Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Практическое задание №4

«Настройка Брандмауэра Windows»

Подготовил: студент ФИТ 2 курса 5 группы Древотень Е.В.

Проверил: асс. Берников В.О.

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

Теоретическое введение

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

Большая часть проблем с информационной безопасностью сетей связана с особенностью открытой платформы и среды, что сказалось на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов имеет "бреши" в защите.

Задание на выполнение

1. Создать правила для входящих подключений.

Прежде всего необходимо открыть меню брандмауэра. Для этого откроем панель управления и выберем ссылку «Система и безопасность» (рис. 1.0.1).

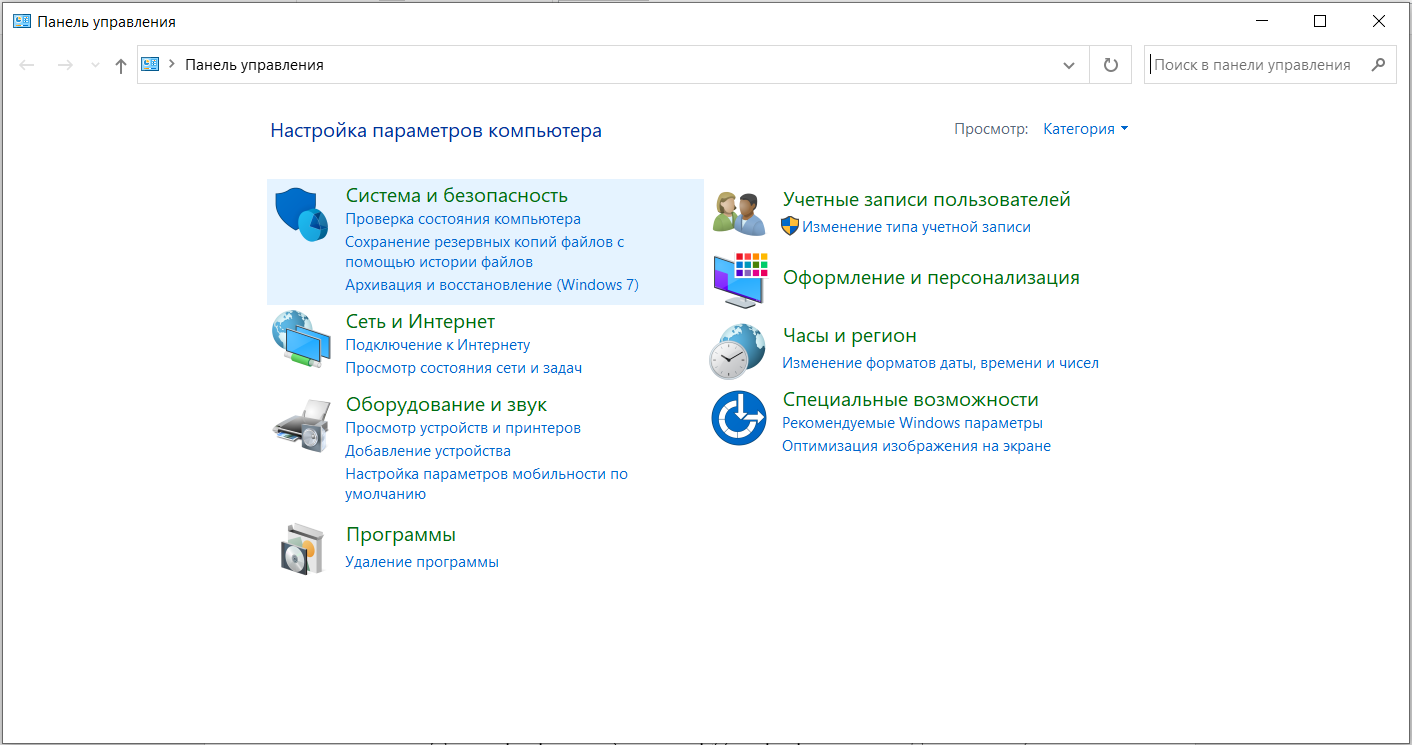


Рисунок 1.0.1. Панель управления

Далее выбираем «Брандмауэр Защитника Windows» (рис. 1.0.2).

