Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Отчет

К практической работе №4:

Основы защиты информации

«Настройка Брандмауэра Windows»

Выполнила:

Студентка 2 курса 3 группы ФИТ

Воронько Елизавета Юрьевна

**Минск, 2021**

**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.

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.

**Задания для самостоятельной работы**

Для 1 программы на блокировку подключения для входящих подключений:

Первым этапом (рис 4.1) необходимо включить брандмауэр, в случае, если он был ранее выключен.

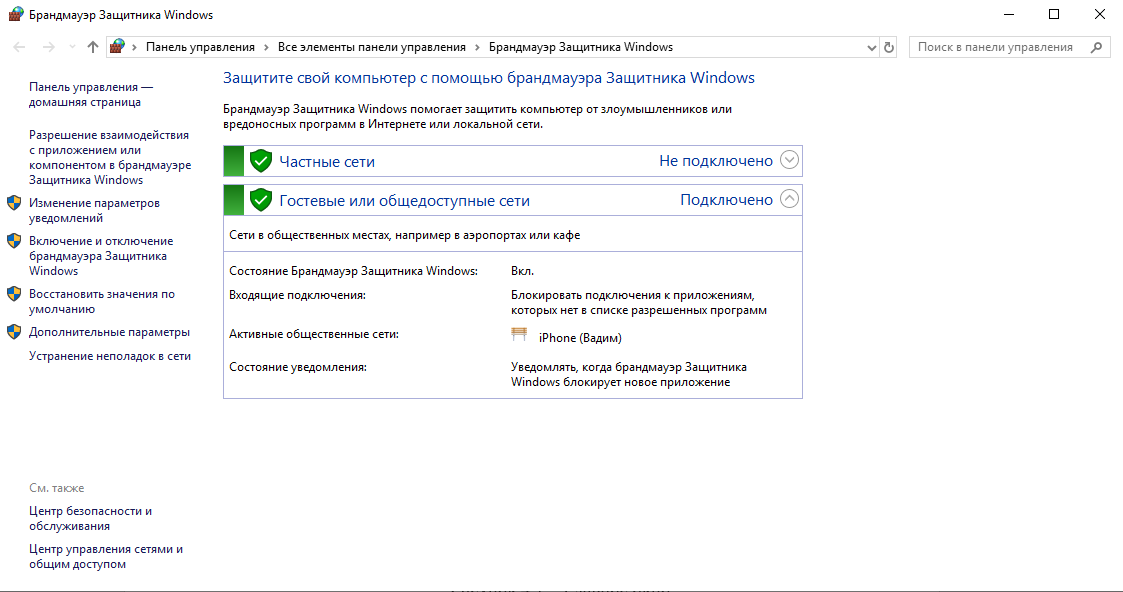


Рисунок 4.1 – Главное окно

В открывшемся окне (рис. 4.2) выбираем в левой панели правила для входящих подключений, затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели.

