Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Выполнил:

студент 2 курса, 7 группы

Бобрович Глеб Сергеевич

Проверил:

Барковский Евгений Валерьевич

Минск 2022

**Практическое занятие №4**

**Тема «**Настройка Брандмауэра Windows**»**

**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.

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 (SMTP);
* протокол передачи файлов (File Transfer Protocol);
* графическая оконная система X Windows.

**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;

Для начала необходимо перейти в панель по следующему адресу Панель управления –> Система и безопасность –> Брандмауэр Windows.

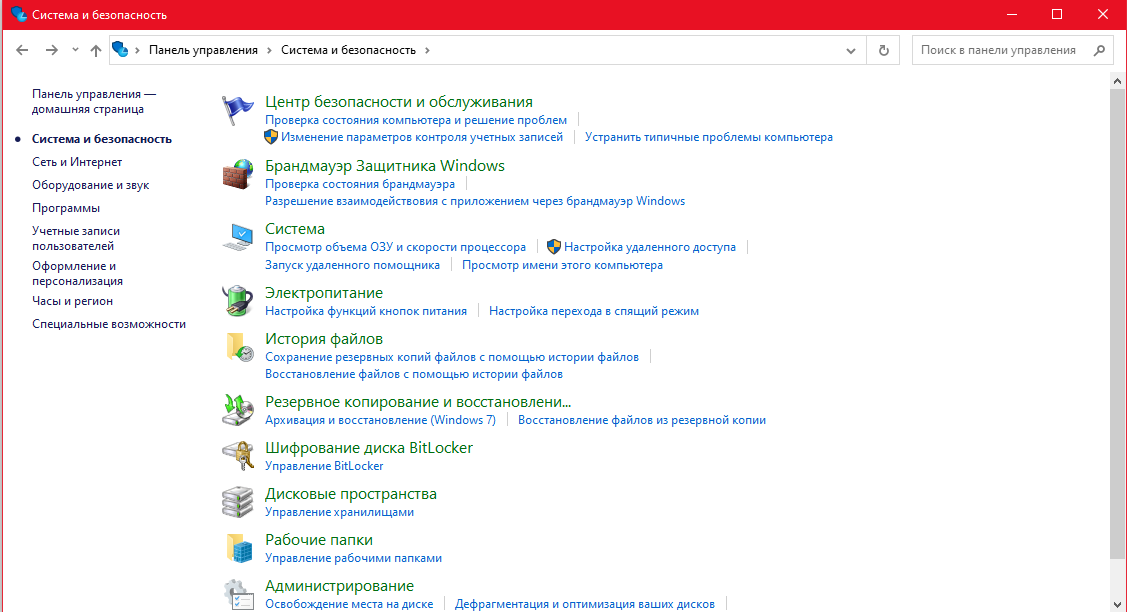


Рисунок 1.1 - Система и безопасность

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

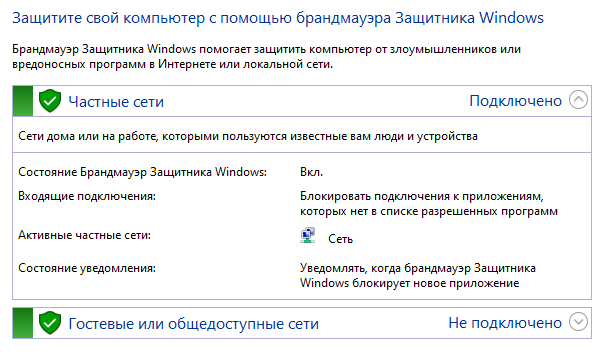


Рисунок 1.2 – Включение брандмауэра Windows

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

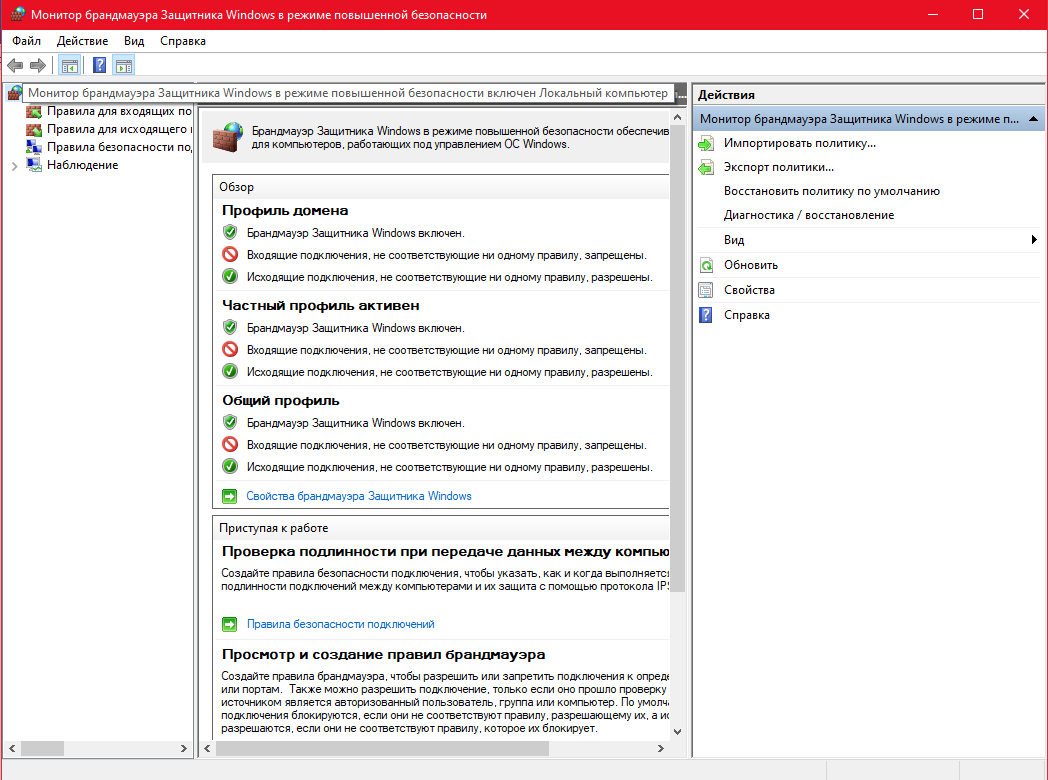


Рисунок 1.3 - Дополнительные параметры

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.

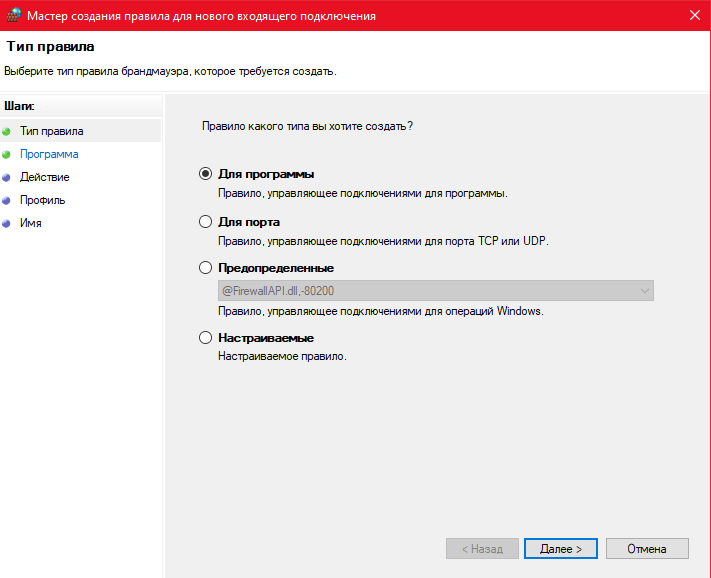


Рисунок 1.4 - Создание правила

В открывшемся мастере создания 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)

