Лабораторная №12,13

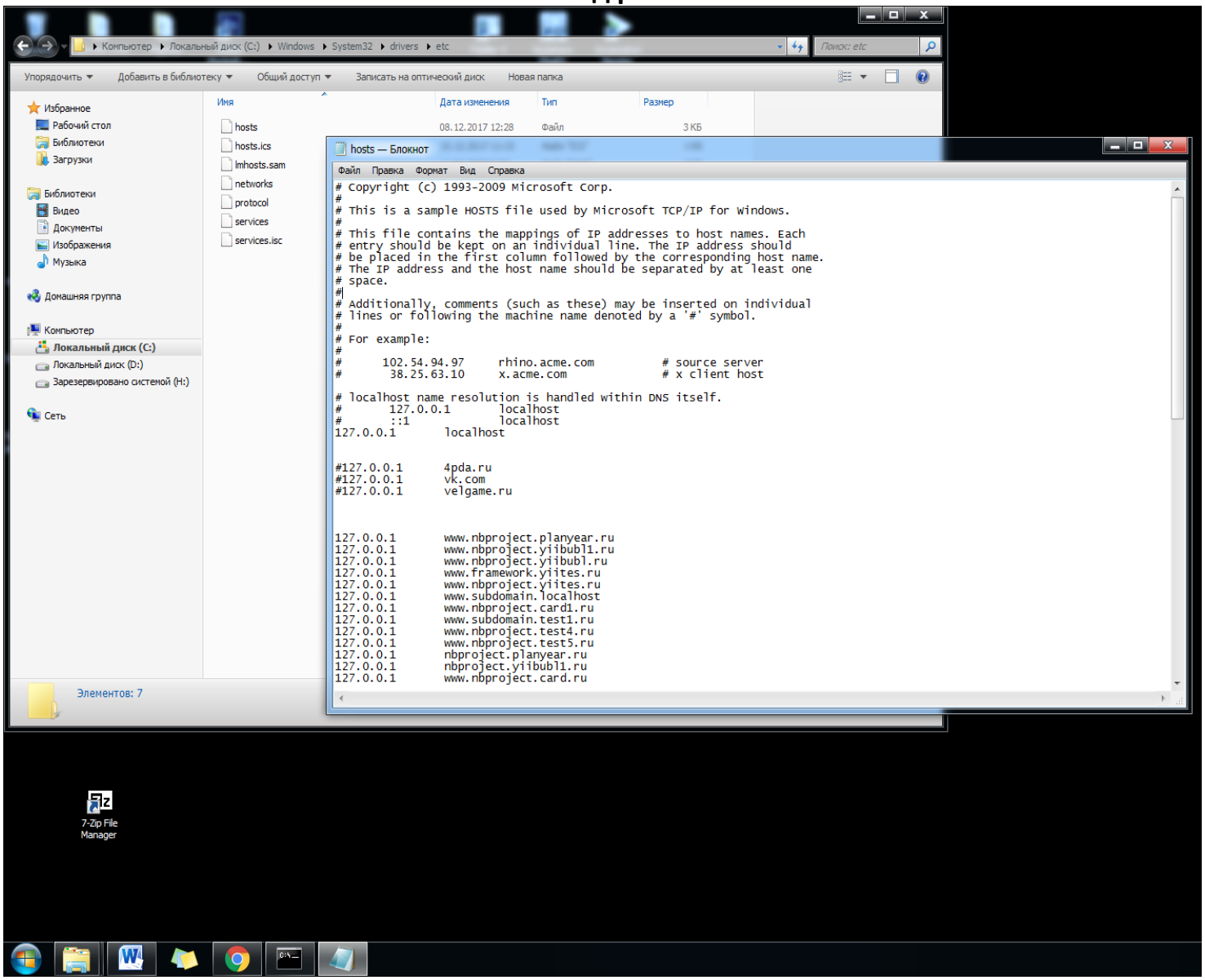
Тема: политика безопасности. Блокировка сайтов, настройка и установка плагинов.

Цель: ознакомится с firewall (брандмауэр), научится настраивать под свои нужды и устанавливать блокировку сайтов функциями встроенного firewall «Брандмауэр Windows», а так же блокировать сайты инструментами Goole и Yandex.

Тип занятия: закрепление материала.

Оборудование: ПК, методические указания.

Ход работы



ЧПройдите в папку ***C:\Windows\System32\drivers\etc***, поставьте отображение всех файлов в блокноте и откройте файл hosts (тот, который без расширения).**Открывать с помощью блокнота!!!**

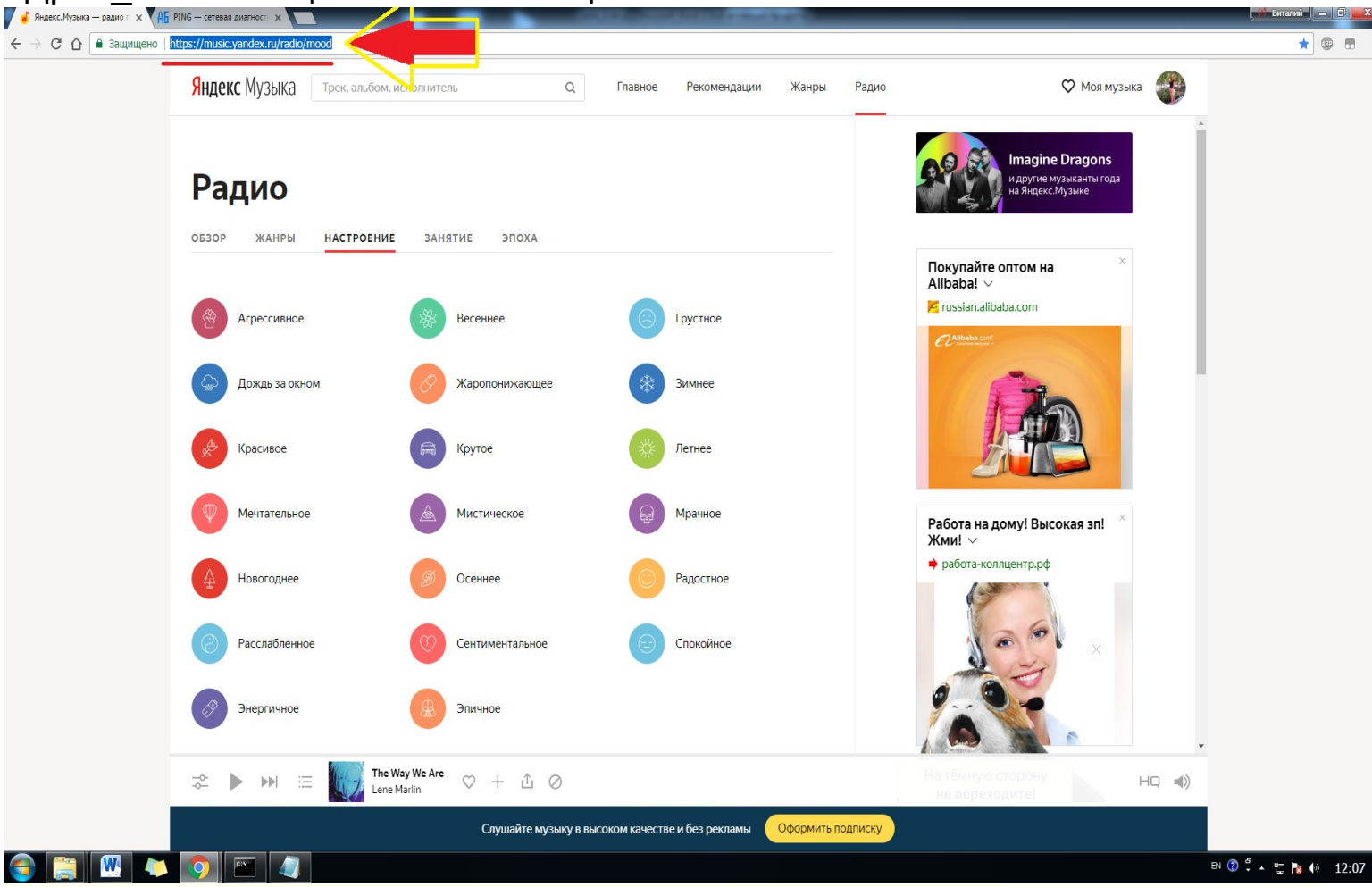
1.сделайте ,чтобы vk.com был заблокирован

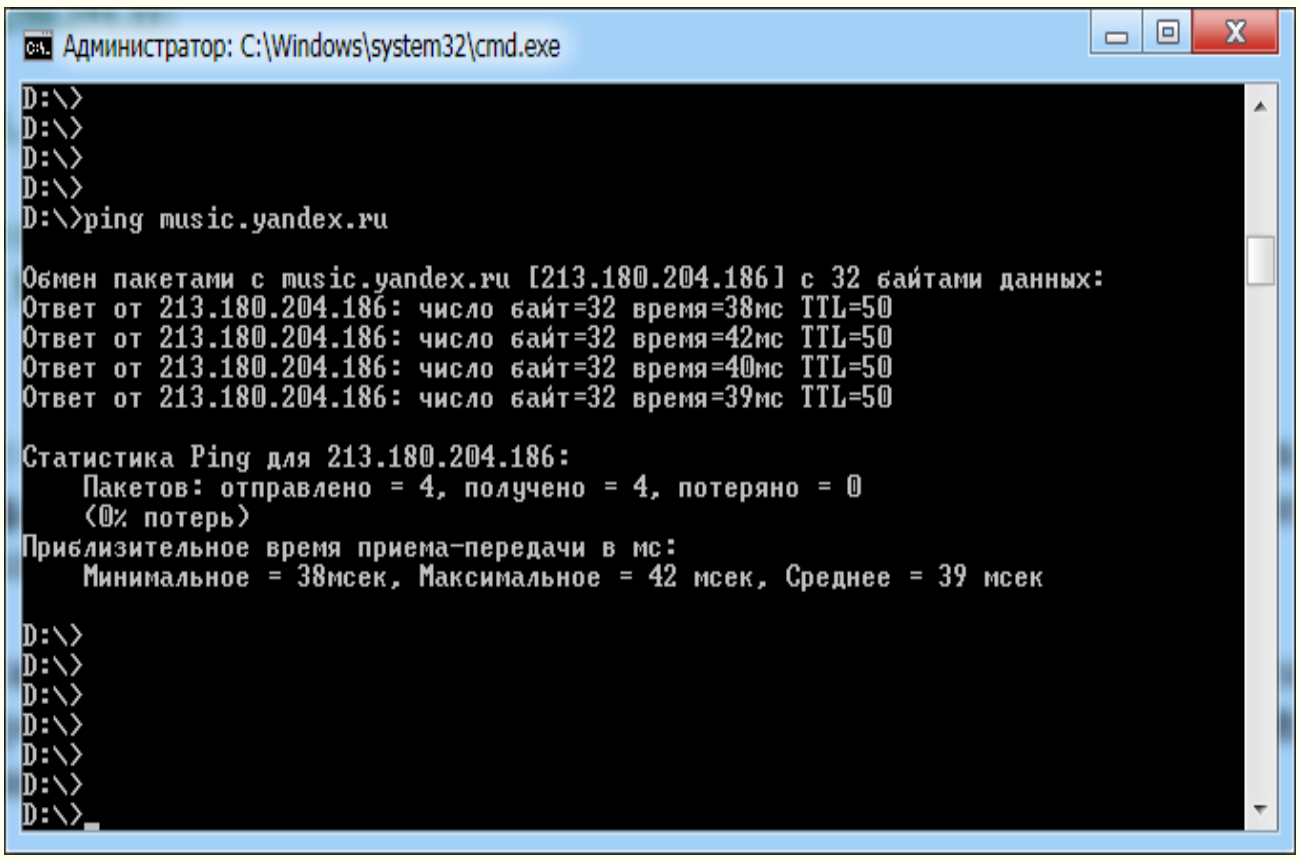
2. сделайте редирект(перенаправление) 4pda.ru на сайт Яндекс-музыки(или любое другое перенаправление сайтов)

Для того, чтобы узнать IP сайта

1. **Откройте командную строку (**В меню Пуск cmd**)**
2. **Введите команду ping адрес_сайта после чего нажмите Enter**

адрес_сайта смотреть в поисковой строке





Информация по команде PING

Команда PING - отправить эхо-запрос по протоколу ICMP на имя или IP-адрес целевого узла

Команда **PING** это, пожалуй, самая используемая сетевая утилита командной строки. **PING** присутствует во всех версиях всех операционных систем с поддержкой сети и является простым и удобным средством опроса узла по имени или его IP-адресу.

Для обмена служебной и диагностической информацией в сети используется специальный протокол управляющих сообщений **ICMP**(Internet Control Message Protocol). Команда **ping** позволяет выполнить отправку управляющего сообщения типа **Echo Request** (тип равен 8 и указывается в заголовке ICMP-сообщения) адресуемому узлу и интерпретировать полученный от него ответ в удобном для анализа виде. В поле данных отправляемого icmp-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос, опрашиваемый узел дожжен отправить icmp-пакет с теми же данными, которые были приняты, и типом сообщения **Echo Reply** (код типа в ICMP-заголовке равен 0) . Если при обмене icmp-сообщениями возникает какая-либо проблема, то утилита ping выведет информацию для ее диагностики.