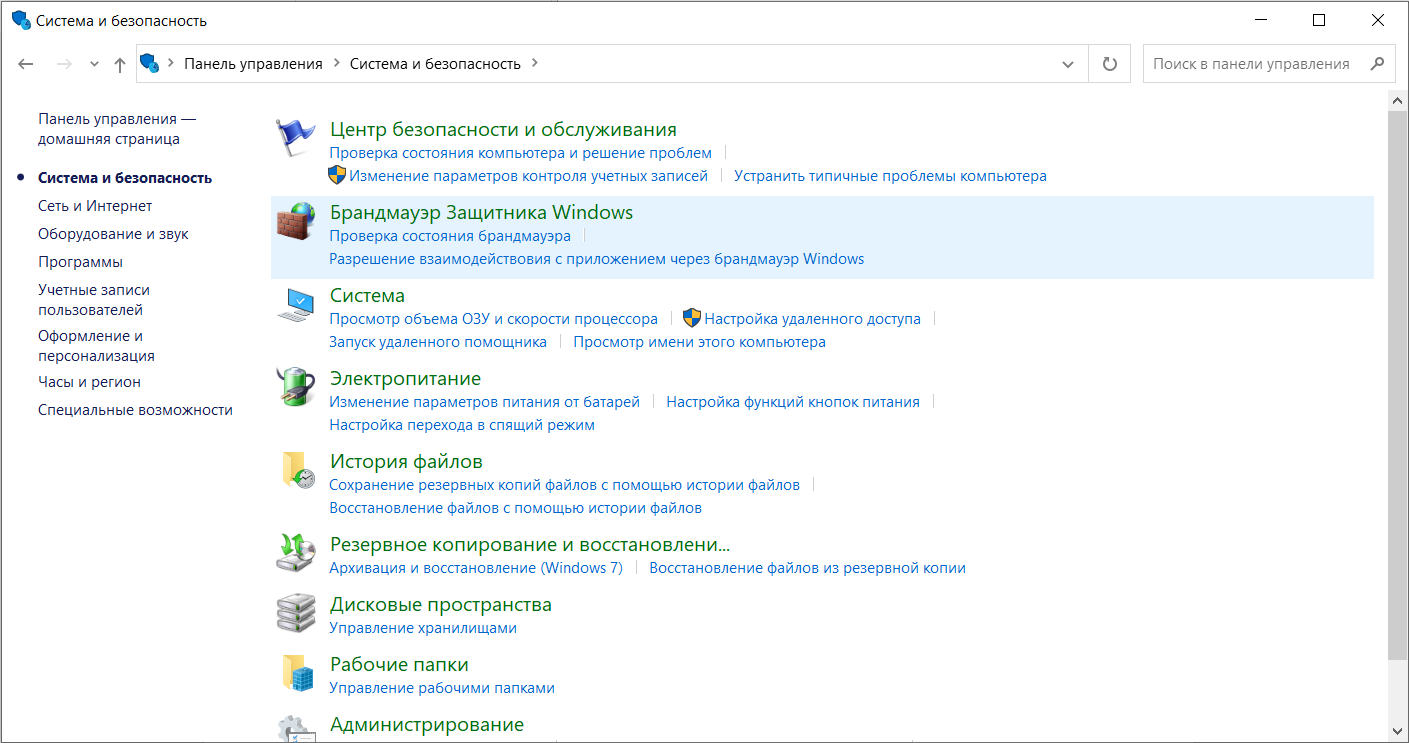


Рисунок 1.0.2. Система и безопасность

Проверяем, подключён ли брандмауэр для частных, гостевых или общедоступных сетей, после этого выбираем ссылку «Дополнительные параметры» (рис. 1.0.3).

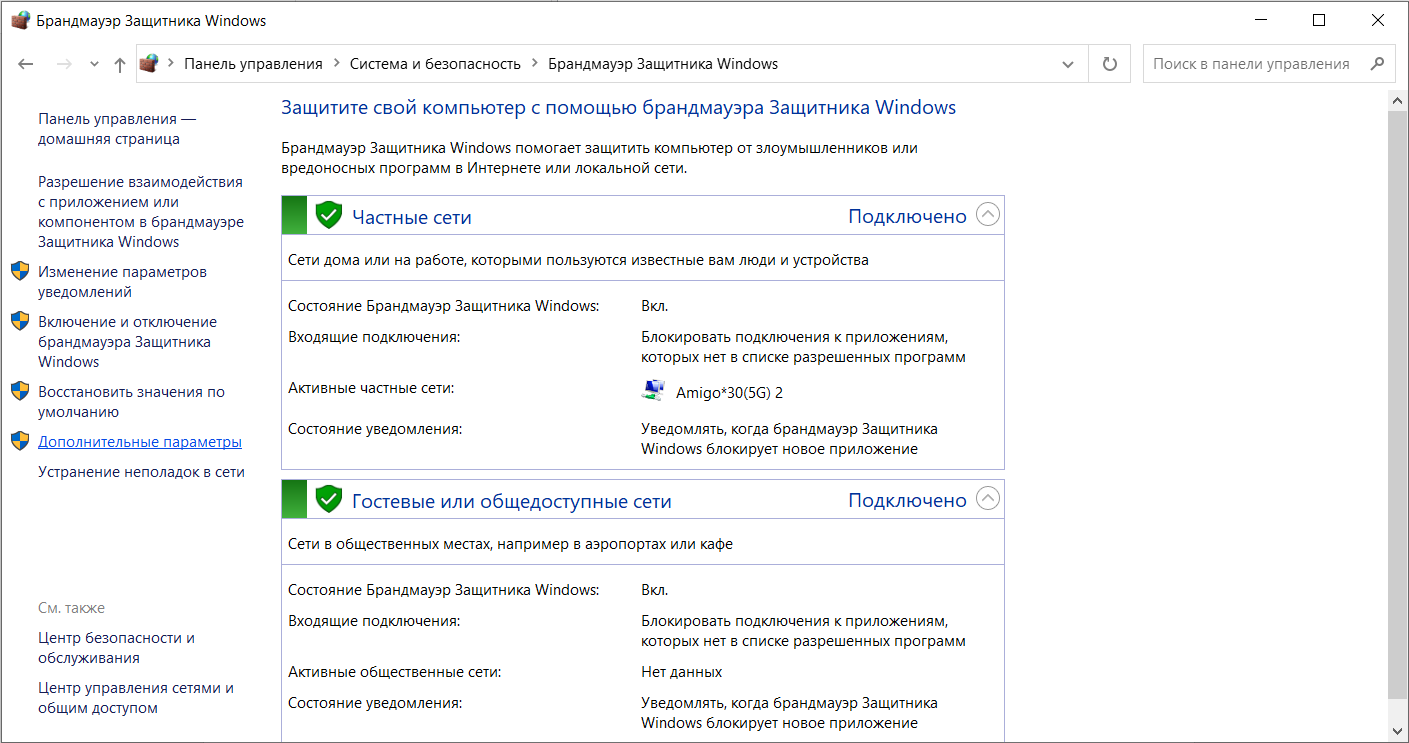


Рисунок 1.0.3. Брандмауэр Защитника Windows

* 1. Для 1 программы (по выбору) на блокировку подключения.

В дополнительных параметрах выбираем вкладку «Правила для входящих подключений» (рис. 1.1.1).