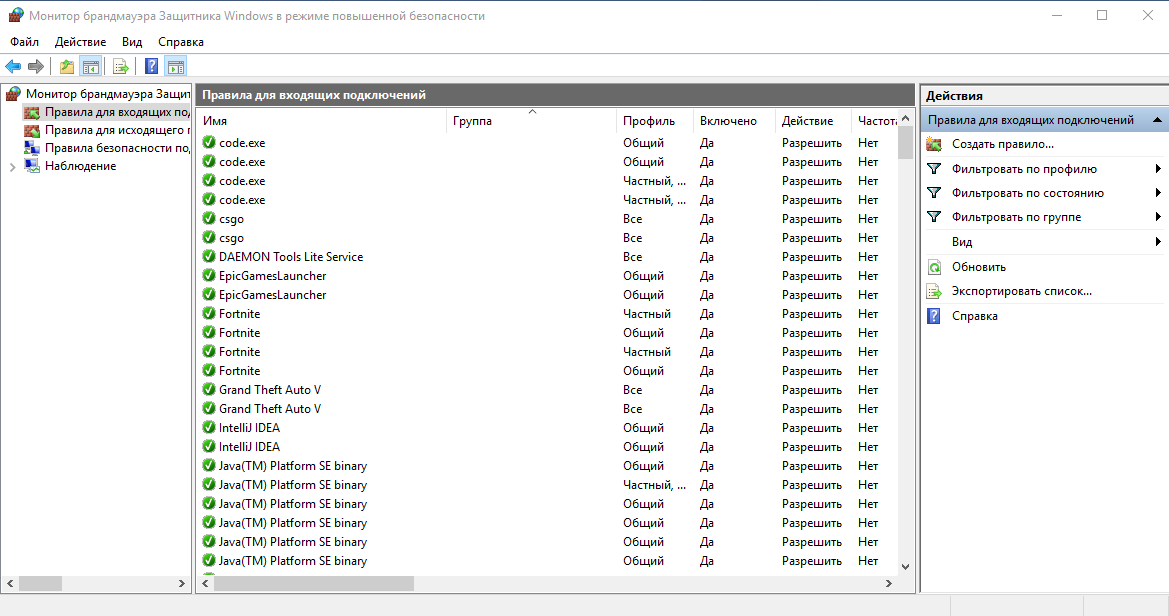


Рисунок 4.2 – Правила для входящих подключений

В открывшемся мастере создания (рис. 4.3) правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы).

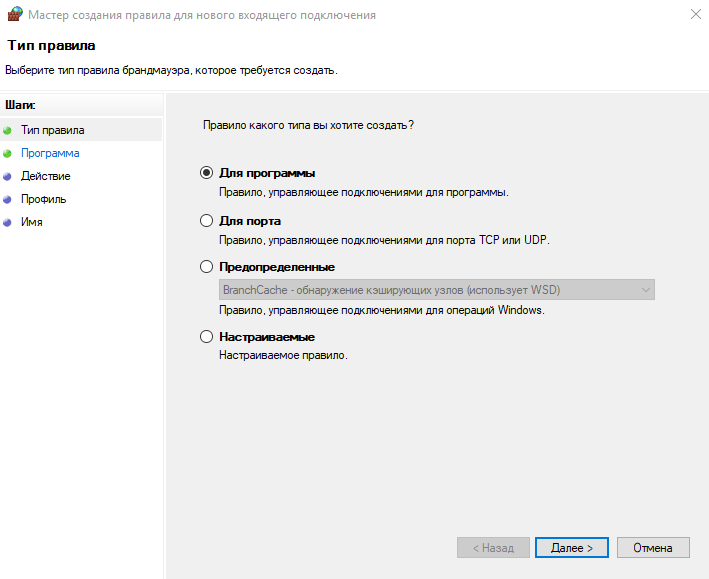


Рисунок 4.3 – Тип правила

При ограничении работы программы далее необходимо указать её путь, обязательно через папку, в которой она установлена, а не через ярлыки (рис. 4.4).