Формат командной строки:

ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]] [-w таймаут] конечноеИмя

Параметры:

-t - Непрерывная отправка пакетов. Для завершения и вывода статистики используются комбинации клавиш **Ctrl + Break** (вывод статистики и продолжение), и **Ctrl + C** (вывод статистики и завершение).
-a - Определение адресов по именам узлов.
-n число - Число отправляемых эхо-запросов.
-l размер - Размер поля данных в байтах отправляемого запроса.
-f - Установка флага, запрещающего фрагментацию пакета.
-i TTL - Задание срока жизни пакета (поле "Time To Live").
-v TOS - Задание типа службы (поле "Type Of Service").
-r число - Запись маршрута для указанного числа переходов.
-s число - Штамп времени для указанного числа переходов.
-j списокУзлов - Свободный выбор маршрута по списку узлов.
-k списокУзлов - Жесткий выбор маршрута по списку узлов.
-w таймаут - Максимальное время ожидания каждого ответа в миллисекундах.

Примеры использования:

ping google.com - эхо-запрос к узлу с именем **google.com** с параметрами по умолчанию - количество пакетов равно 4, длина массива данных = 32 байта.

ping -6 ya.ru - пинг узла **ya.ru** с использованием протокола Ipv6

ping -a 192.168.1.50 - выполнить пинг с определением имени конесного узла по его адресу.

ping -s 192.168.0.1 computer - пинг узла **computer** от источника 192.168.0.1. Используется когда на компьютере имеется несколько сетевых интерфейсов.

ping w 5000 ya.ru - пинг с таймаутом ожидания равным 5 секунд (по умолчанию — 4 сек).

ping -n 5000 -l 1000 ab57.ru - опрос узла **ab57.ru** 5000 раз, пакетами с данными длиной в 1000байт. Допустимая максимальная длина данных — 65500.

ping -n 1 -l 3000 -f ya.ru - пинг с запретом фрагментации пакета.

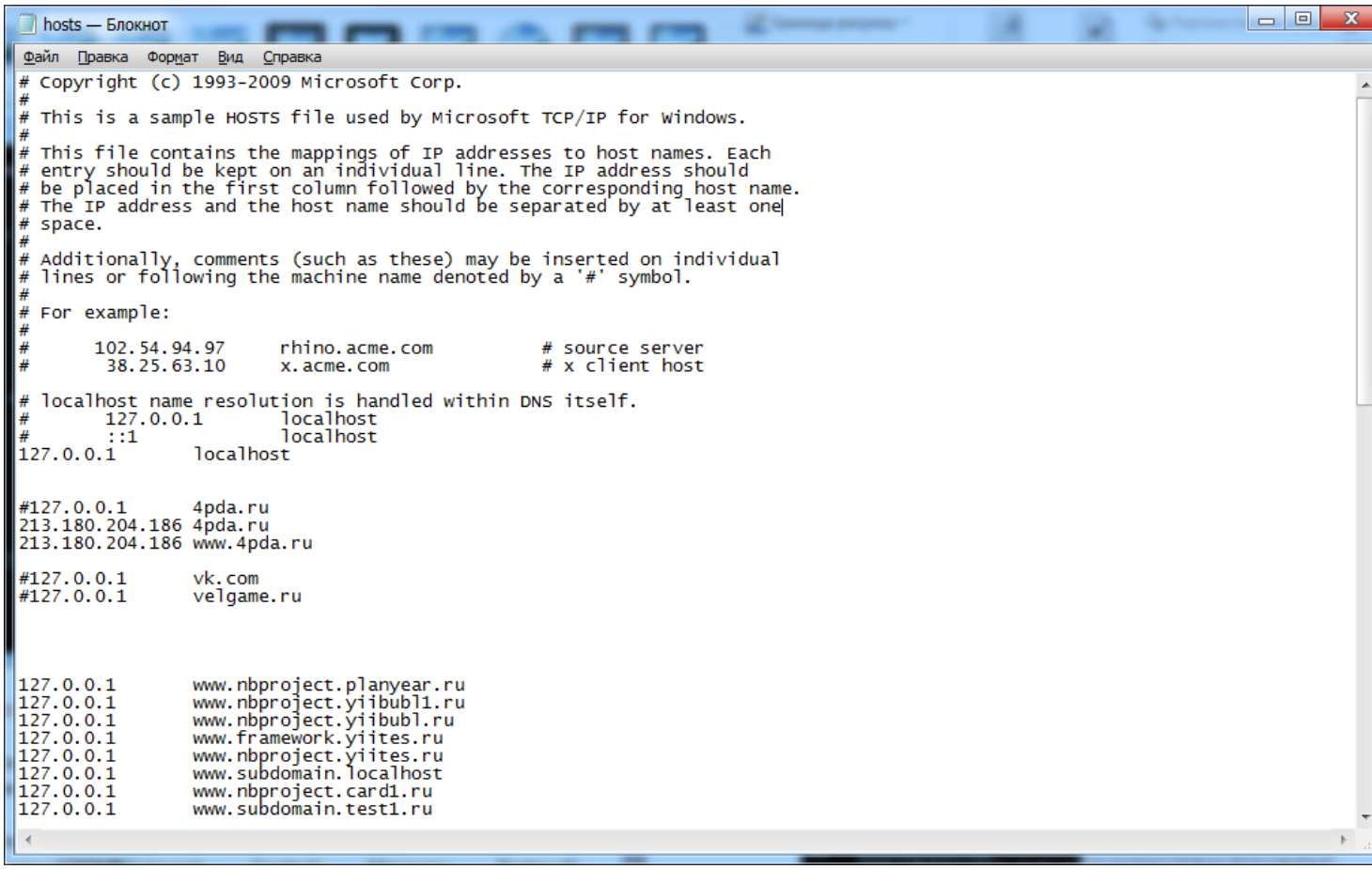
ping -n 1-r 3 ya.ru - отправить 1 эхо-запрос на узел **ya.ru** с отображением первых 3-х переходов по маршруту.

ping -i 5 ya.ru - пинг с указанием времени жизни TTL=5. Если для достижения конечного узла потребуется большее количество переходов по маршруту, то маршрутизатор, прервавший доставку ответит сообщением ”Превышен срок жизни (TTL) при передаче пакета.”

http://ab57.ru/cmdlist/ping.html можно почитать подробней)

3. **Открываем файл хоста и вписываем замену**

На первое место ставиться IP того, что откроется в место сайта 4pda.ru , т.е. IP сайта яндекс музыки(213.180.204.186), далее через пробел или Tab пишем IP домена или название с которого, будет перенаправляться(4pda.ru).



Очень важный момент: большинство сайтов имеют как бы 2 адреса – с www и без www перед именем домена, поэтому для полного перенаправления на другой сайт необходимо делать в файле hosts две записи – собственно, с www и без www. Выглядит это примерно так:

77.88.21.11 vk.com
77.88.21.11 www.vk.com

Блокировка сайт в брандмауэре(firewall) Windows

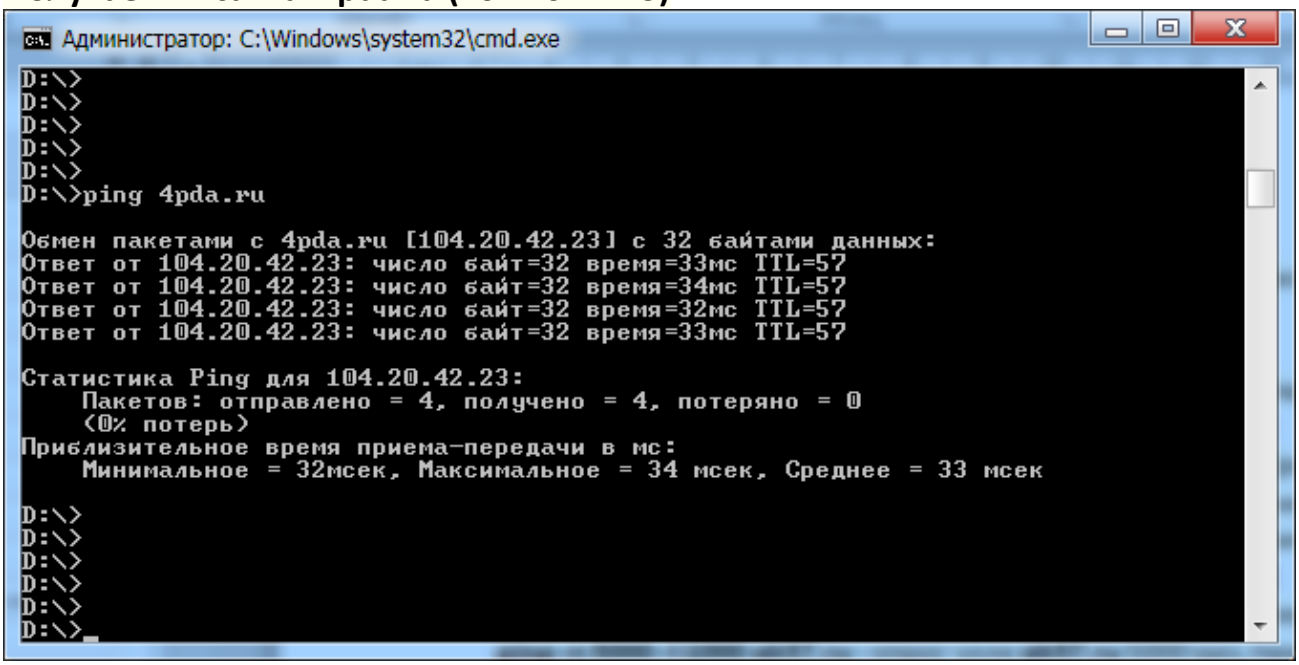
Встроенный фаервол «Брандмауэр Windows» в Windows 10, 8 и Windows 7 также позволяет заблокировать отдельные сайты, правда делает это по IP-адресу (который может меняться для сайта со временем).

Процесс блокировки будет выглядеть следующим образом:

1. **Откройте командную строку и введите *ping адрес_сайта* после чего нажмите Enter. Запишите IP-адрес, с которым ведется обмен пакетами.**

Это, то что мы определяли выше (IP сайта)

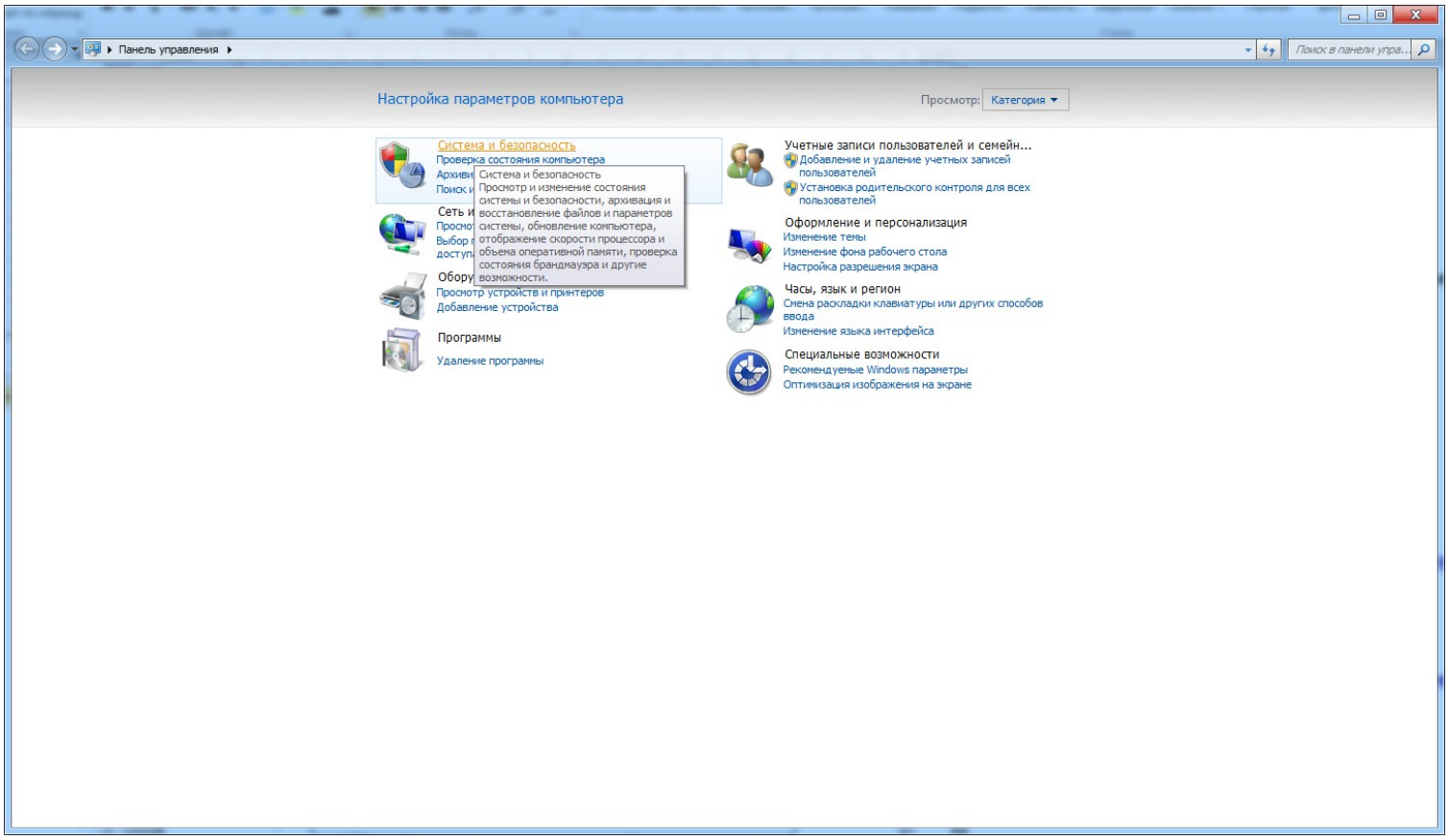
Получаем IP сайта 4 pda.ru (104.20.42.23)



