**Лабораторная работа No 18**

Тема: «Настройка безопасности ПК. Брандмауэр Windows».

Цель: изучить возможности защиты компьютера с помощью брандмауэра Windows.

Задание 1. Изучить и выполнить порядок настройки брандмауэра Windows.

1. Для того чтобы открыть Брандмауэр запустите панель управления, нажав Win+R, ввёв команду «control».

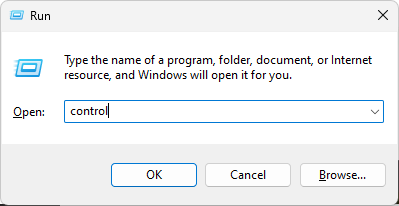
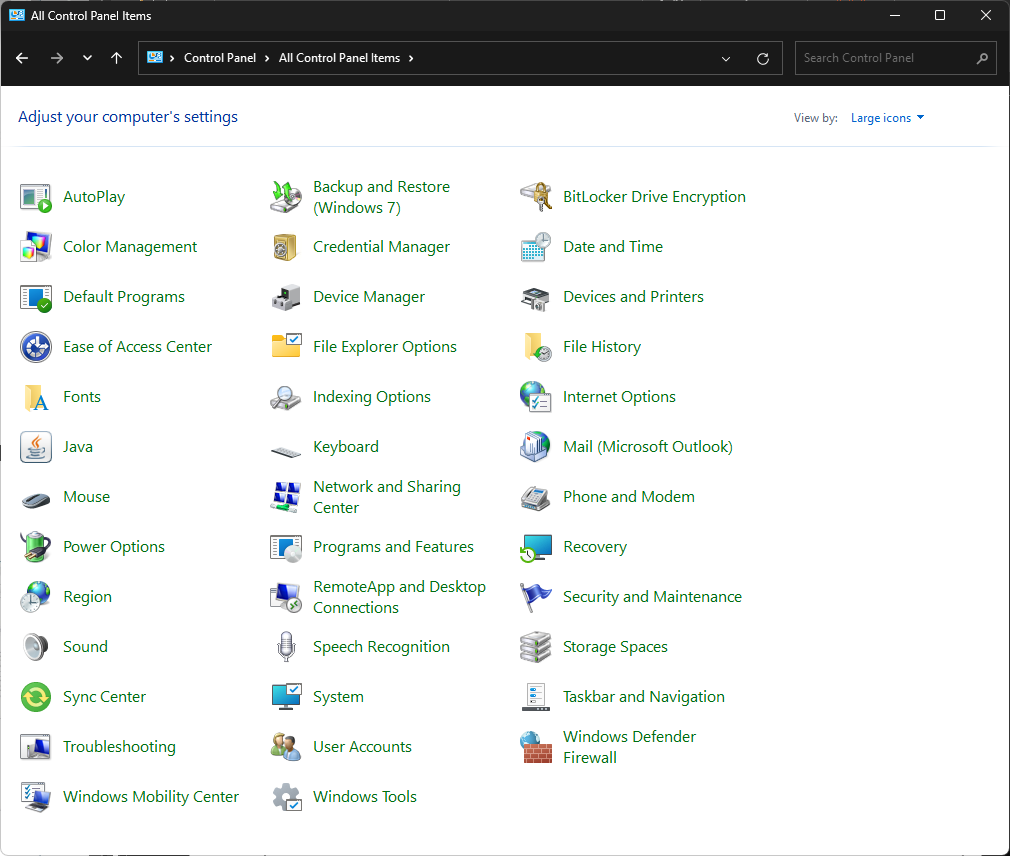
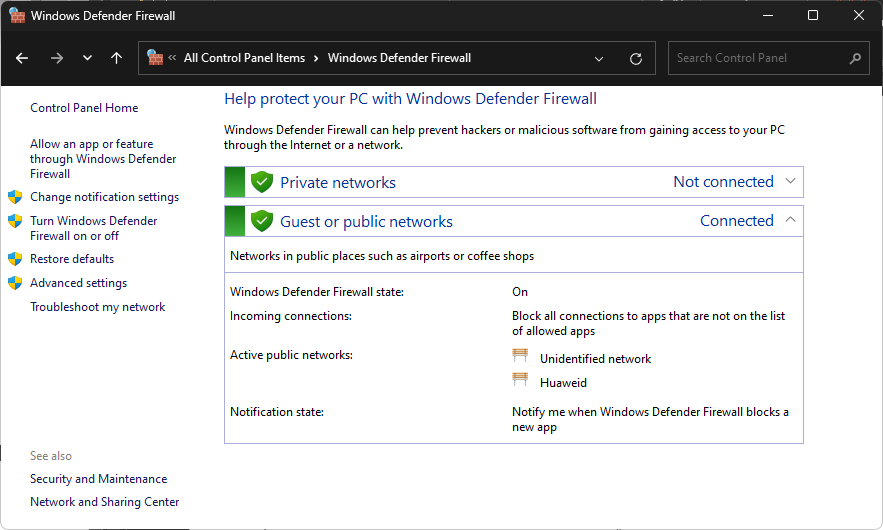


Рисунок 1 – Окно «Выполнить»

В открывшемся окне найдите раздел «Брандмауэр Windows» и кликните по нему как показано на рисунке 2.

Рисунок 2 – Панель управления.

Это и есть системный фаервол, отсюда и будет проводиться его настройка (рисунок 3).