Указываем путь. Мы должны указать полный путь к нашему исполняемому файлу либо выбрав пункт все программы, наше правило примениться ко всем программам.

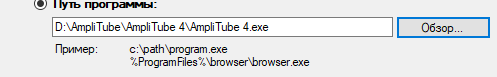


Рисунок 1.5 – Путь к файлу

Блокируем подключение. На данном этапе настройки нам необходимо указать действие над нашим правилом. Мы можем как разрешить подключение, так и блокировать.

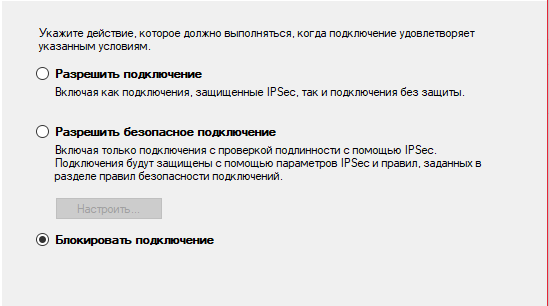


Рисунок 1.6 – Действие над правилом

Указываем имя. Тут ничего сложного нет, нам просто нужно дать имя нашему правило, а также дать ему краткое описание.

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

Все происходит аналогично прошлому алгоритму за исключением действия над правилом, где нам необходимо выбрать пункт “Разрешить подключение”.

Результат выполнения первого и второго пункта.



Рисунок 1.7 – Входящие подключения

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;

Здесь необходимо выбрать пункт “Правила для исходящих подключений” и выполнить все по тому же алгоритму, что и первое задание.

Результат (рис.8). Как мы видим в исходящих правилах подключения добавились 2 правила, одно разрешающее, а второе блокирующее.



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

Для выполнения команд используем командную строку.

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.

