**Практическая работа**

**«Настройка браузера. Настройка брандмауэра»**

ЦЕЛИ РАБОТЫ:

1. Научиться настраивать браузер и устанавливать расширения.

2. Изучение понятия системного брандмауэра. Получение практических навыков по включению и настройке системного брандмауэра.

ОБОРУДОВАНИЕ: ПК, Windows 10.

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

**Браузер -** прикладное программное обеспечение для просмотра страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями.

В глобальной сети браузеры используют для запроса, обработки, манипулирования и отображения содержания веб-сайтов. Многие современные браузеры также могут использоваться для обмена файлами с серверами FTP, а также для непосредственного просмотра содержания файлов многих графических форматов (GIF, JPEG, PNG, SVG), аудио-видео форматов (MP3, MPEG), текстовых форматов (PDF, DJVU) и других файлов.

Функциональные возможности браузеров постоянно расширяются и улучшаются благодаря конкуренции между их разработчиками и высоким темпом развития и внедрения информационных технологий. Браузеры распространяются, как правило, бесплатно. Потребителям браузер может быть поставлен в форме самостоятельного (автономного) приложения или в составе комплектного программного обеспечения.

В настоящее время наиболее популярными являются: Internet Explorer; Mozilla Firefox; Opera; Google Chrome; Safari.

**Брандмауэр Windows** - встроенный в Microsoft Windows межсетевой экран. Одним из отличий от предшественника (Internet Connection Firewall) является контроль доступа программ в сеть. Брандмауэр Windows является частью Центра обеспечения безопасности Windows.

Первоначально Windows ХР включала Internet Connection Firewall, который (по умолчанию) был выключен из-за проблем совместимости. Настройки Internet Connection Firewall находились в конфигурации сети, поэтому многие пользователи не находили их.

Microsoft решила значительно улучшить интерфейс и функциональность Internet Connection Firewall и переименовать его в «Брандмауэр Windows».

В брандмауэр Windows встроен журнал безопасности, который позволяет фиксировать IP-адреса и другие данные, относящиеся к соединениям в домашних и офисной сетях или в Интернете. Можно записывать как успешные подключения, так и пропущенные пакеты. Это позволяет отслеживать, когда компьютер в сети подключается, например, к web-сайту. Данная возможность по умолчанию отключена (её может включить системный администратор).

Изначально Брандмауэр Windows вышел в составе Windows ХР Service Pack 2. Брандмауэр по умолчанию фильтрует все типы сетевых подключений: беспроводное, проводное, FireWire и VPN. Это позволяет решить проблему уязвимости, связанную с тем, что правило фильтрации начинает действовать лишь по истечении нескольких секунд после установления соединения.

**Брандмауэр Windows возможности:**

1. Применяя расширенный пакетный фильтр, появляется возможность использовать правила к определенным диапазонам портов и 1Р-адресов;

2. Новая оснастка консоли Брандмауэр Windows в режиме повышенной безопасности позволяет поддерживать удаленное администрирование и сделать доступными дополнительные возможности. Доступ к ней можно получить следующим образом: Пуск - Панель управления - Администрирование - Брандмауэр Windows в режиме повышенной безопасности. Либо наберите команду «wf.msc»;

3. Фильтрация исходящего трафика позволяет бороться с различными шпионскими программными обеспечениями и вирусами;

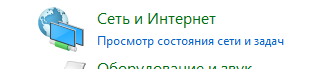
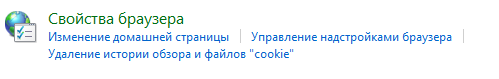
4. Фильтр соединений IPv6.