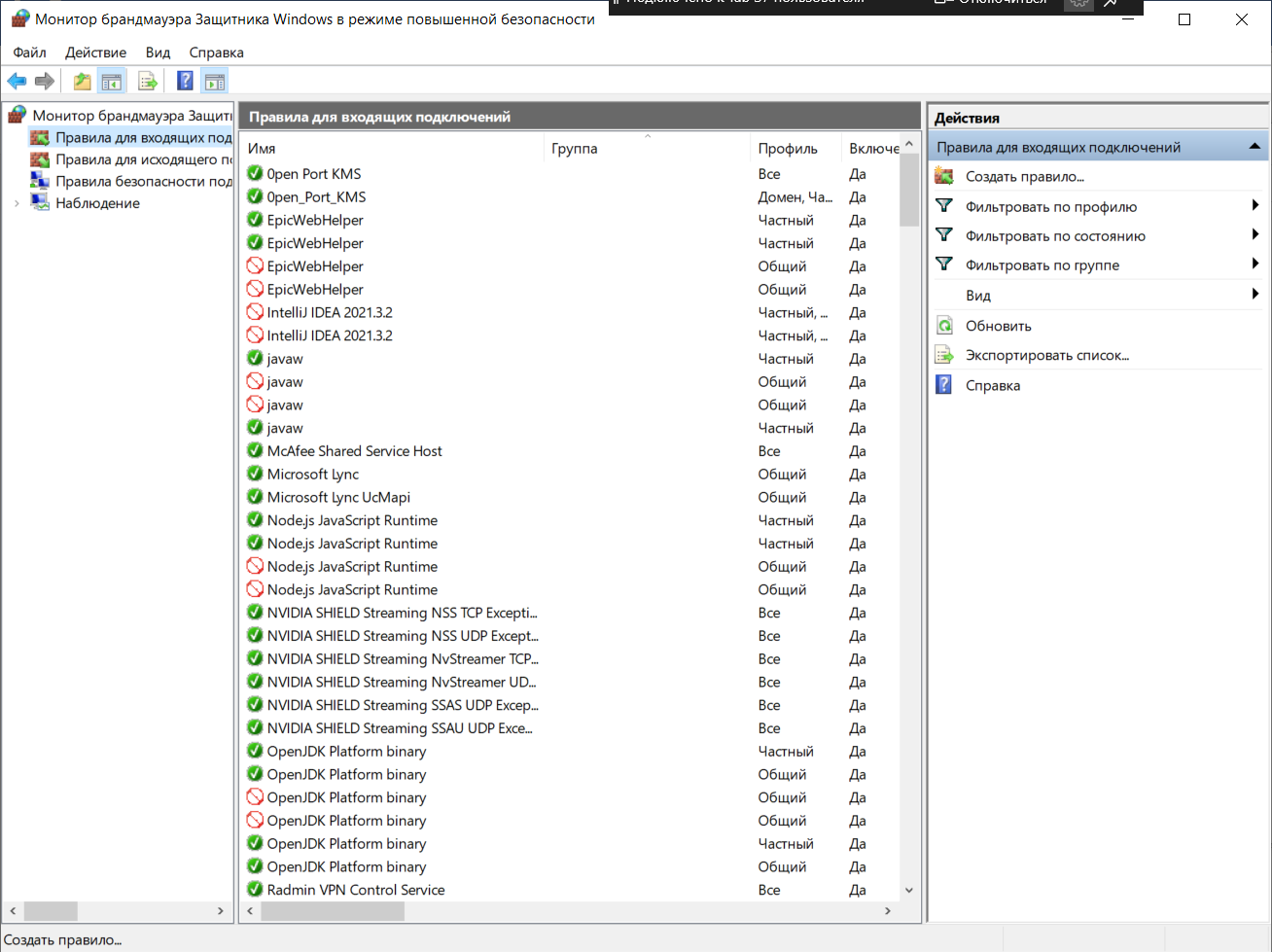


Рисунок 1.1.1. Правила для входящих подключений

Создадим правило для программы dotnet.exe (рис. 1.1.2, 1.1.3, 1.1.4 и 1.1.5).

