Практикум. Брандмауэр Windows 7.

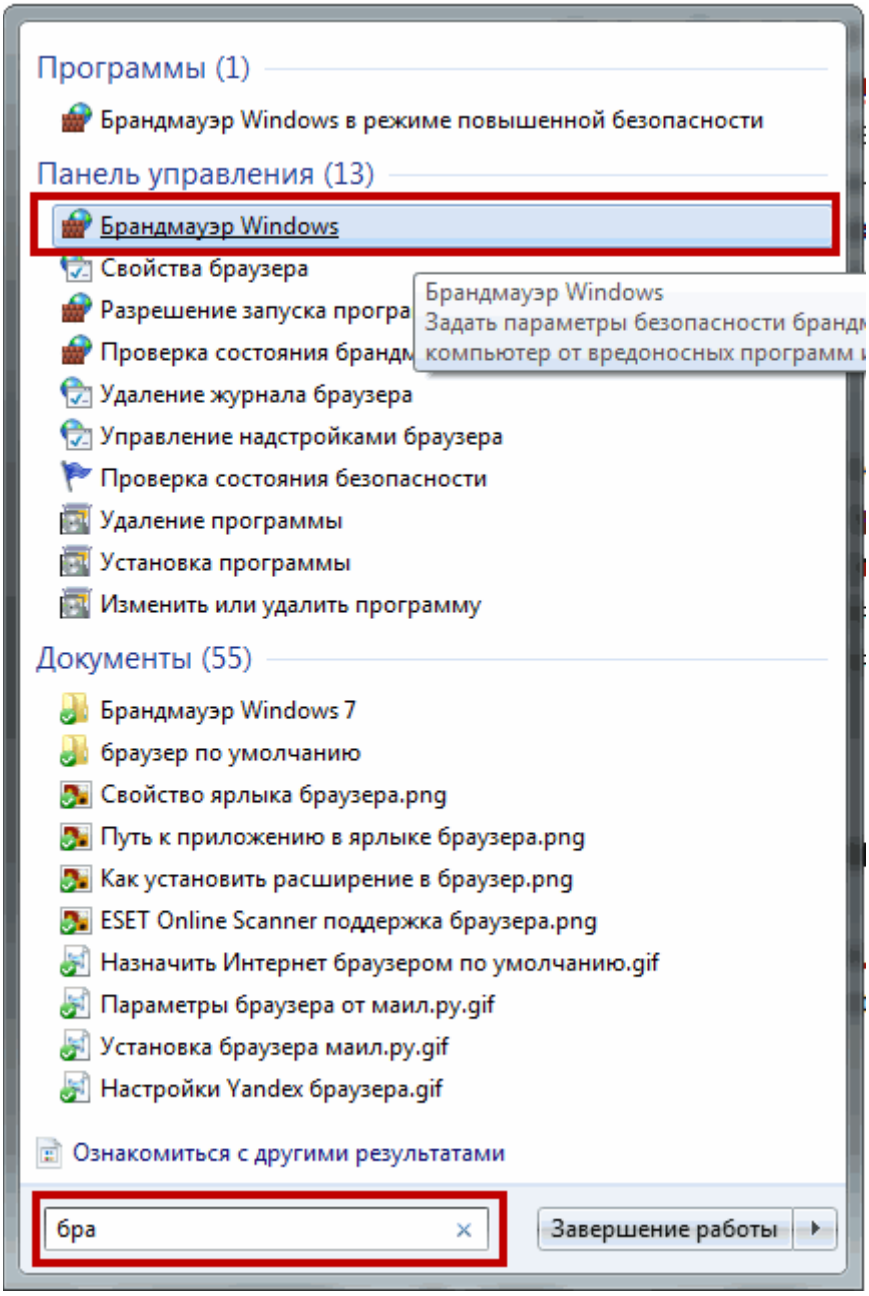
Задание

1. Включите Брандмауэр Windows 7 и настройте его для уведомления о блокировании программ.
2. Проведите настройку разрешения запуска программ. Проверьте, как это работает.
3. Проведите настройку блокирования исходящих подключений.
4. Создайте правила подключения для известных программ.
5. Создайте правила подключения для служб и гаджетов Windows.
6. Создайте разрешение для команды Ping.
7. Проверьте работу Брандмауэра с помощью программы 2ip Firewall Tester. Добавьте программу в список разрешенных программ и проверьте как она будет выполняться. Удалите программу в список разрешенных программ и проверьте как она будет выполняться. Переименуйте программу и проверьте как она будет выполняться при ее внесении в список разрешенных программ и при удалении из него.

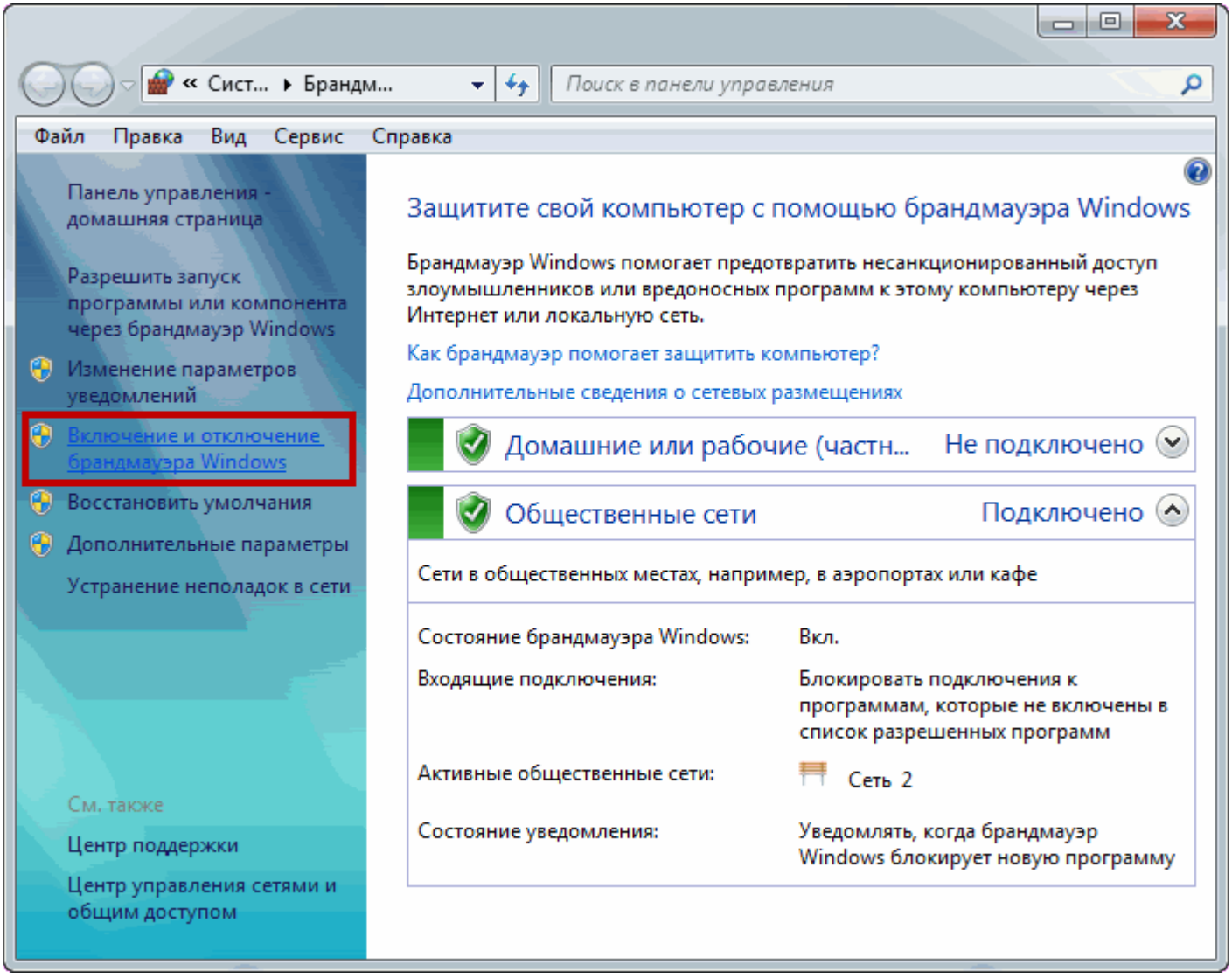
Методические указания по выполнению заданий

1. Включение и отключение брандмауэра Windows 7

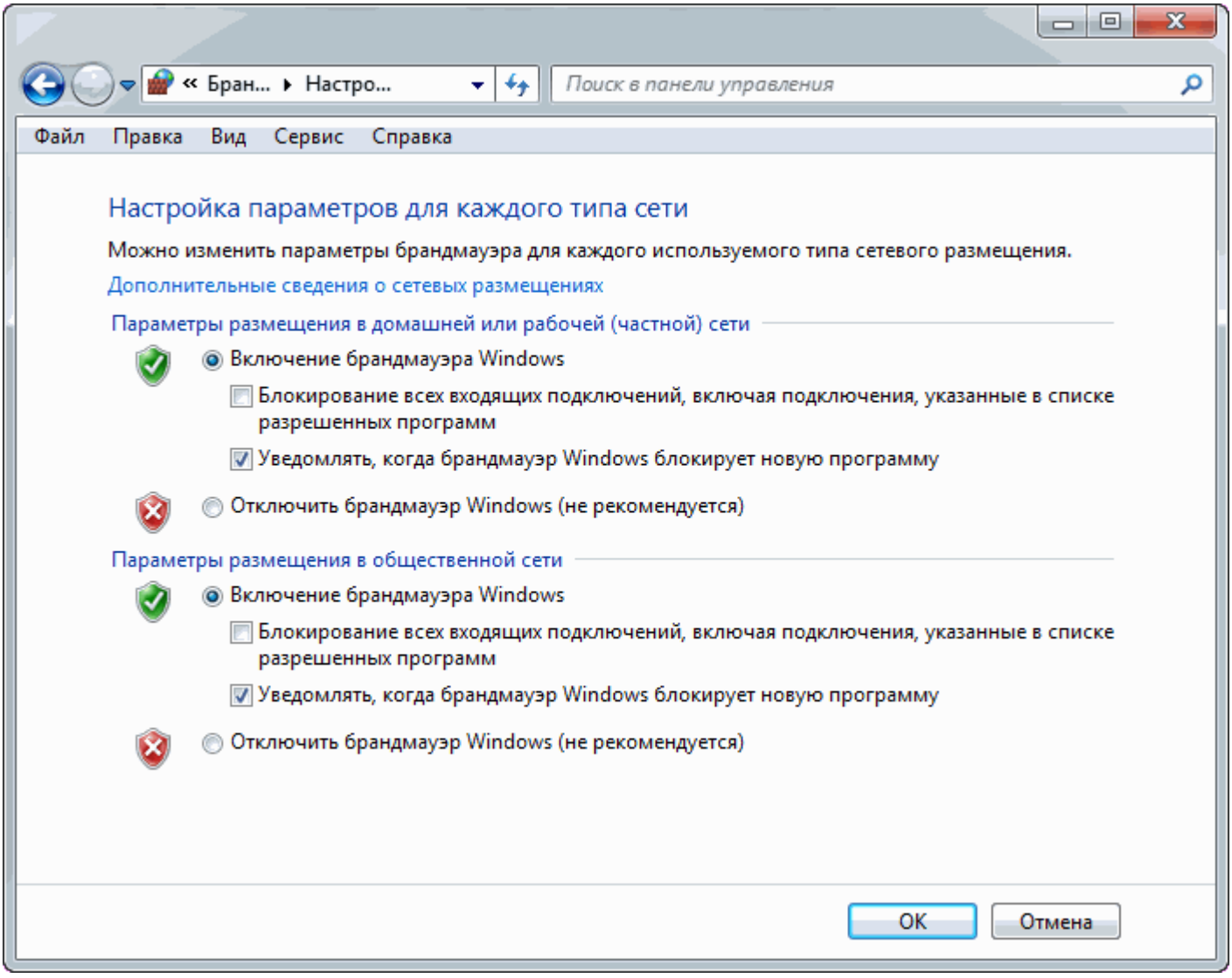
Для управления брандмауэром его необходимо открыть. Что бы его открыть нужно его найти. Воспользуется поиском Windows 7. Открываем меню Пуск и пишем «бра» и выбираем простой брандмауэр Windows



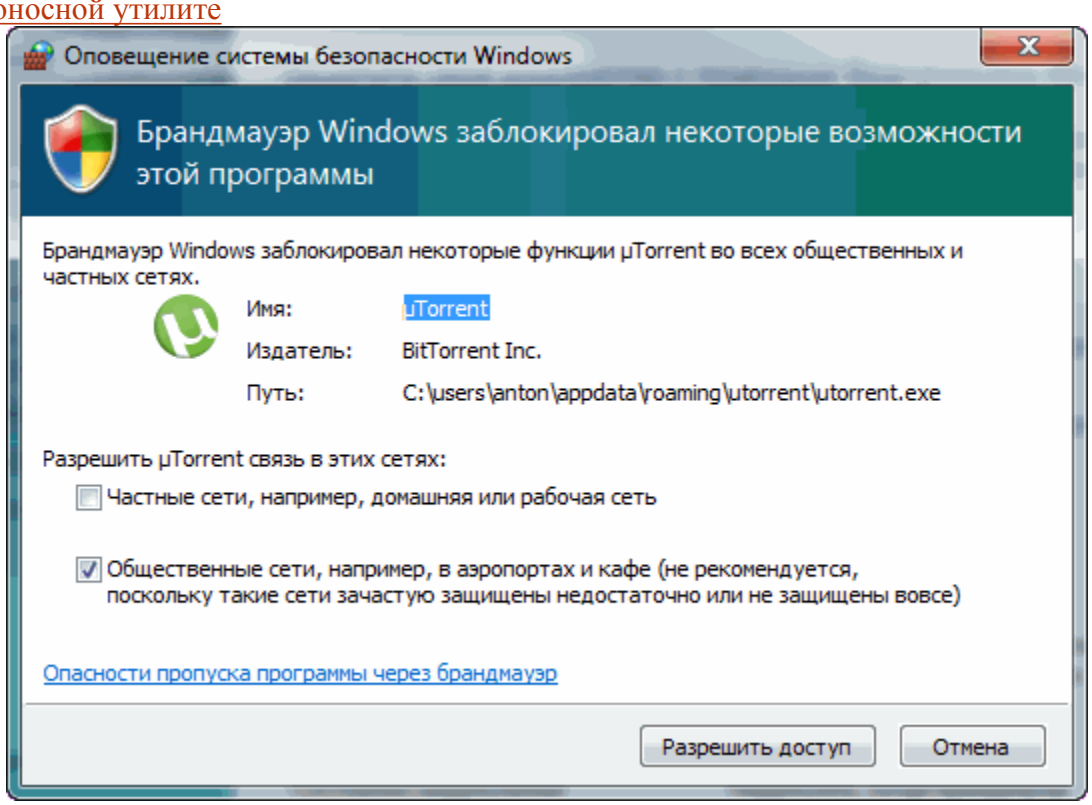
В левой части окошка выбираем Включение и отключение брандмауэра Windows