Рисунок 3 – Windows Defender Firewall.

2. Как включить брандмауэр Windows 10

По умолчанию системный фаервол должен быть включен, однако, если по каким-то причинам это не так, то необходимо включить программу. Для этого необходимо выполнить следующие действия:

• Откройте приложение, способом, который был описан выше, и перейдите в раздел «Включение и отключение брандмауэра Windows» рисунок 4.

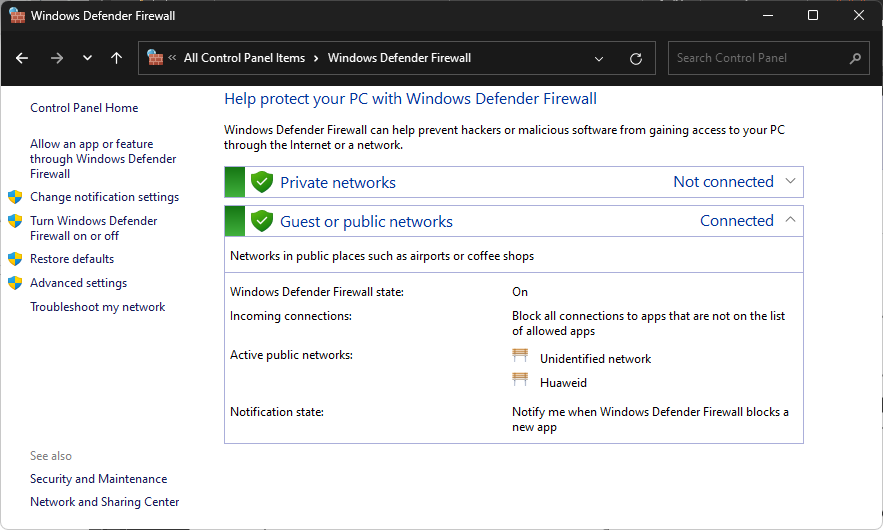
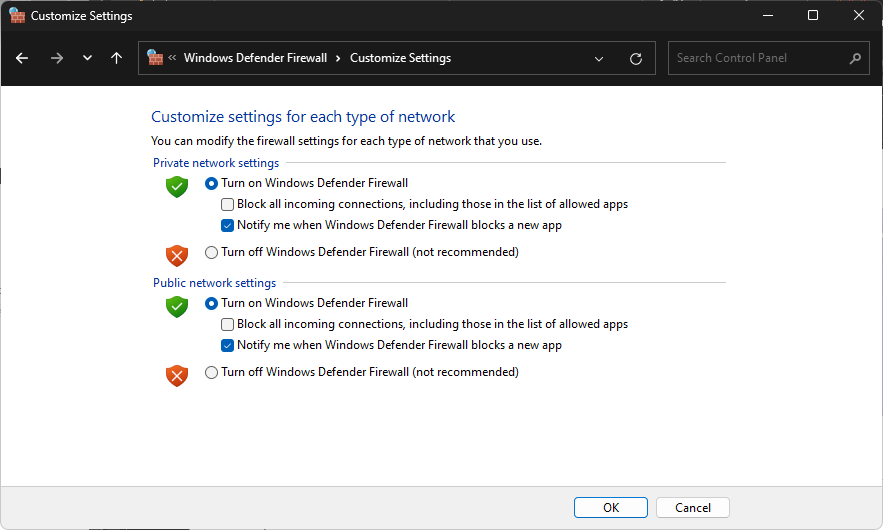


Рисунок 4 – Панель управления.

В данном разделе настройки фаервола разделены на две категории: для частной сети и для общественной. Соответственно, чтобы включить защиту для каждой из них, переместите флажок триггера в положение включения. Для того чтобы получать уведомления безопасности, предварительно поставьте флажки на пункты, обозначенные на рисунке 5.

Рисунок 5 – Настройка параметров.

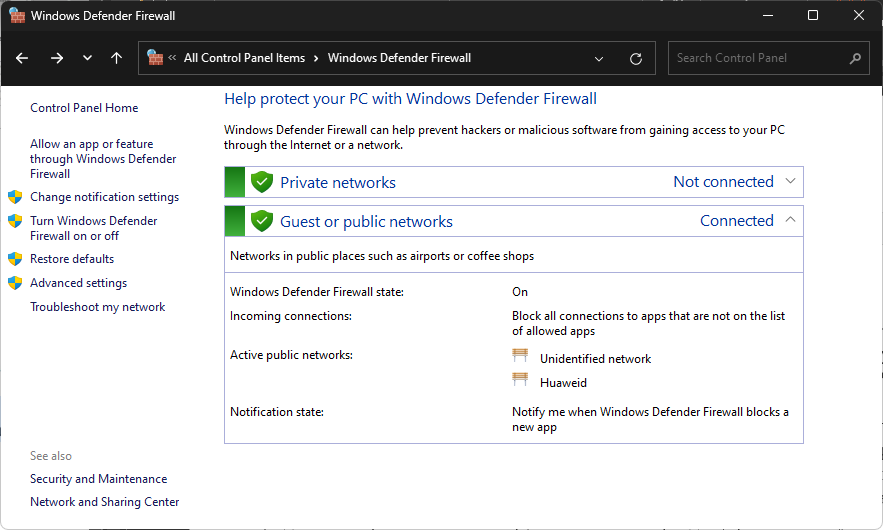
Настройки брандмауэра Windows.