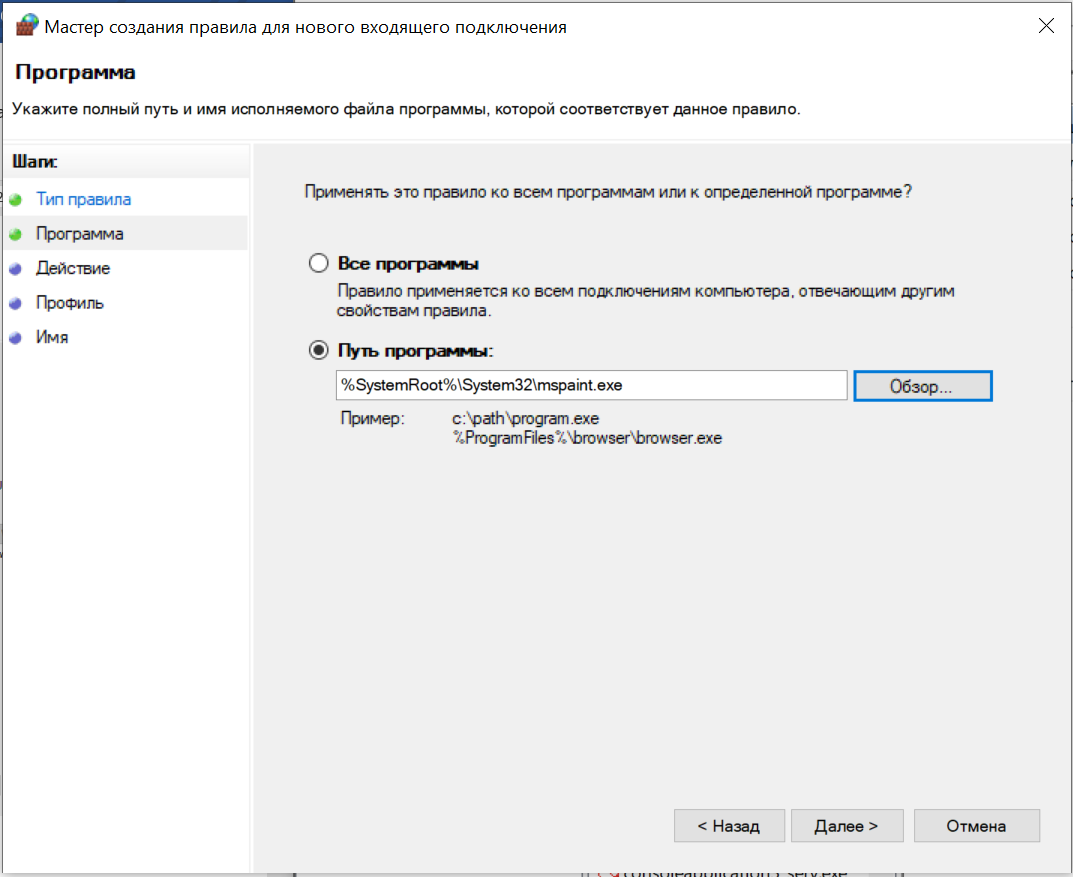


Рисунок 4.4 – Программы

Далее указывается какое именно действие вы хотите применить. В данном случае (рис. 4.5) необходимо блокировать подключение.

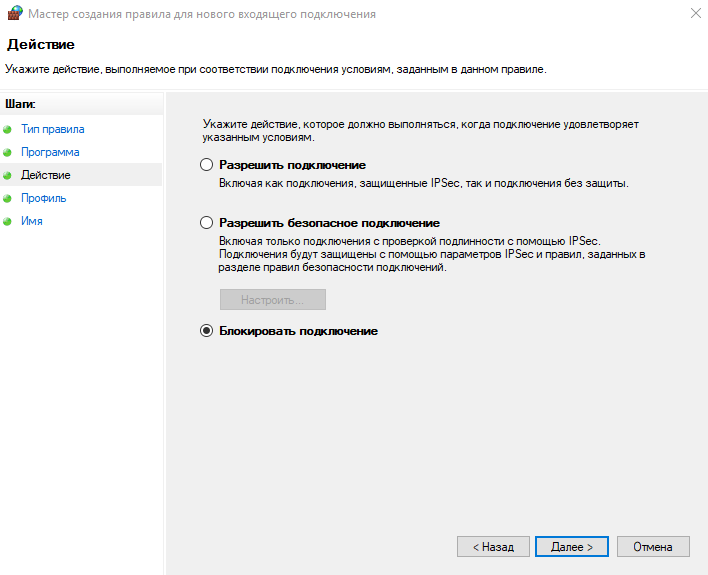


Рисунок 4.5 – Действие

Далее указывается профиль правила (рис. 4.6).

