# Практическое занятие № 17

## Настройка персонального межсетевого экрана Windows

**Цель:** Получить теоретические знания и практические навыки работы с персональным межсетевым экраном (брандмауэром) Windows.

По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

# Содержание:



По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

# Теоретическая часть
## Что может и чего не может брандмауэр Windows

| Он может: | Он не может: |
|---|---|
| Блокировать компьютерным вирусам и «червям» доступ на компьютер. | **Обнаружить или обзевредить компьютерных вирусов или «червей»,** если они уже попали на компьютер. По этой причине необходимо также установить антивирусное программное обеспечение и своевременно обновлять его, чтобы предотвратить повреждение компьютера вирусами, «червями» и другими опасными объектами, а также не допустить использования данного компьютера для распространения вирусов на другие компьютеры. |

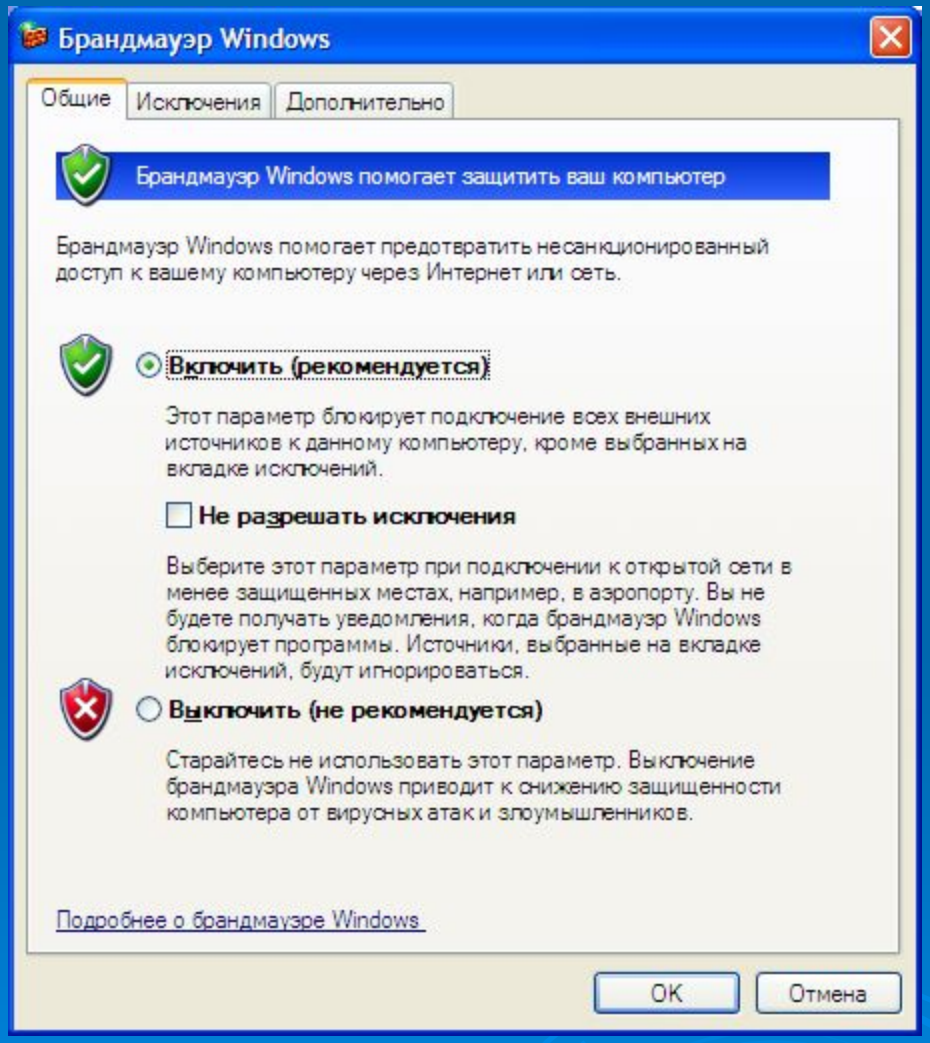
# Теоретическая часть
## Что может и чего не может брандмауэр Windows

| Он может: | Он не может: |
|---|---|
| **Запросить пользователя о выборе** блокировки или разрешения для определенных запросов на подключение. | **Запретить пользователю открывать сообщения электронной почты с опасными вложениями.** Не открывайте вложения в сообщениях электронной почты от незнакомых отправителей. Следует проявлять осторожность, даже если источник сообщения электронной почты известен и заслуживает доверия. При получении от знакомого пользователя электронного письма с вложением внимательно почтите тему сообщения перед тем, как открыть его. Если тема сообщения представляет собой беспорядочный набор знаков или не имеет смысла, не открывайте письмо, пока не свяжетесь с отправителем для получения подтверждения. |