В открывшемся окошке вы можете отключить или включить брандмауэр для выбранной вами сети или для всех сразу

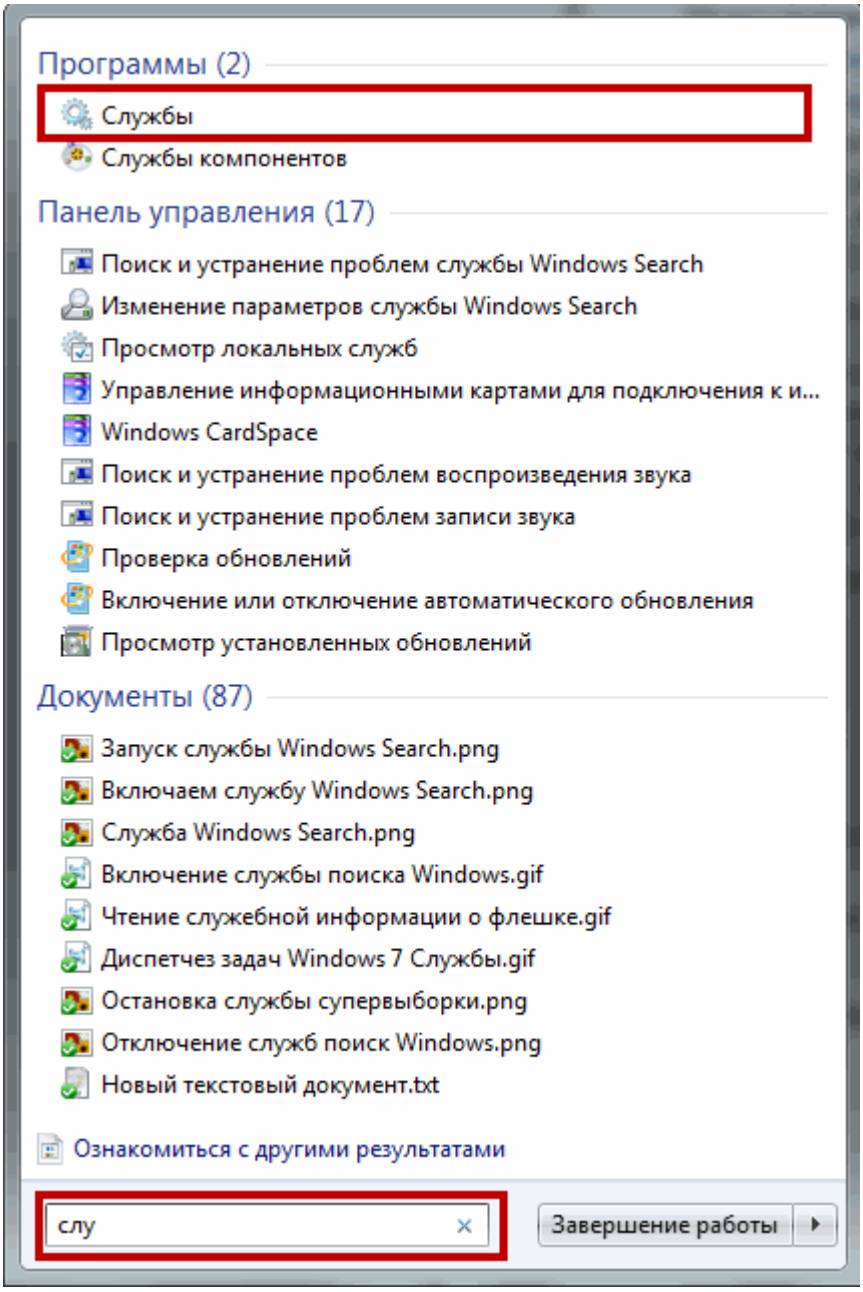


В этом окошке так же можно отключить уведомления о блокировке программы. Оповещения очень удобны так как вы можете вовремя запретить доступ к интернету неизвестной вам и скорее всего вредоносной утилите

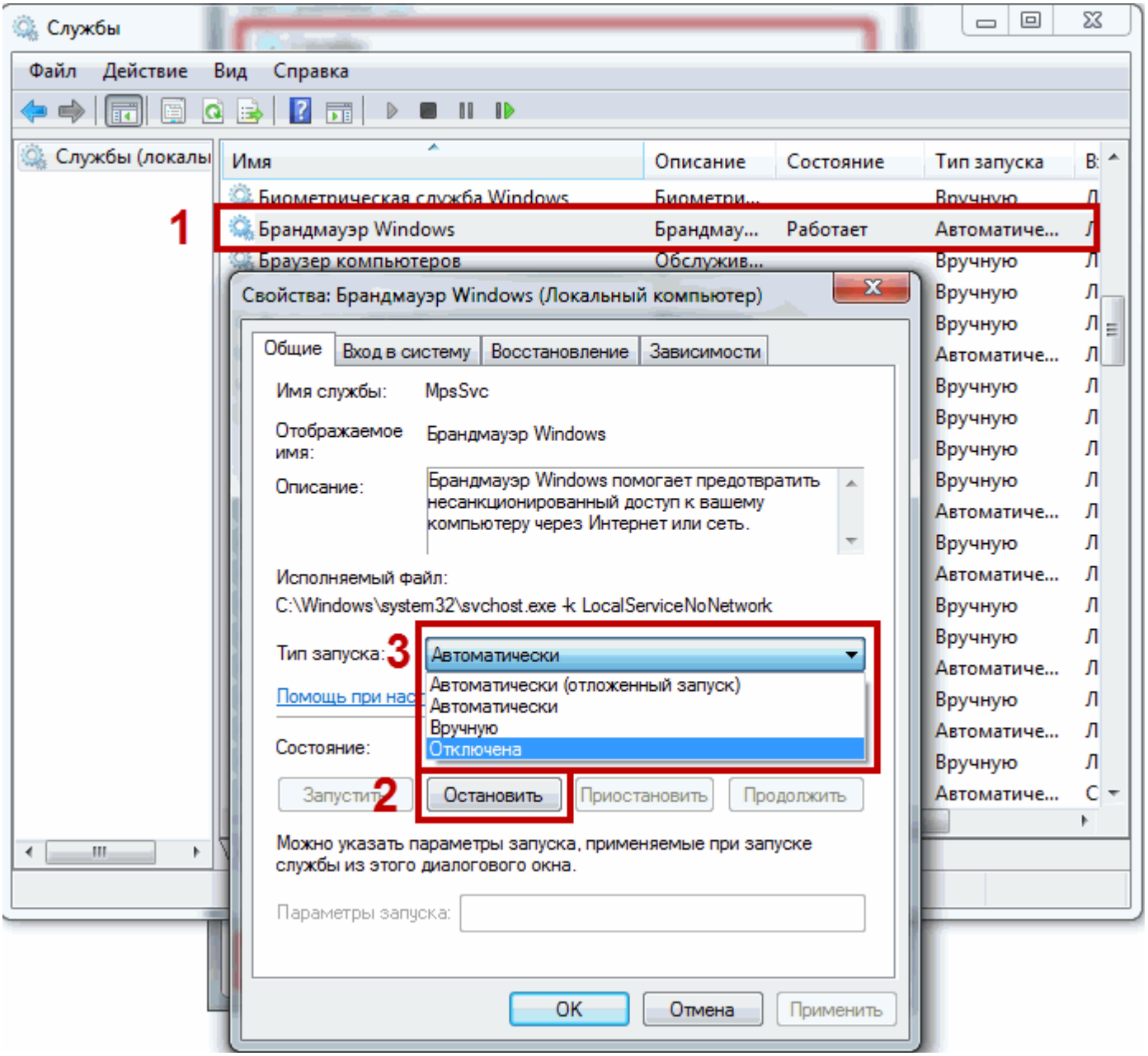


Если программу вы знаете и нужно ей дать доступ, то галочками устанавливаете в каких сетях разрешить связь и жмете Разрешить доступ. По умолчанию галочка стоит в той сети в которой вы сейчас находитесь.

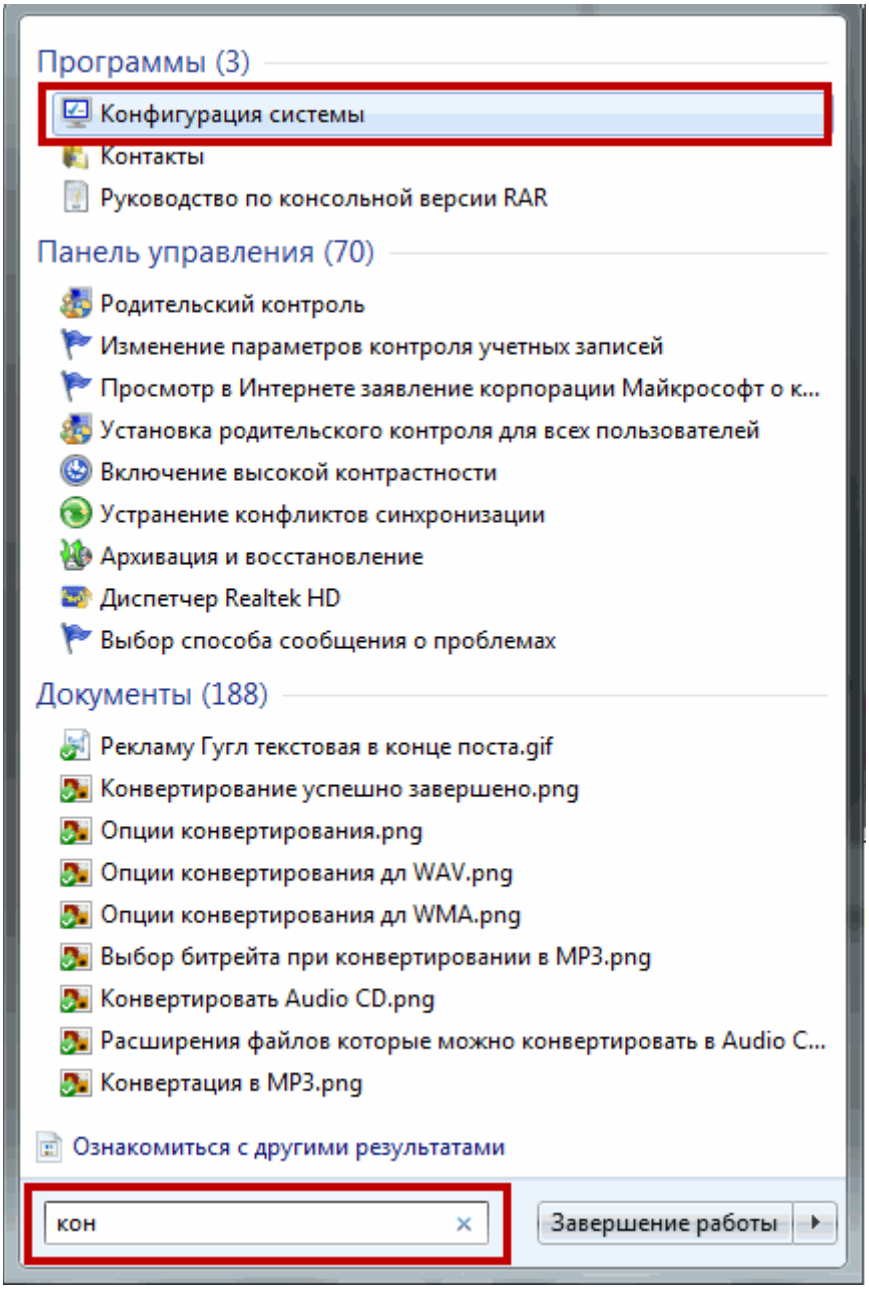
После, необходимо выключить службу Брандмауэр Windows. Воспользуемся поиском из меню Пуск