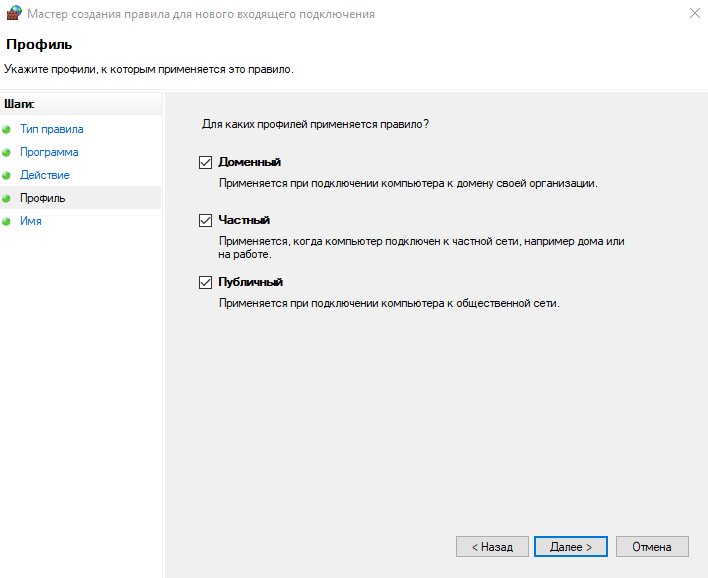


Рисунок 4.6 – Профиль

В следующем окне (рис. 4.7) указывается имя правила.