# Теоретическая часть
## Что может и чего не может брандмауэр Windows

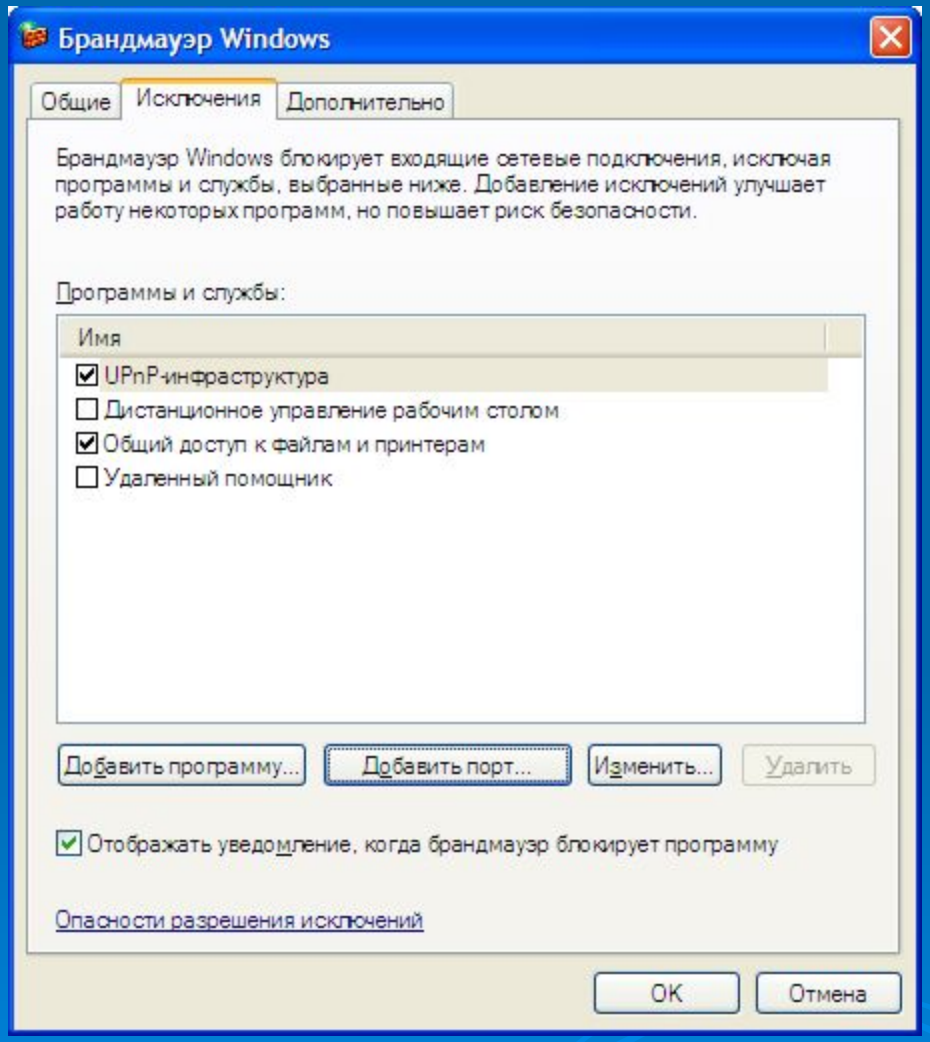
| Он может: | Он не может: |
|---|---|
| **Вести учет (журнал безопасности)** – по желанию пользователя – записывая разрешенные и заблокированные попытки подключения к компьютеру. Этот журнал может оказаться полезным для диагностики неполадок. | **Блокировать спам или несанкционированные почтовые рассылки,** чтобы они не поступали в папку входящих сообщений. Однако некоторые программы электронной почты способны делать это. Ознакомьтесь с документацией своей почтовой программы, чтобы выяснить ее возможности. |

# *Настройка*




Во-первых, необходимо проверить, включен ли Брандмауэр. Если нет, необходимо осуществить включение, как показано на рисунке.