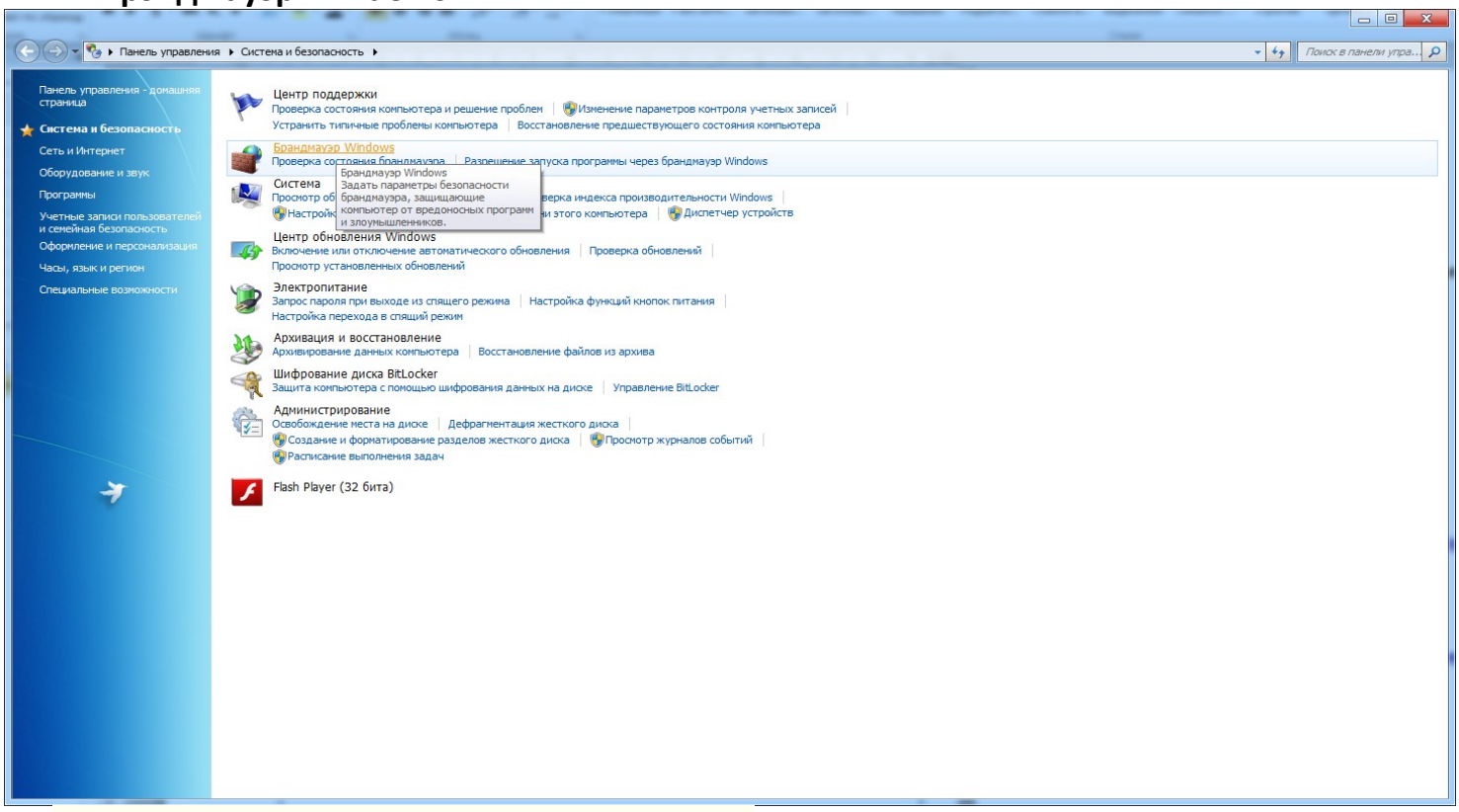
2. **Запустите брандмауэр Windows в режиме повышенной безопасности (можно использовать поиск Windows 10 и 8 для запуска, а**

в 7-ке — Панель управления — Система Безопасности — Брандмауэр Windows — включение отключение брандмауэра — Дополнительные параметры).