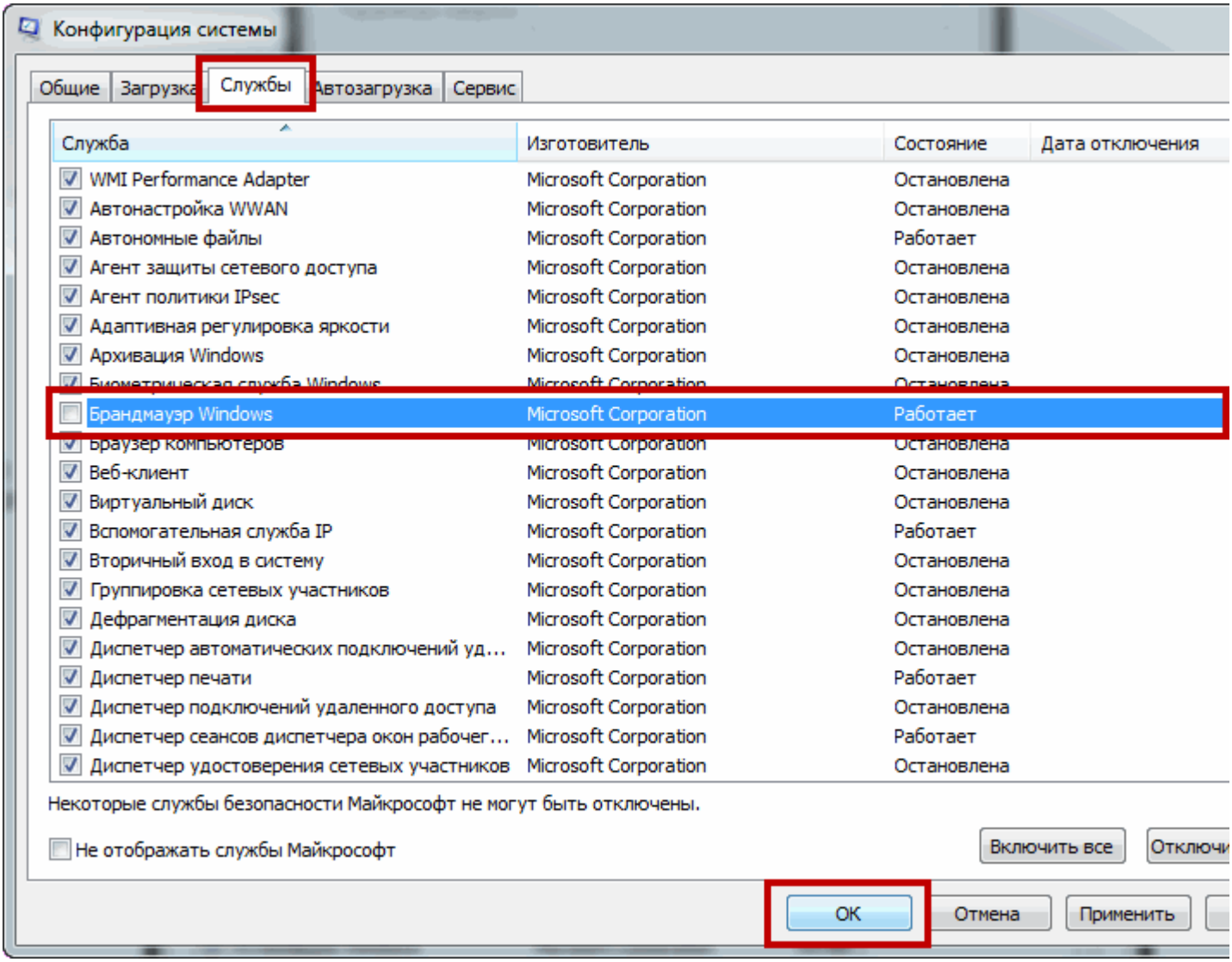
В открывшемся окошке находим службу Брандмауэр Windows и дважды кликаем по ней левой кнопкой мышки — 1. В открывшемся окошке Свойства нажимаем Остановить — 2. Затем в поле Тип запуска из выпадающего меню выбираем Отключена -3. Нажимаем ОК



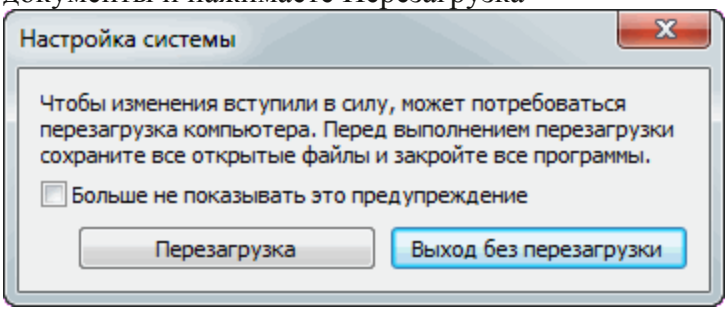
Отредактируем конфигурацию системы. Открываем Пуск и пишем «кон». Выбираем Конфигурация системы



В открывшемся окошке переходим на вкладку Службы ищем Брандмауэр Windows. Снимаем галочку и жмем ОК



Выйдет окошко с предложением перезагрузки. Закрываете все открытые программы и документы и нажимаете Перезагрузка

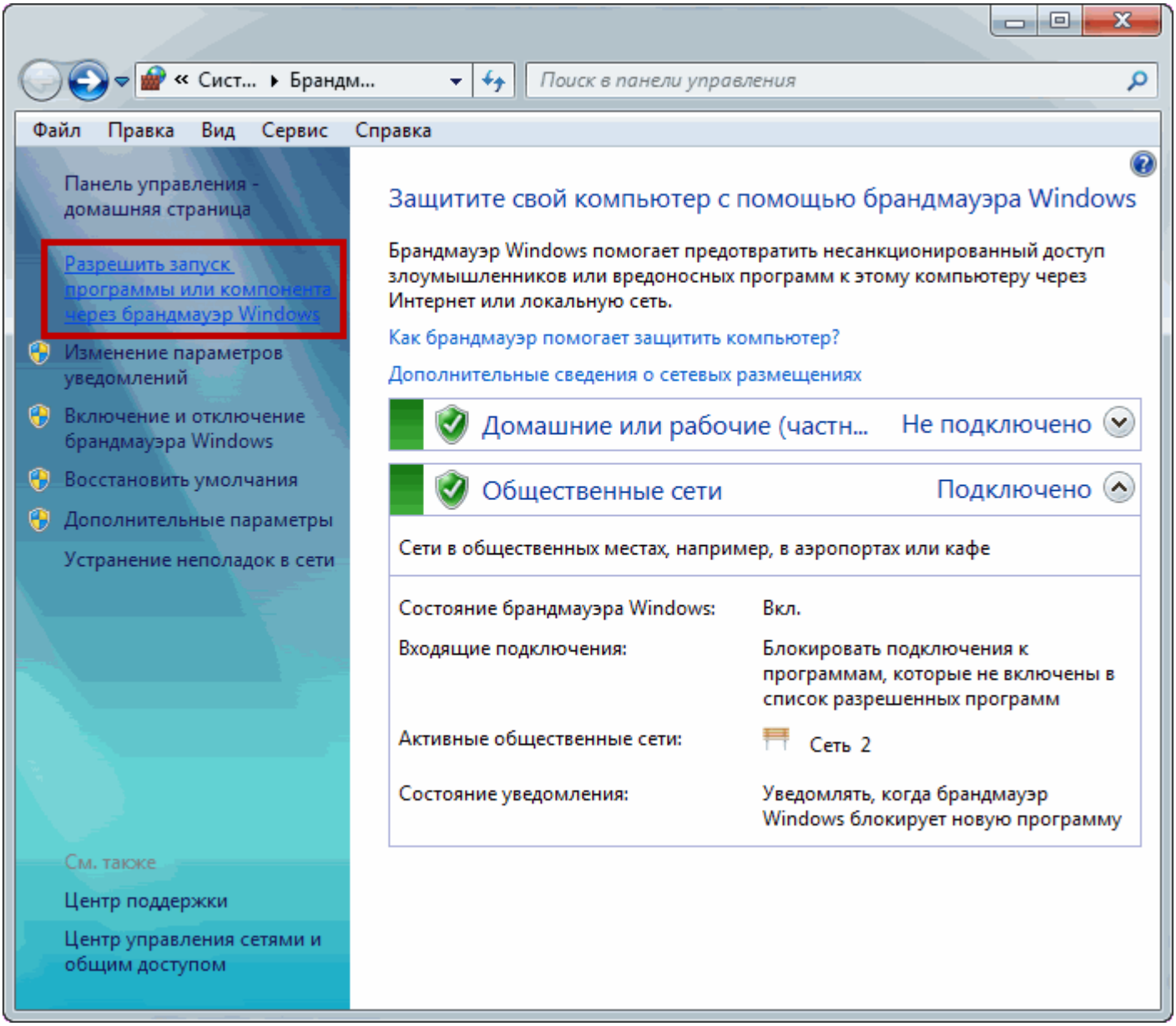


Брандмауэр Windows 7 отключен.

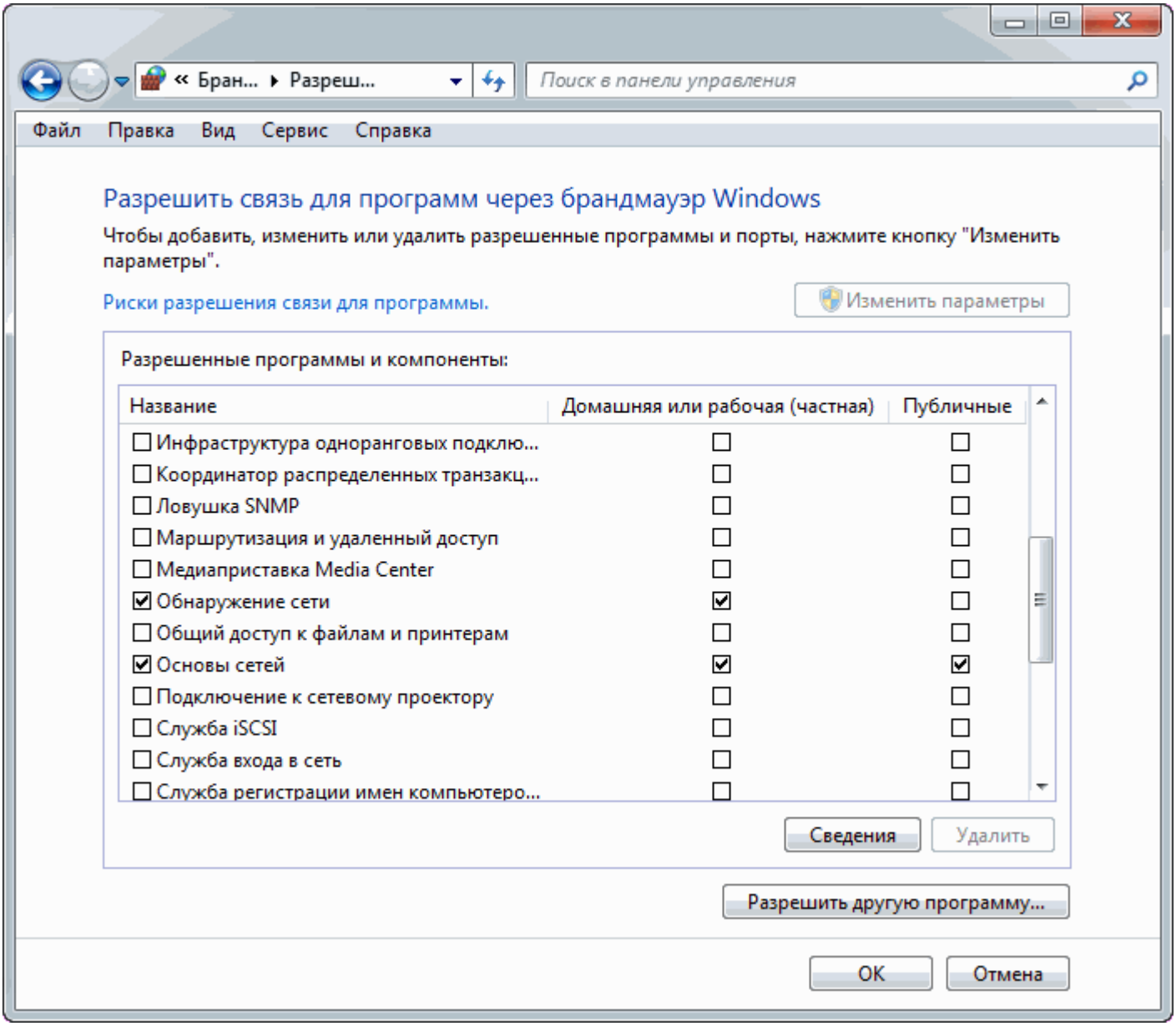
Для включения необходимо повторить все действия в обратной последовательности.

2. Разрешенные программы и сброс настроек

Если брандмауэр заблокировал какую-то программу (у меня такого наверное не было никогда), то можно, не влезая в расширенные настройки, дать доступ в выбранной сети (общественной или частной). Для этого в окошке фаервола выбираем Разрешить запуск программ или компонентов через брандмауэр Windows



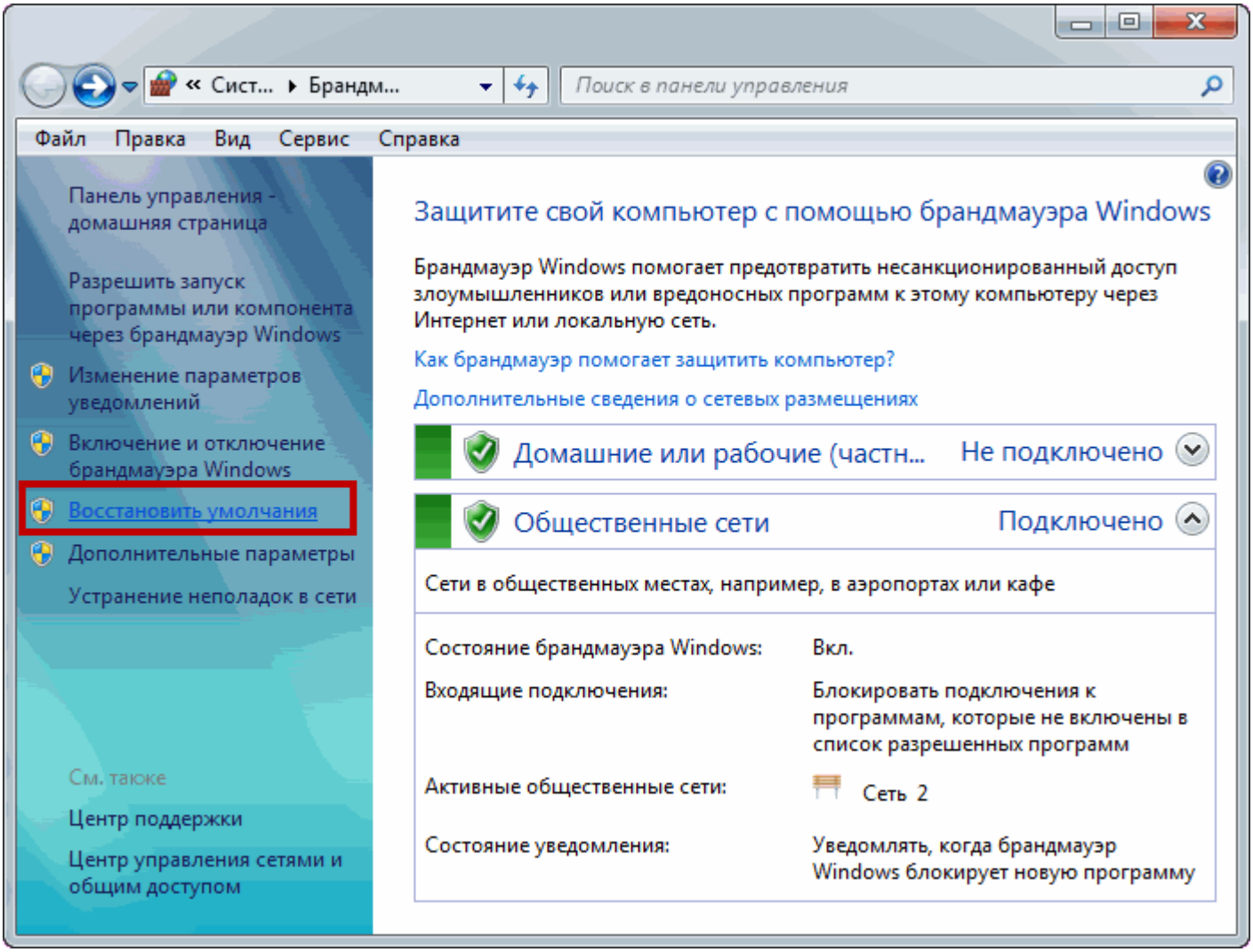
В открывшемся окошке вы можете галочками поставленными в в столбиках Домашняя или рабочая и Публичная разрешить программе соединение через брандмауэр в соответствующей сети



Если нужной вам программы не оказалось, то с помощью кнопки Разрешить другую программу… можно легко ее добавить.