# *Пример создания исключения*



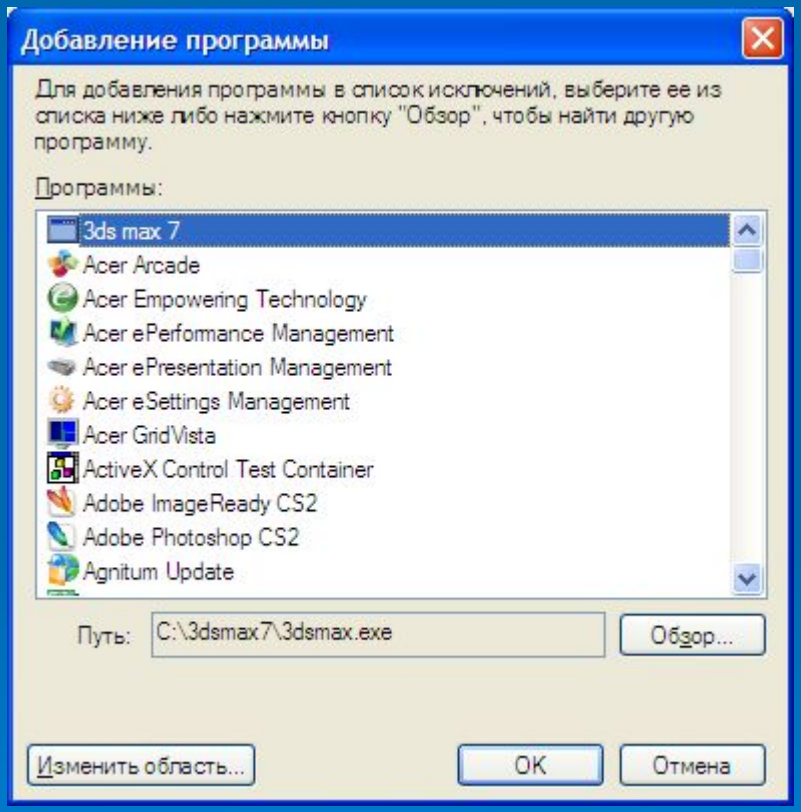

По умолчанию все программы и службы блокируются. Для того, чтобы добавить исключения, необходимо проделать операции, указанные ниже.

Рассмотрим пример создания исключения для **outlook express**.