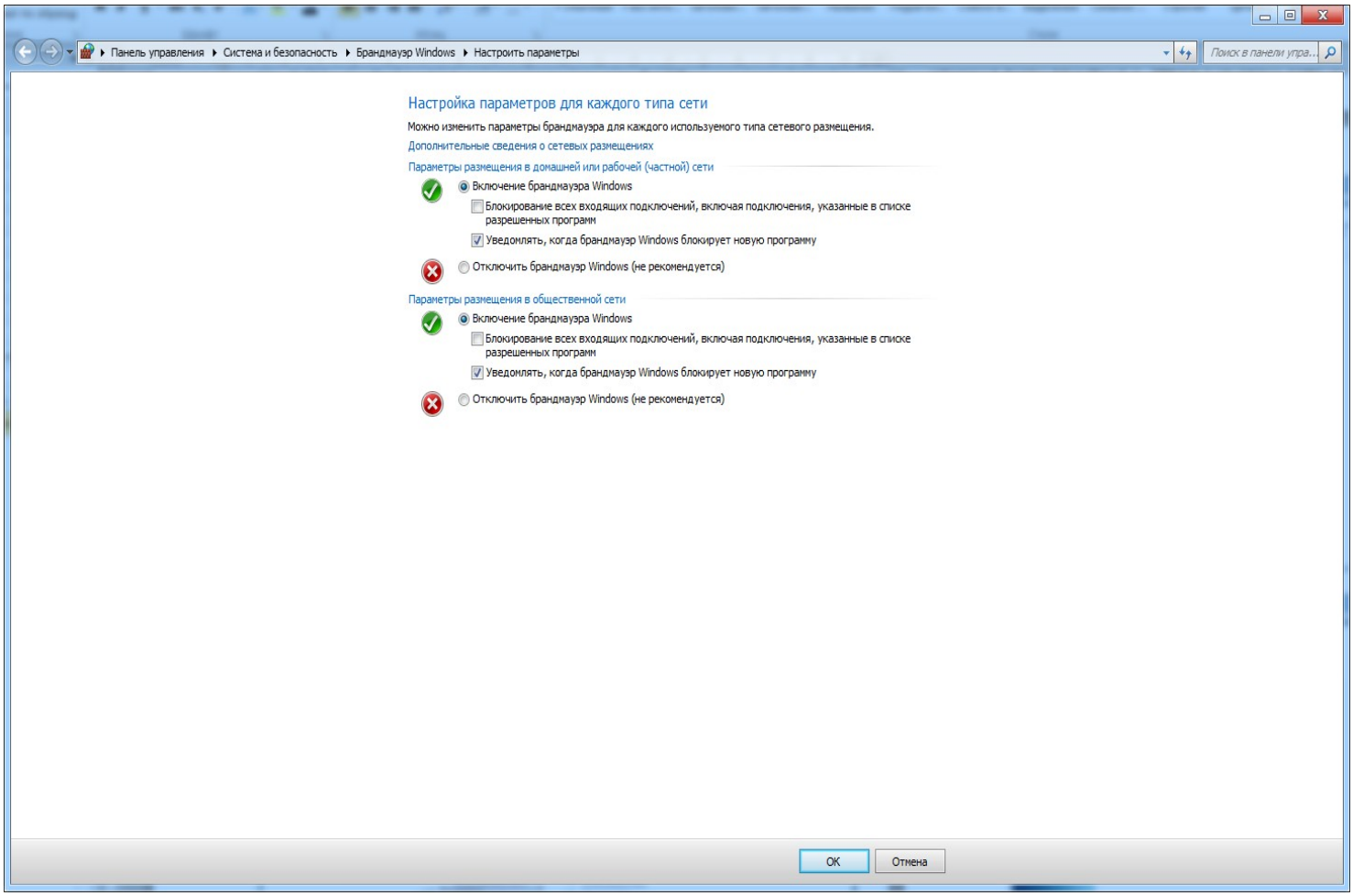
1. **Система Безопасности**



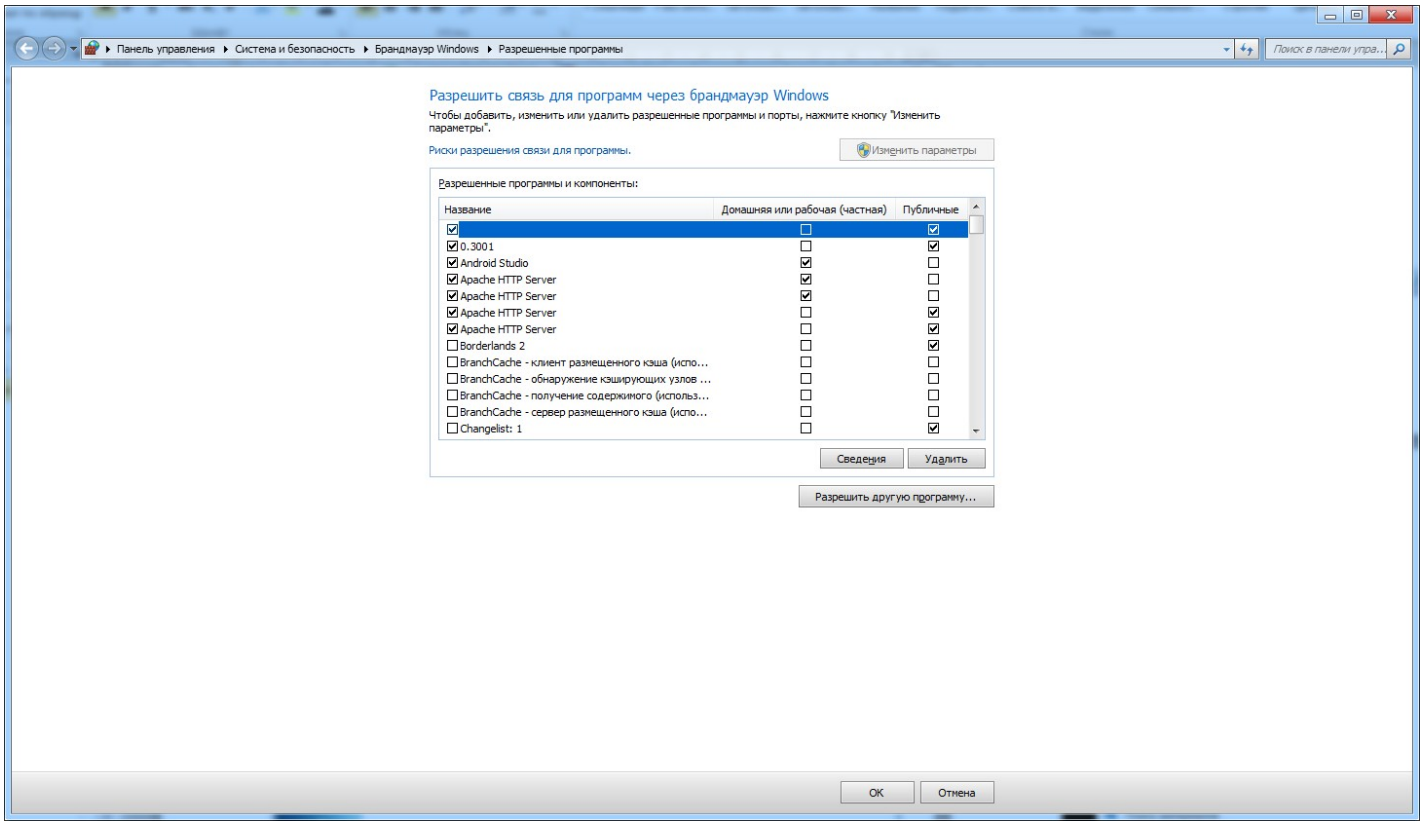
2. Брэндмауэр Windows



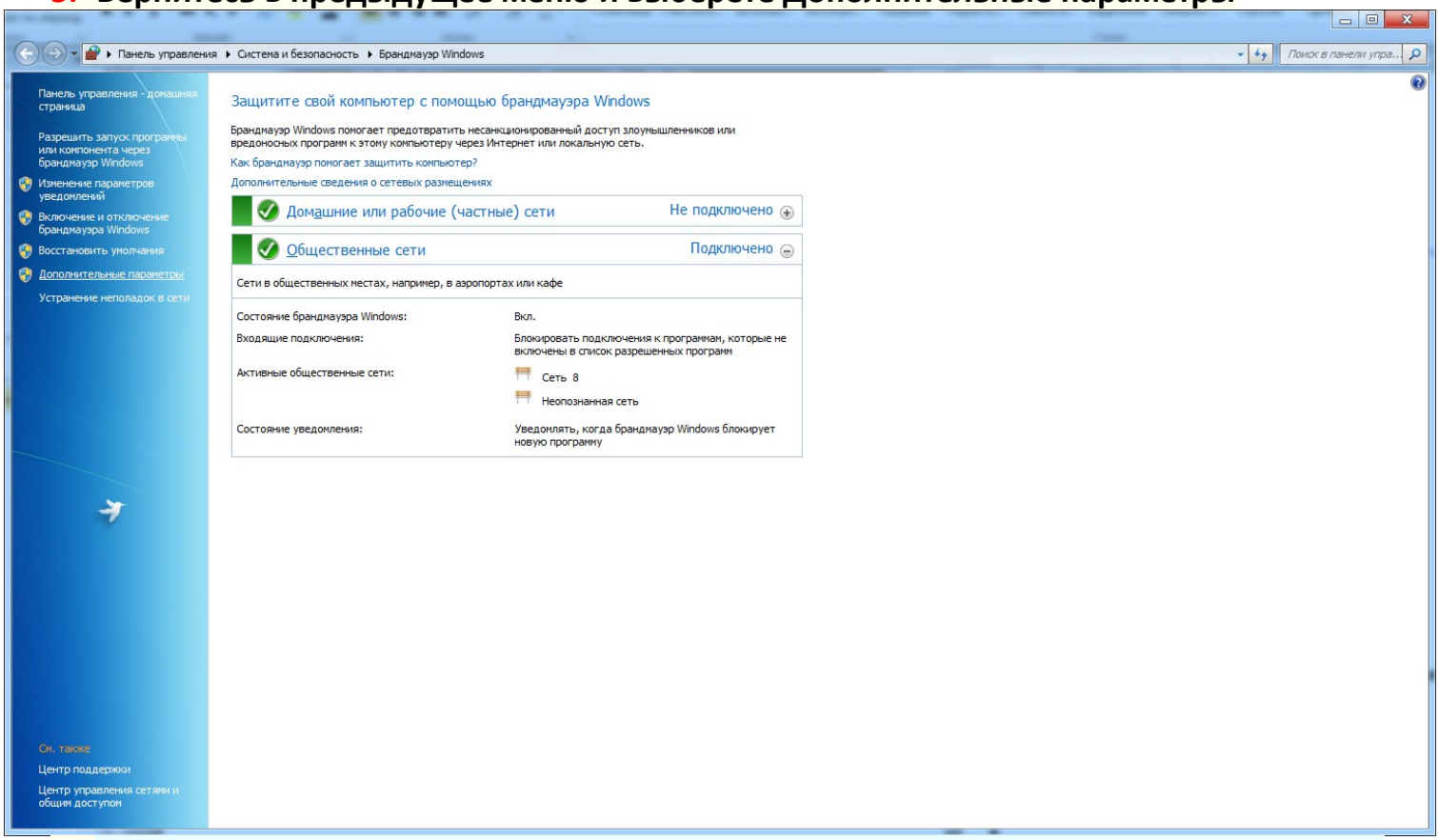
3. Включите, если не включен у вас firewall



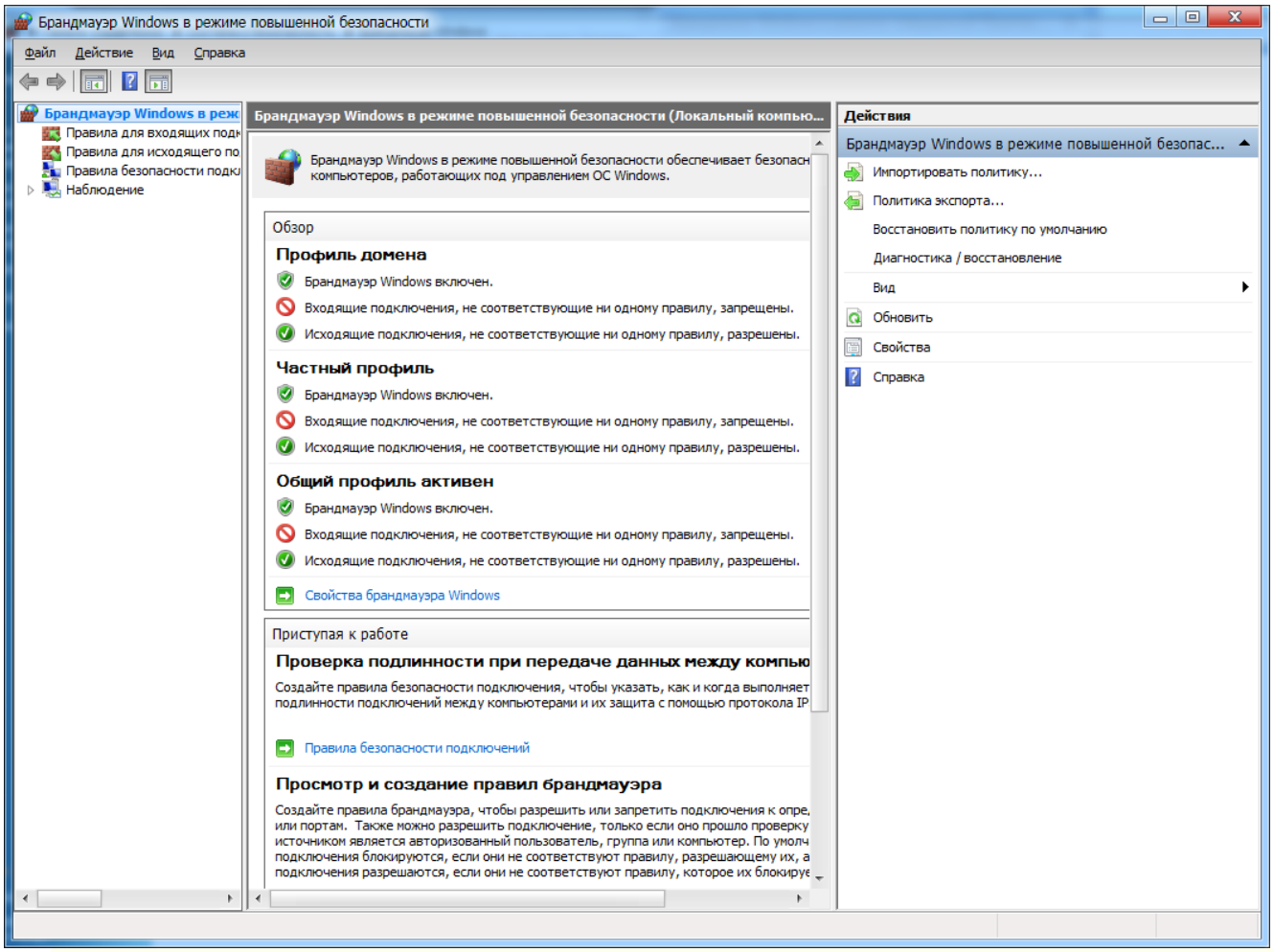
4. **Вернитесь в предыдущее меню и выберете Разрешенные программы. Выберете те программы, которые вы хотите, чтобы запускались через firewall.**



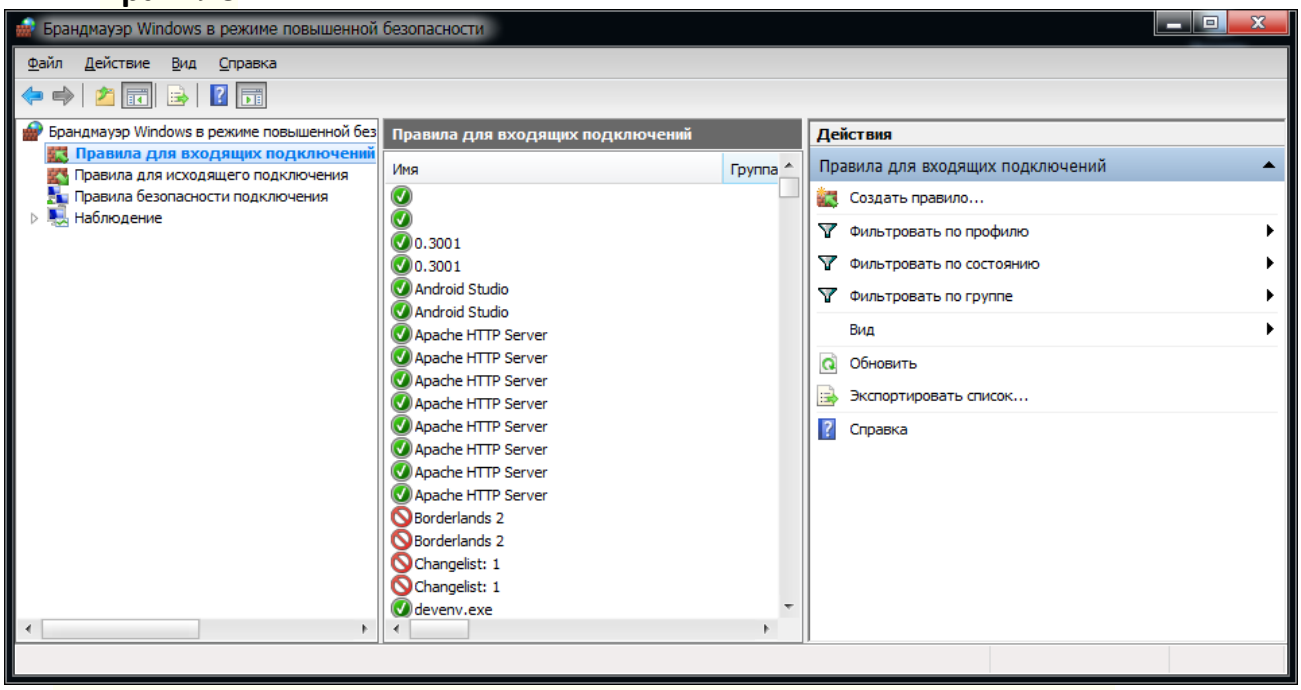
5. Вернитесь в предыдущее меню и выберете Дополнительные параметры



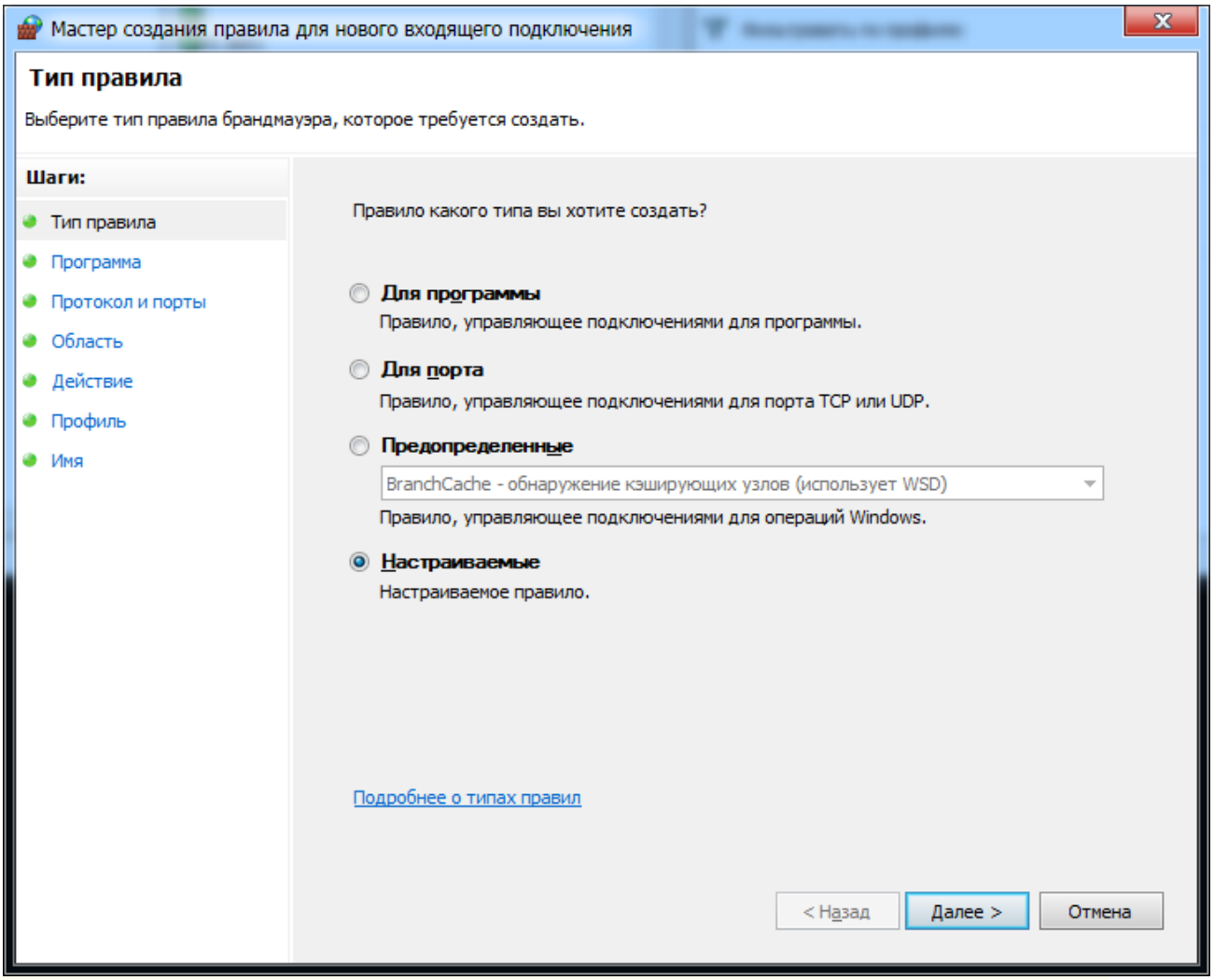
6. В открывшемся окне и происходит настройка дополнительных параметров, таких, как правила подключения (можно создать свое) и профиль домена.



