Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Коржова В.С.

ФИТ 2 курс 4 группа

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 –> Брандмауэр Windows.

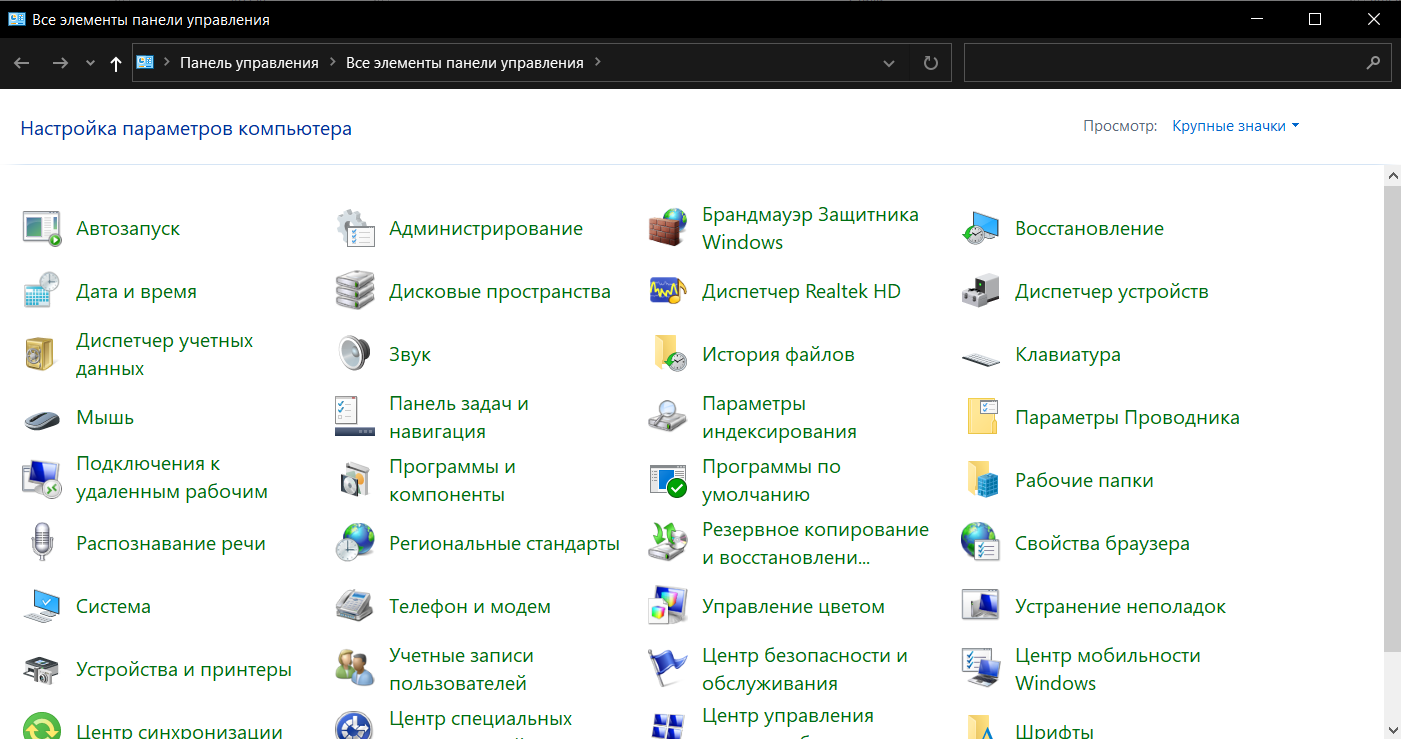


Рис. 1. Панель управления

Первым этапом необходимо включить брандмауэр, в случае, если он был ранее выключен. Необходимо выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows» (рис. 2).

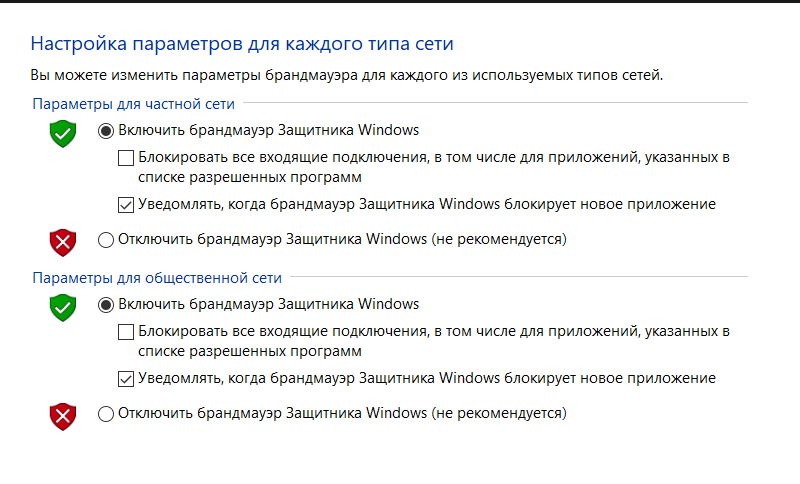


Рис. 2. Настройка параметров

Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого во вкладке «Дополнительные параметры» (рис. 3).