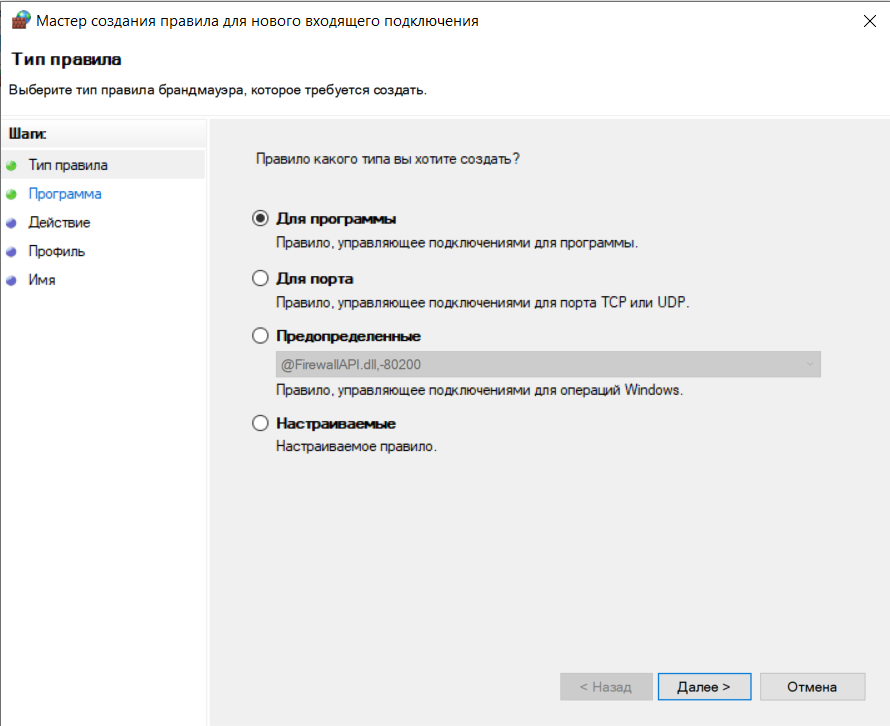


Рисунок 1.1.2. Создание правила для вход. подключ. на блокировку 1

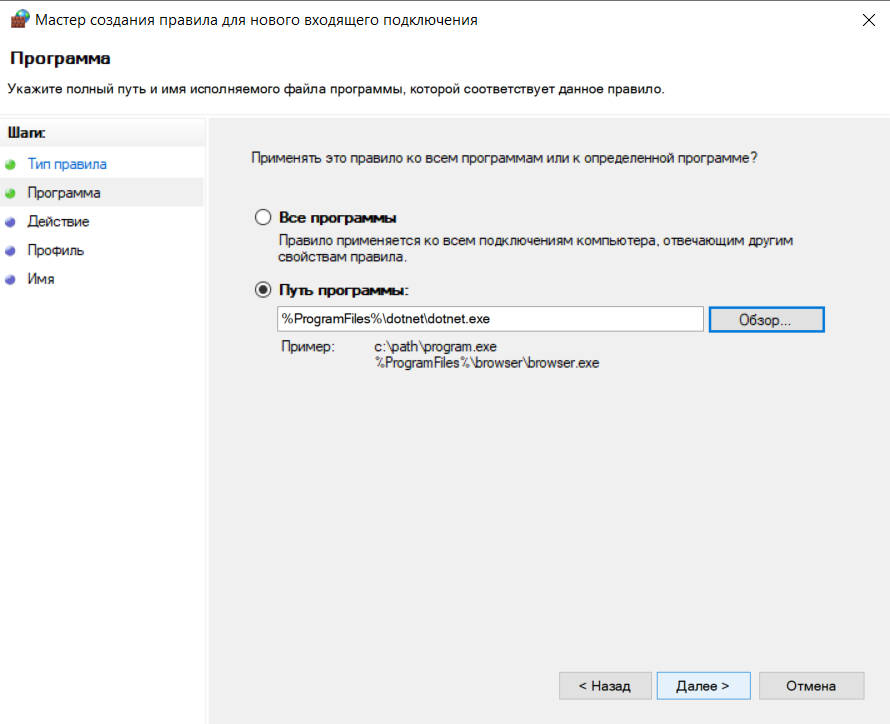


Рисунок 1.1.3. Создание правила для вход. подключ. на блокировку 2

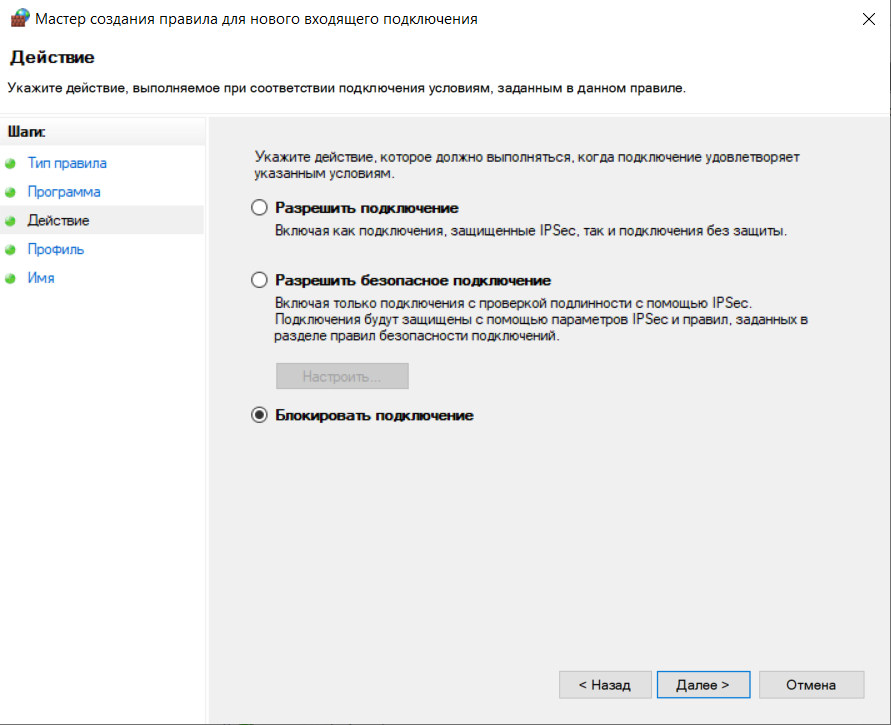


Рисунок 1.1.4. Создание правила для вход. подключ. на блокировку 3

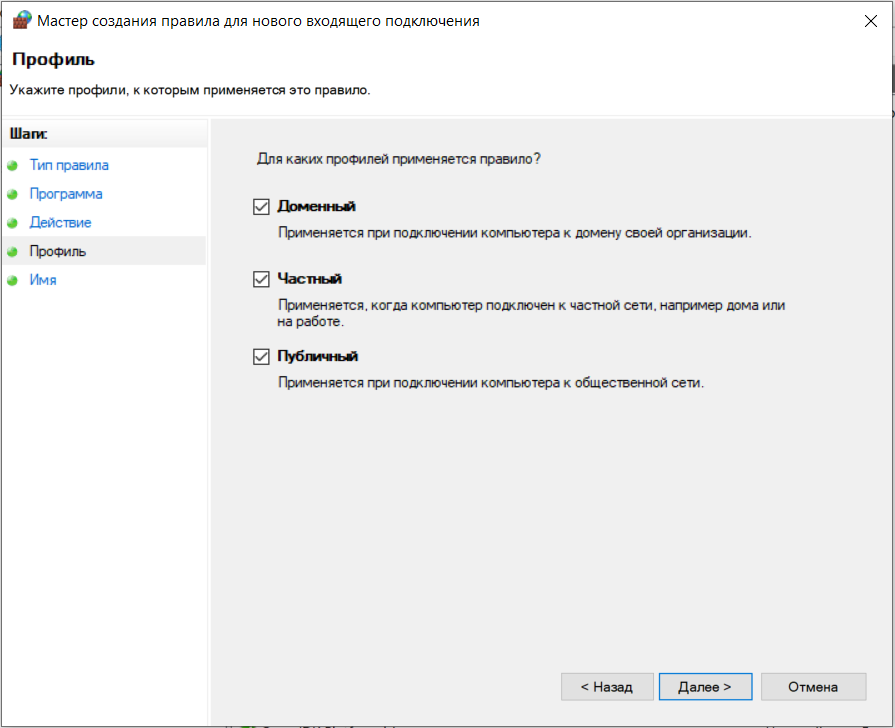


Рисунок 1.1.5. Создание правила для вход. подключ. на блокировку 4

После этого вводим название нового правила. В итоге получено правило для блокировки подключения программы dotnet.exe с названием dotnet\_BLOCK (рис. 1.1.6).