Запретить же какой-либо программе выход в интернет здесь не получиться. (По крайней мере у меня не получилось. Снимал галочки для программы µTorrent все равно качает).

В окошке для разрешения программ можно экспериментировать и не волноваться что у браузера не будет доступа в интернет (мой случай). Все можно вернуть назад с помощью функции Восстановить умолчания

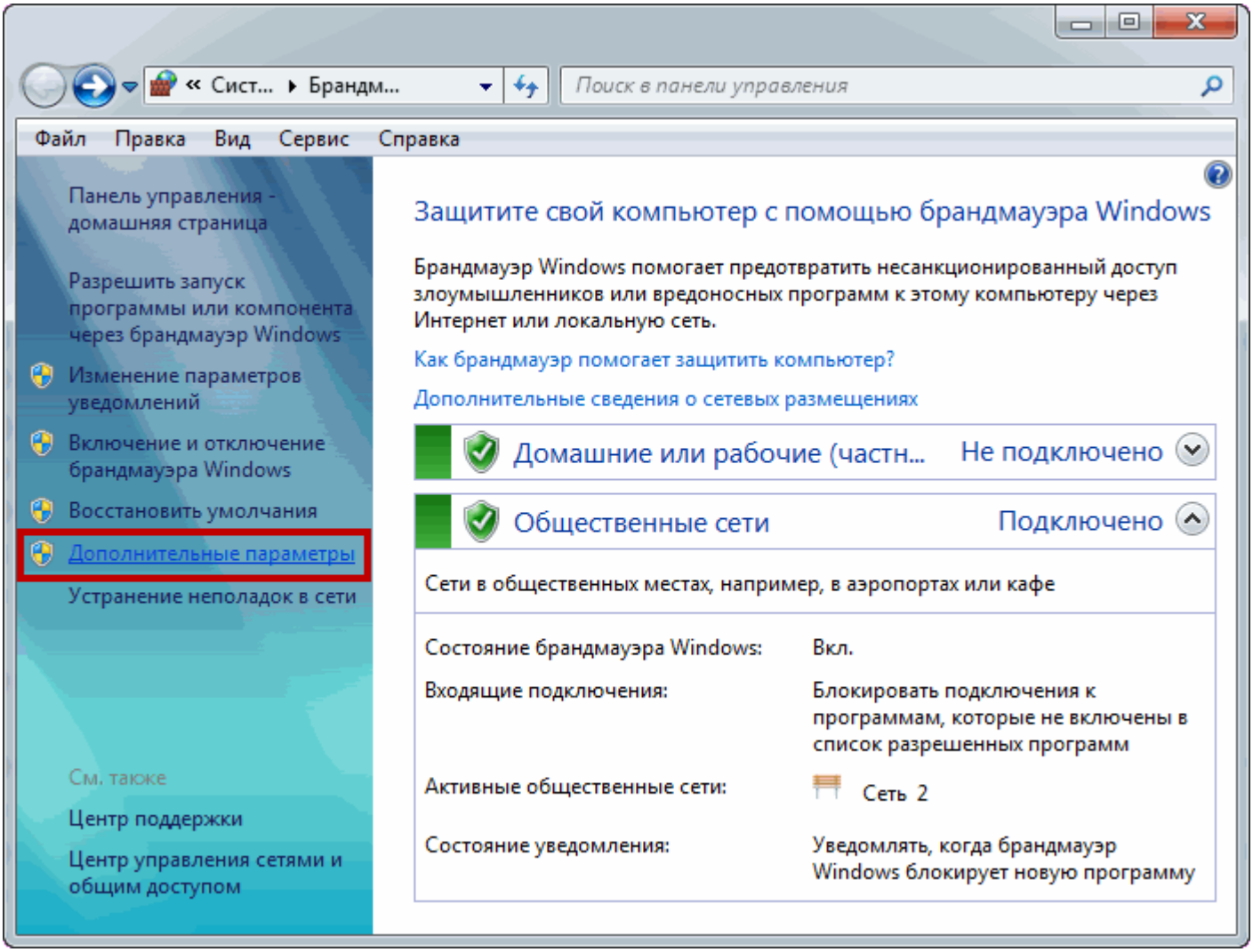


По умолчанию все должно работать исправно.

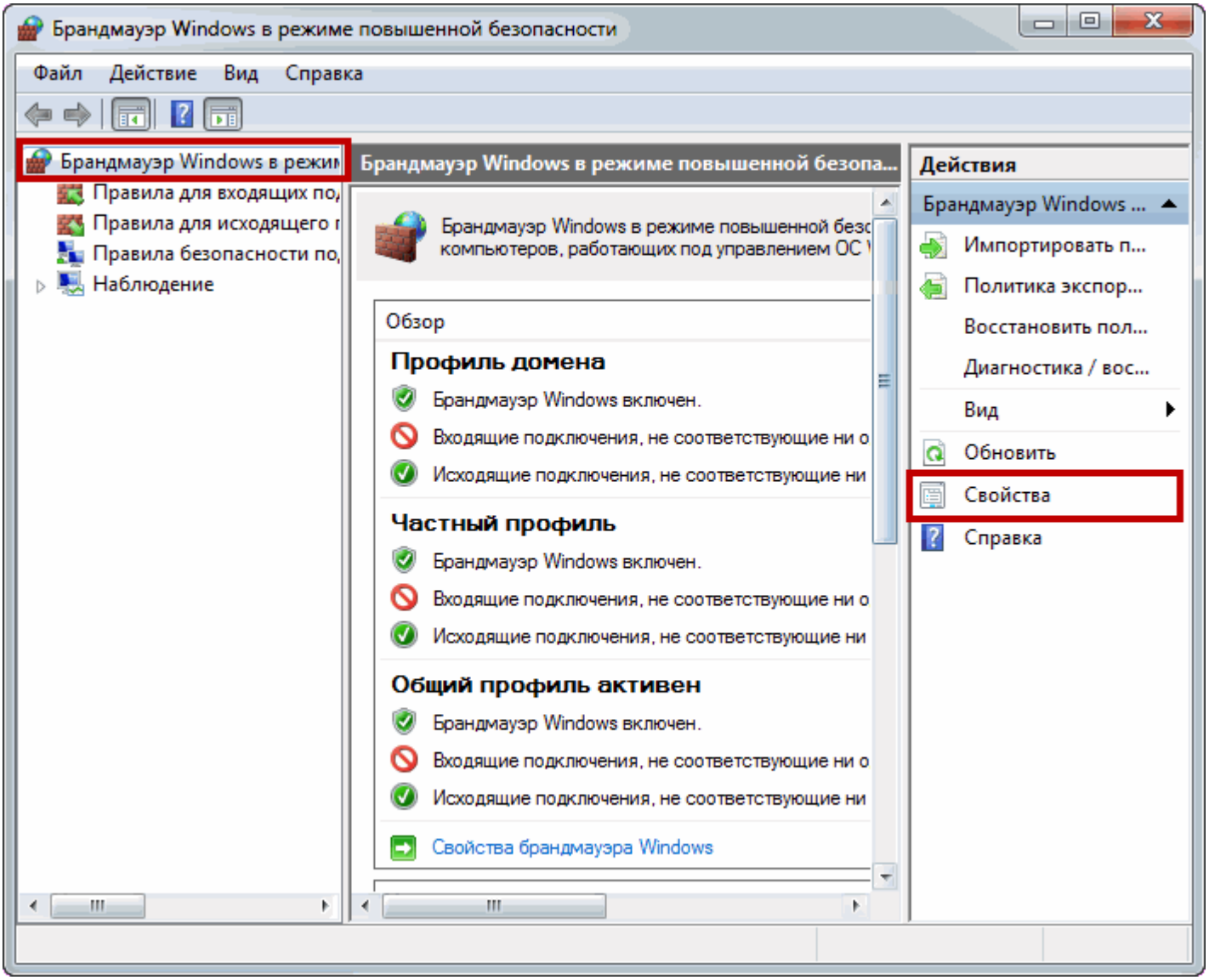
3. Блокирование исходящего трафика

Если мы хотим добиться большей безопасности, то одним из возможных вариантов будет блокировка исходящего трафика полностью и задание разрешений для нужных нам программ и служб. Здесь нужно отметить, что исходящим подключением считается то, которое было инициировано программой вашего компьютера. То есть если ваш браузер запрашивает какую-либо страницу в интернете и эта страница пересылается к вам в компьютер — это все исходящее подключение.

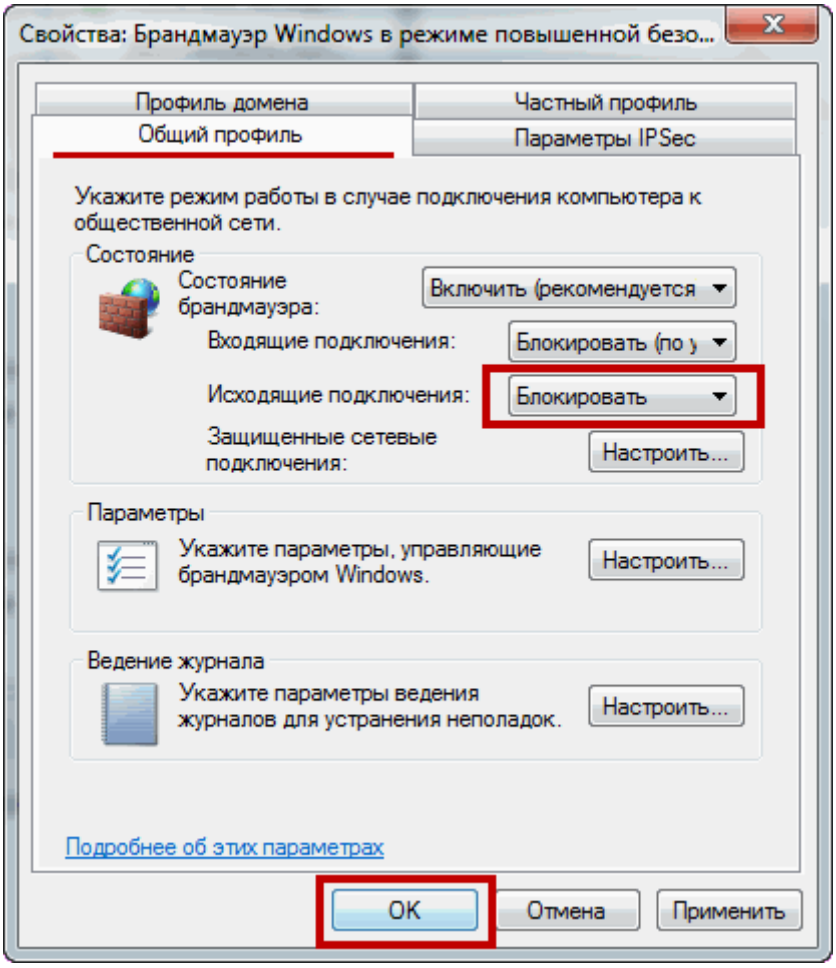
Для этого необходимо выбрать Дополнительные параметры в окошке Брандмауэра.