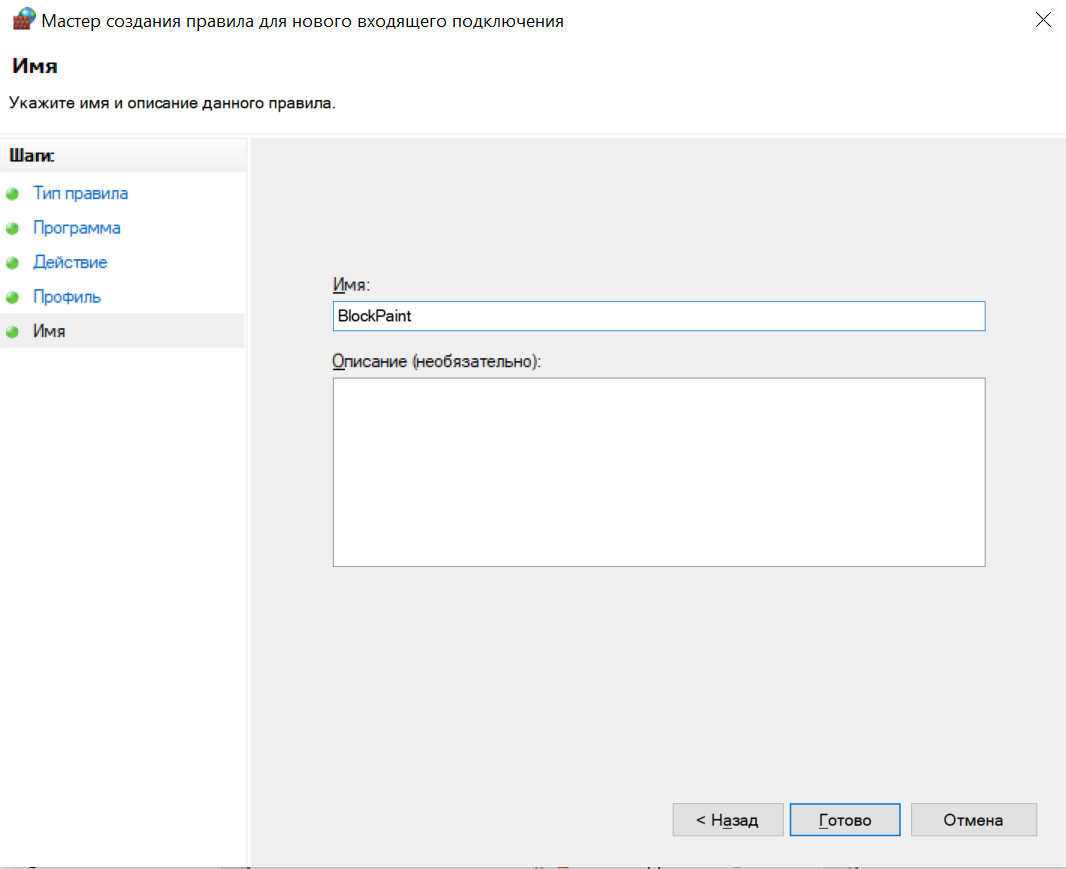


Рисунок 4.7 – Имя

В общем списке (рис. 4.8) появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели.