Вся суть работы Windows-фаервола в основном заключается в его неправильной настройке. Знающие пользователи редко оставляют конфигурацию по умолчанию. Необходимо разобраться с данными вопросами подробнее.

Добавление исключений в брандмауэре Windows.

Если фаервол заблокировал одно из нужных приложений или игру, его необязательно отключать, а можно просто сделать так, чтобы компьютер начал «доверять» приложению. Это следует сделать в том случае, если приложение является безопасным для системы. Далее будет рассмотрено, как правильно добавить приложение или игру в исключение брандмауэра Windows.

Для начала нужно открыть брандмауэр в панели управления, как показано на рисунок 6, и перейти в раздел «Разрешение взаимодействия с приложением и компонентом в брандмауэре Windows».

Рисунок 6 – Панель управления.

Нажмите по кнопке «Изменить параметры», как показано на рисунок 7, но если данная кнопка не активна, нужно проверить включен ли брандмауэр, затем закрыть панель управления, перезагрузить компьютер и ещё раз попробовать повторить операцию.

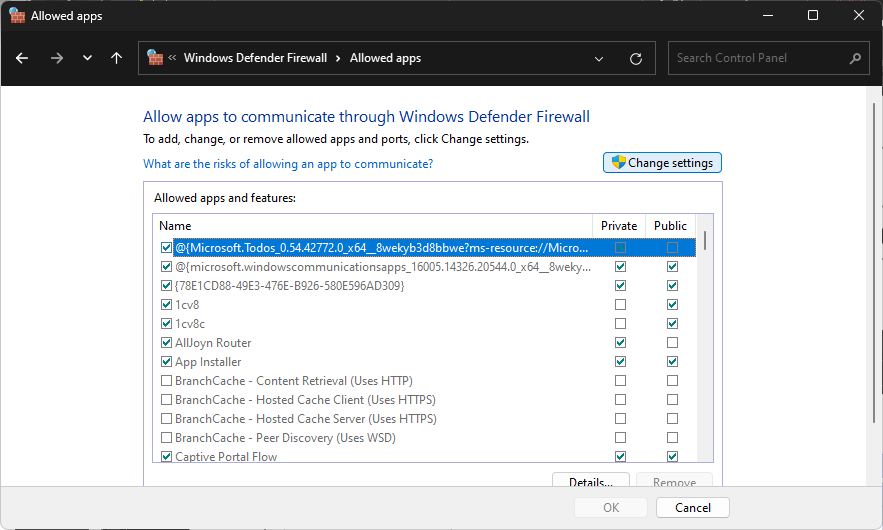
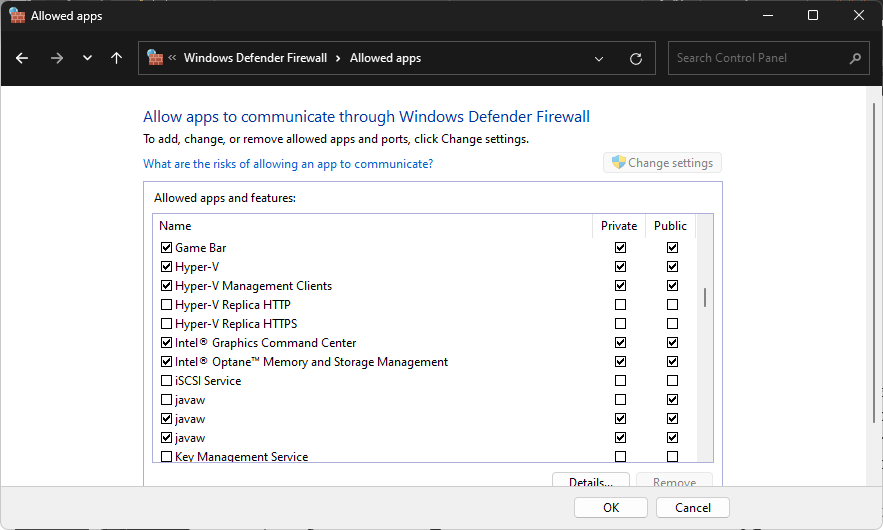


Рисунок 7 – Разрешение обмена данными.

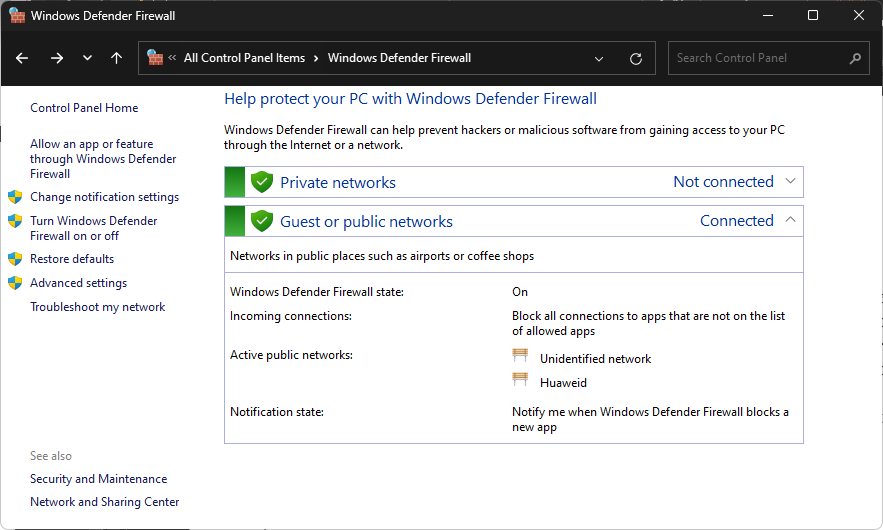
Активируется список всех программ, которые есть на компьютере, для того чтобы разрешить одной или нескольким из них доступ, установите флажки напротив нужных пунктов, как на рисунке 8.