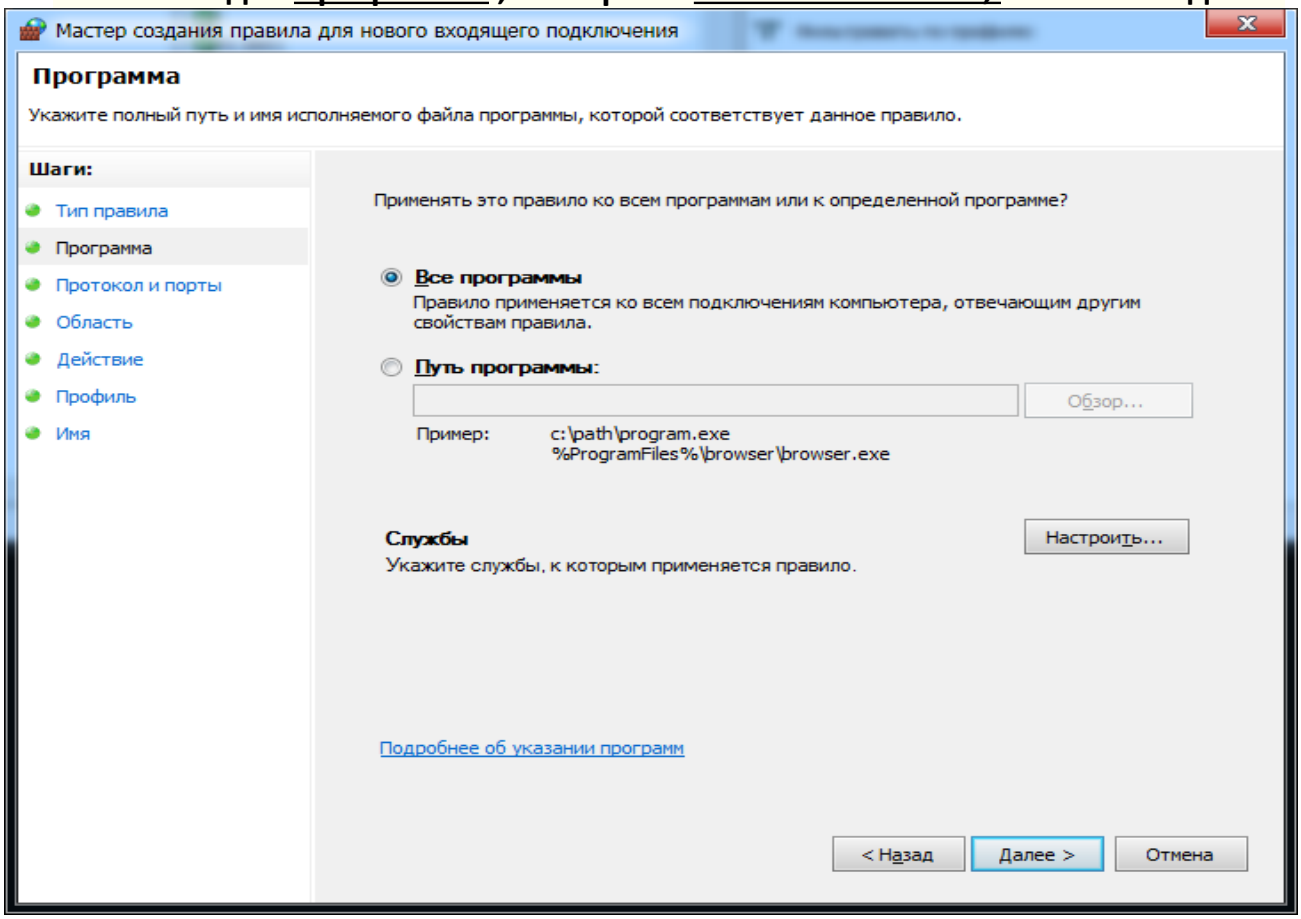
7. **Выбираем Правило входящих подключений и в окне Действия выбираем Создать правило**



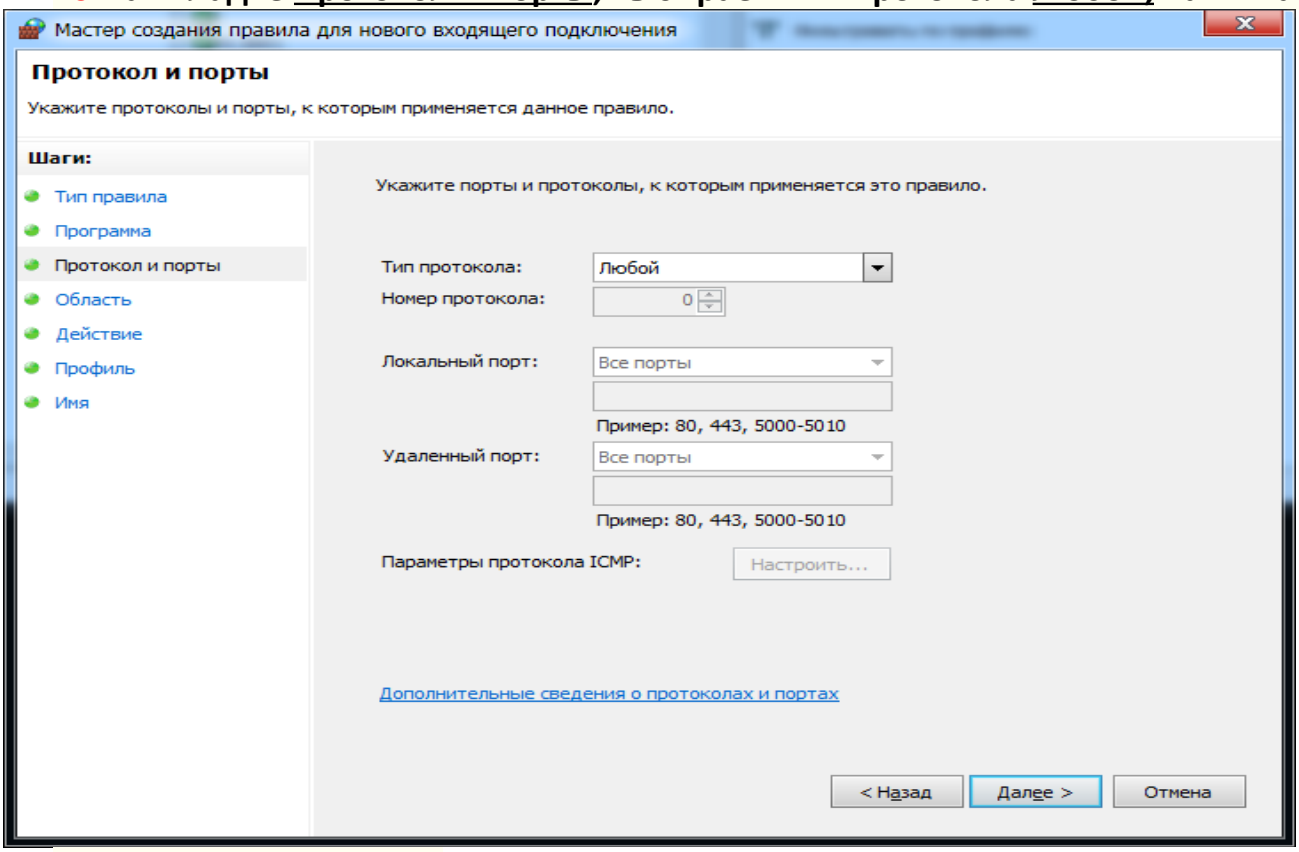
8. **В <u>Тип правила</u> выбираем <u>НАСТРАИВАЕМЫЕ</u> ,нажимаем далее**



9. На вкладке Программы , выбираем ВСЕ ПРОГРАММЫ, нажимаем далее

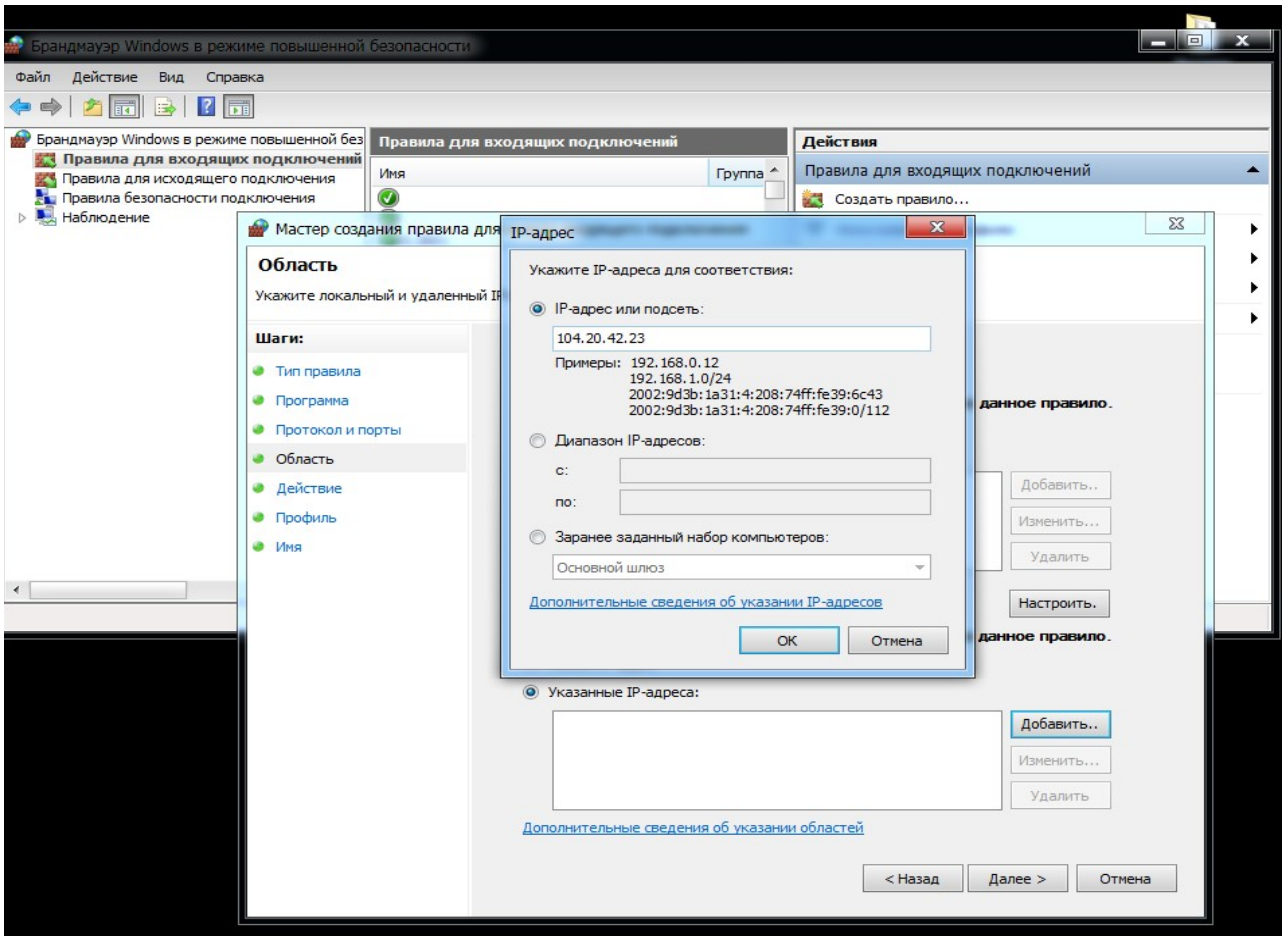


10.На вкладке Протокол и Порты, выбираем тип протокола Любой, нажимаем далее

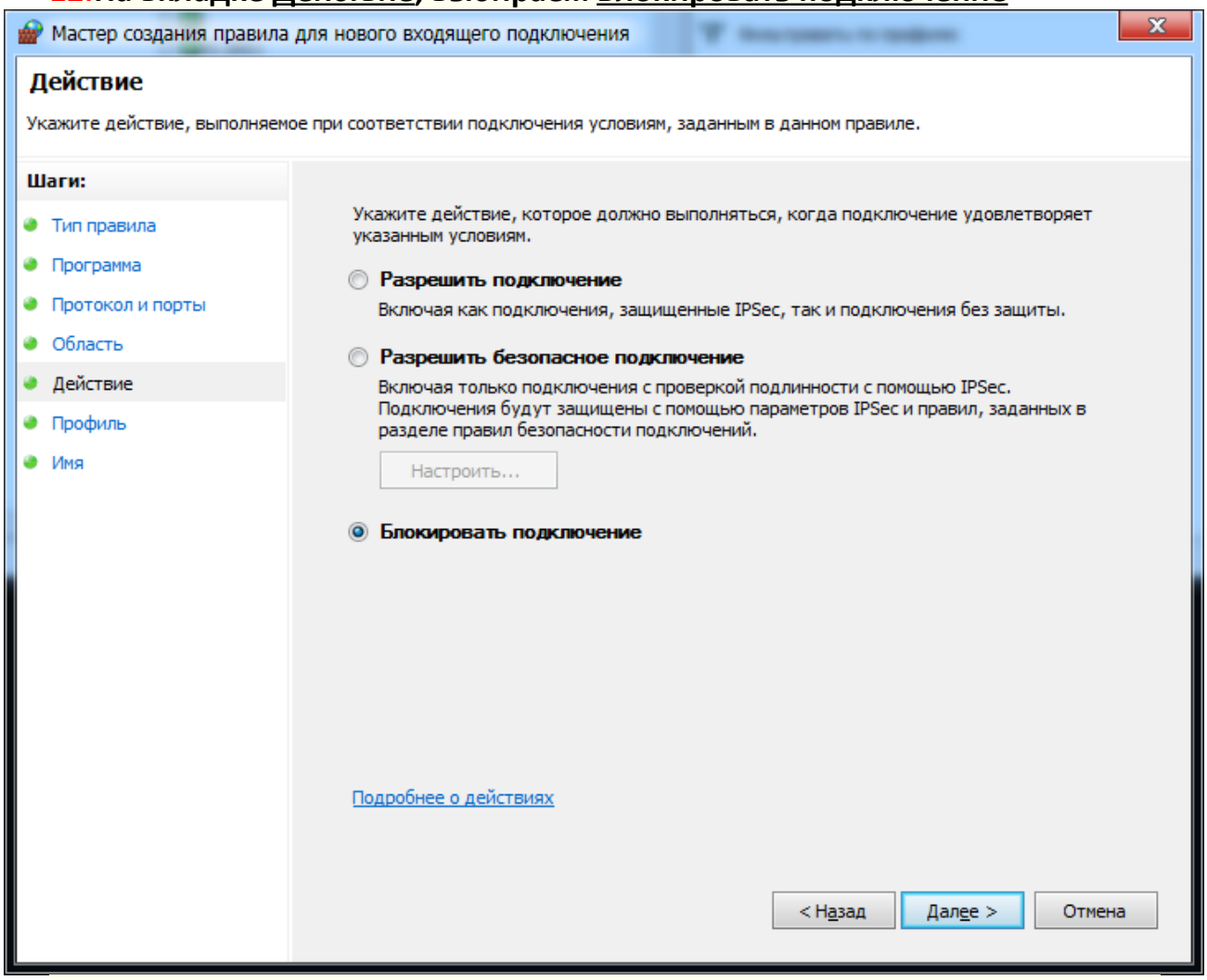


11.На вкладке Область, «Укажите удаленные IP-адреса, к которым применяется правило» отметьте пункт «Указанные IP адреса», затем нажмите «Добавить» и добавьте IP-адрес сайта, который нужно заблокировать., нажимаем далее