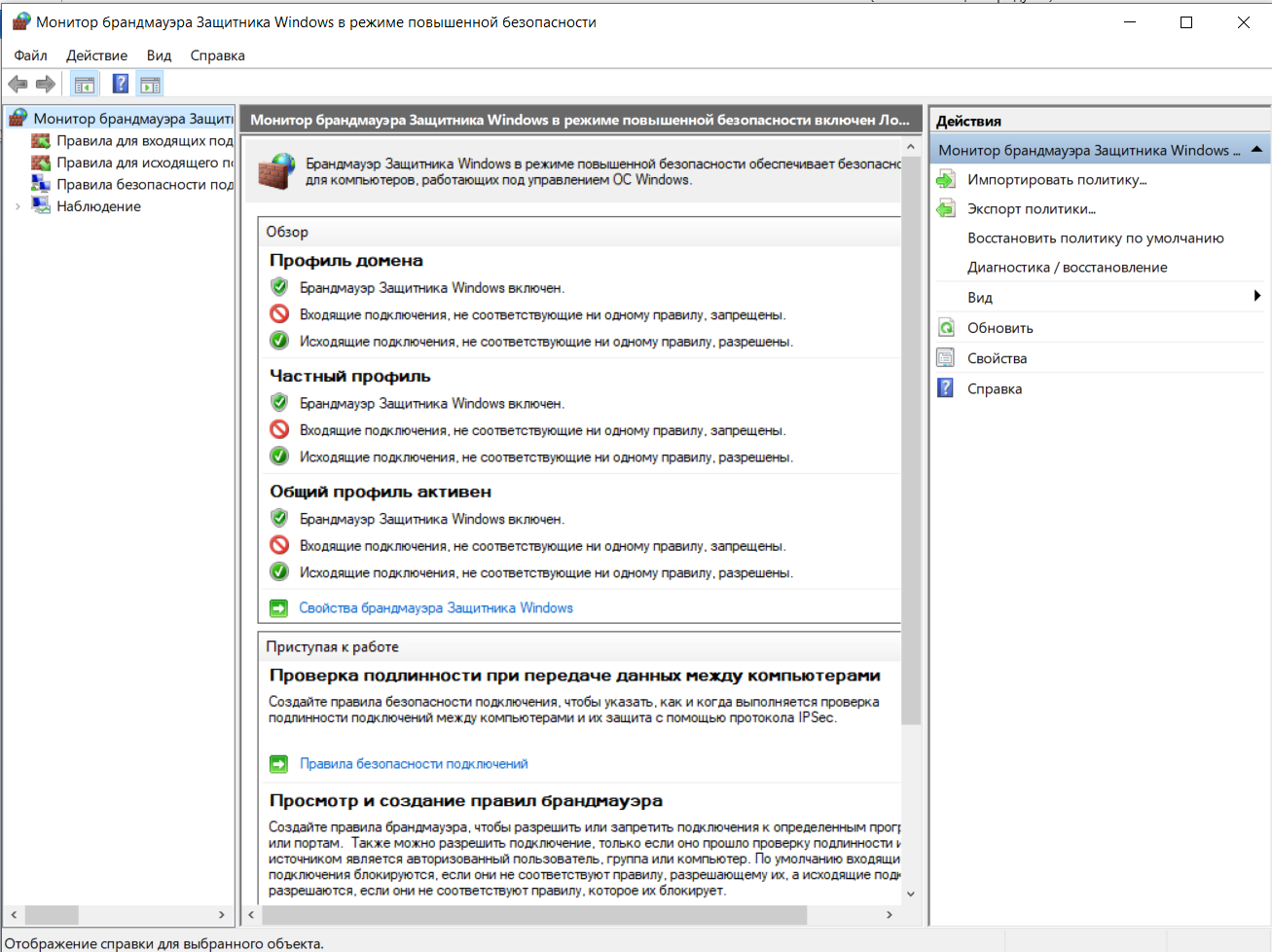


Рис. 3. Дополнительные параметры

Далее во вкладке меню «Действие» выбираем «Создать правило» (рис. 4)