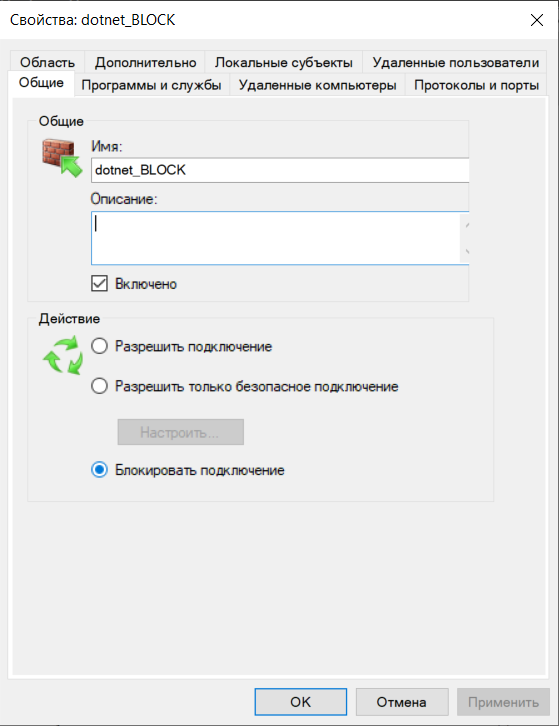


Рисунок 1.1.6. Свойства правила dotnet\_BLOCK

* 1. Для 1 программы (по выбору) на разрешение подключения.

Аналогично правилу на блокировку подключения реализуем разрешение на подключения. На рисунке 1.2.1 указано различие настройки, на рисунке 1.2.2 – результат.

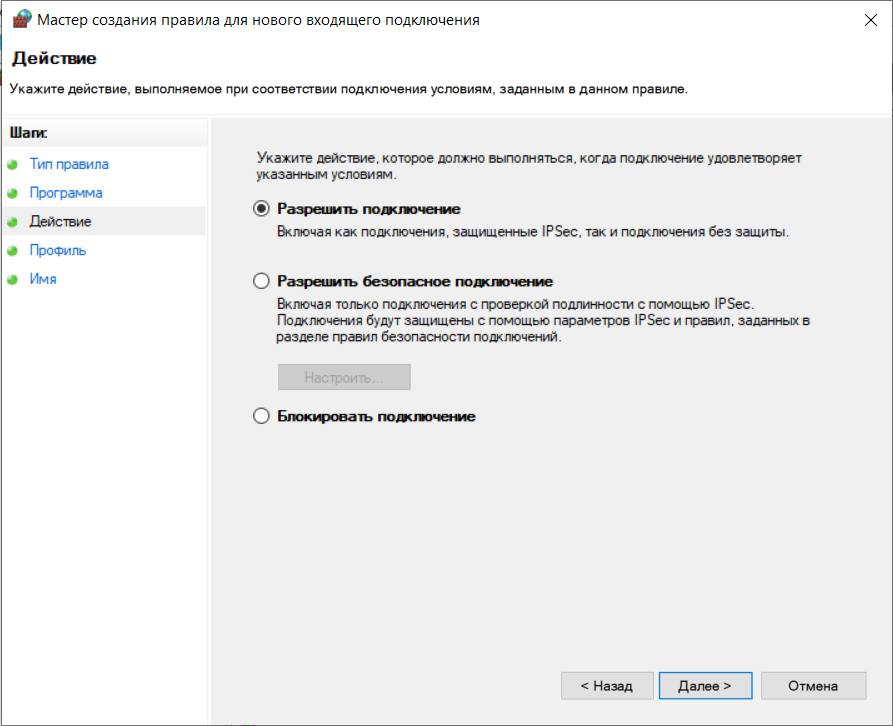


Рисунок 1.2.1. Разрешение подключения

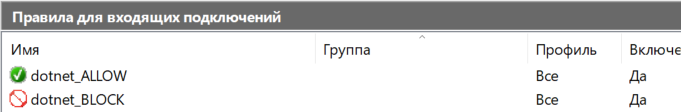


Рисунок 1.2.2. Результат создания правил в задании 1

1. Создать правила для исходящих подключений.

Для создания правил для исходящих подключений нужно перейти во вкладку «Правила для исходящего подключения».