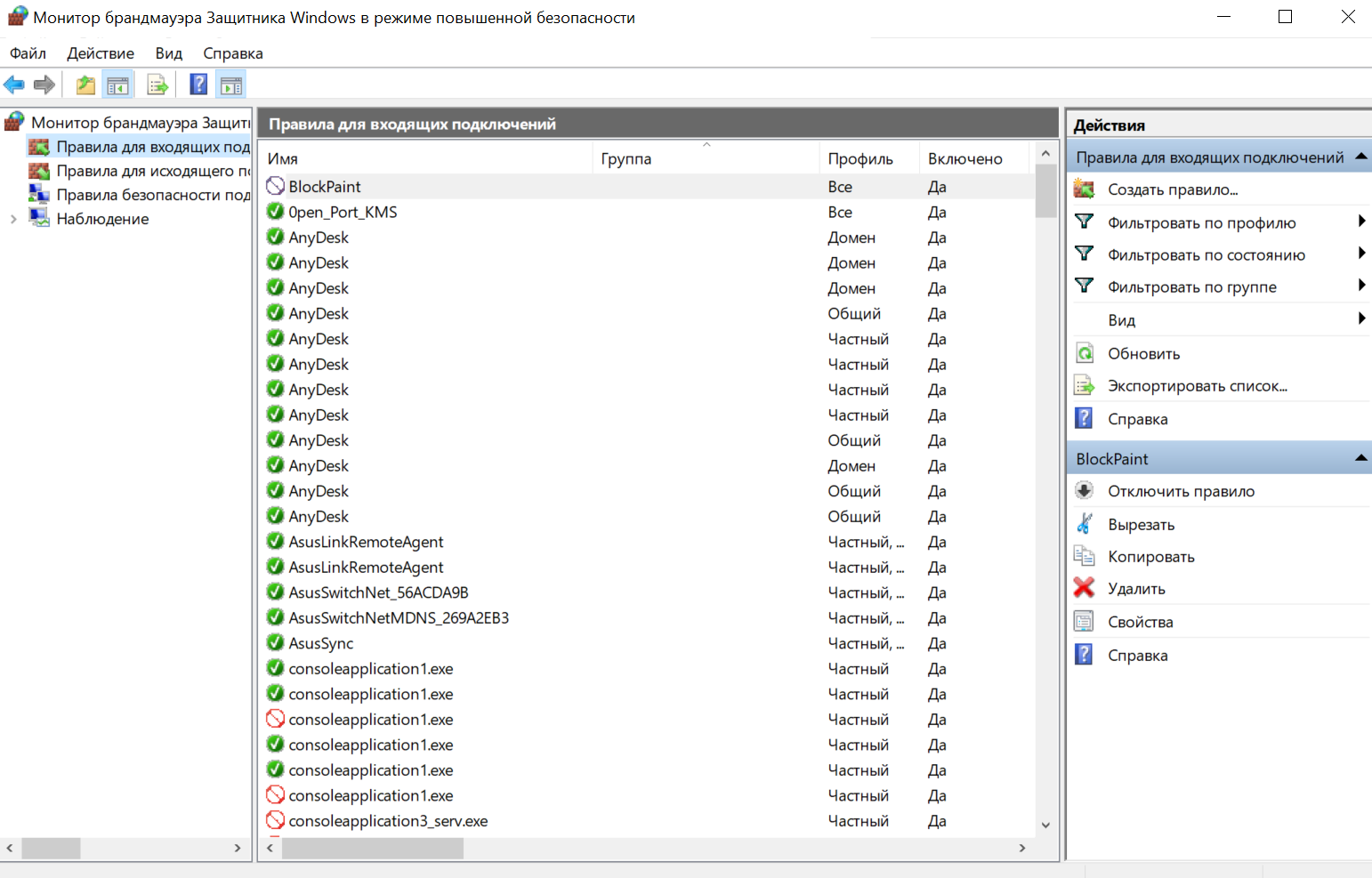


Рисунок 4.8 – Правила для входящих подключений

* Для 1 программы на разрешение подключения(рис. 4.9):

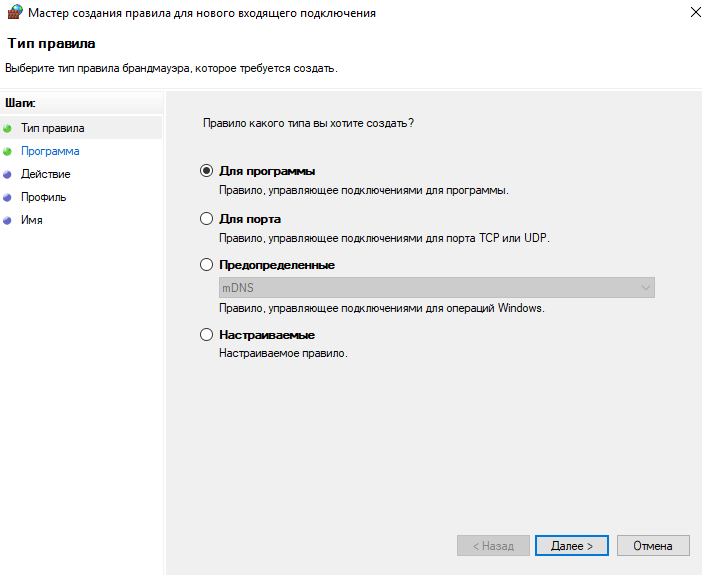


Рисунок 4.9 – Тип правила

При ограничении работы программы далее необходимо указать её путь, обязательно через папку в которой она установлена, а не через ярлыки! (рис. 4.10):

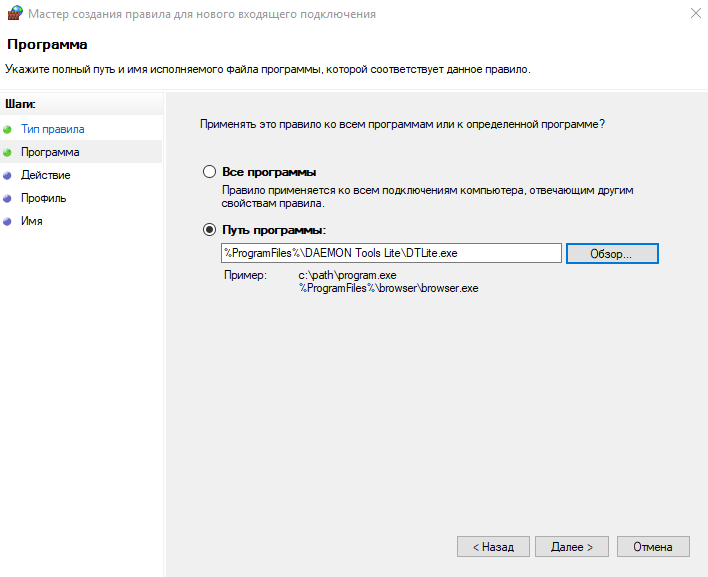


Рисунок 4.10 – Программа

Далее указывается какое именно действие вы хотите применить. В данном случае (рис. 4.11) необходимо разрешить подключение.