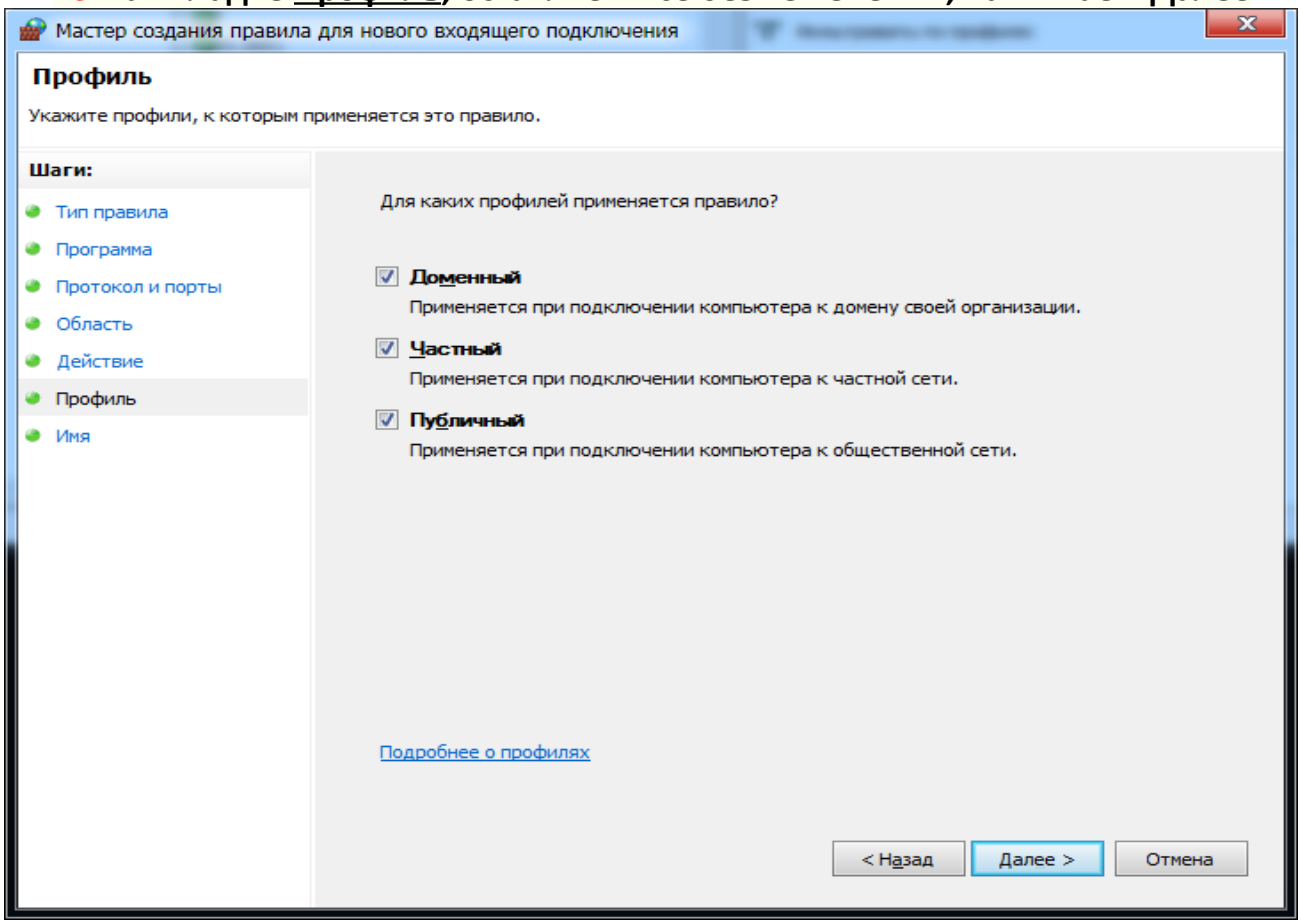
В нашем случае мы выбираем удаленный IP-адрес, нажимаем Добавить, в сплывающем окне указываем наш IP 4pda.ru (**104.20.42.23**), нажимаем окей



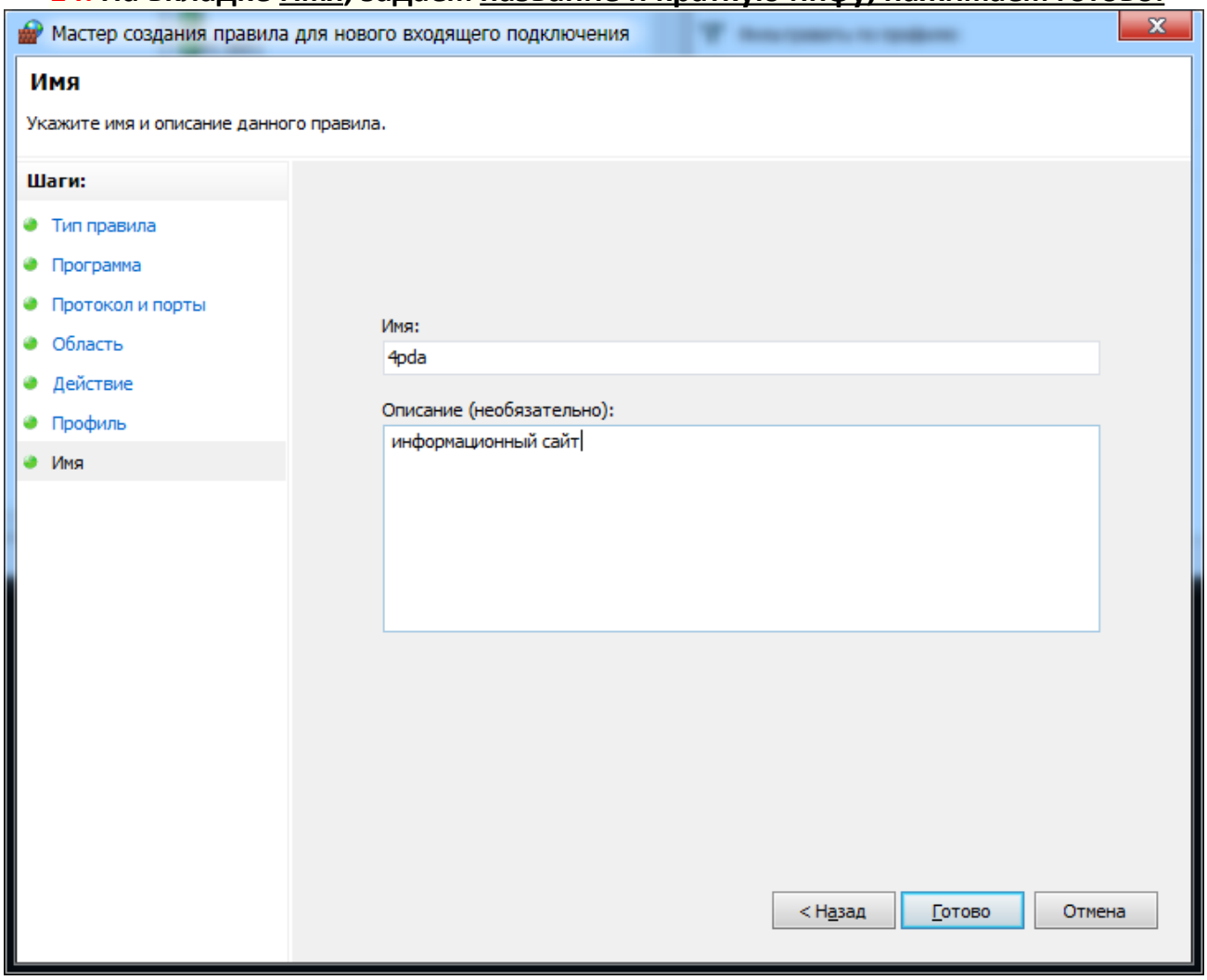
12.На вкладке Действие, выбираем Блокировать подключение



13.На вкладке Профиль, оставляем все без изменений, нажимаем Далее

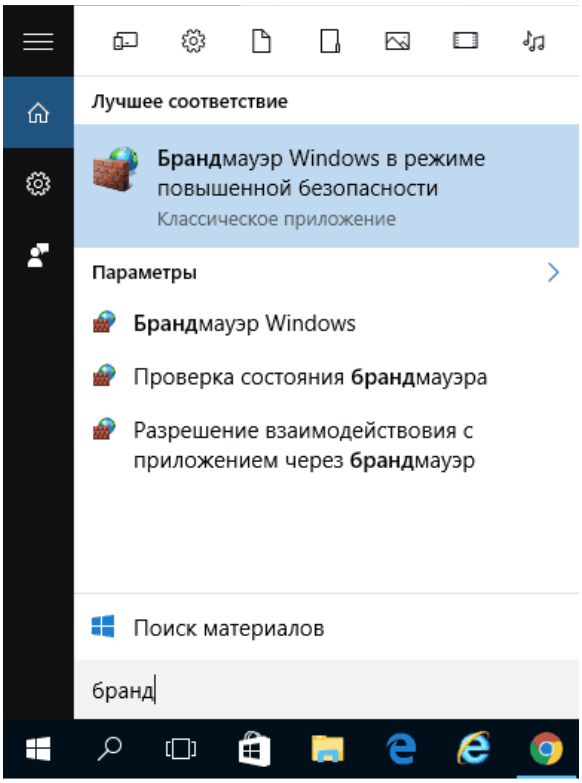


14. На вкладке Имя, задаем название и краткую инфу, нажимаем готово.