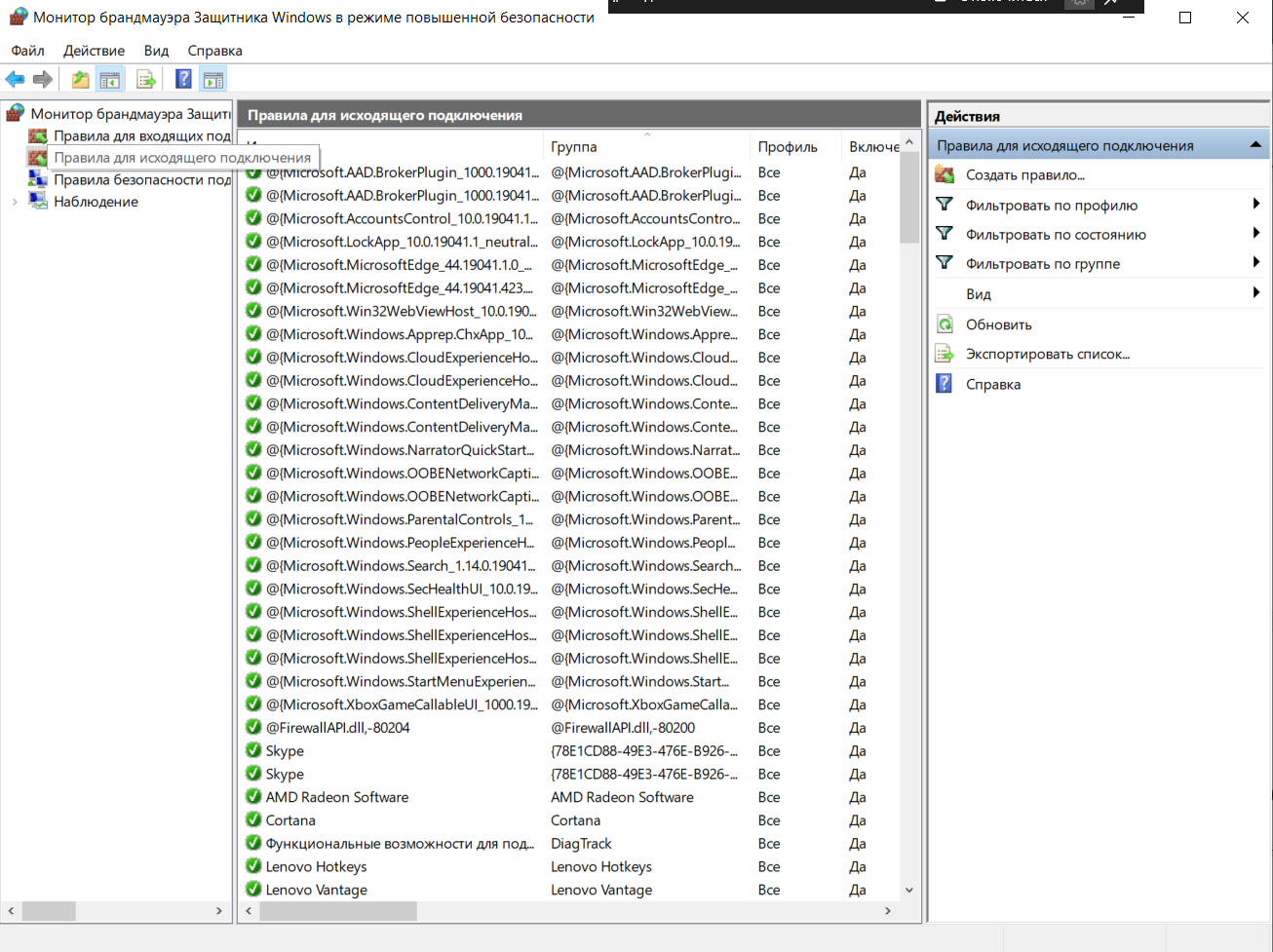


Рисунок 2.0.1. Правила для исходящих подключений

* 1. Для 1 программы (по выбору) на блокировку подключения.

Создание правил для исходящих правил полностью аналогично созданию правил для входящих сообщений. Результат для программы fraps.exe представлен на рисунке 2.1.1.

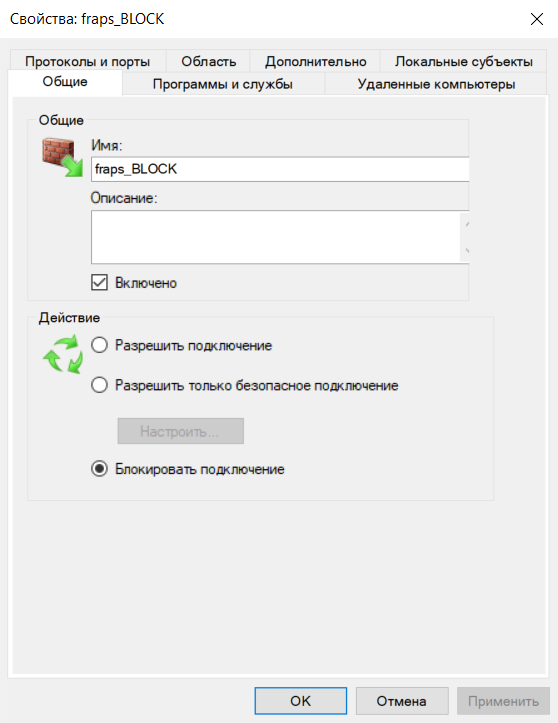


Рисунок 2.1.1. Правило fraps\_BLOCK

* 1. Для 1 программы (по выбору) на разрешение подключения.

Результат разрешения подключения для приложения fraps.exe – правило fraps\_ALLOW (рис. 2.2.1).

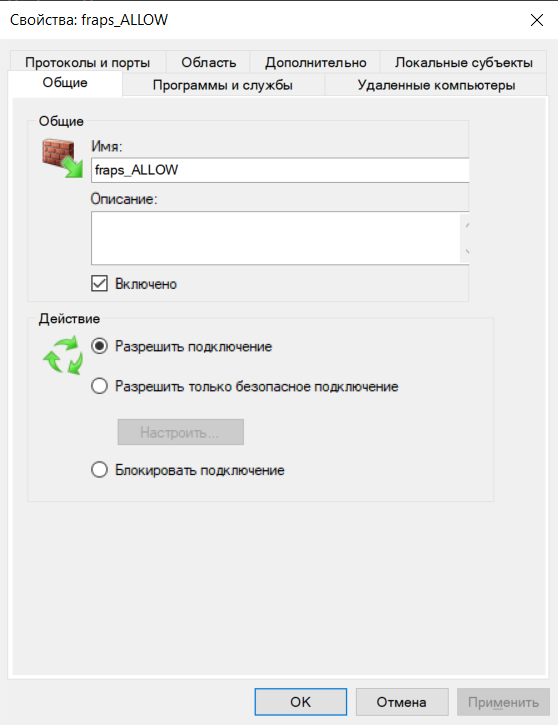


Рисунок 2.2.1. Правило fraps\_ALLOW

1. Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.

При удалении правил появляется предупреждение с уточнением, действительно ли мы хотим удалить правила (рис. 3.1).

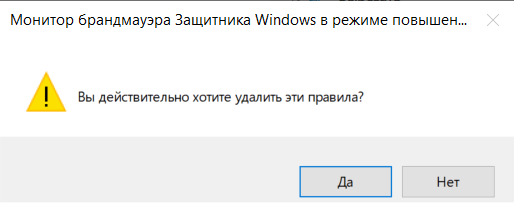


Рисунок 3.1. Окно предупреждения

На рисунках 3.2 и 3.3 демонстрируется отсутствие созданных ранее правил.

