|  |
| --- |
| **МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ** |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ** |
| **УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ** |
| **«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»** |
|  |
| Институт информационных технологий и управления в технических системах |
| (полное название института) |
|  |
| кафедра «Информационные системы» |
| (полное название кафедры) |

**ОТЧЁТ**

по лабораторной работе №10

на тему«брандмауэр windows»

по дисциплине **«**Операционные системы»

Выполнил

студент ИИТУТС

группы ИС/б-18-2-о

Радыгина Екатерина

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | | | | | |
|  | (должность, учёная степень преподавателя) | | | | | | | | |
|  |  | | | | | | | | |
|  | (ФИО преподавателя) | | | | | | | | |
|  | « |  | » |  |  |  | 20 | 20 | г. |
|  |  | | | | | | | | |
|  | (оценка) | | | | | | | | |
|  |  | | | | | | | | |
|  |  | | | | | | | | |

Севастополь 2020

**10.1 Цель работы**

Ознакомиться со встроенными средствами защиты от сетевых угроз в ОС Windows 10.

**10.2 Ход работы**

10.2.1 Для того чтобы открыть брандмауэр Windows выполните следующие действия: *Пуск –>Панель управления –> Система безопасности–>Брандмауэр Windows.*

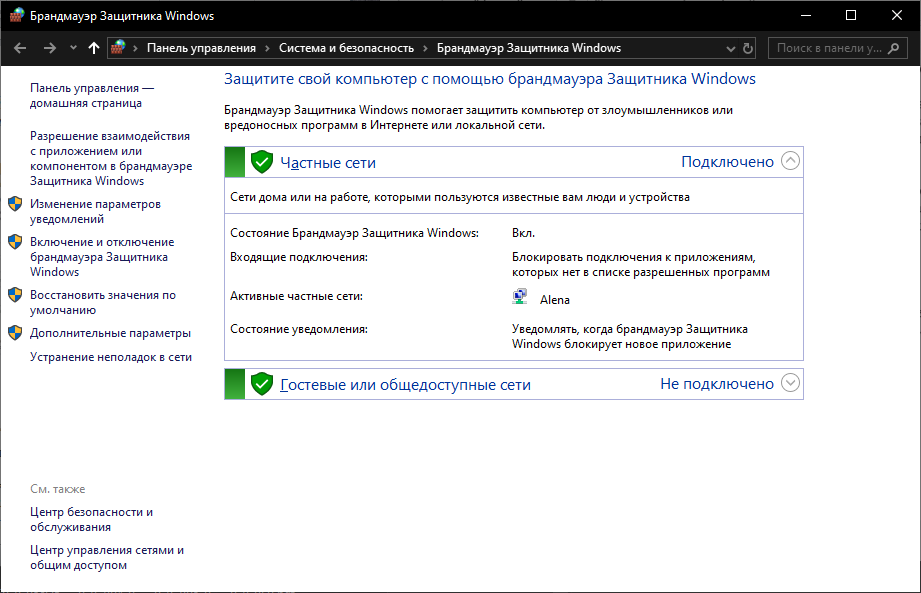


Рисунок 10.1 – Окно Брандмауэра Windows

Переход по ссылке *Разрешить запуск программы* приведёт к открытию окна *«Разрешенные программы».* Программы и службы, не блокируемые брандмауэром Windows, будут помечены флажками.