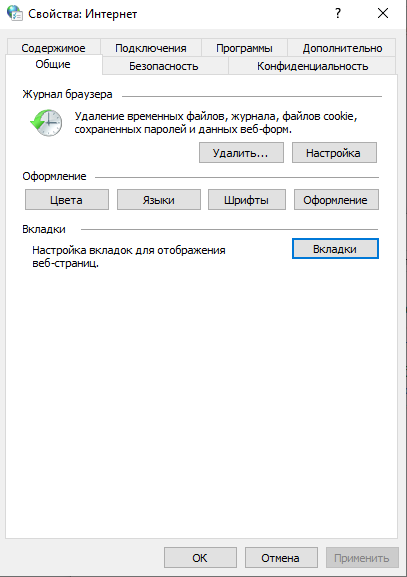
***ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:***

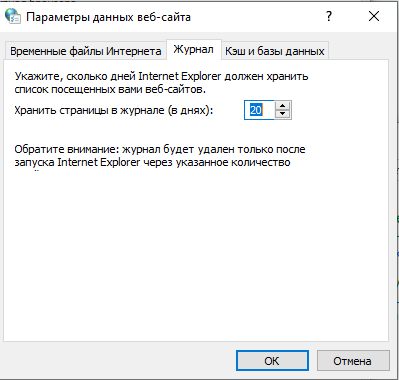
**Задание 1. Сделать сравнительный анализ популярных браузеров. Результаты анализа оформить в таблице.**

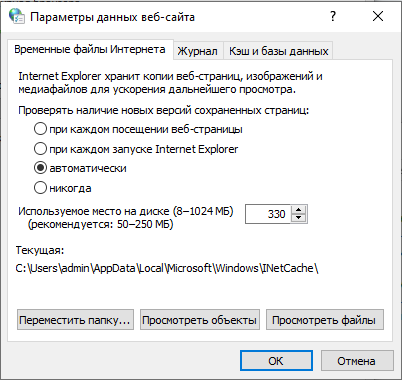
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Название** | **Дата первой публичной версии** | **Последний релиз** | **Стоимость** | **Текущее ядро** | **Производитель** |
| Яндекс | Октябрь 2012 | 23.11.3.955 | Бесплатно | Blink | Яндекс |
| Google Chrome | Сентябрь 2008 | 1.0.154.42 | Бесплатно | Linux | Google |
| Microsoft Edge | Март 2015 | 121.0.2277.84 | Бесплатно | EdgeHTML | Microsoft |
| Opera GX | Июнь 2019 | 105.0.4970.63 | Бесплатно | Сhromium | Opera Software |
| Mozilla Firefox | Сентябрь 2002 | 122.0 | Бесплатно | Quantum | Mozilla Corporation |

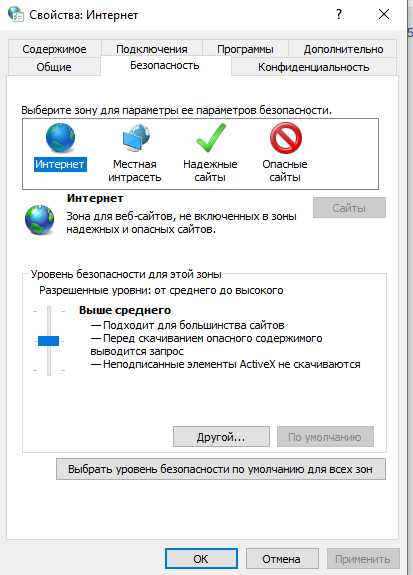
**Задание 2. Осуществить настройку браузера.**

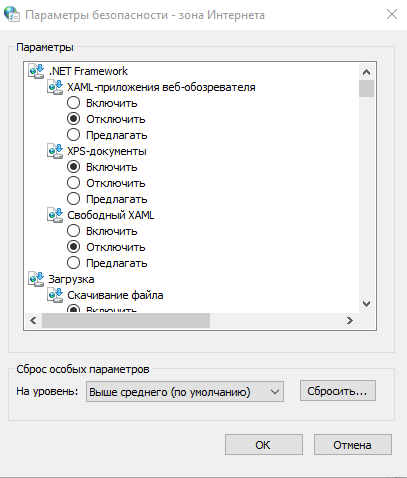
1. Выбирать Панель управление - Сеть и Интернет - Свойства обозревателя.