Рисунок 8 – Разрешение обмена данными.

Открытие портов.

По умолчанию брандмауэр блокирует все порты, которые считаются неосновными. Но что делать, если вы, например, хотите организовать подключение FTP-сервера, для работы которого нужны порты 20 и 21? Нужно просто открыть их. Рассмотрим, как это делается через брандмауэр, запущенный в режиме повышенной безопасности.

В очередной раз перейдите в брандмауэр, открыв панель управления, выберете раздел «Дополнительные параметры» рисунок 9.

Рисунок 9 – Дополнительные параметры.

В открывшемся окне выберете раздел «Правила для входящих подключений» и в меню «Действия» расположенном справа выбираете «Создать правило» как показано на рисунок 10.

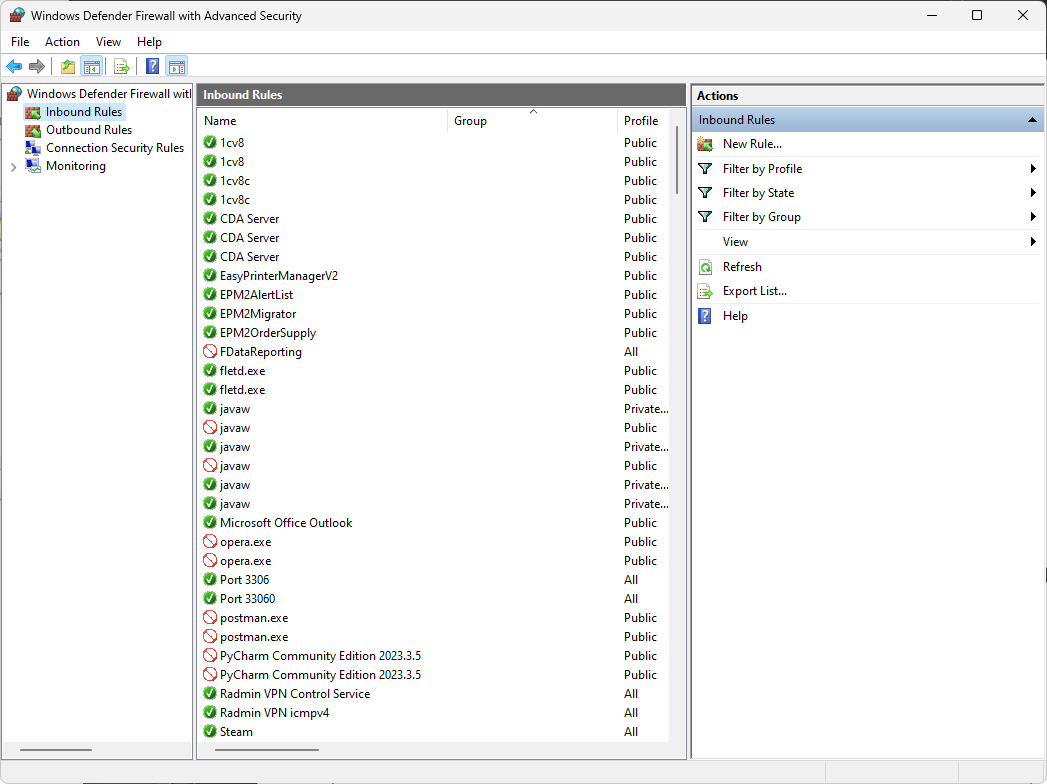
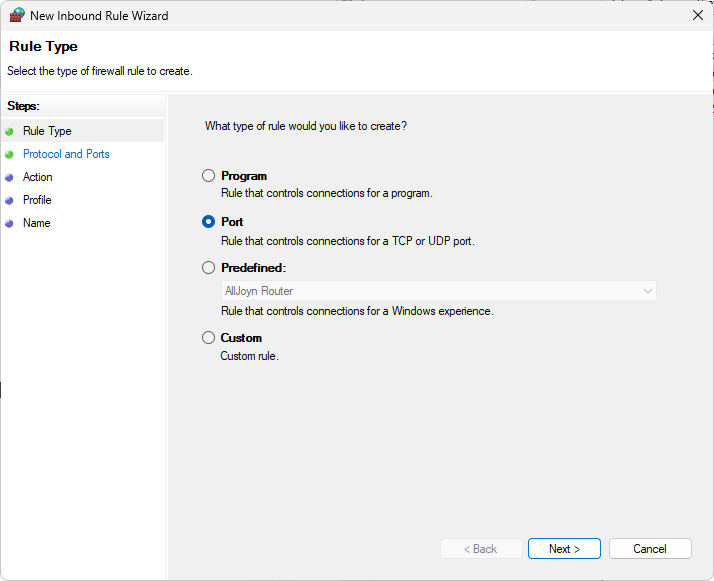


Рисунок 10 – Брандмауэр Windows в режиме повышенной безопасности.

В новом окне выберете пункт «Для порта» и нажмите по кнопке «Далее» рисунок 11.

Рисунок 11 – Мастер создания правил.