**1)** Откройте вкладку **Исключения**:

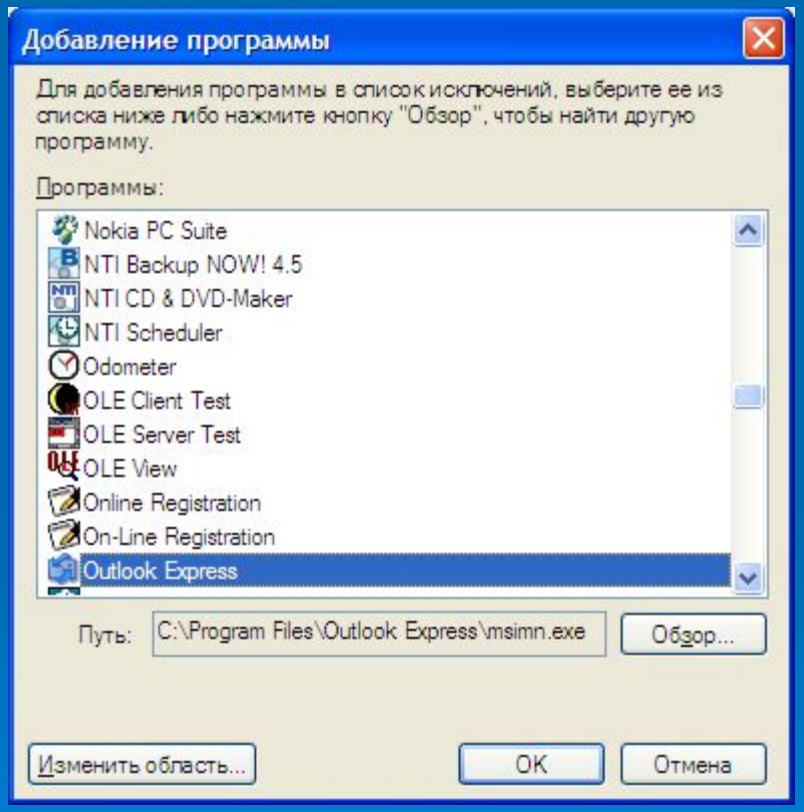
# *Пример создания исключения*

**2)** Нажмите **Добавить программу**:



# *Пример создания исключения*

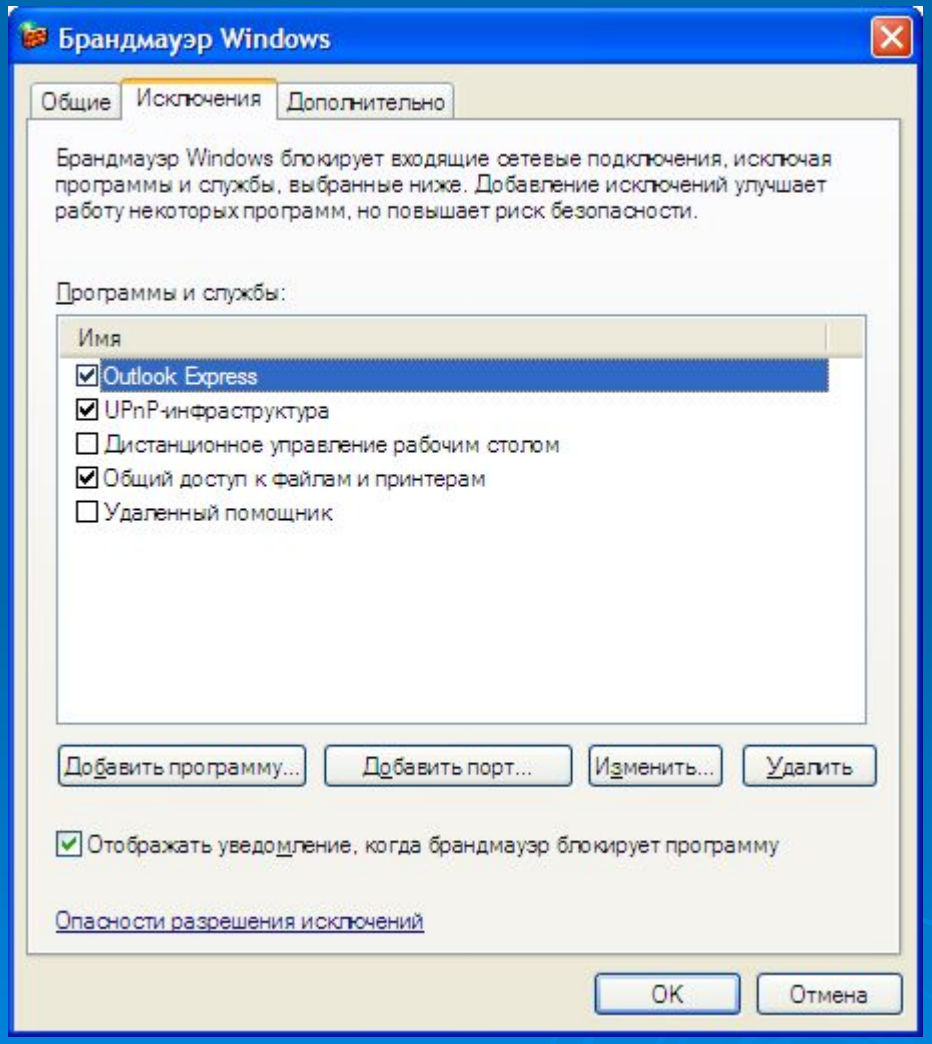
**3)** Выберите программу из списка, или указать программу вручную:



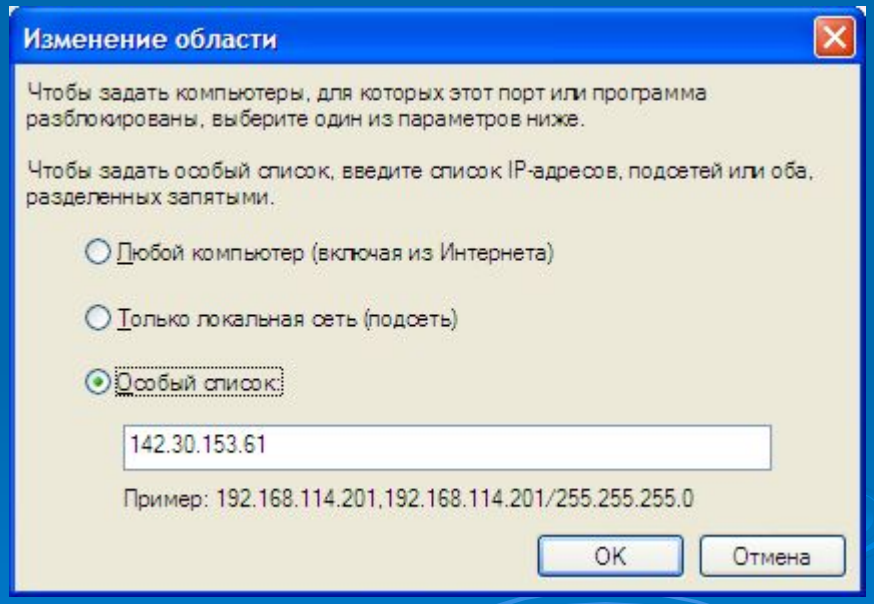

Этими действиями мы разрешили выполнять любые сетевые операции Outlook Express. Теперь необходимо изменить область (подсеть), с которой программа будет работать. К примеру, почтовый сервер расположен по адресу 142.30.153.61, там нужно разблокировать этот адрес. При попытке приложения обратиться к другому **ip**-адресу мы увидим уведомление.