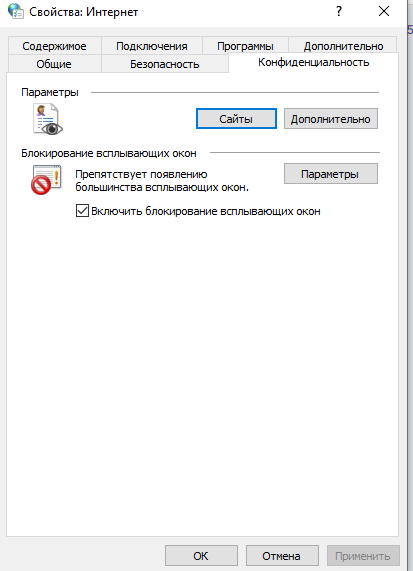
2. Вкладка «Общие» позволяет задать адрес домашней страницы, которая будет автоматически загружаться в окно браузера при его запуске, цвета гиперссылок по умолчанию, название шрифта по умолчанию.

3. Здесь же определяется, сколько дней будет храниться ссылка посещенных страниц в журнале.

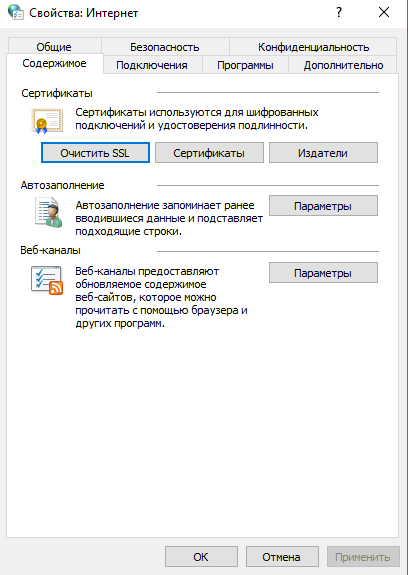
4. Кроме того, для ускорения просмотра. Все посещенные страницы помещаются в специальную папку, и с помощью кнопки «Параметры» можно задать разные способы обновления таких страниц.

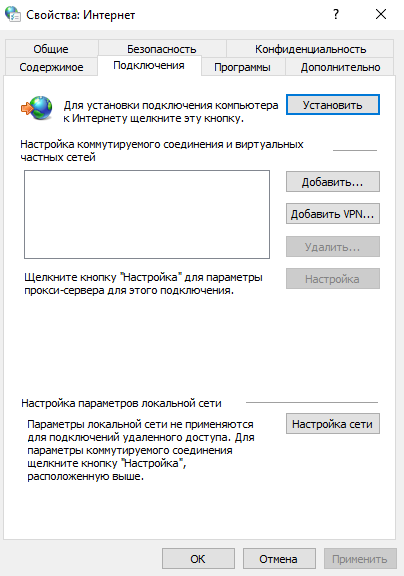
5. С помощью вкладки «Безопасность» можно создать списки надежных узлов и узлов с ограниченными функциями. Зона Интернет будет при этом включать все остальные узлы, не вошедшие в эти две папки. Для каждой из них с помощью кнопки «Другой» можно изменить параметры безопасности, установленные для них по умолчанию. Здесь можно запретить выполнение сценариев, отображение всплывающих окон, загрузку файлов и т.д.



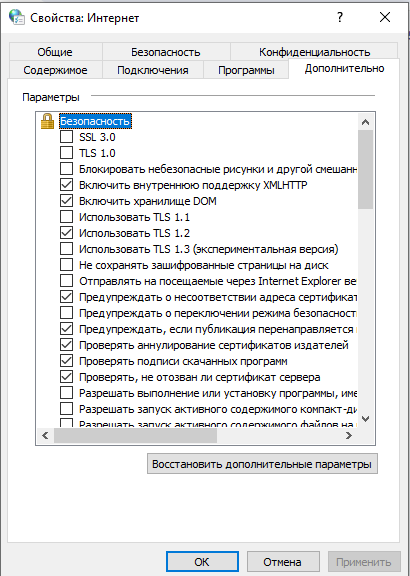
6. Вкладка «Конфиденциальность» дает возможность настроить работу с файлами cookie, с помощью которых информация о пользователе автоматически передается на сервер.