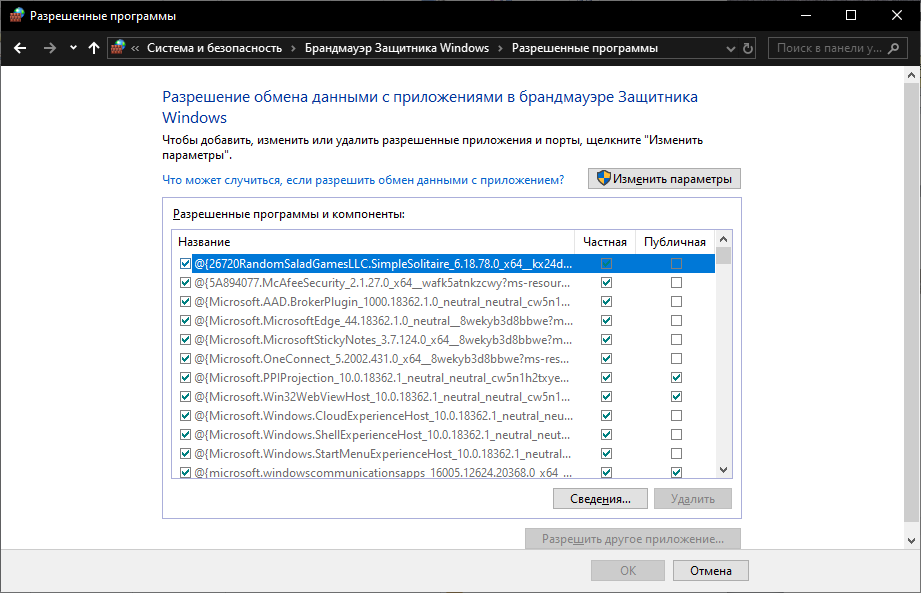


Рисунок 10.2 – Окно разрешённых программ

10.2.2 Выполним *команду Пуск > Панель управления > Администрирование > Брандмауэр Windows в режиме повышенной безопасности > Правила для входящих подключений.* Развернув окно, чтобы можно было увидеть полное имя правил для входящих подключений. Найдём «Общий доступ к файлам и принтерам (эхо-запрос – входящий трафик ICMPv4)». Щёлкнем правой кнопкой мыши, выбрать *Свойства > вкладка Дополнительно*. Нажать кнопку *Настроить.*

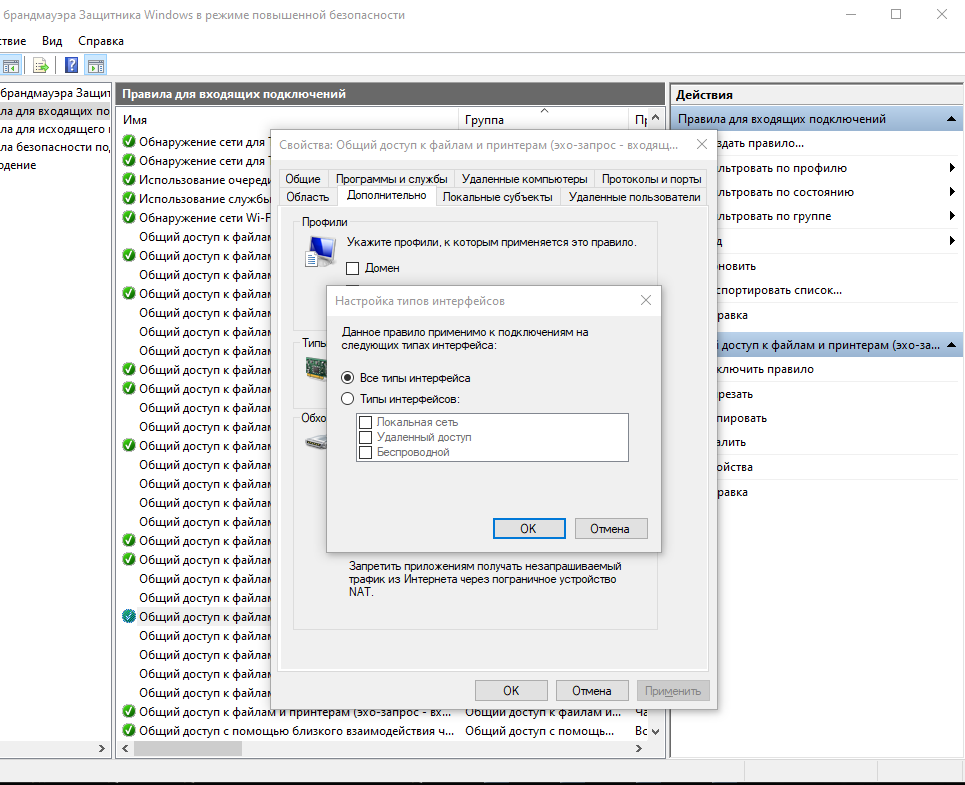


Рисунок 10.3 – Окно Брандмауэр Windows в режиме повышенной безопасности

На вкладке *«Дополнительно*» отображаются профили, используемые компьютером, а в окне *«Настройка типов интерфейсов*» отображаются различные подключения, настроенные на компьютере. Нажать кнопку ОК.

Перейдём на вкладку *Программы и службы*. Откроется окно «Настройка параметров службы». Нажмём кнопку *Параметры*.