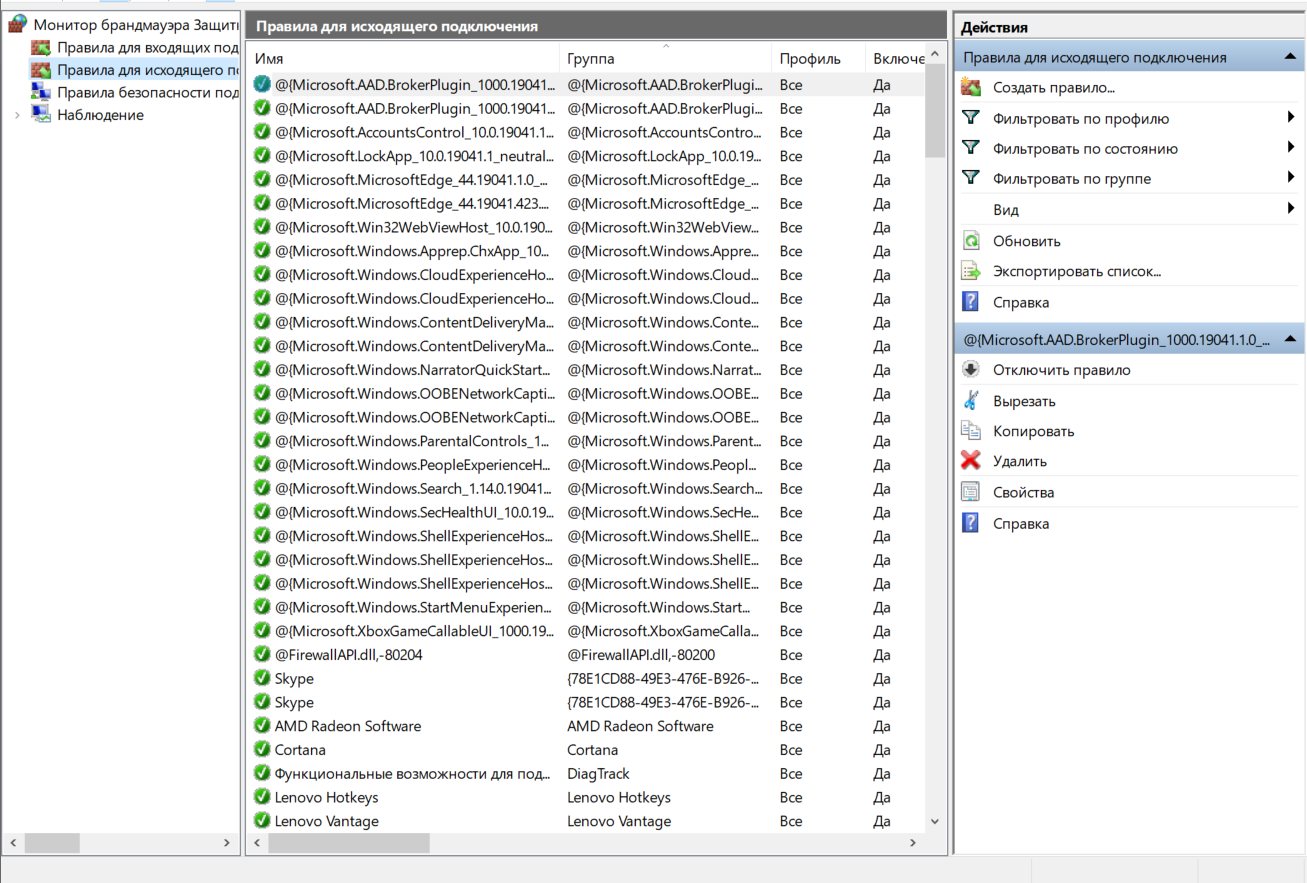


Рисунок 3.2. Правила для исходящего подключения

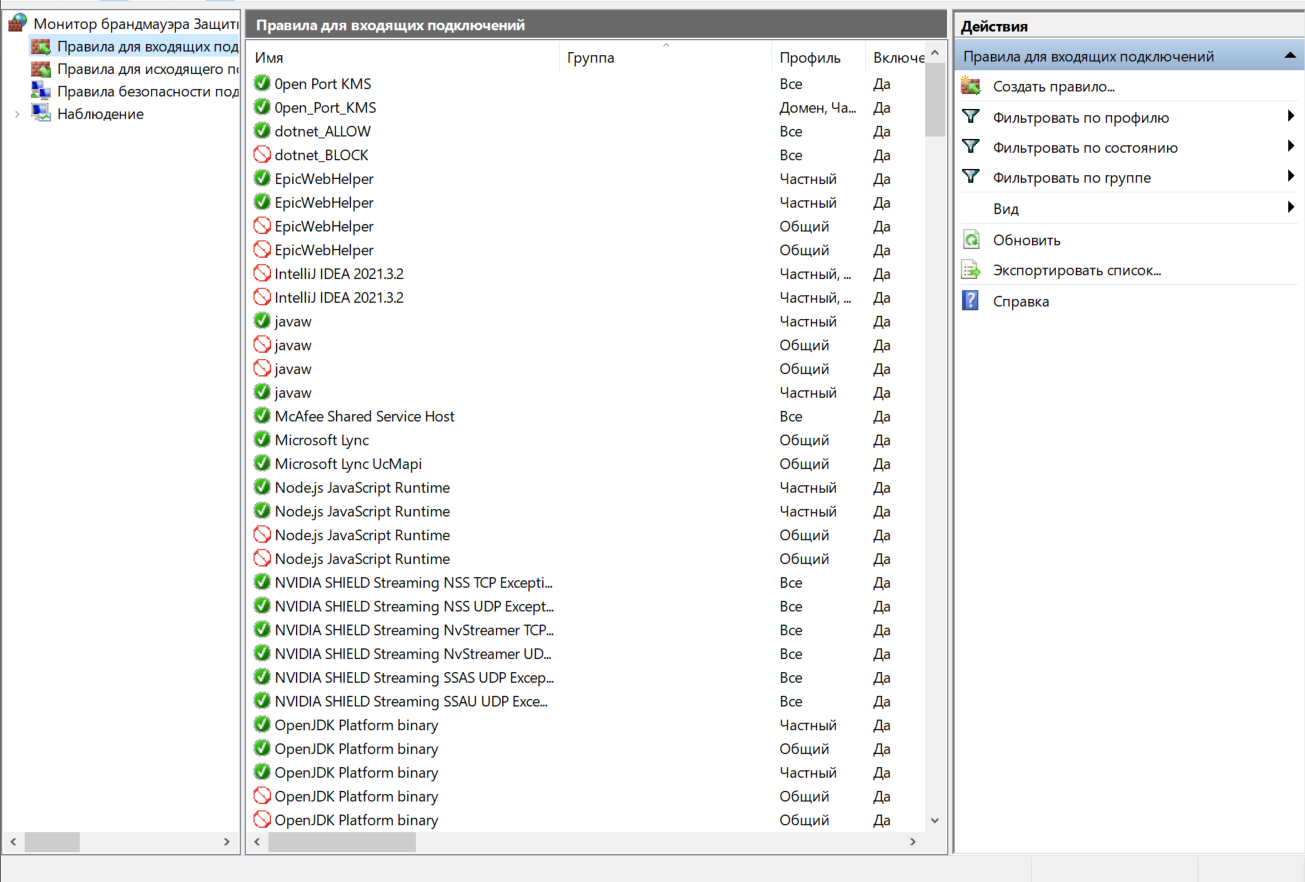


Рисунок 3.3 Правила для входящего подключения

1. Опробовать действие нескольких команд.

Для включения службы диагностики DirectX используется команда dxdiag (рис 4.1).

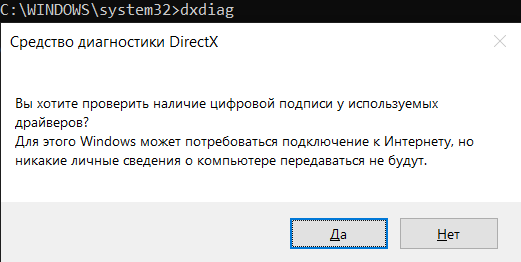


Рисунок 4.1. dxdiag

Для удаления вредоносных программ с ПК есть команда mrt.exe (рис. 4.2).

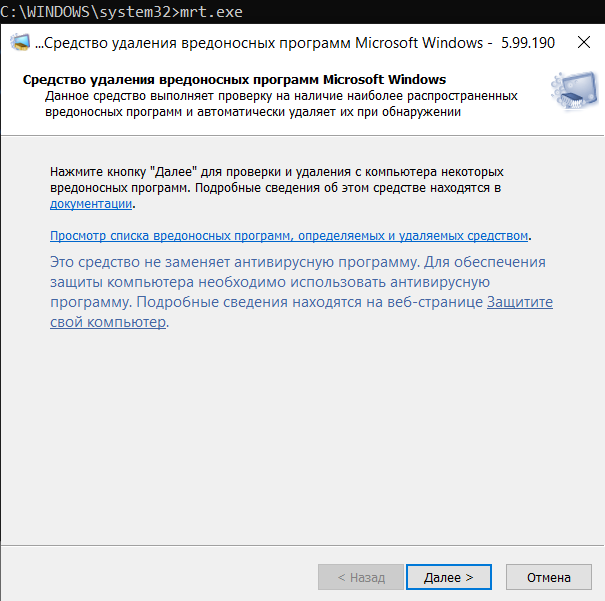