Для того что бы заблокировать все исходящие подключения нужно в левой колонке выбрать Брандмауэр Windows в режиме повышенной безопасности и в правой колонке нажать Свойства



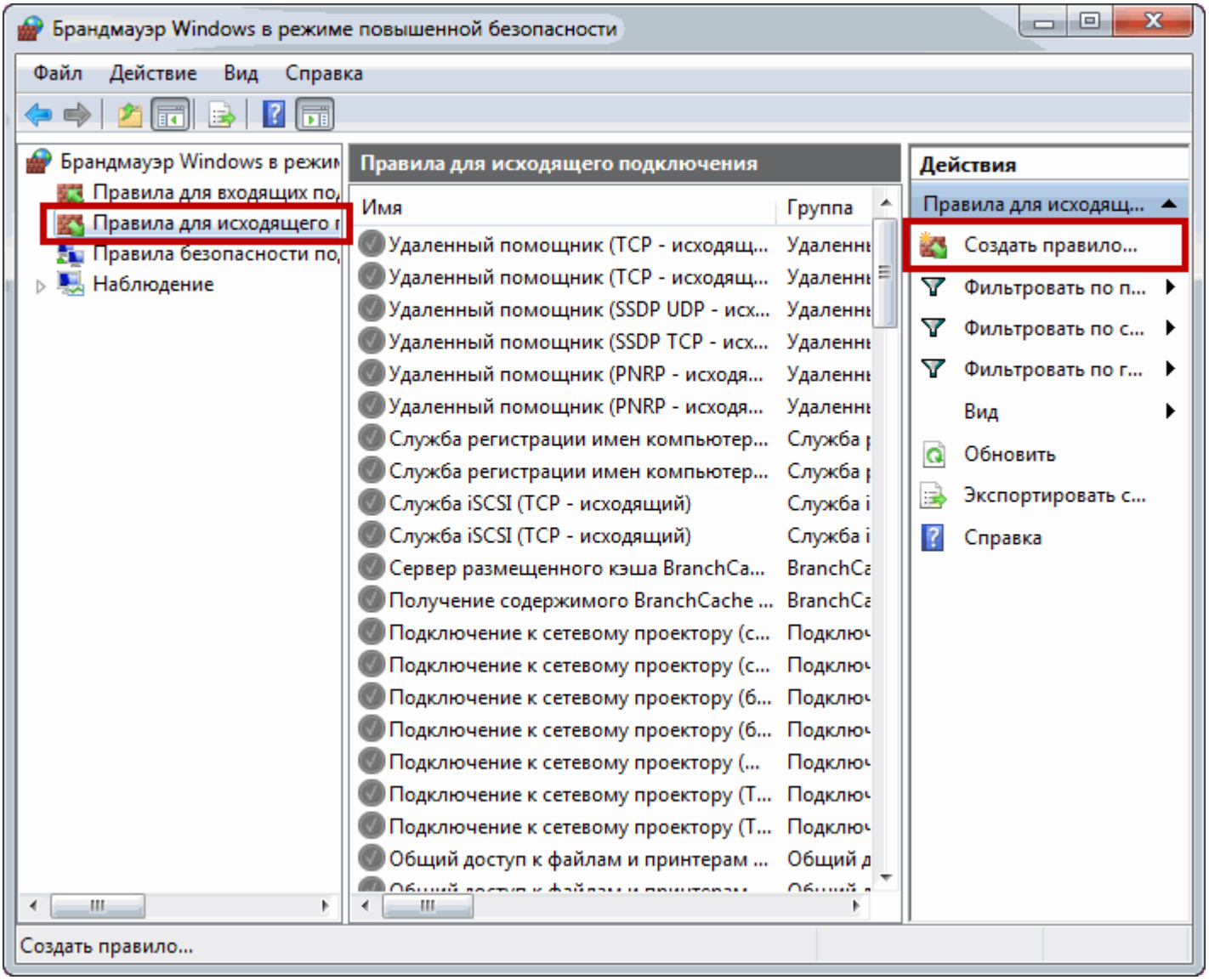
В открывшемся окошке переходите на вкладку с настройками нужной сети (общественная сеть — общий профиль, домашняя сеть — частный профиль). В разделе Исходящие подключение из выпадающего меню выбираете Блокировать. Нажимаете ОК или Применить



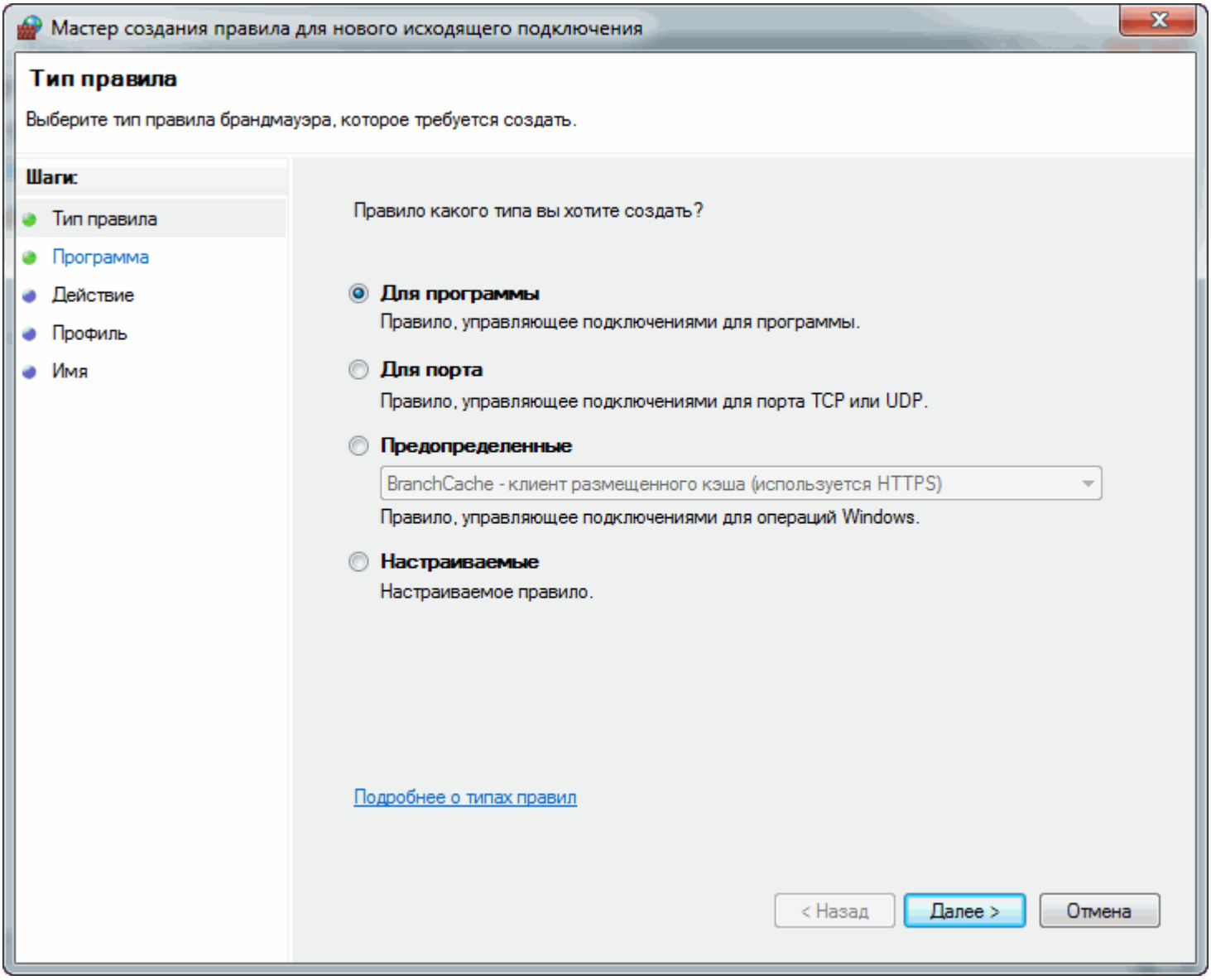
Для большей безопасности можно заблокировать исходящие подключения в обеих сетях.

4. Разрешение для программ

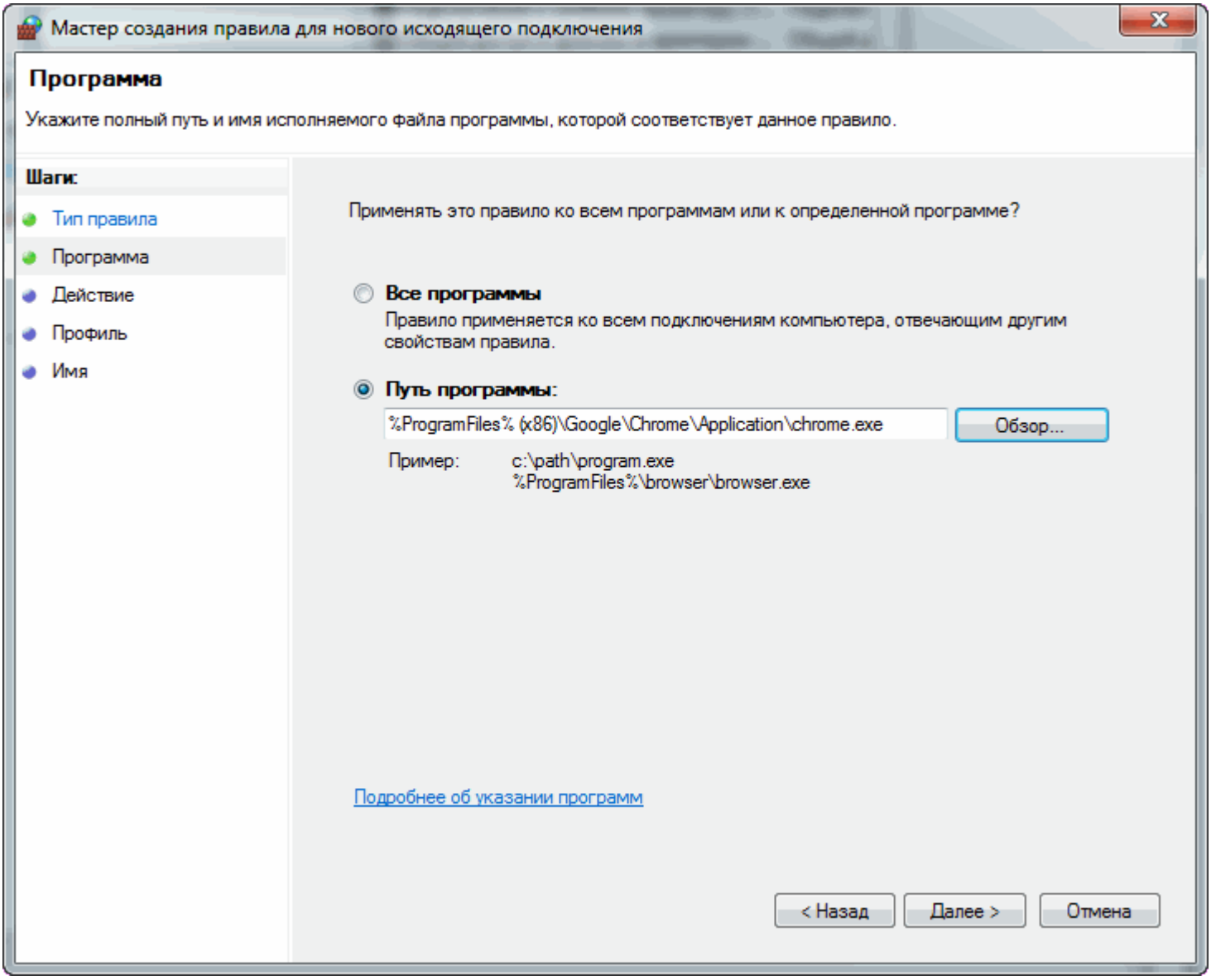
После блокировки исходящих подключений необходимо дать доступ в интернет тем программам которыми пользуемся. Например браузеру Google Chrome. Для этого переходим в левой части на Правила для исходящего подключения и в колонке Действия справа нажимаем Создать правило…



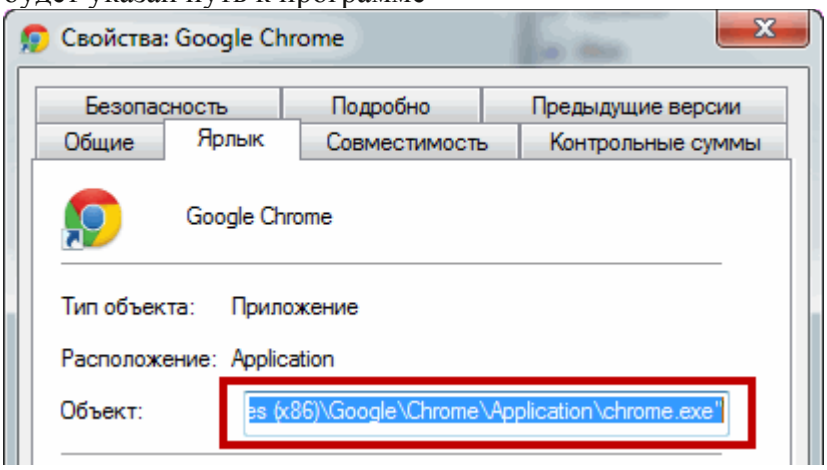
В открывшемся мастере выбираем Для программы. Жмем Далее >



С помощью кнопки Обзор… указываем путь к нашей программе. (На примере браузера Google Chrome)



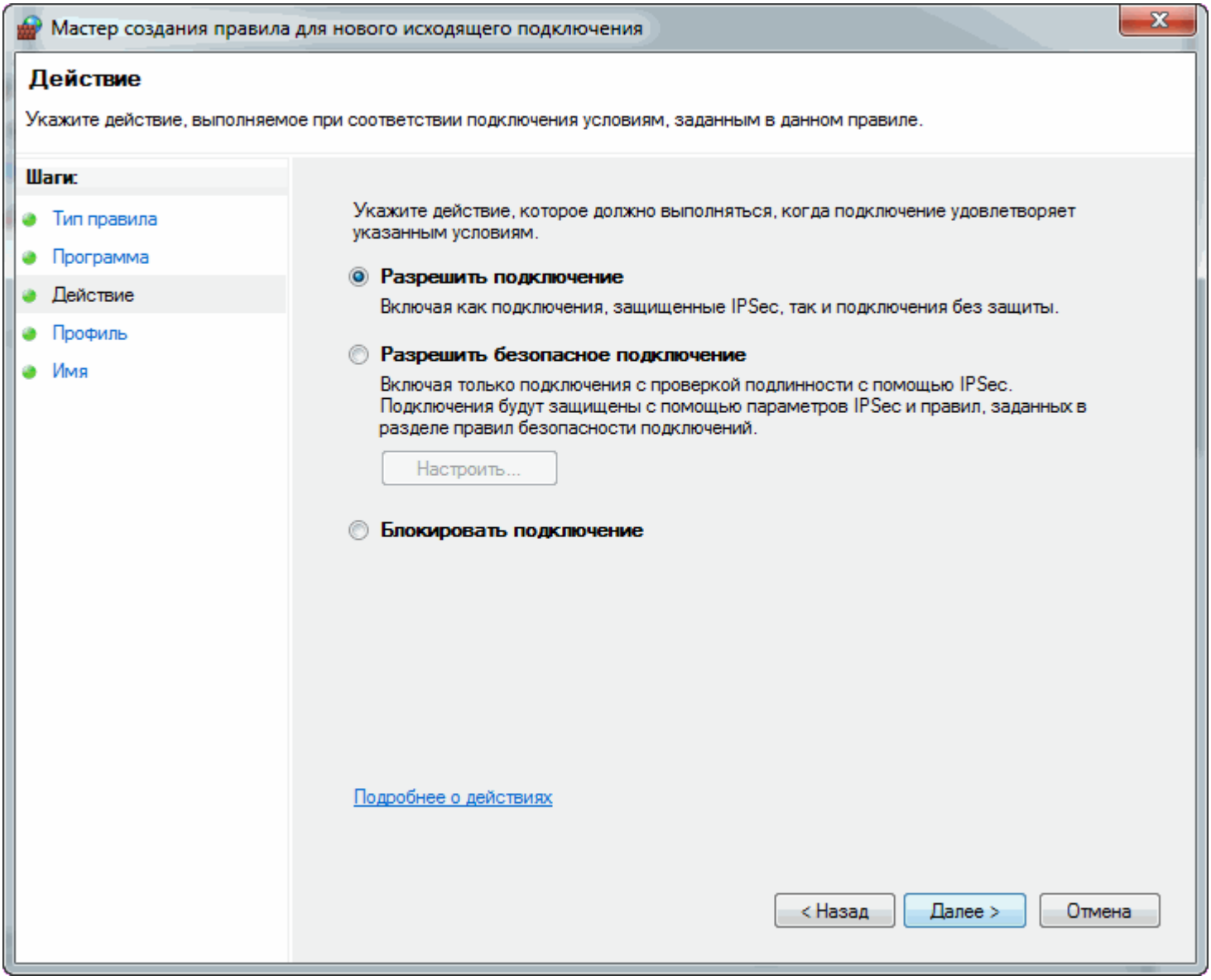
Если не знаете где установочный файл программы можно воспользоваться поиском в Windows 7 или нажать правой кнопкой на ярлыке программы и выбрать Свойства. В разделе Объект будет указан путь к программе