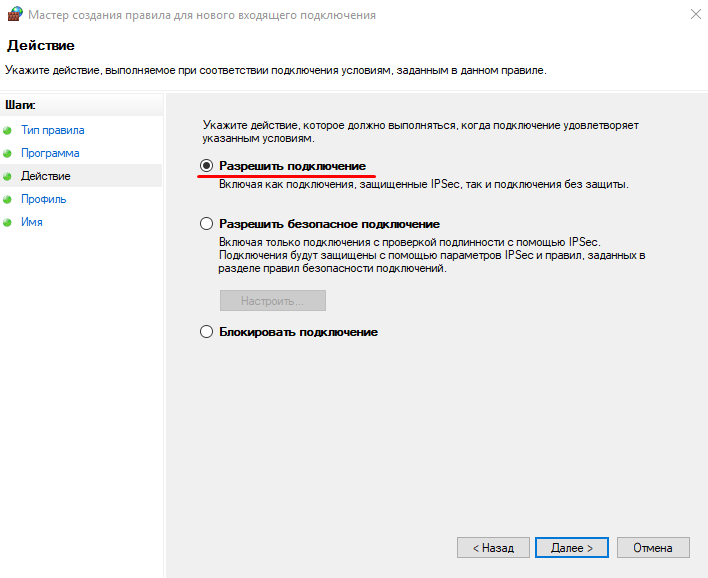
- 

Рисунок 4.11 – Действие

Открываем интерпретатор командной строки (рис. 4.13)

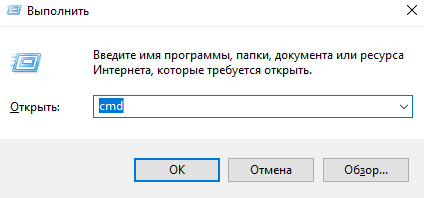


Рисунок 4.12 – Вызов командной строки

Команда DATE без параметров отображает текущую дату и запрашивает ввод новой даты. Для сохранения текущей даты нажмите клавишу ENTER.(рис 4.14)

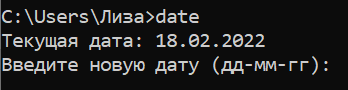


Рис 4.13 ­– Команда date

Команда PATH используется для указания или просмотра путей поиска исполняемых файлов. Пути поиска представляют собой строки, определяющие перечень каталогов файловой системы, в которых находятся исполняемые файлы (файлы с расширением .bat, .cmd, .exe, .vbs и т.п. ), разделенные точкой с запятой.(рис 4.15)

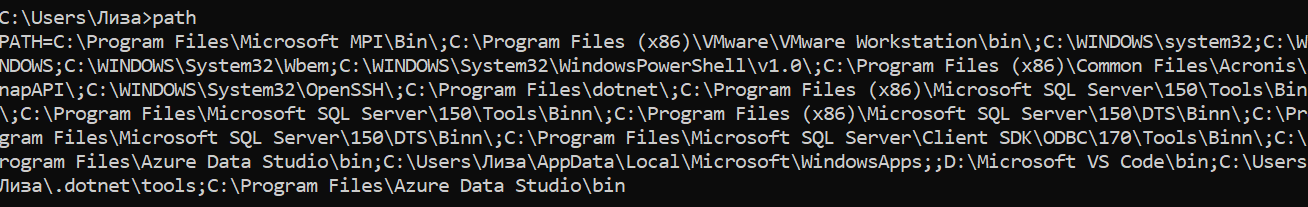


Рисунок 4.14 – Команда path

Команда WHOAMI используется для получения сведений об имени пользователя и группе, а также о соответствующих идентификаторах безопасности (SID), привилегиях, идентификаторах входа (ID) текущего пользователя (токене доступа) на локальном компьютере (рис 4.16).



Рисунок 4.15 – Команда whoami

При запуске whoami.exe без параметров, отображается имя пользователя в формате NTLM (домен\пользователь).

**Вывод**

Я овладела навыками настройки и использования Брандмауэра Windows. Создала правила для входящих и исходящих подключений на разрешение и блокировку подключения.