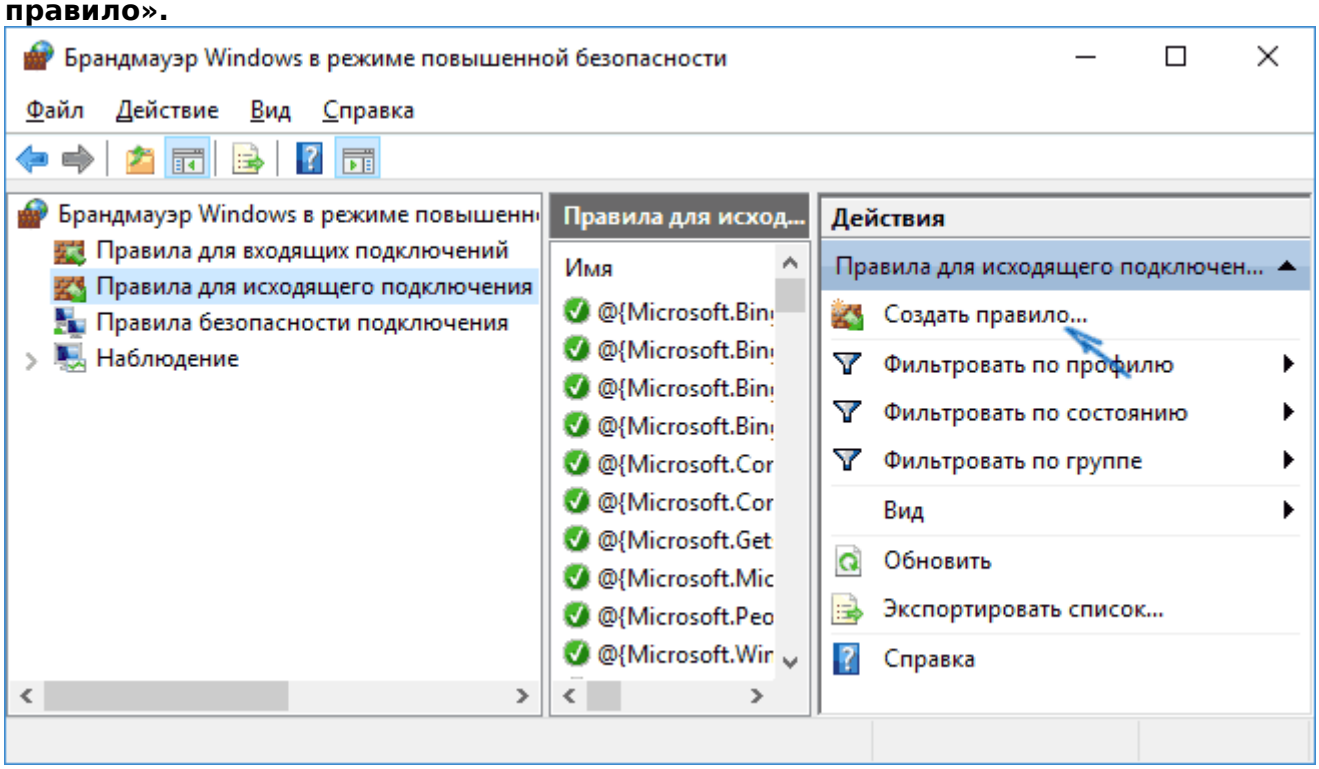


В windows 10

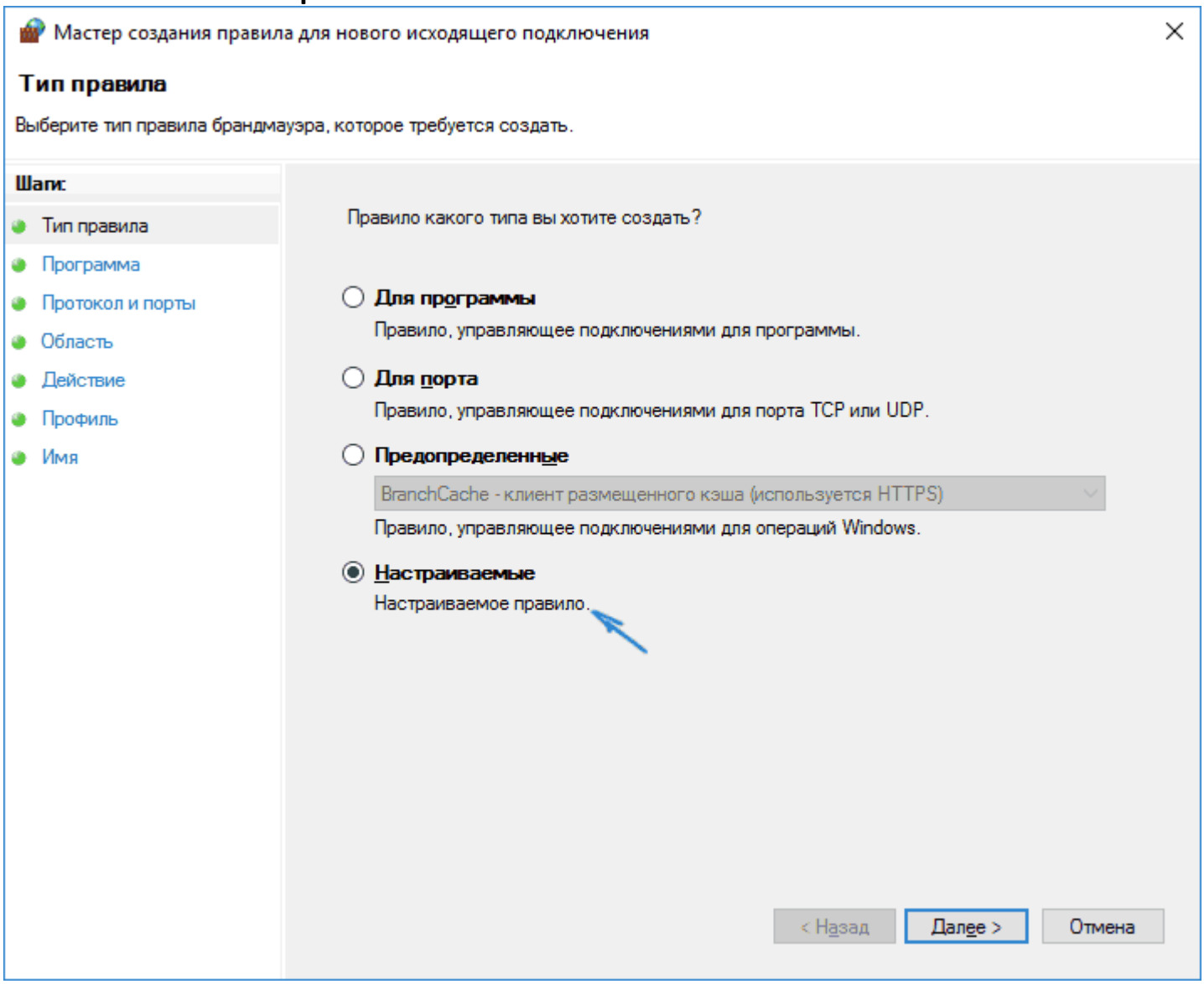
1. **В поиск вводим «брандмауэр» и выбираем в Режиме повышенной безопасности**



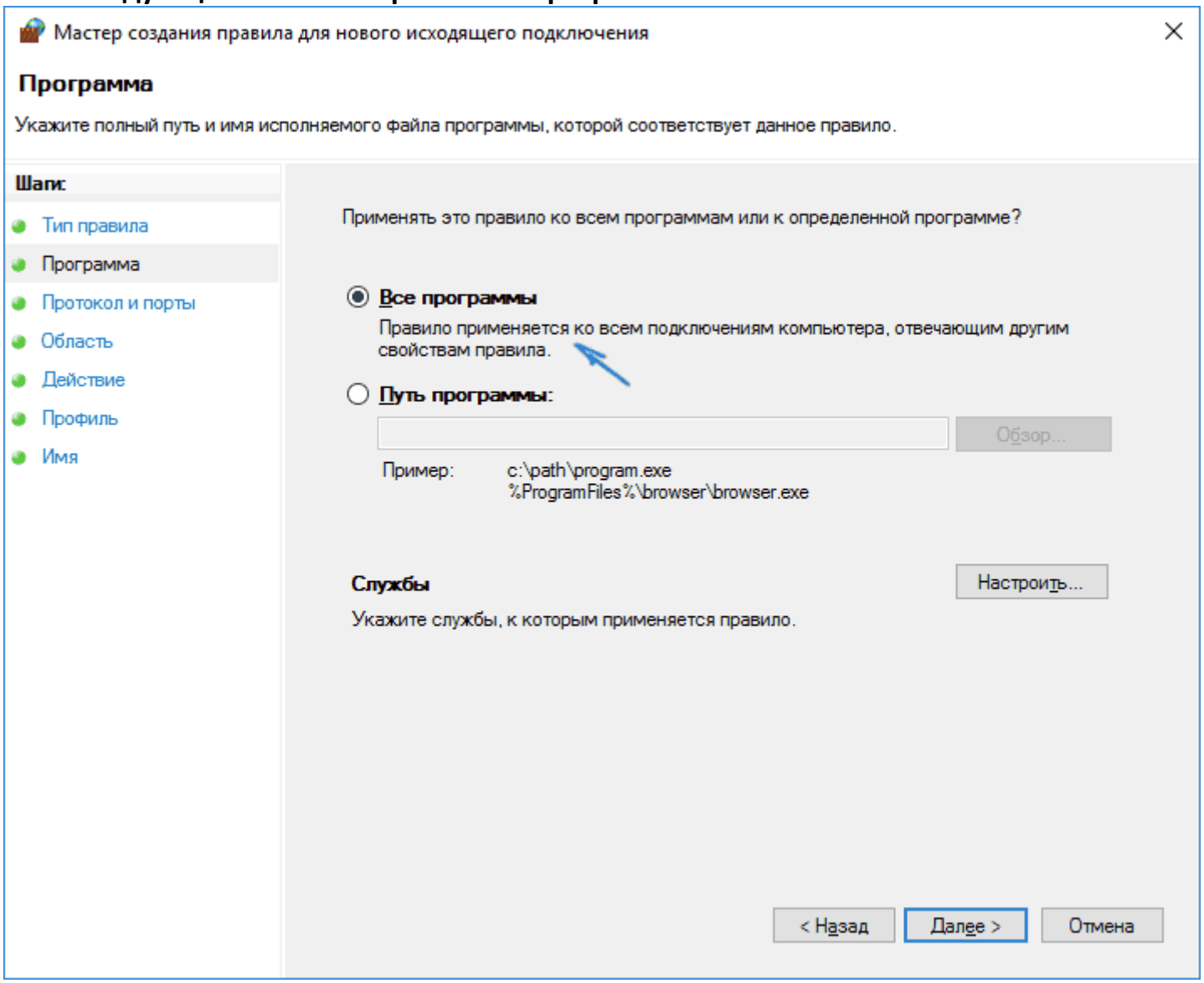
2. Выберите пункт «Правила для исходящего подключения» и нажмите «Создать правило».



3. Укажите «Настраиваемые»



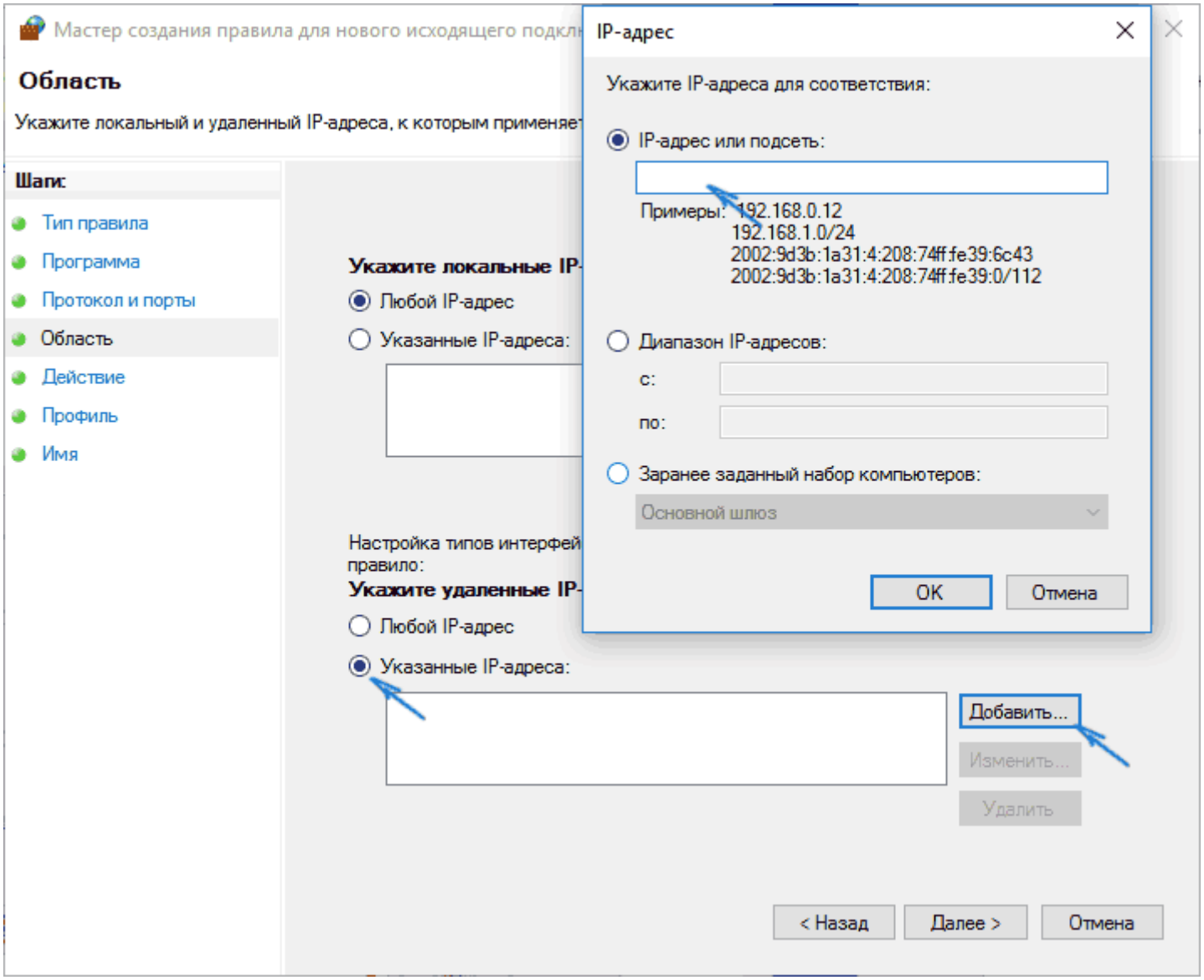
4. В следующем окне выберите «Все программы».



