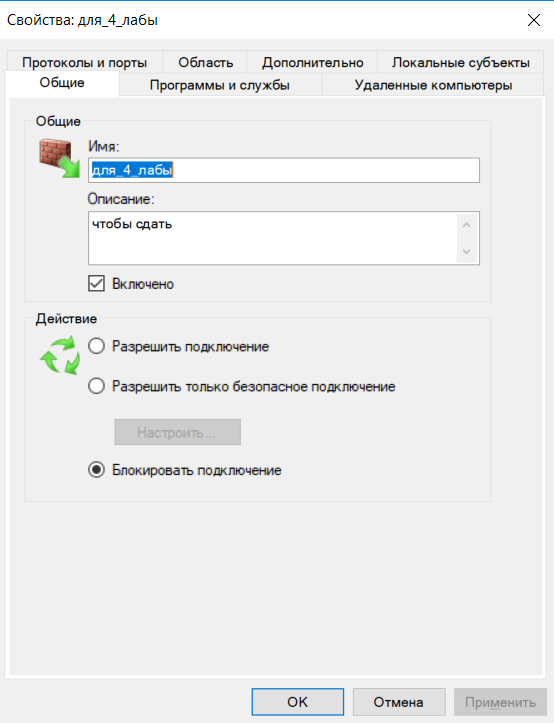
 Потом выбираем окно свойств (Рисунок 4.10)

Рисунок 4.10 – Свойство правила

Аналогичные действия производим над вторым приложением

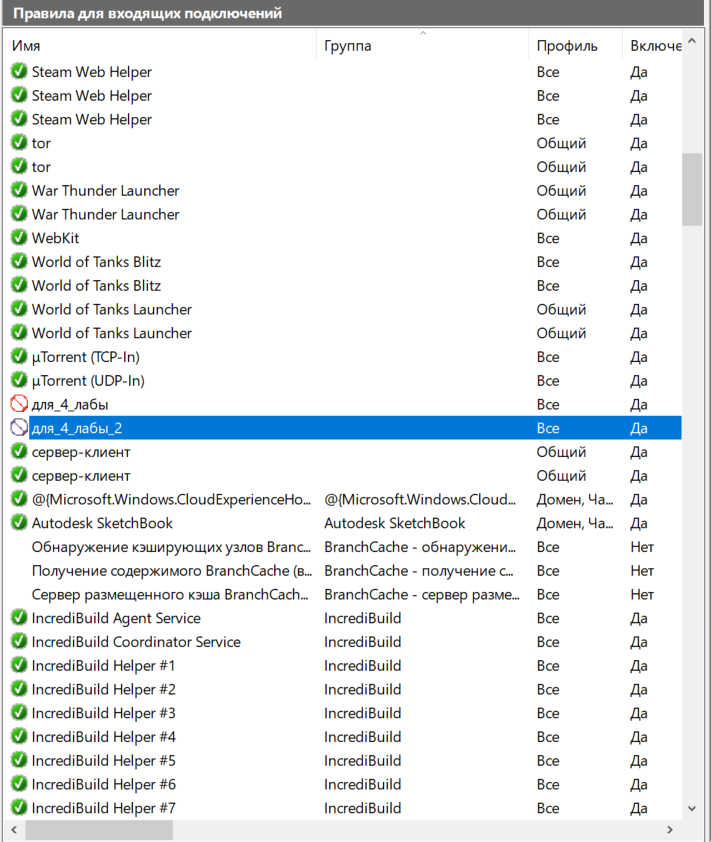
Демонстрация создания правил (Рисунок 4.11)

Рисунок 4.11 – Окно ввода имени

Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания

Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий)

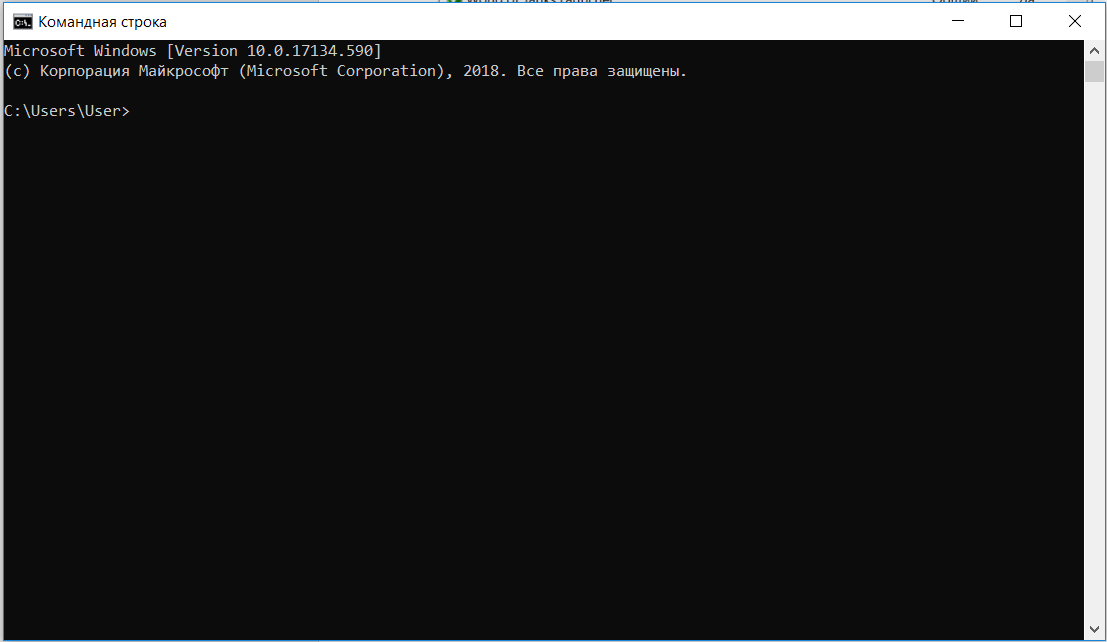
Для выполнения команд используем командную строку (Рисунок 4.12)