Затем укажите протокол, как показано на рисунок 12, который будет использоваться: TCP или UDP и перечислите нужные порты. По завершении нажмите «Далее».

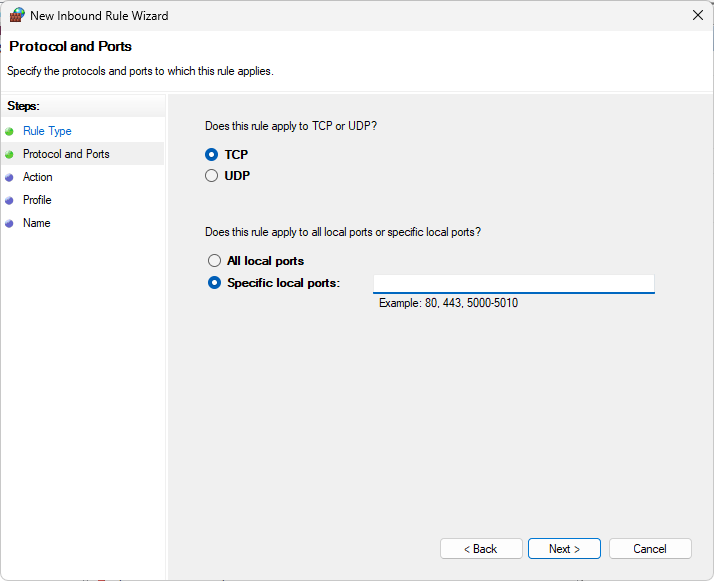
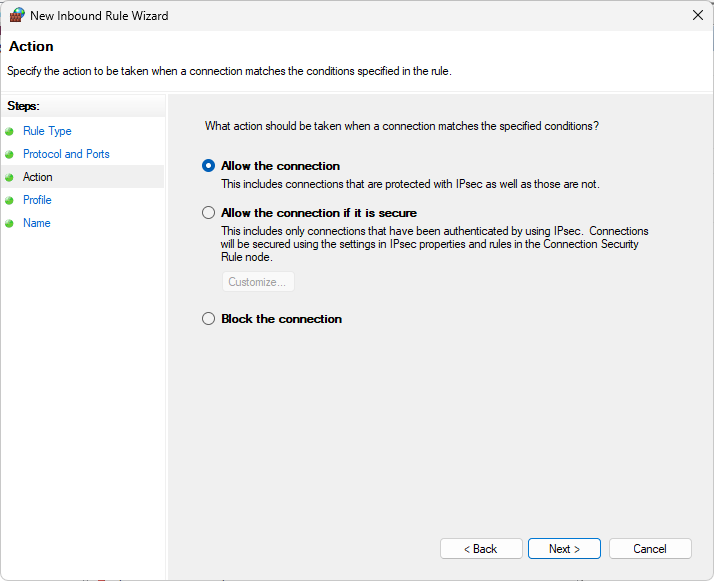


Рисунок 12 – Протоколы и порты.

Установите переключатель в положение «Разрешить подключение» и нажмите на кнопку «Далее», как на рисунке 13.

Рисунок 13 – Мастер создания правил.

Укажите профили, к которым будет назначено созданное разрешение открытия портов, и снова жмите «Далее», как на рисунке 14.

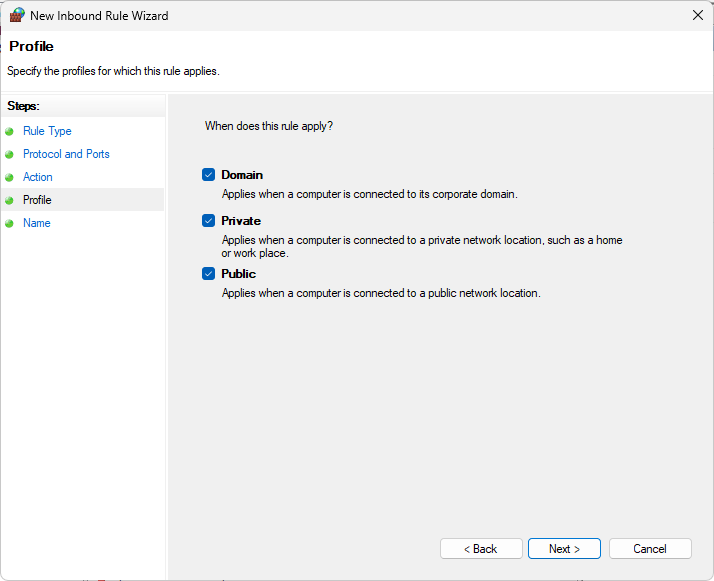
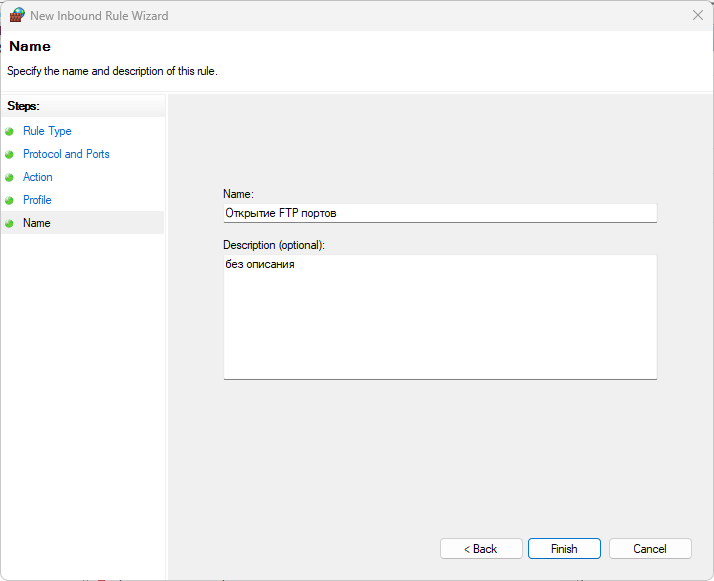


Рисунок 14 – Профиль.