Рисунок 4.2. mrt.exe

Для проверки подписи файлов используется команда sigverif (рис. 4.3).

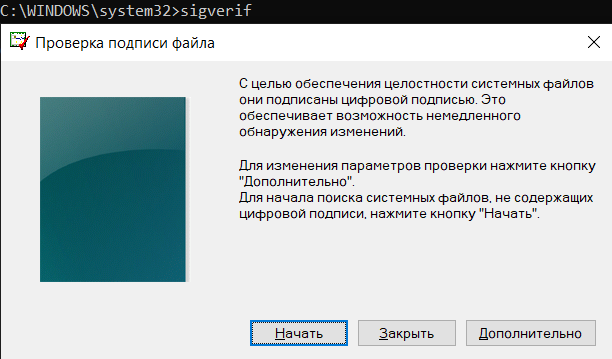


Рисунок 4.3. sigverif

Для открытия окна параметров используется команда utilman (рис 4.4).

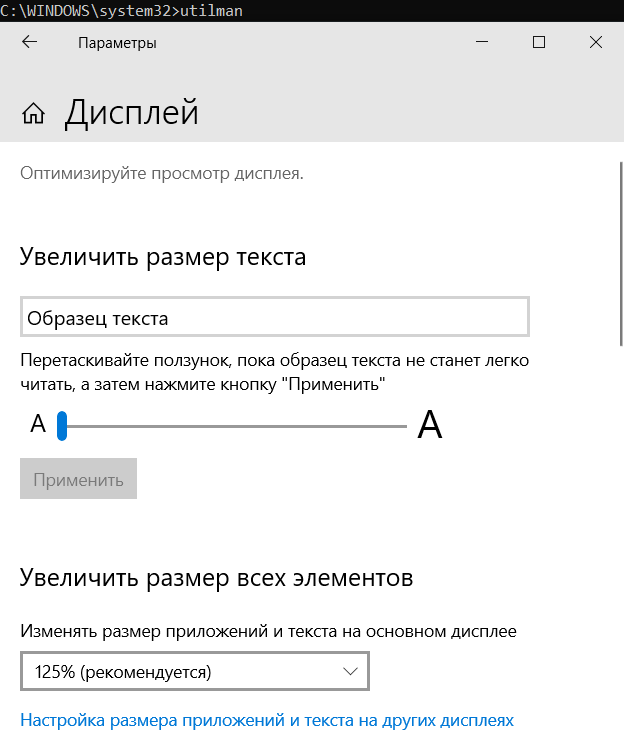


Рисунок 4.4. utilman

Вывод: в процессе выполнения задания овладели навыками настройки и использования с брандмауэром Windows, его функциями и попробовали в действии команды администратора.