# *Пример создания исключения*

**4)** Выберите из списка **Outlook Express:**

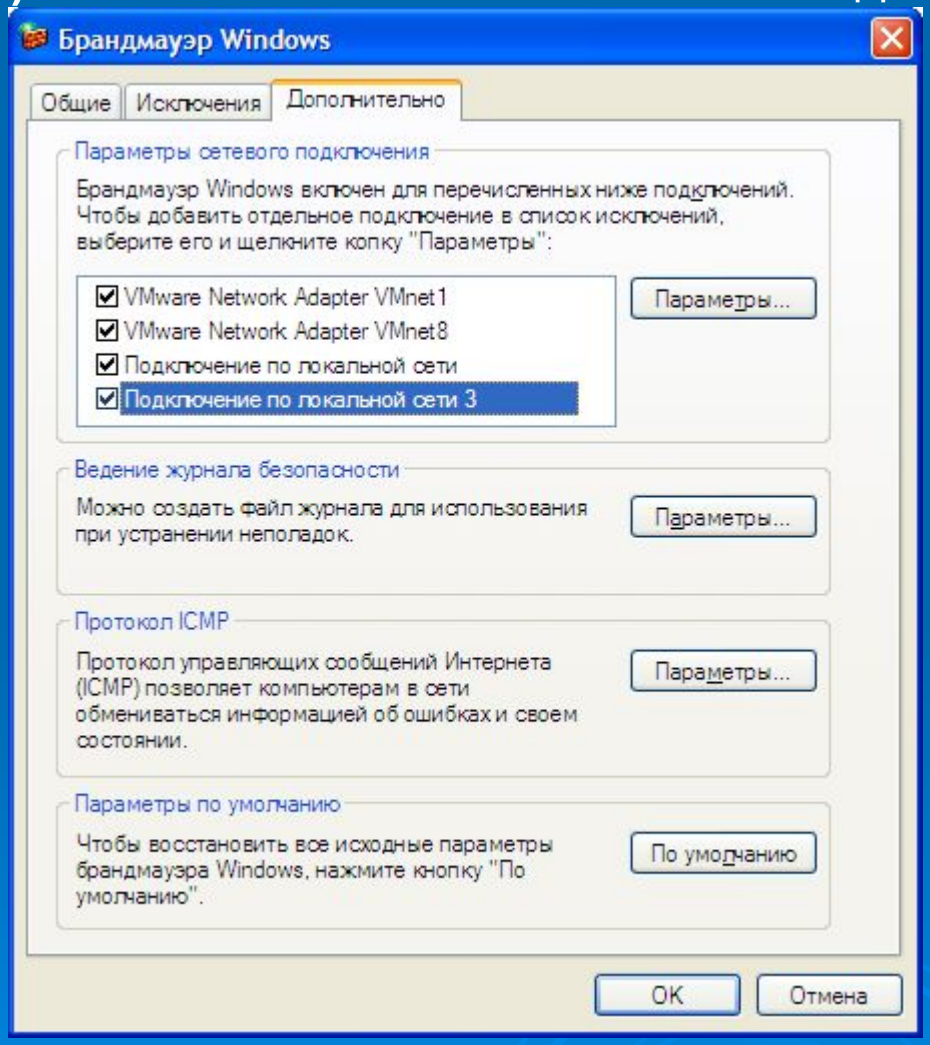



**5)** Нажмите **изменить**:



# *Пример создания исключения*

**6)** Укажите в особом списке необходимый **ip**-адрес.

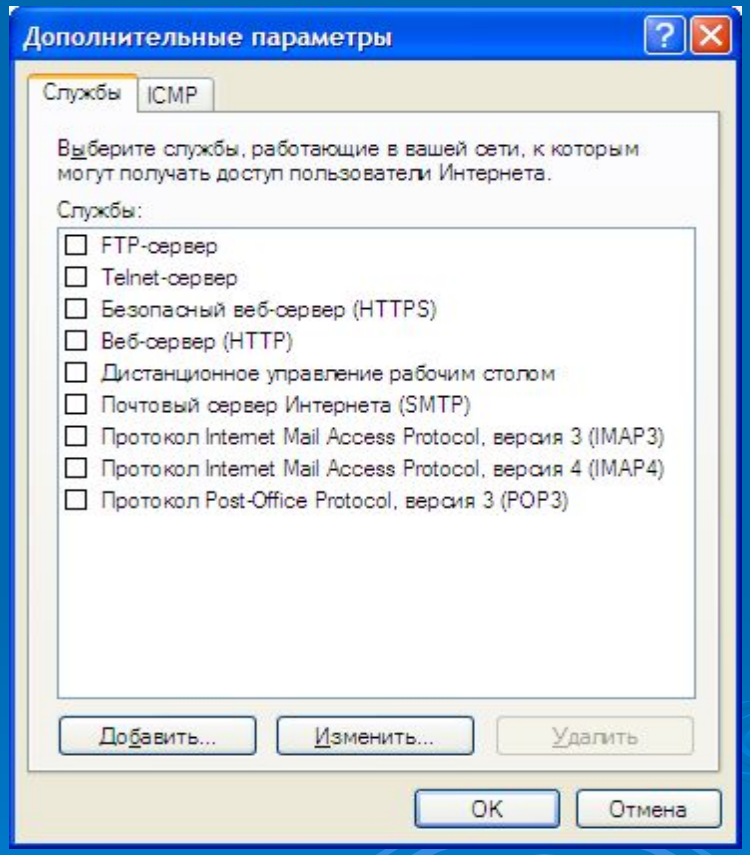



Чтобы определить правило для сетевого подключения, необходимо выбрать вкладку **Дополнительно**:

# *Пример создания исключения*

Правила можно указать или из предложенного списка, или вручную. Отличия состоят в том, что в предложенном списке вбиты порты для работы сервиса.

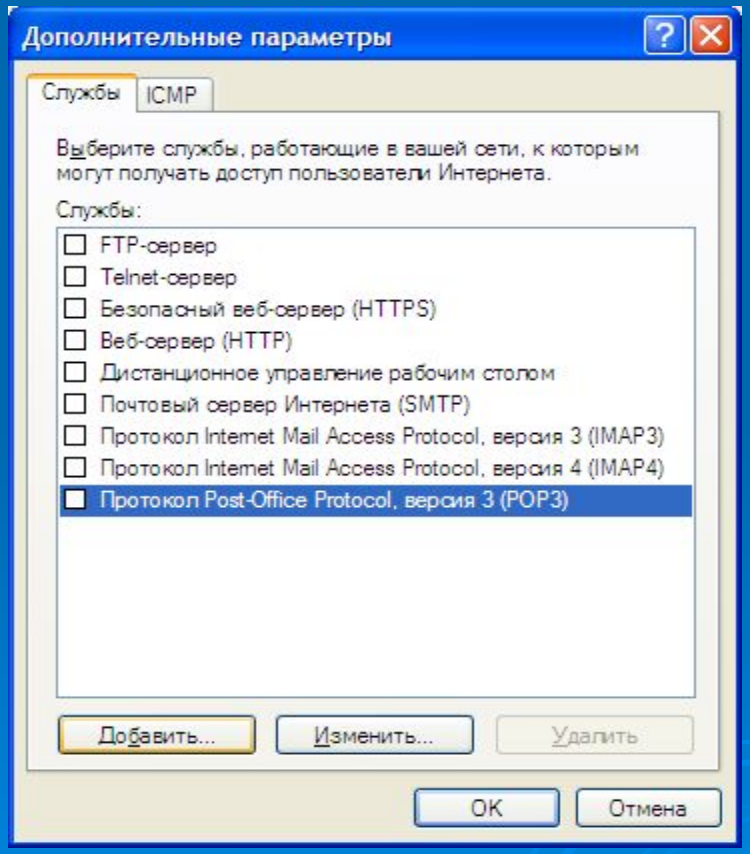
Отличия создания правила для сети от создания исключения от программы состоит в том, что при создании правила для сети нет привязки к определенной программе и порту.