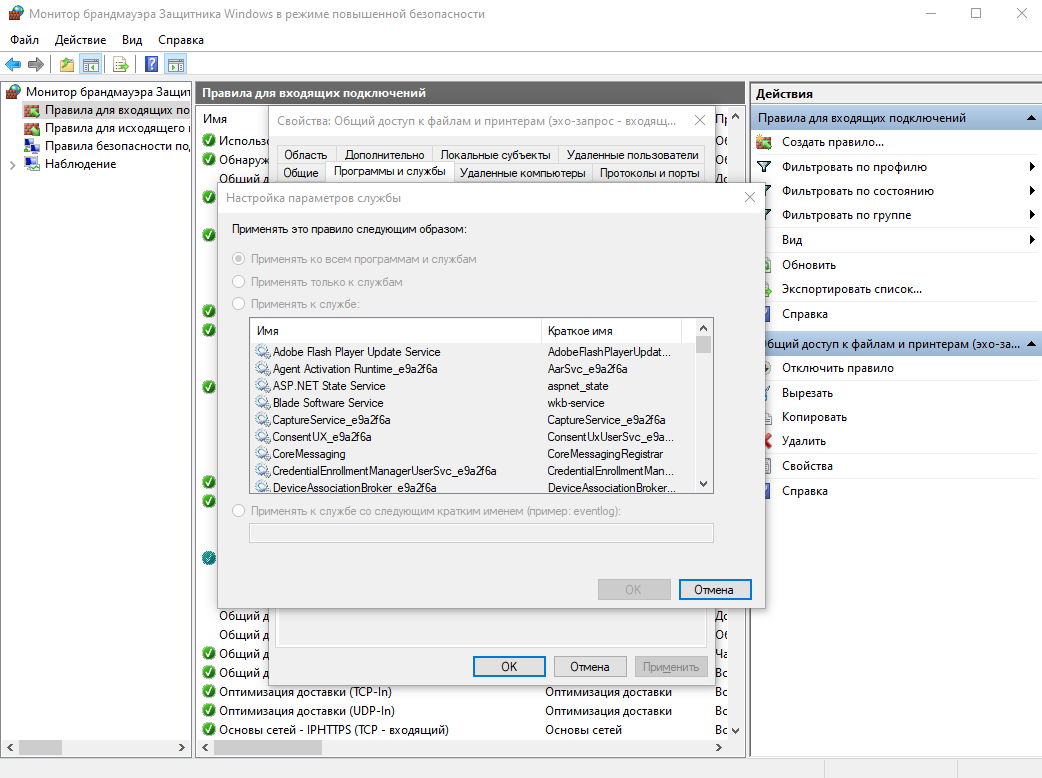


Рисунок 10.4 – Настройка параметров служб

Перейти на вкладку Протоколы и порты. Для настройки ICMP нажать кнопку Настроить. Можно будет увидеть меню, в котором настраиваются исключения ICMP