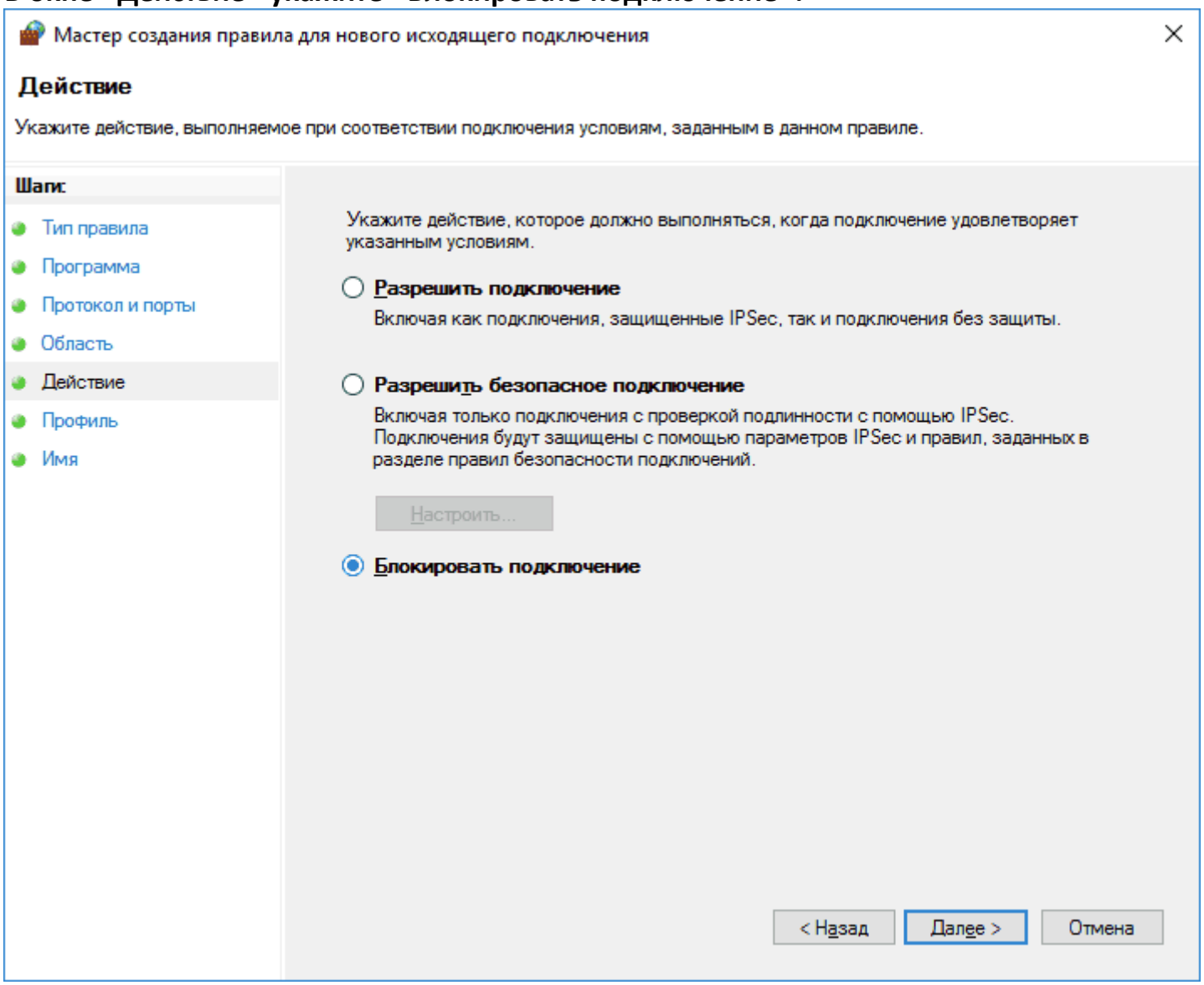
5. В окне «Протокол и порты не изменяйте настроек.

6. **В окне «Область» в разделе «Укажите удаленные IP-адреса, к которым применяется правило» отметьте пункт «Указанные IP адреса», затем нажмите «Добавить» и добавьте IP-адрес сайта, который нужно заблокировать(104.20.42.23).**

Нажмите ОК, там же можно задавать сразу несколько IP-сайтов для блокировки, просто перечислить списком нужно.



7. **В окне «Действие» укажите «Блокировать подключение».**



8. **В окне «Профиль» оставьте отмеченными все пункты.**
9. **В окне «Имя» назовите свое правило (название на ваше усмотрение),описание не обязательно и нажмите ГОТОВО.**

На этом все: сохраните правило и теперь брандмауэр Windows будет блокировать сайт по IP-адресу, при попытке открыть его.

В браузерах

В Chrome нельзя заблокировать ресурсы штатными средствами. Для этого необходима установка дополнительных расширений. Поэтому этот способ подойдет для интернет-обозревателей, поддерживающих установку дополнений.

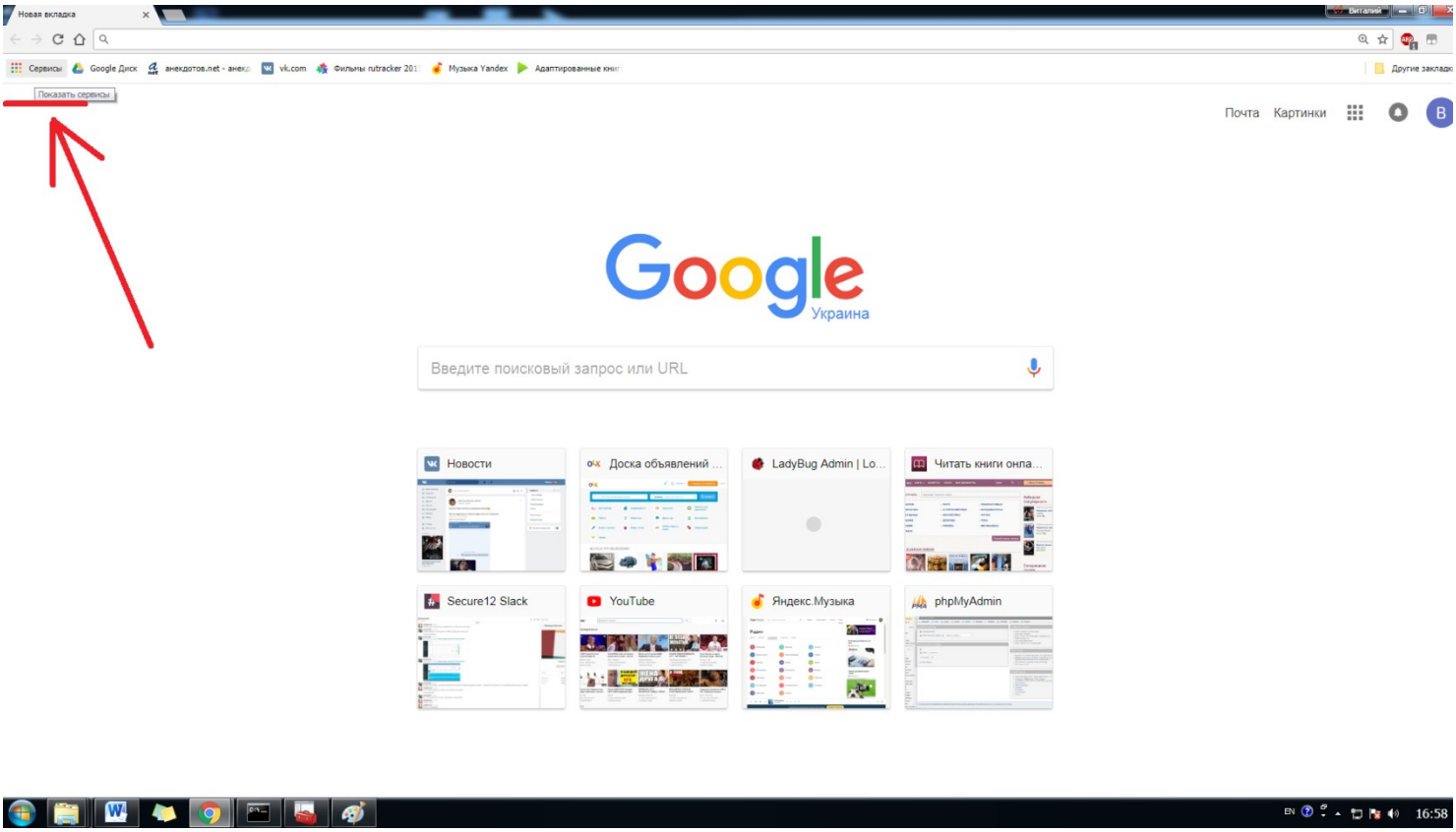
Дополнительное задание

Блокировка сайта в Google Chrome

Здесь рассмотрим, как заблокировать сайт в Google Chrome, хотя этот способ подойдет и для других браузеров с поддержкой расширений. В магазине Chrome для этой цели есть специальное расширение Block Site.

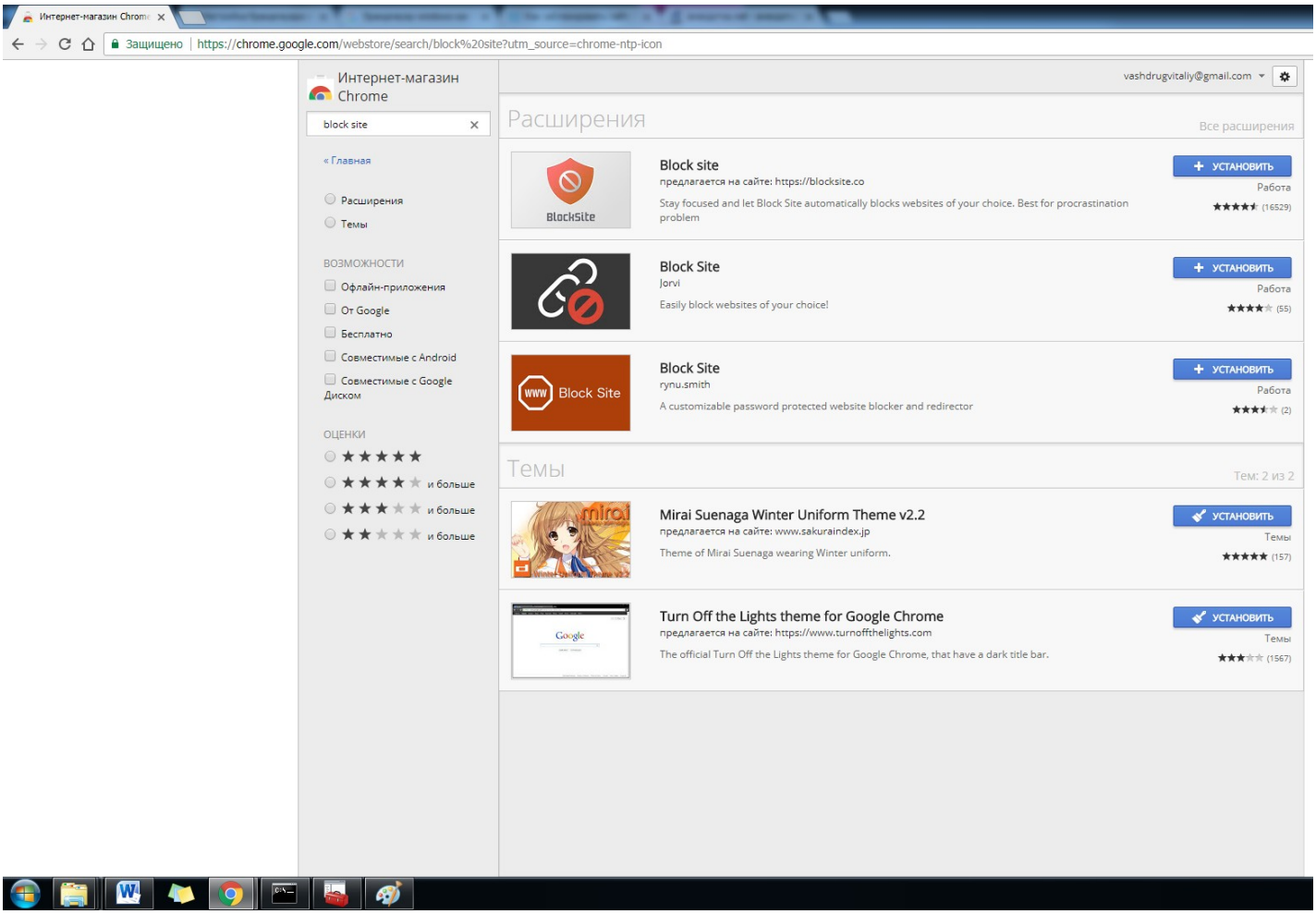
Для этого:

1. **Открываете Google Chrome нажимаете Сервисы**



2. **В интернет-магазине в Google Chrome вводите block site**

Скачайте один из сервисов(расширений для хрома) и заблокируйте доступ к любому из сайтов и предоставите скрин заблокированного сайта!!!!



После установки расширения, вы можете получить доступ к его настройкам через правый клик в любом месте открытой страницы в Google Chrome, или же в правом углу меню настроек goole Chrome .

После установки расширения выполните следующие действия:

1. Заблокируйте доступ по времени и дням недели.
2. Установите пароль на изменение параметров блокировки (в разделе «убрать защиту»).
3. заблокируйте сайта по адресу, если такое предусмотрено в расширении (и перенаправление на любой другой сайт при попытке входа на указанный.
4. заблокируйте слов (если слово встречается в адресе сайта, он будет заблокирован).

Блокировка рекламы в Google Chrome

1. **Открываете Google Chrome нажимаете Сервисы**
2. **В интернет-магазине в Google Chrome вводите adblock, устанавливаете расширения для Goole и реклама у вас на всех сайтах будет заблокирована.**

Контрольные вопросы:

1. **В каких случаях может не пройти перенаправление(редирект) сайта через файл hosts?**
2. **Для чего нужен firewall?**
3. **Как определить IP адрес сайта?**
4. **В каких случаях используют правила исходящих подключений, а в каких исходящих подключений?**
5. **Как добавить новое правило и заблокировать определенный IP адрес?**
6. **Сколько IP адресов можно блокировать одновременно?**
7. **Можно ли блокировать IP адреса в определённом диапазон? Если да, то как?**
8. **Что делает команда ping?**
9. **Как установить расширение для блокировки страниц в goole Chrome?**
10.

Список использованных источников:

1. http://studydoc.ru/doc/178007/laboratornaya-rabota.-sistemnyj-reestr-windows
2. http://ab57.ru/reestr.html
3. http://remontka.pro/block-website/
4. https://windows-9.net/kak-nastroit-brandmauer-windows-7.html

Содержание отчета:

1. Тема, цель лабораторной работы
2. Поэтапное описание выполнения лабораторной работы
3. Скриншоты выполнения и результирующий скриншот экрана
4. Краткие ответы на контрольные вопросы
5. Выводы