Введите имя, и описание для созданного правила и жмите кнопку «Готово» рисунок 15.

Рисунок 15 – Открытие FTP-портов.

В итоге правило создано и нужные порты готовы к работе.

Задание 2.

1. Включить и настроить брандмауэр для запрета нежелательного трафика, научиться запрещать и разрешать использование утилиты ping, настроить разрешающее правило для программы DownloadMaster.

Для запрета использования утилиты ping открываем Firewall, заходим в дополнительные настройки, в древовидной панели нажимаем правой кнопкой по исходящему трафику и выбираем новое правило (рисунок 16).

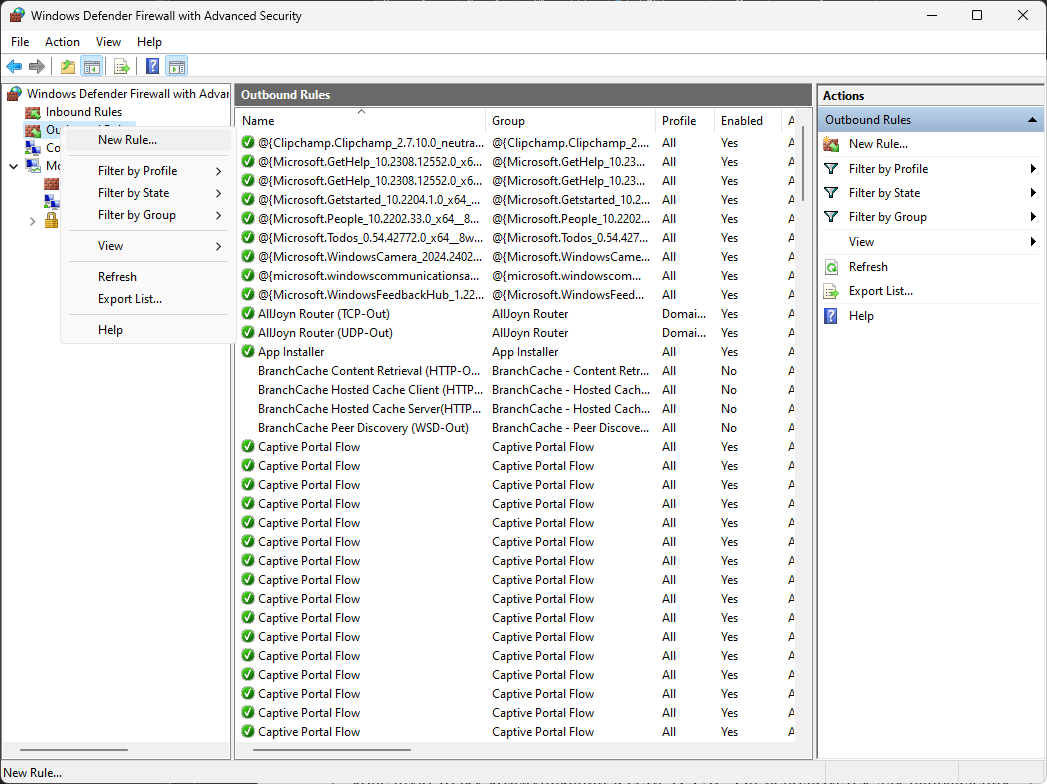


Рисунок 16 – Новое правило.

Выбираем кастомное правило (рисунок 17).