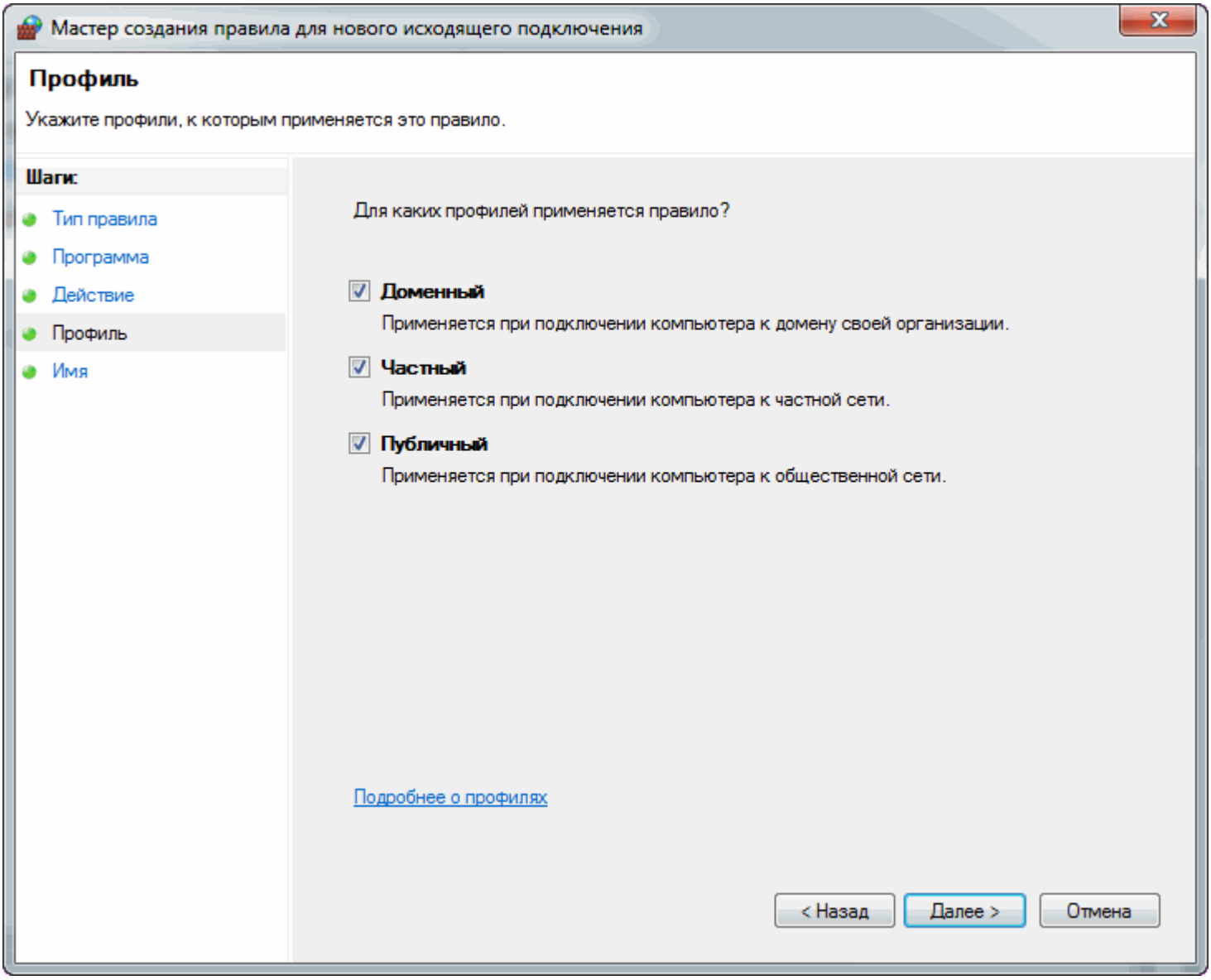
Можно его скопировать и вставить в мастер создания правила, только убрать кавычки при необходимости.

Указав путь к программе нажимаем Далее >

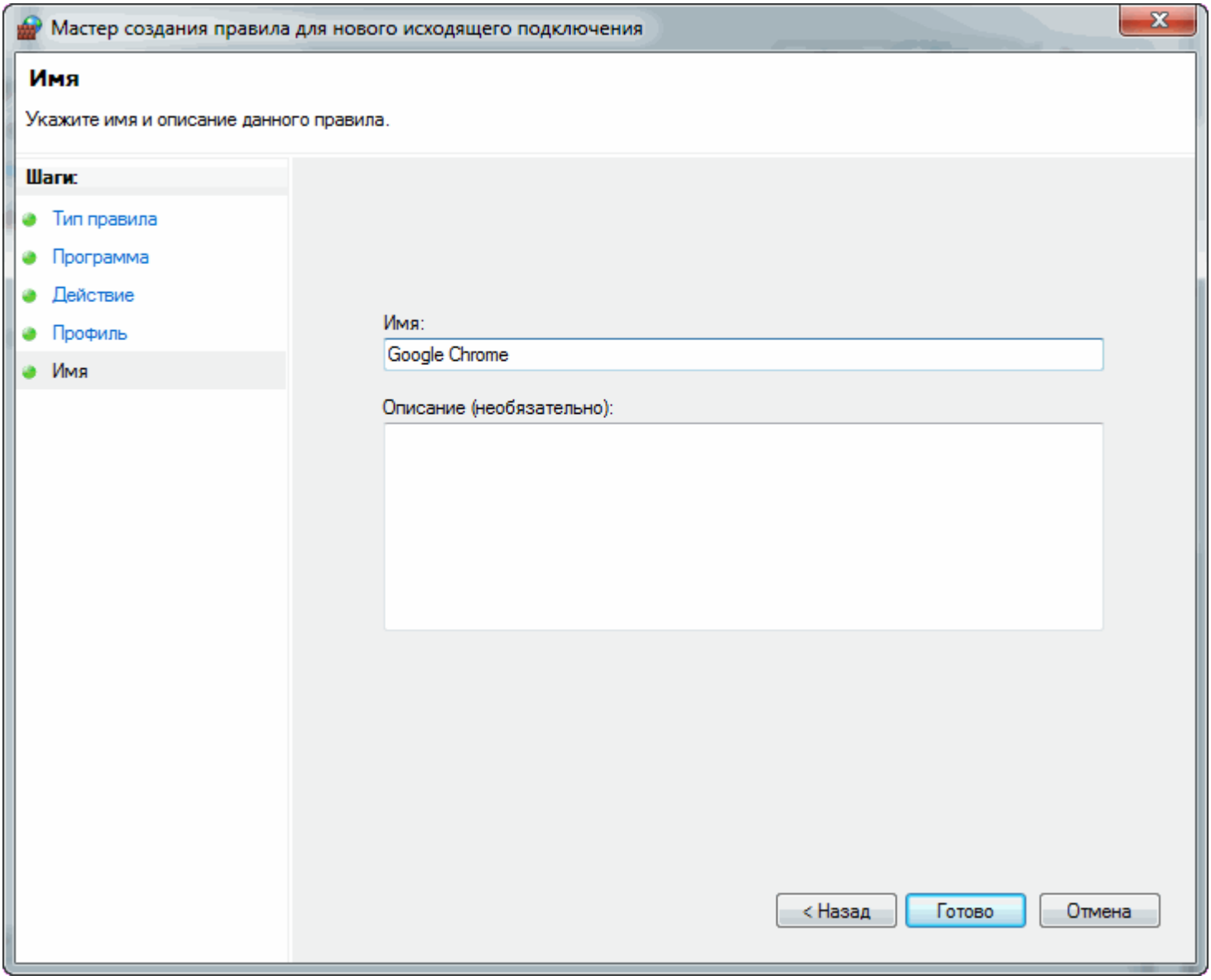
На следующем шаге выбираем Разрешить подключение и Далее >



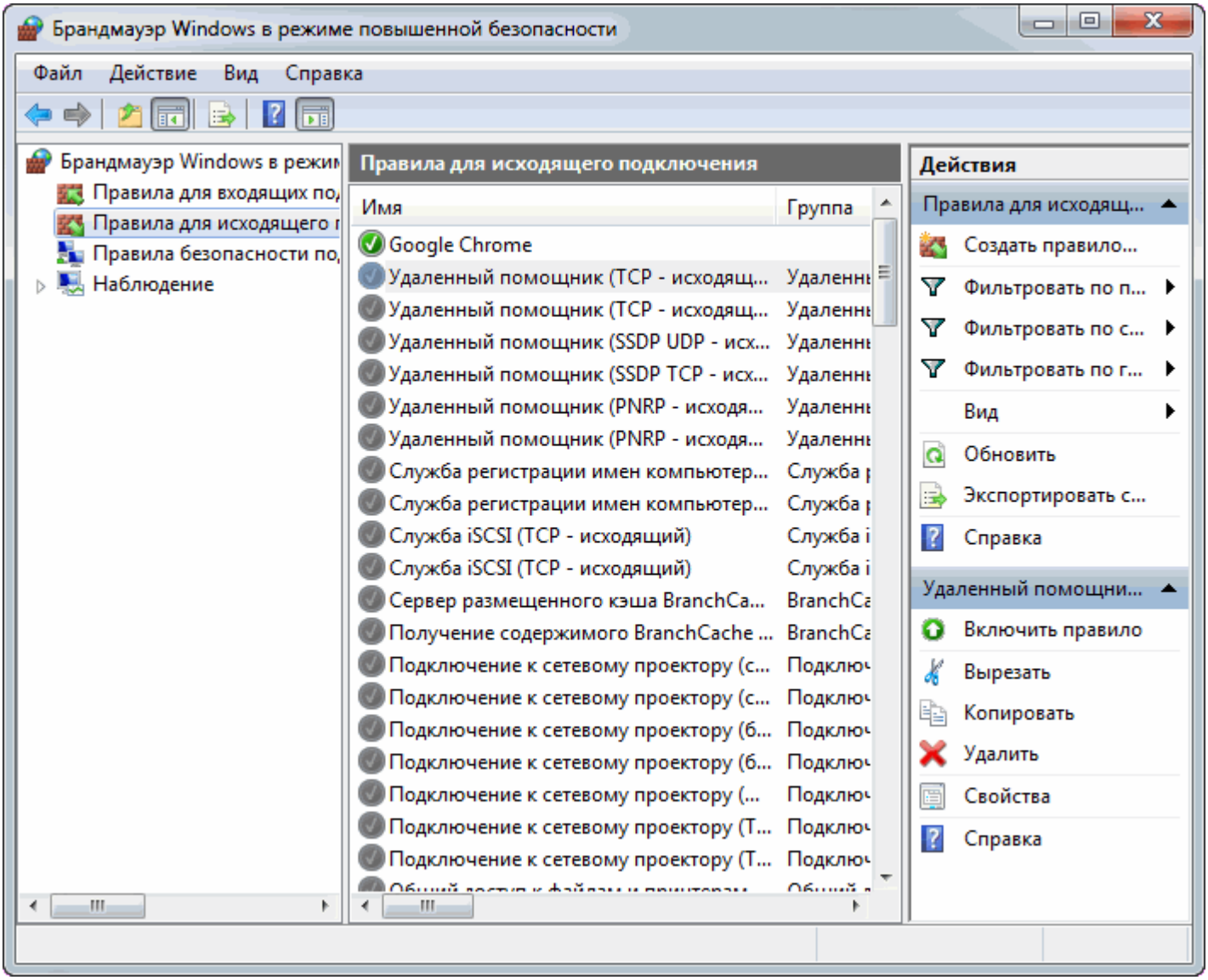
Указываем профили или сети в которых будет действовать создаваемое правило. Применяем правило для всех профилей и жмем Далее >



На следующем шаге задаем имя и при необходимости описание правила. Нажимаем Готово



Правило создано и работает (отмечено зеленой галочкой)



Теперь мы можем в Google Chrome выходить в интернет.