Рисунок 4.12 – Командная строка

Командная строка – специальная программа, позволяющая управлять операционной системой при помощи текстовых команд, вводимых в окне приложения. Её интерфейс полностью текстовый, в отличие от привычного вида операционной системы.

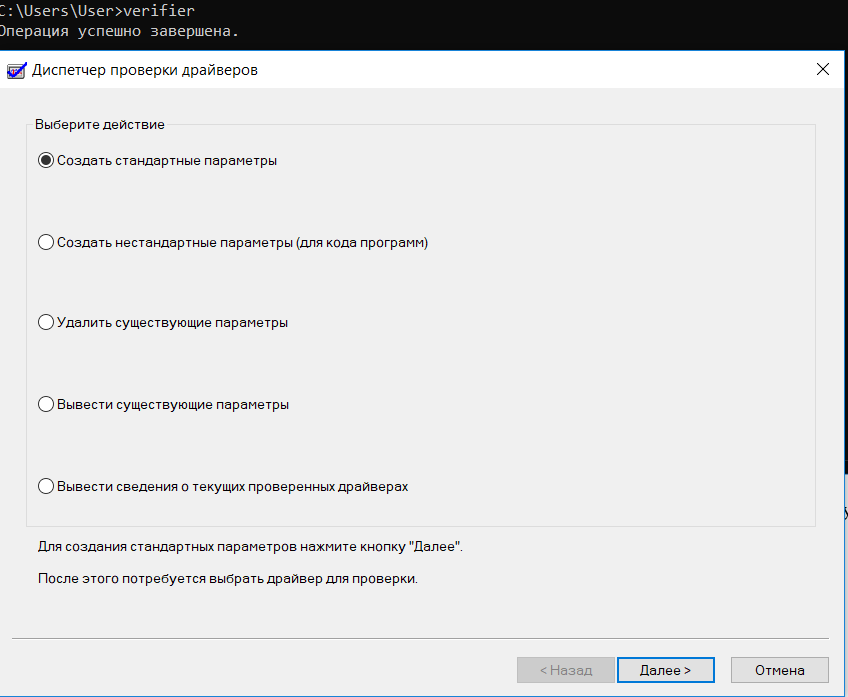
Диспетчер проверки драйверов-verifier (Рисунок 4.13)

Рисунок 4.13–Вызов диспетчера драйверов

Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий)

Калькулятор-calc (Рисунок 4.14)

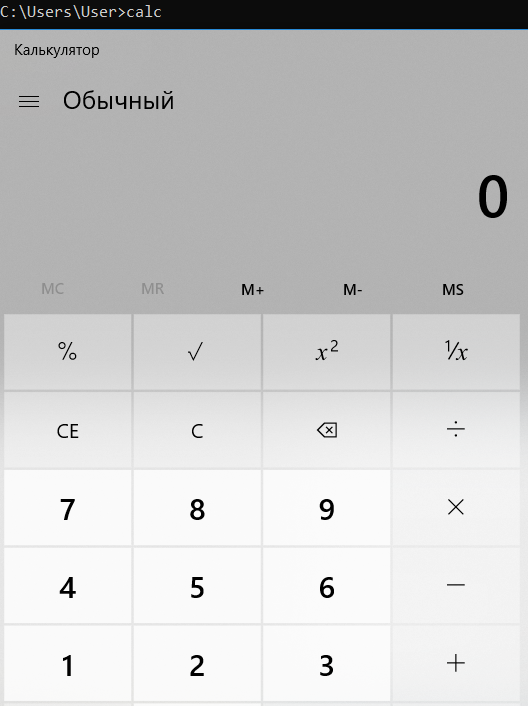


Рисунок 4.14 – Запуск калькулятора

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