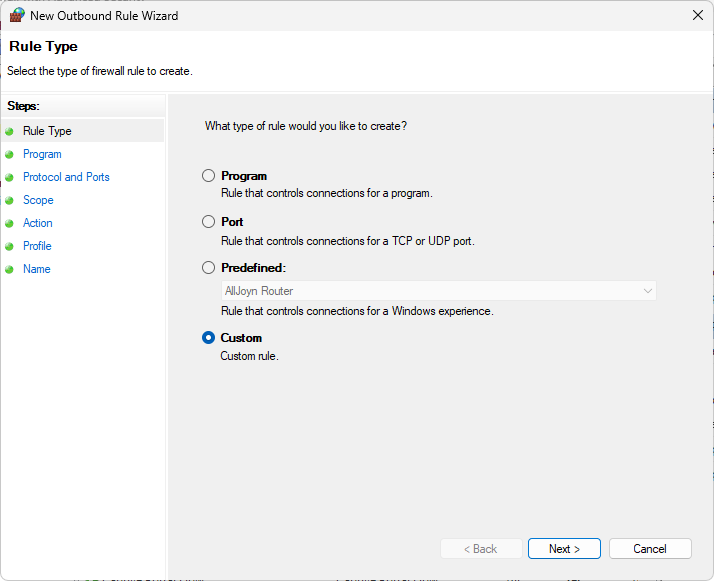
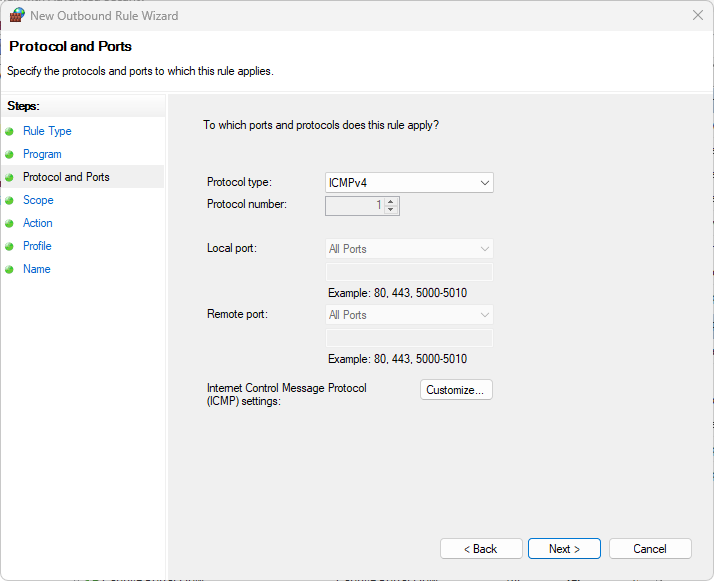
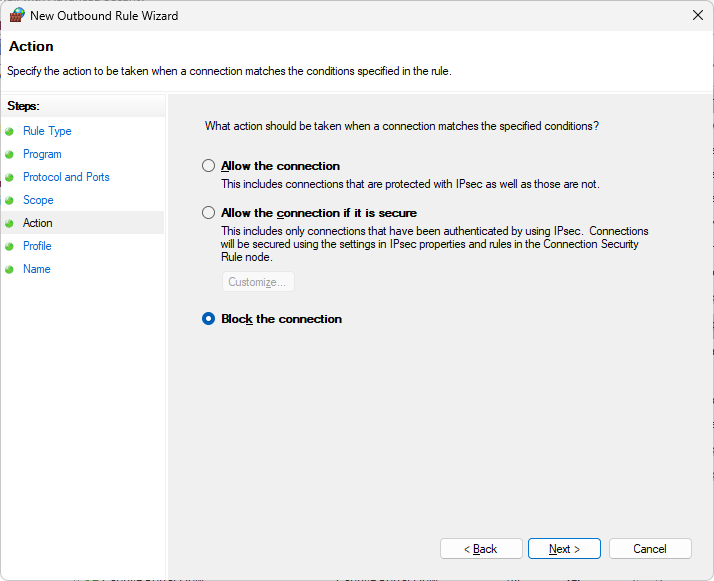


Рисунок 17 – Выбор типа правила.

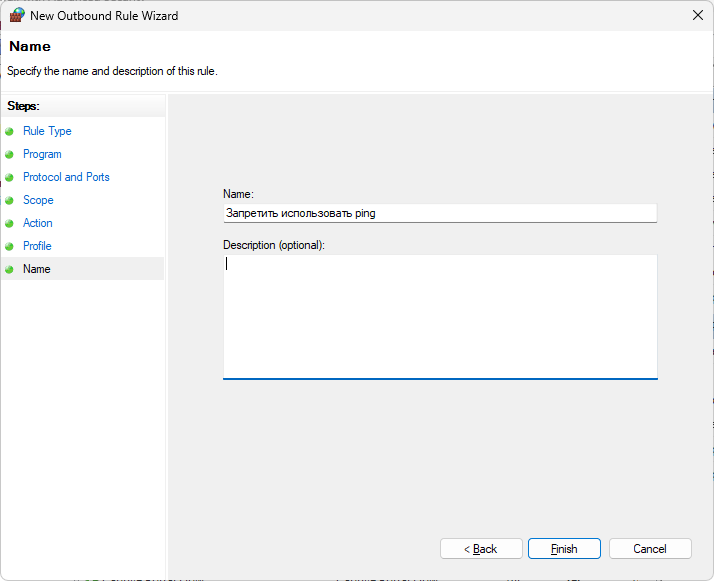
Нажимаем Далее, на шаге «Программа» ничего не изменяем и нажимаем «Далее». На шаге «Протоколы и порты» выбирает тип протокола «ICMPv4» (рисунок 18).

Рисунок 18 – Выбор протокола.

Нажимаем «Далее», пока не попадаем на шаг «Действие». Убеждаемся, что выбран пункт «Блокировать подключение» (рисунок 19).

 Рисунок 19 – Выбор действия.

также нажимаем «Далее» до шага «Название» (рисунок 20), где вводим любое имя.

Рисунок 20 – Название.

Теперь при попытке использования утилиты ping через командную строку, происходит ошибка (рисунок 21), значит правило успешно отработало.

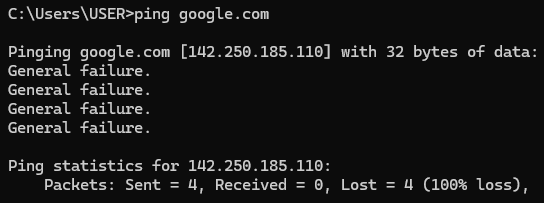


Рисунок 21 – Попытка использования утилиты ping.

Разрешение использования утилиты производится таким же образом, за исключением шага на рисунке 19, где необходимо выбрать пункт «Разрешить соединение».