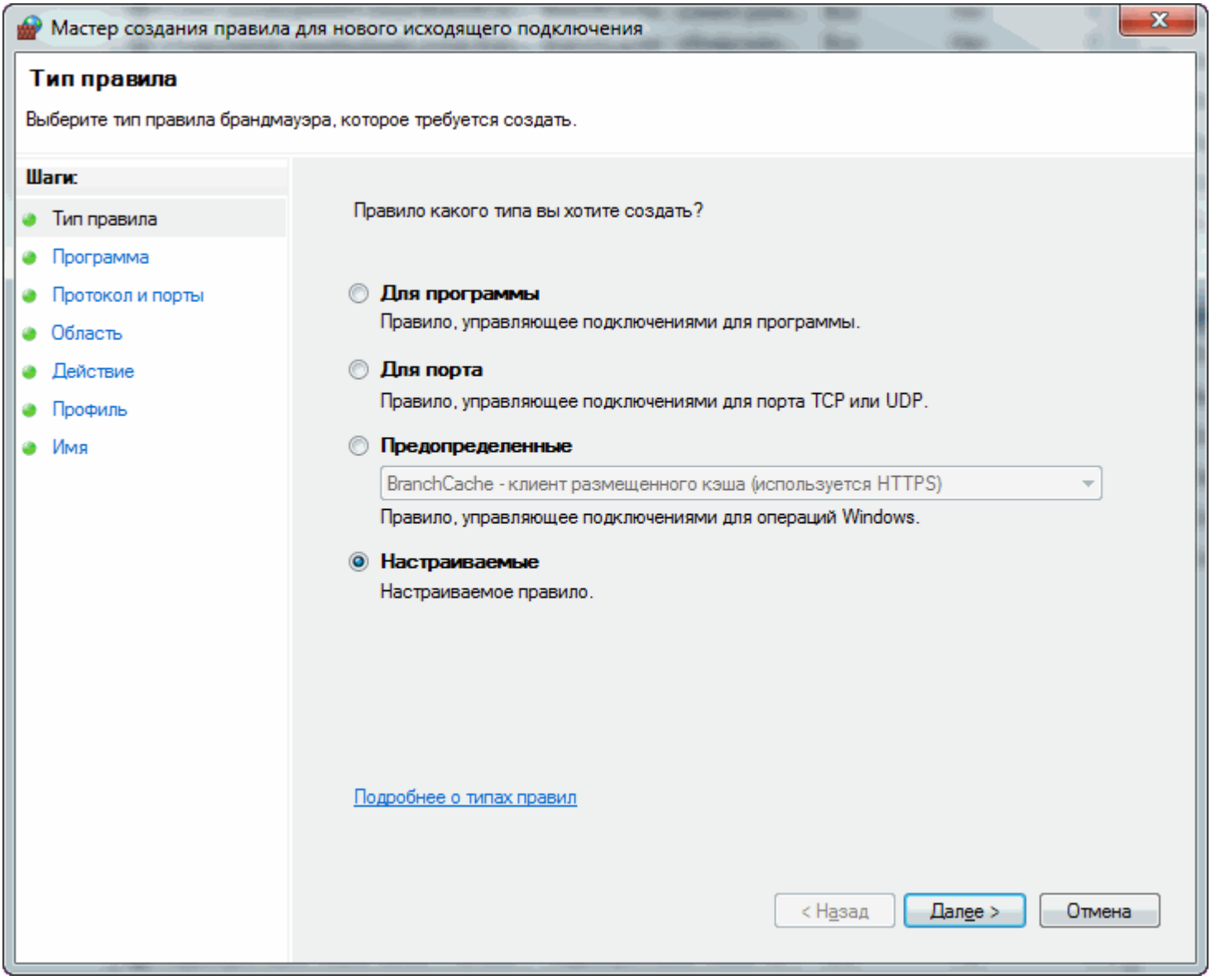
Таким же образом необходимо создать правила для других программ.

5. Разрешение для служб и гаджетов Windows

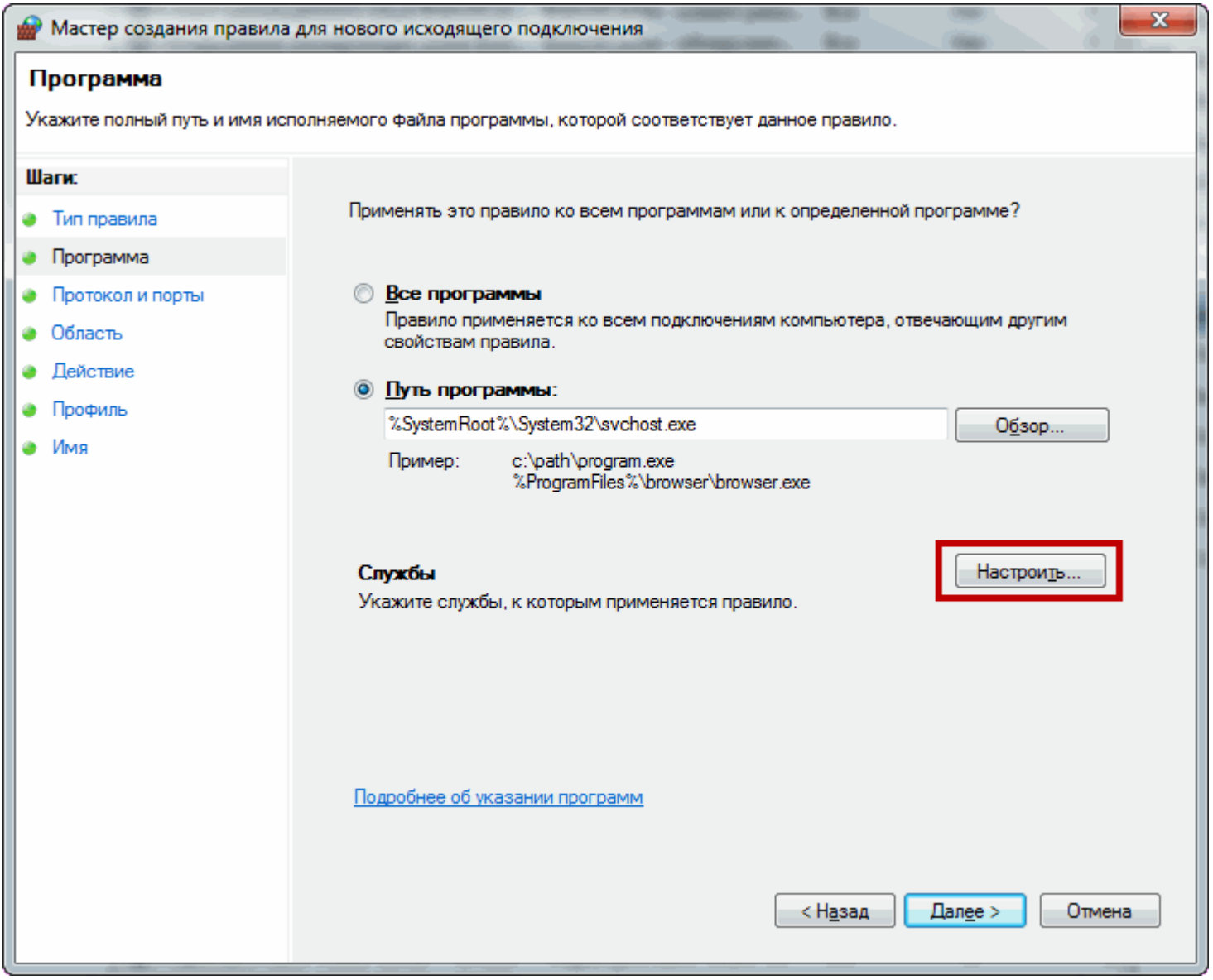
Что бы работали гаджеты в Windows 7 необходимо дать доступ к интернету программе C:\ Program Files (x86)\Windows Sidebar\sidebar.exe так же как и браузеру Google Chrome в предыдущем разделе.

Что бы дать доступ в интернет службе Обновление Windows необходимо сделать следующее:

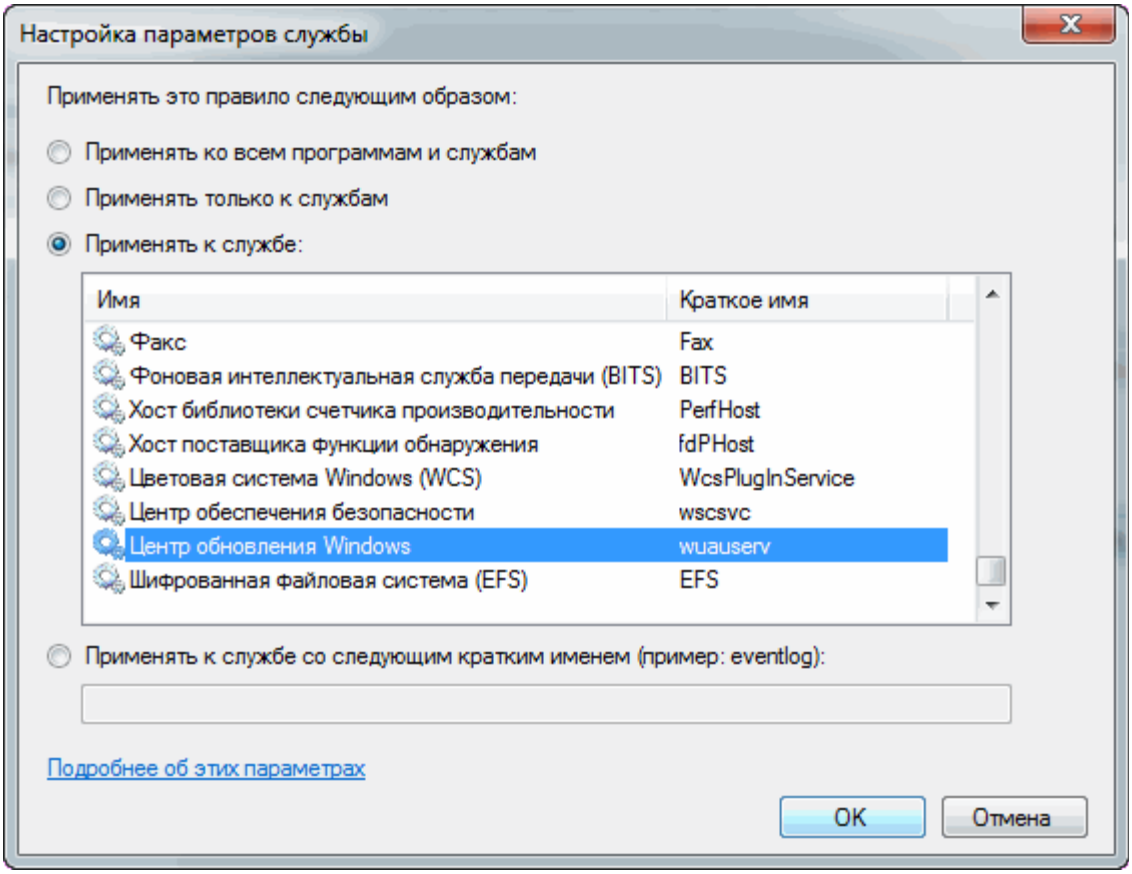
Создаем настраиваемое правило



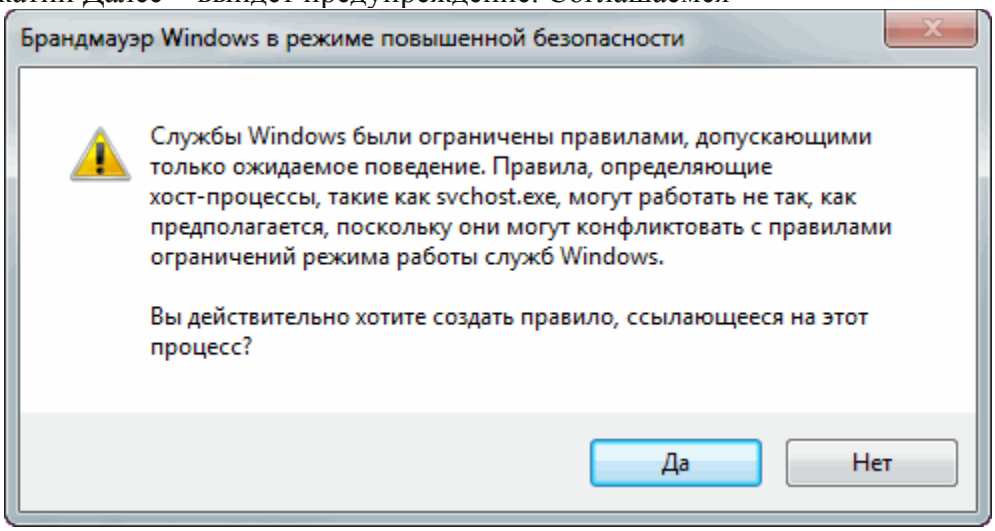
Указываем путь к программе %SystemRoot%\System32\svchost.exe так как обновление выполняется под этим процессом. В разделе Службы нажимаем Настроить…



В открывшемся окошке выбираем Применять к службе и в списке выделяем Центр обновления Windows (краткое имя — wuauserv). Нажимаем ОК