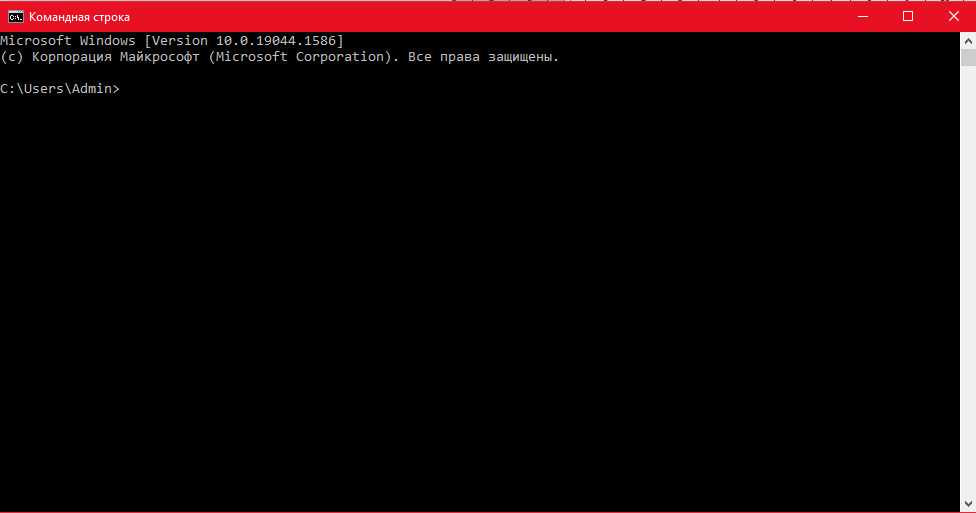


Рисунок 4.1 – Командная строка

Диспетчер проверки драйверов-verifier

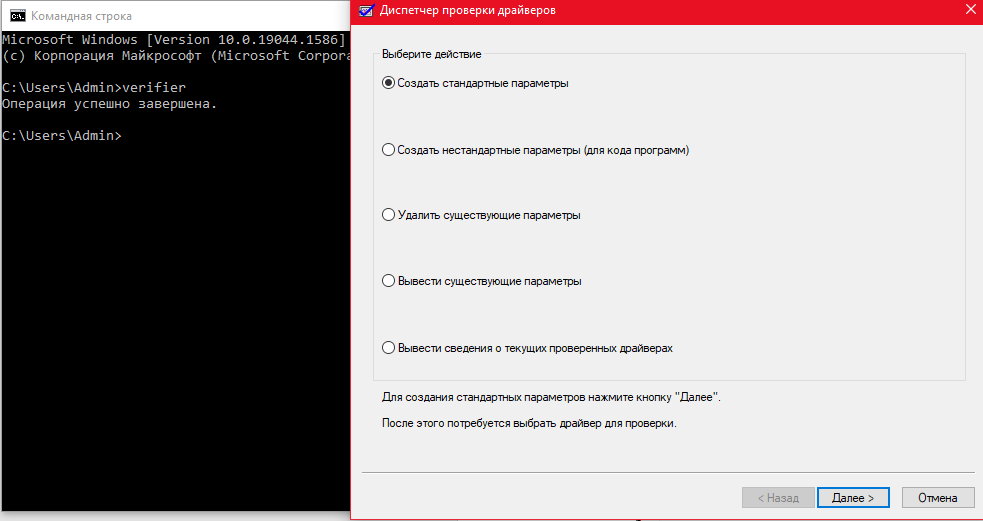


Рисунок 4.2–Вызов диспетчера драйверов

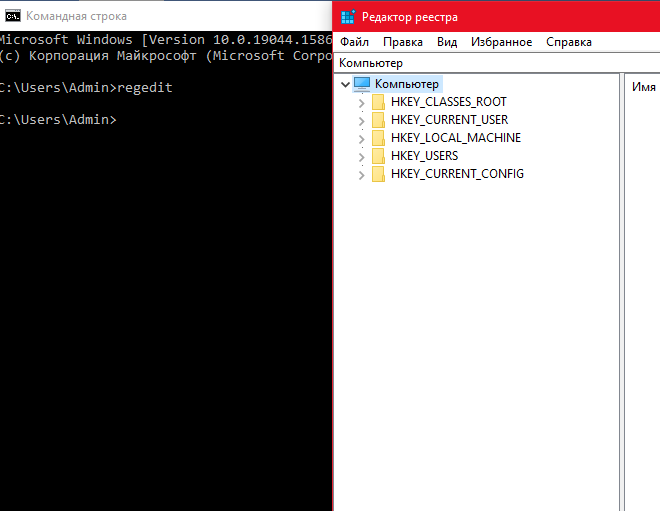


Рисунок 4.3 – Запуск редактора рееста

**Вывод:** в процессе выполнения задания ознакомились с брандмауэром Windows, его функциями и попробовали в действии команды администратора. Брандмауэр одно из наиболее эффективных средств для закрытия дыр в информационной защите операционной системы. Он фильтрует входящие и исходящие потоки данных из сети, препятствуя снижению информационной защиты аппаратного средства.