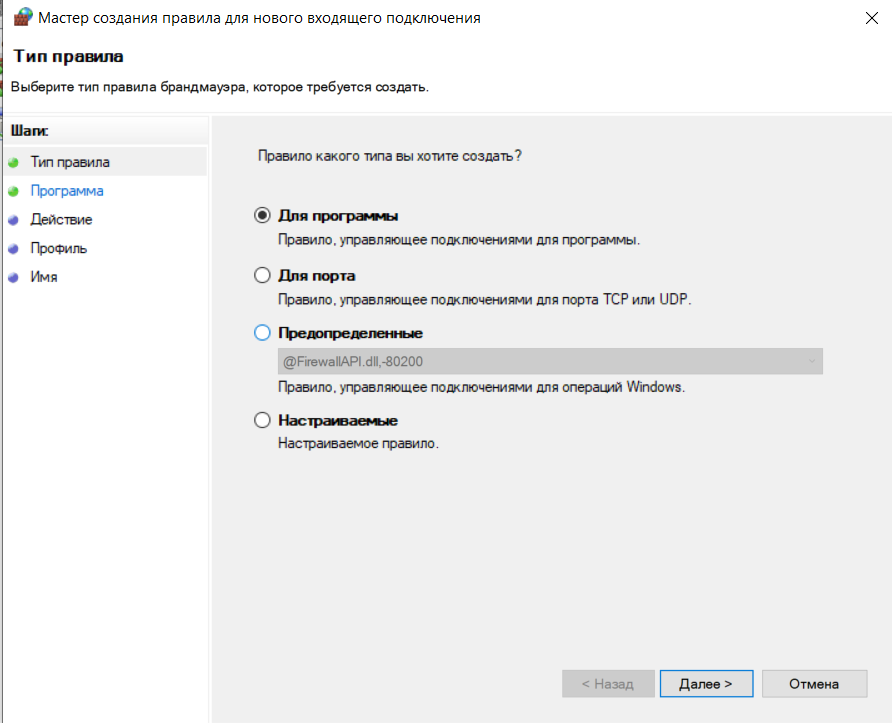


Рис. 4. Создать правило

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 (рис. 5) к нашему исполняемому файлу либо выбрав пункт все программы, наше правило примениться ко всем программам.

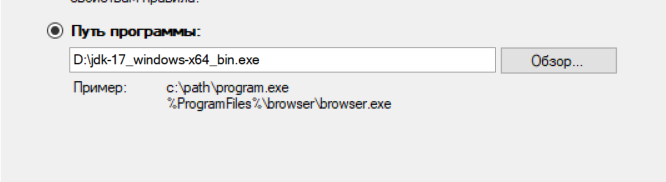


Рис. 5. Путь программы

Блокируем подключение (рис. 6). На данном этапе настройки нам необходимо указать действие над нашим правилом. Мы можем как разрешить подключение, так и блокировать.

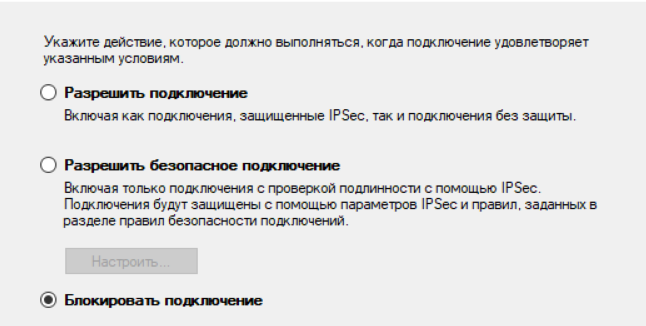


Рис. 6. Блокировка подключения

* 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 (рис 7).

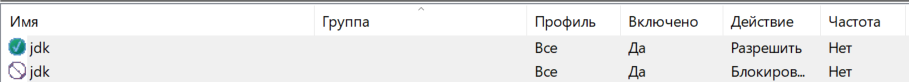


Рис. 7. Результаты входящих правил

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.

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

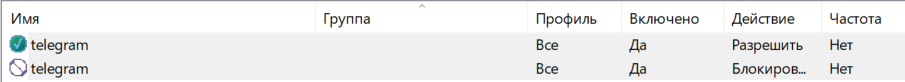


Рис. 8. Результаты исходящих правил

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

Для выполнения команд используем командную строку.

Командная строка (рис. 9) – 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.