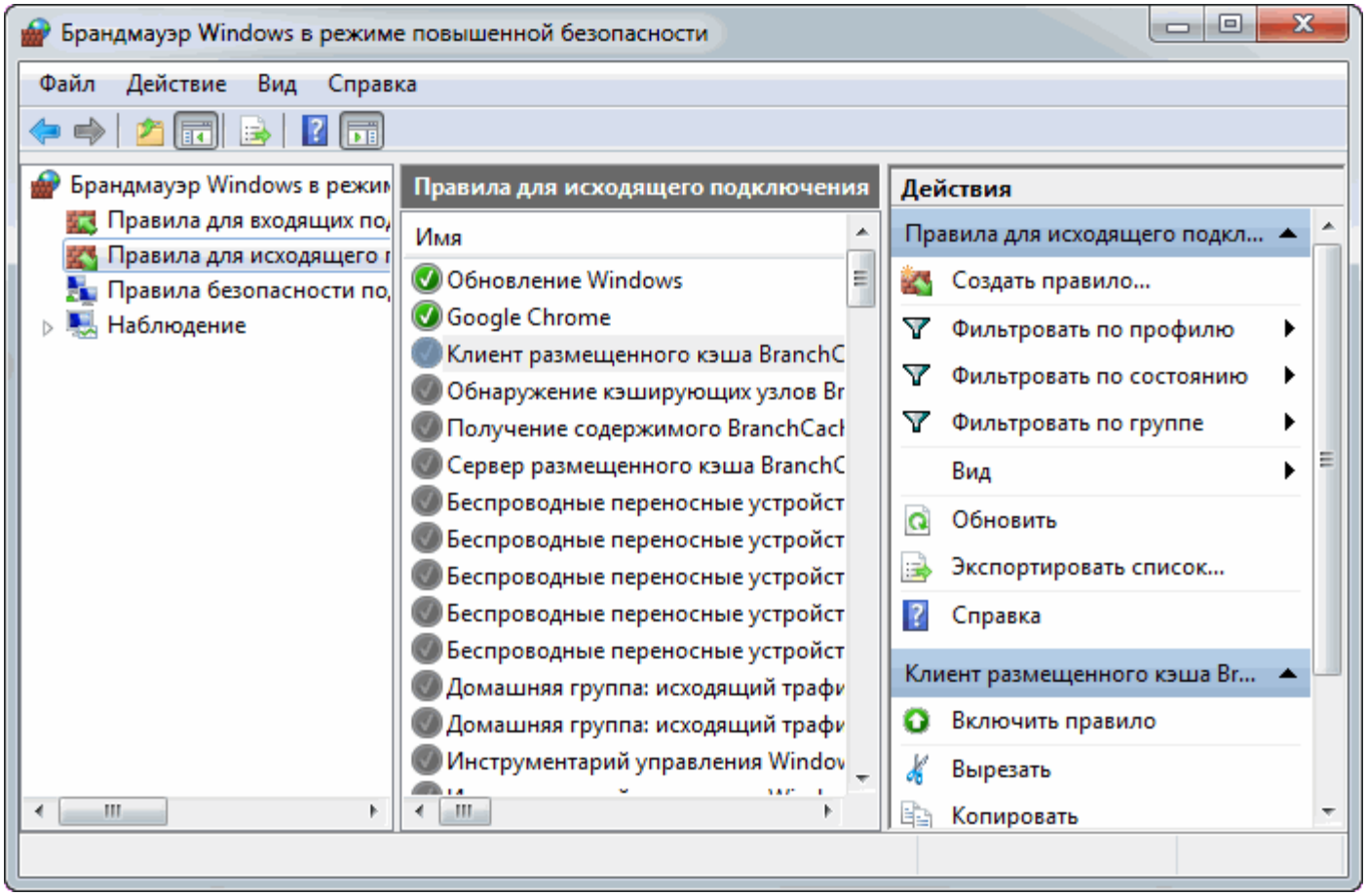


При нажатии Далее > выйдет предупреждение. Соглашаемся



Затем нажимаем все время Далее > не меняя никаких настроек, только не забываем становить Разрешить подключение.

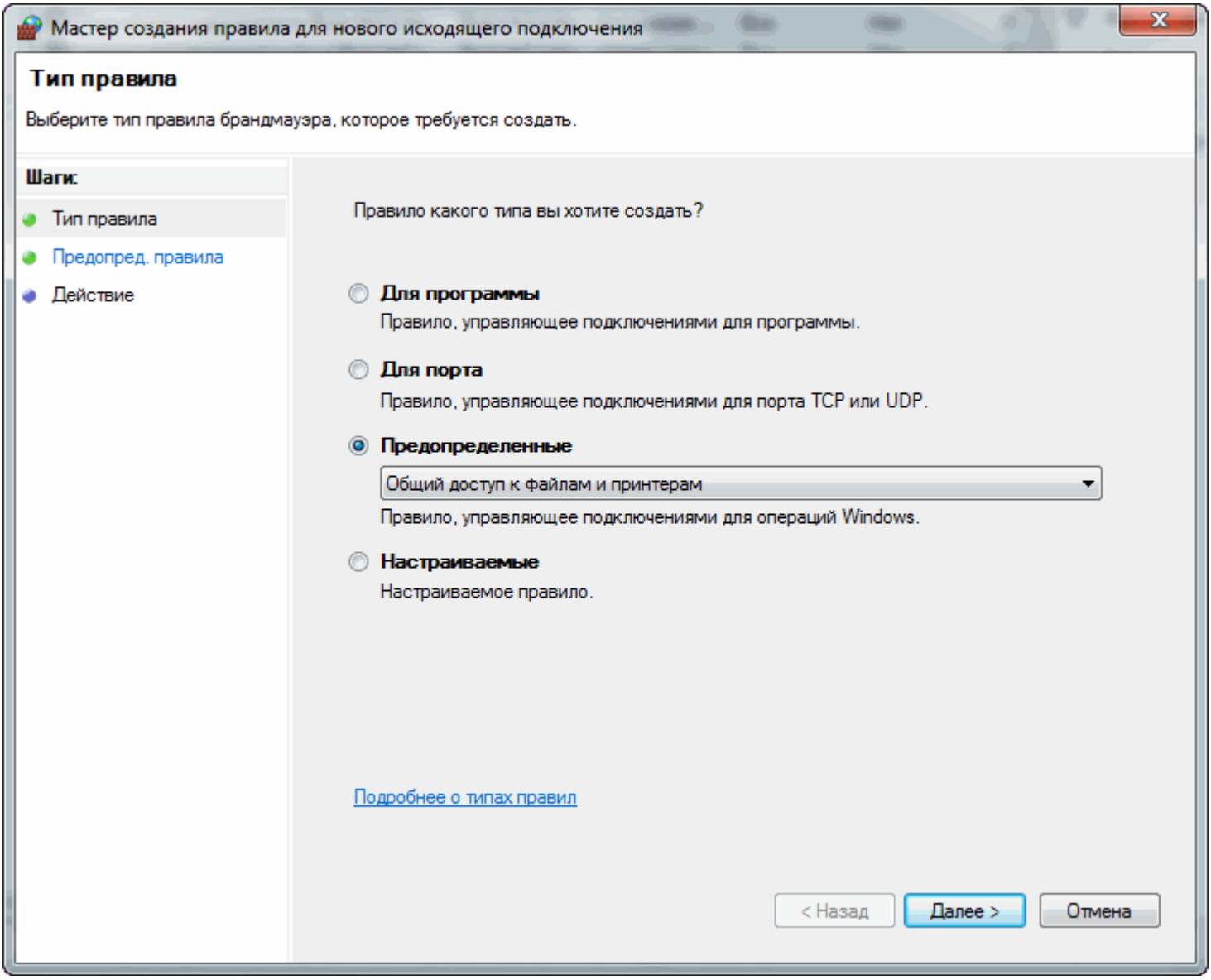
После этого у нас добавиться еще одно правило



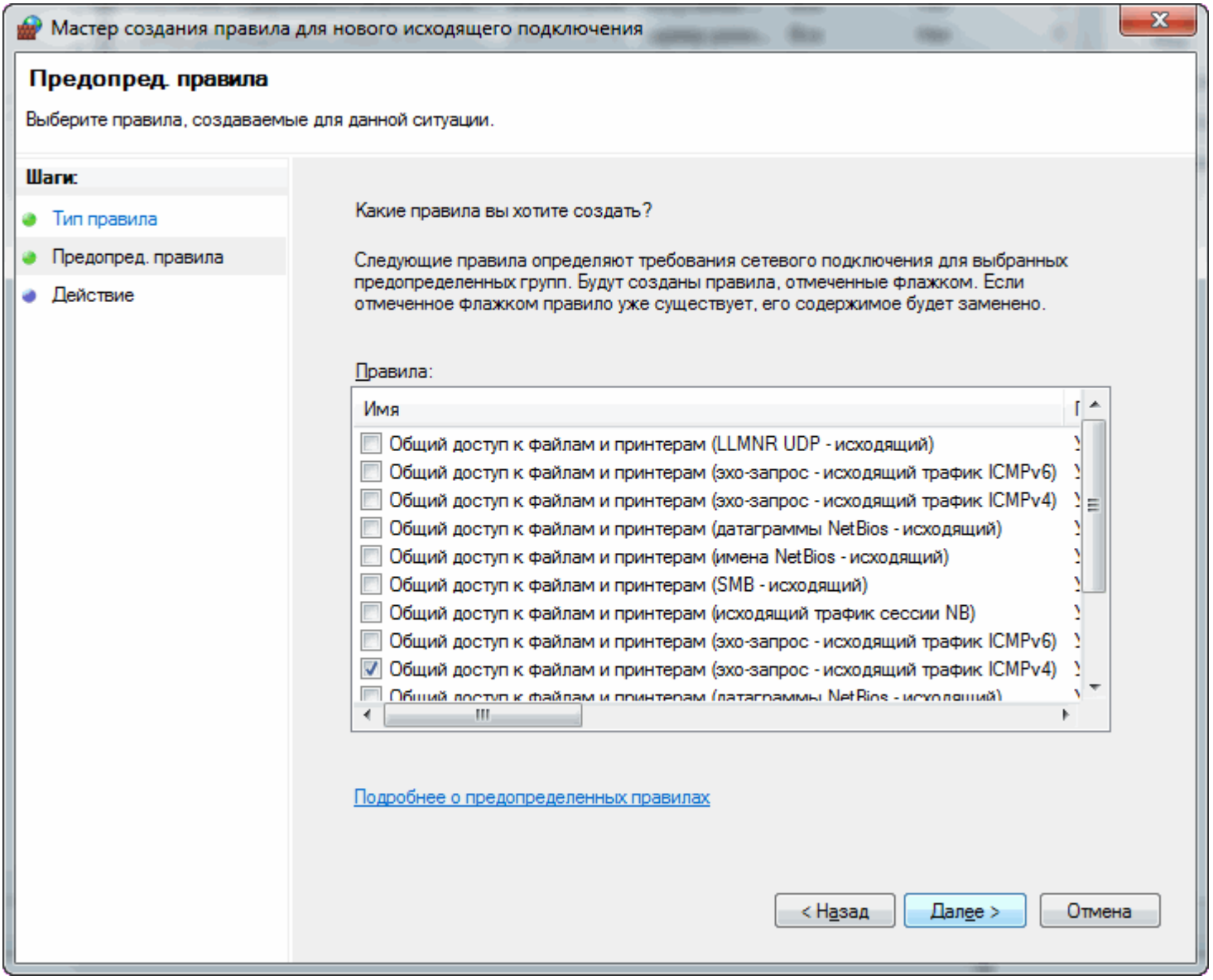
и Windows будет свободно обновляться.

6. Разрешение для команды Ping

Создаем правило и выбираем **Предопределенные**. Из выпадающего списка выбираем Общий доступ к файлам и принтерам и жмем Далее >



В разделе правила выбираем Общий доступ к файлам и принтерам (**эхо-запрос — исходящий трафик ICMPv4**) и нажимаем Далее >



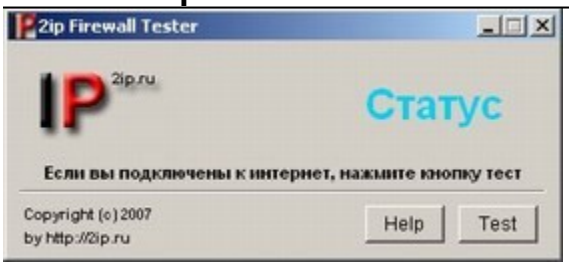
Затем разрешаем подключение и так же Далее >

После этого мы сможем «пинговать» все что хотим.

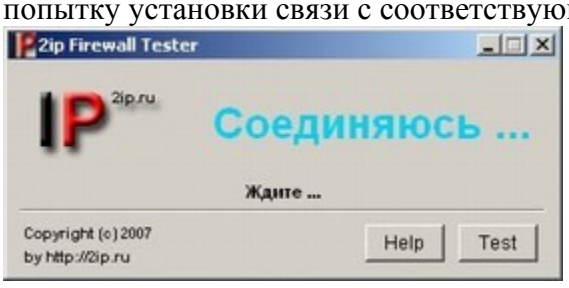
7. Как проверить Firewall

После всех настроек можно проверить работу брандмауэра. Это можно сделать с помощью программы 2ip Firewall Tester.

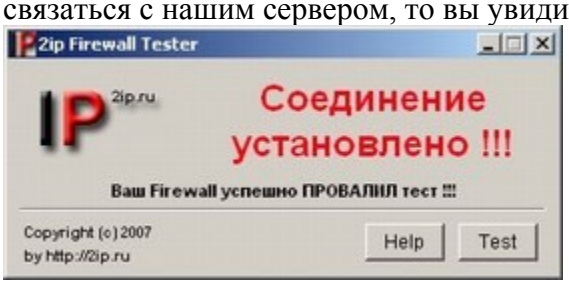
Работа с 2ip Firewall Tester



При установленном интернет соединении просто нажмите кнопку Test. Программа произведет попытку установки связи с соответствующим сервером.



Если у вас установлен Firewall, то скорее всего он не допустит этого соединения и спросит, разрешить ли выход в интернет этой программе. Если же все пройдет гладко и тестер сможет связаться с нашим сервером, то вы увидите вот такое окошко

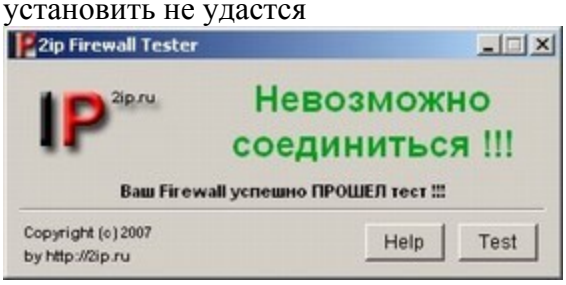


Этим все сказано. Или у вас вообще нет firewall или ваш firewall совершенно не пригоден к использованию.

Предположим, что все же вы получили предупреждение о том, что наша программа пытается установить соединение с нашим сервером, дайте единоразово разрешение на это. После чего закройте окно программы 2ip Firewall Tester.

Теперь переименуйте ее во что-нибудь хорошо известное вашему компьютеру, во что-нибудь, что постоянно использует интернет соединение. Например, это может быть программа Internet Explorer, соответственно переименуйте файл FireWallTest.exe в iexplore.exe. Таким образом мы попытаемся обмануть ваш Firewall, который наверняка уже хорошо знает эту программу и постоянно и автоматически выпускает ее в интернет. Заставим его думать, что наш тестер и есть самый настоящий Internet Explorer.

После переименования запустите наш переименованый тестер снова и нажмите кнопку Test. Ждите результата, если соединение будет установлено, смените ваш Firewall. Если же соединение установить не удастся



то можете быть спокойны, ваша система находится под надежной защитой.