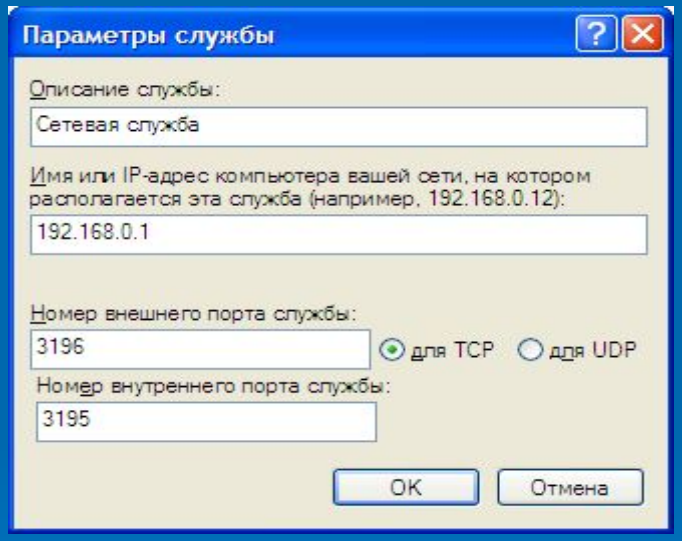


# *Пример создания исключения*

Пример создания правила для собственного сервиса с портом 3195.

В дополнительных параметрах **Добавить** указать имя **ip** и порты:

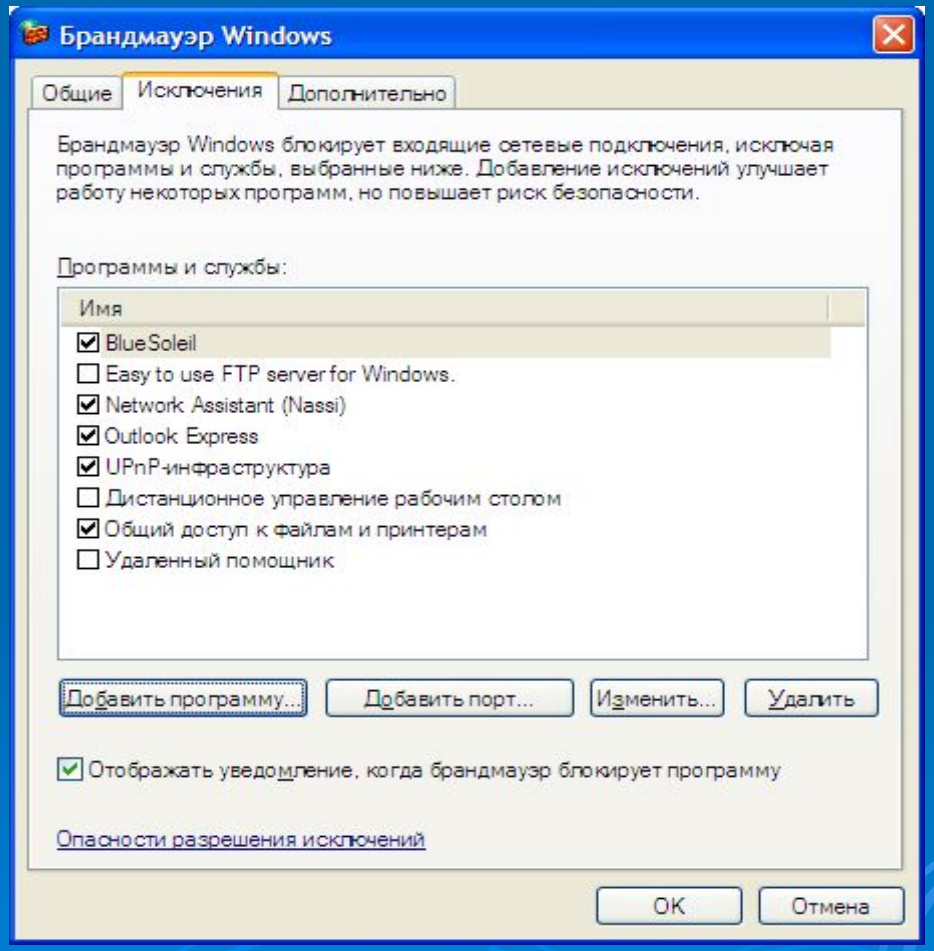



Внутренний порт будет использоваться сервером, внешний для подключения к серверу со стороны клиента.