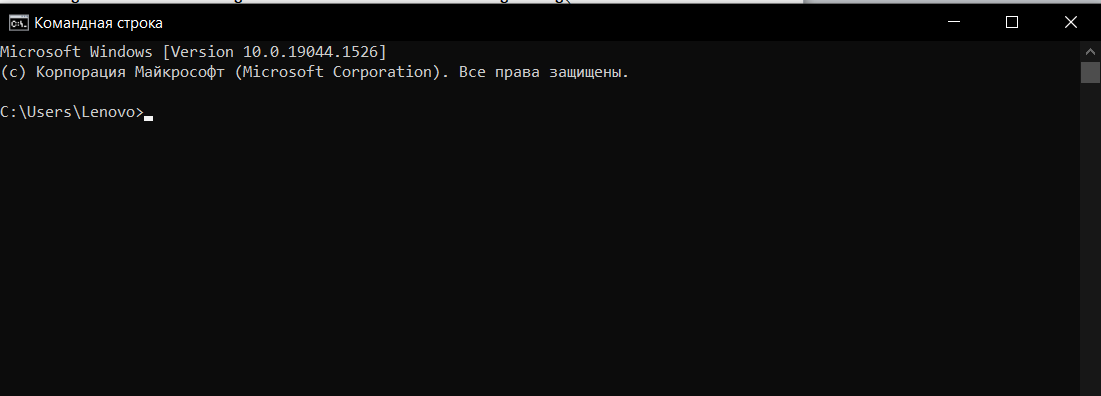


Рис. 9. Командная строка

Диспетчер проверки драйверов-verifier (рис. 10)

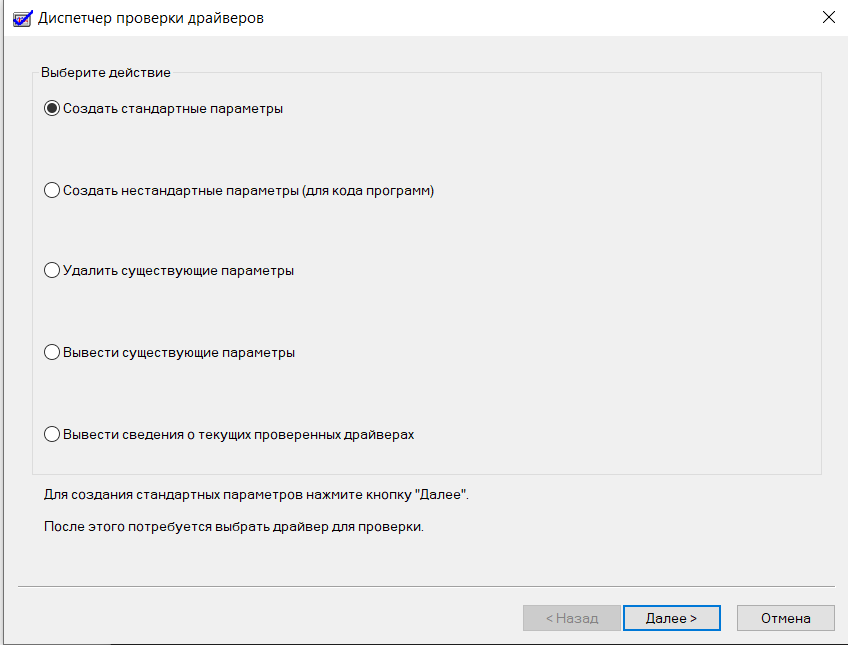


Рис. 10 Verifier

Калькулятор-calc (рис. 11).

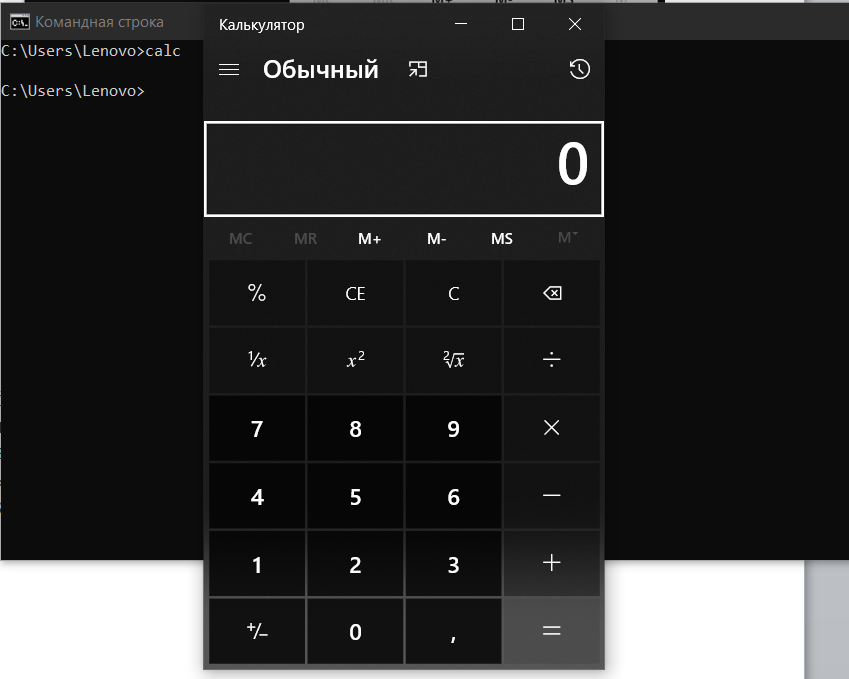


Рис. 11. Calc

**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.