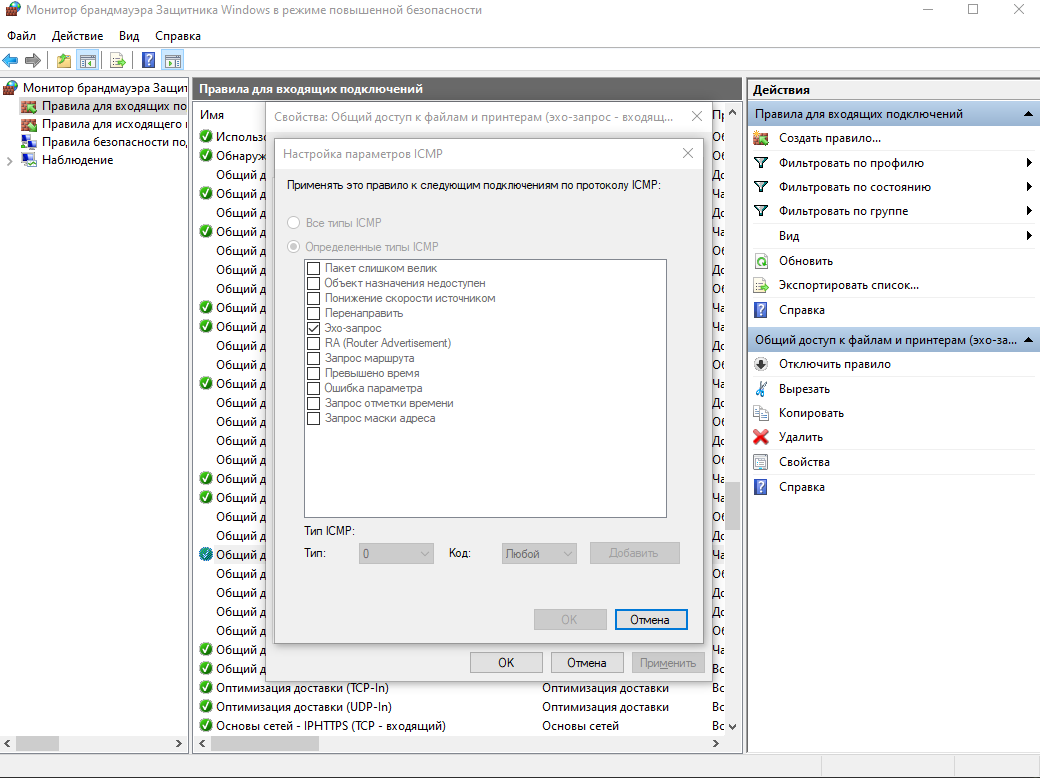


Рисунок 10.5 – Настройка параметров ICMP.

Вернёмся в окно *«Правила для входящих подключений».* На вкладке *«Действия»* с помощью команды *«Создать правило»* можно настроить параметры некоторых приложений.

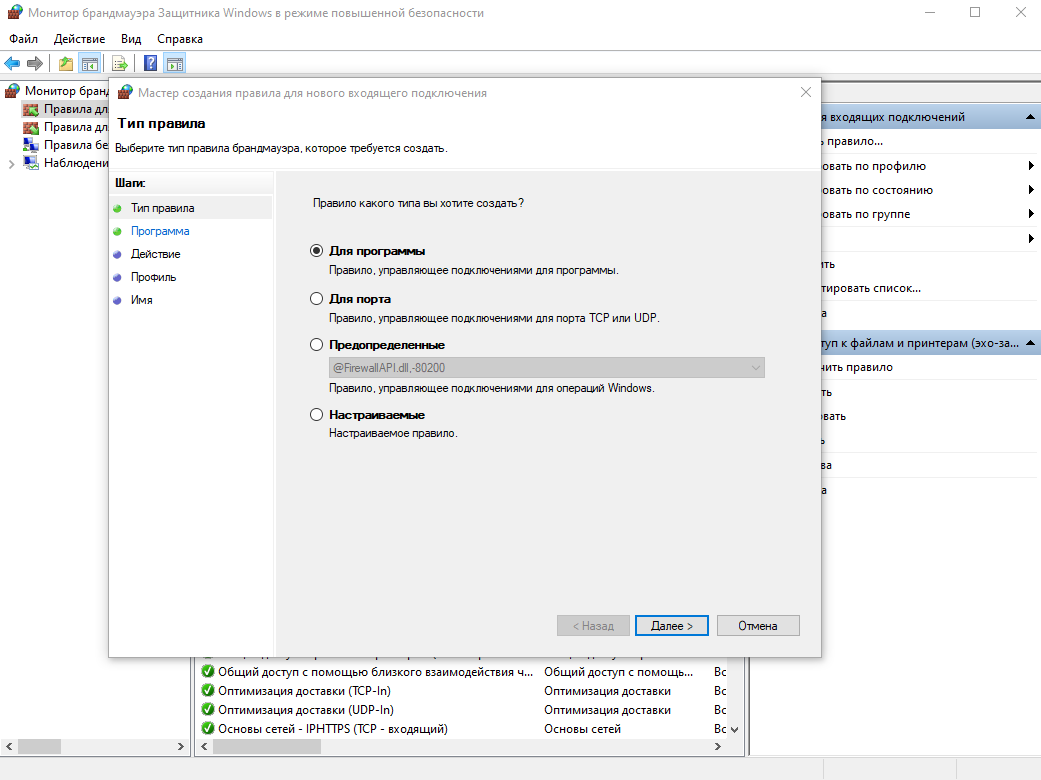


Рисунок 10.6 – Окно «Мастер создания правил»

**Вывод**

В ходе лабораторной работы мы ознакомились со встроенными средствами защиты от сетевых угроз в ОС Windows 10.