# *Пример настройки исключения для* ***Internet Explorer***

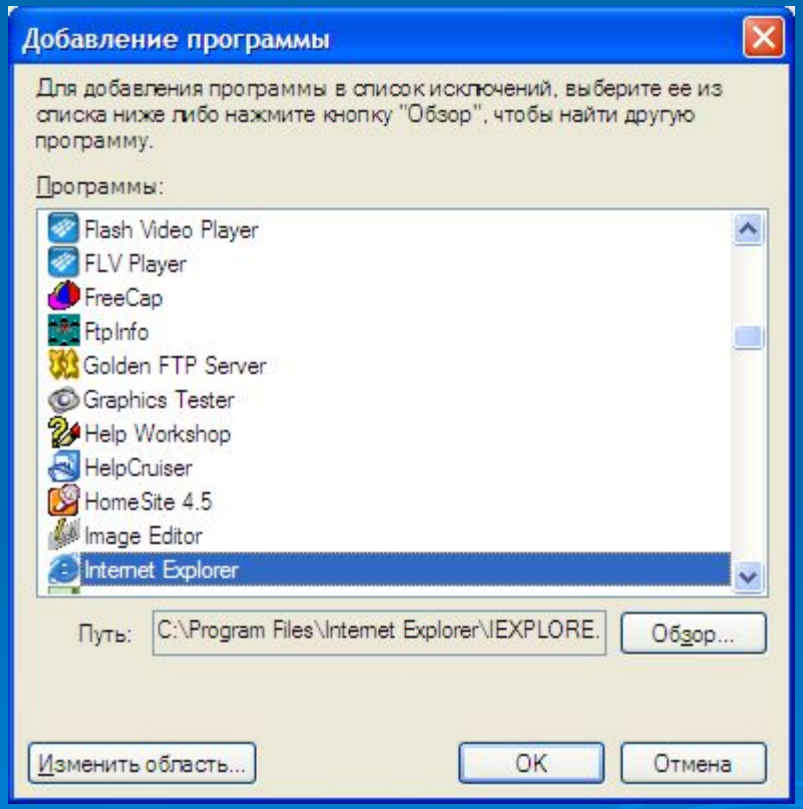
**1)** Откройте вкладку **Исключения**



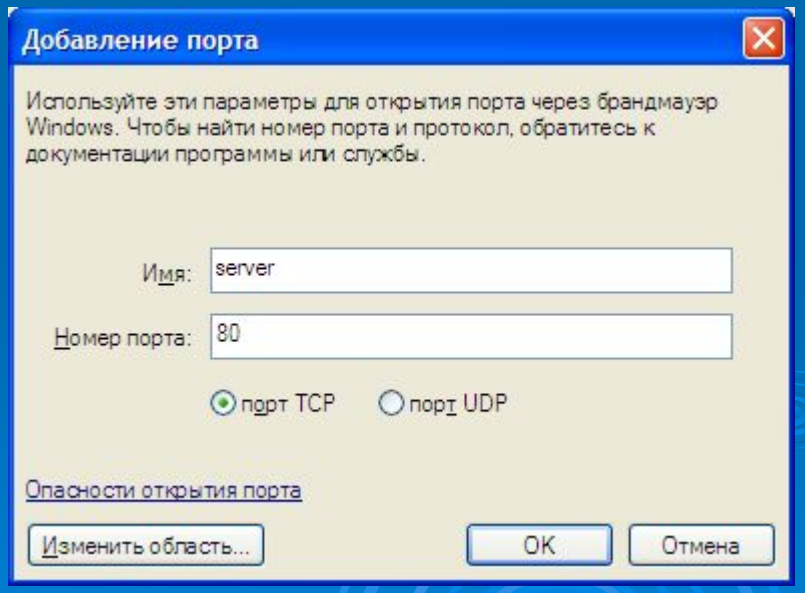
# *Пример настройки исключения для **Internet Explorer***

**2)** Нажмите **Добавить программу**.

**3)** Выберите из списка или нажать **Обзор**, указать путь.




**4)** Нажмите **Добавить порт**, указать имя и номер порта **web**-сервера.



# Практическая часть

**1).** Настройте **брандмауэр Windows** разрешив **Outlook Express** выполнять любые сетевые операции, если при этом почтовый сервер находится по **ip 185.10.24.43** и используется нестандартный порт **8494**.
**2).** Настройте **Internet Explorer** для работы через **Proxy server**, **ip** которого **192.168.0.1** и порт **8080**.
**Результат:** Выполнив работу, вы научитесь использовать брандмауэр Windows для появления возможности фильтрации трафика и повышения уровня безопасности сервера.

Выполнив работу, вы научитесь использовать брандмауэр Windows для появления возможности фильтрации трафика и повышения уровня безопасности сервера.