2. Скачать из сайта www.rusroute.ru брандмауэр Windows выполнить его настройку и установку пользуясь официальной документацией.

После загрузки, установки и запуска, появляется главная форма программы (рисунок 22).

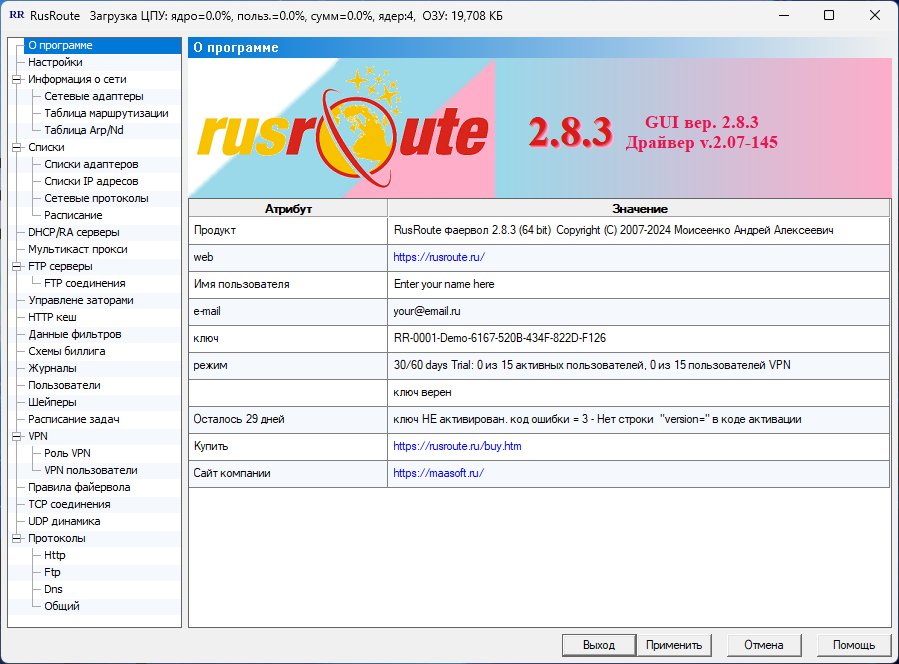


Рисунок 22 – Главная форма.

Меняем в найстроках значение параметра «Отключить RusRoute firewall» на «нет» (рисунок 23).

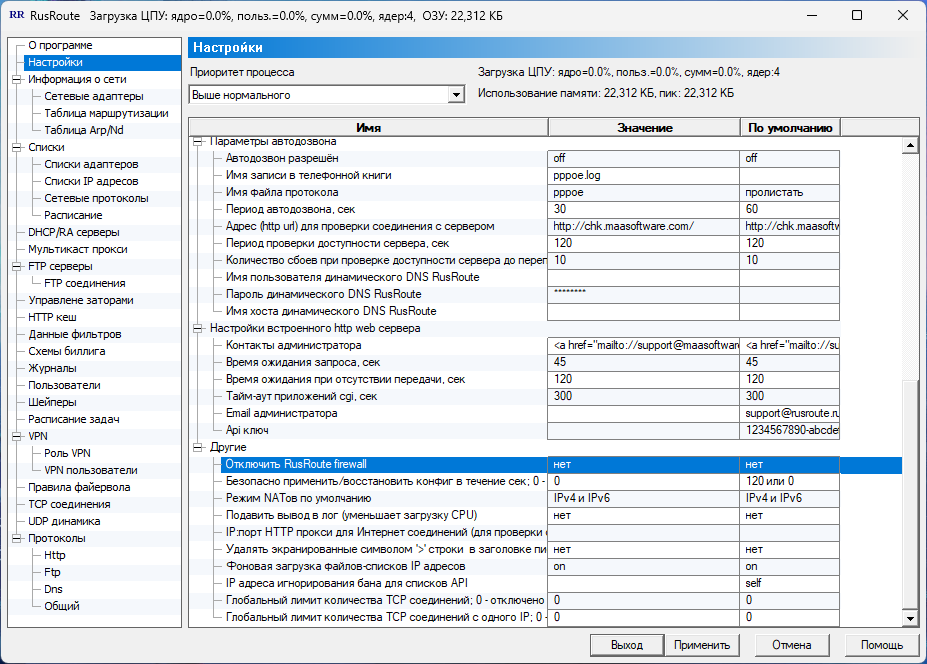


Рисунок 23 – Включение фаерволла.

Контрольные вопросы.

1. Что такое брандмауэр?

Брандмауэр (фаервол) - это программно-аппаратный компонент сетевой защиты, который контролирует входящий и исходящий сетевой трафик на предмет соответствия определенным правилам безопасности.

2. Какие источники сетевых угроз вы знаете?

Источники сетевых угроз могут быть разнообразными, включая вредоносные программы (вирусы, черви, троянские программы), хакерские атаки (DDoS, перехват трафика), социальная инженерия, несанкционированный доступ и другие.

3. Что такое порт протокола TCP?

Порт протокола TCP – это числовой идентификатор, который определяет конечную точку коммуникации в сети TCP/IP. Он используется для направления данных на правильное приложение на конечном устройстве.

4. Какие вы знаете стандартные сетевые порты?

Некоторые стандартные сетевые порты включают порт 80 для HTTP, порт 443 для HTTPS, порт 25 для SMTP, порт 21 для FTP, порт 22 для SSH, порт 53 для DNS и т. д.