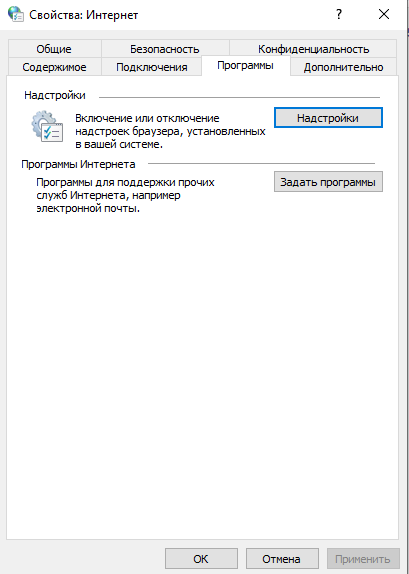
7. Вкладка «Содержание» позволяет ограничить доступ к некоторой информации (насилие, ненормативная лексика и т.д.).



8. Вкладка «Подключения» позволяет установить подключение к Интернету.

9. На вкладке «Дополнительно» можно задать некоторые дополнительные параметры работы (отключить загрузку графических изображений, отменить подчеркивание ссылок, запретить отладку сценариев и т.д.).



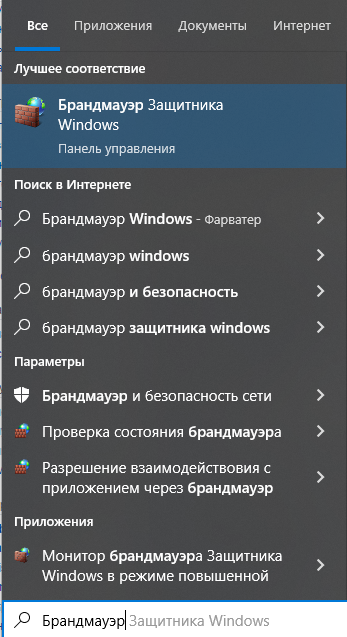
10. Вкладка Программы позволяет определить программы, которые будут по умолчанию использоваться службами Интернета (почтовые программы, HTML редакторы и т.п.).

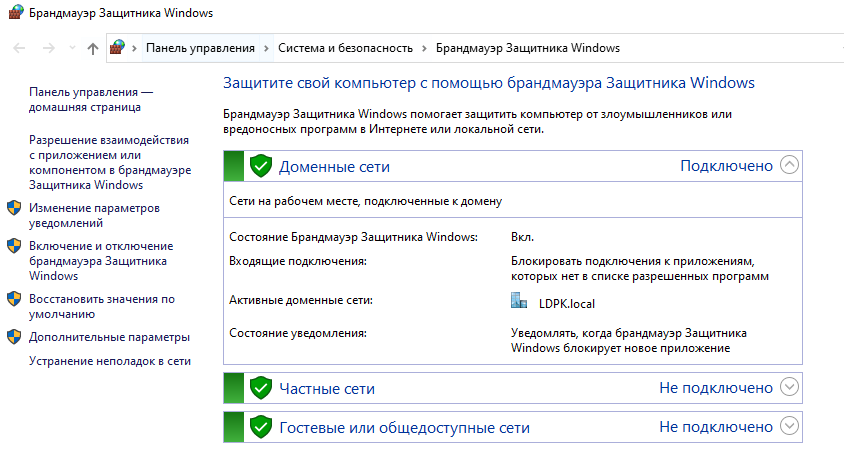
**Задание 3. Сделать сравнительный анализ брандмауэров. Результаты анализа оформить в таблице.**

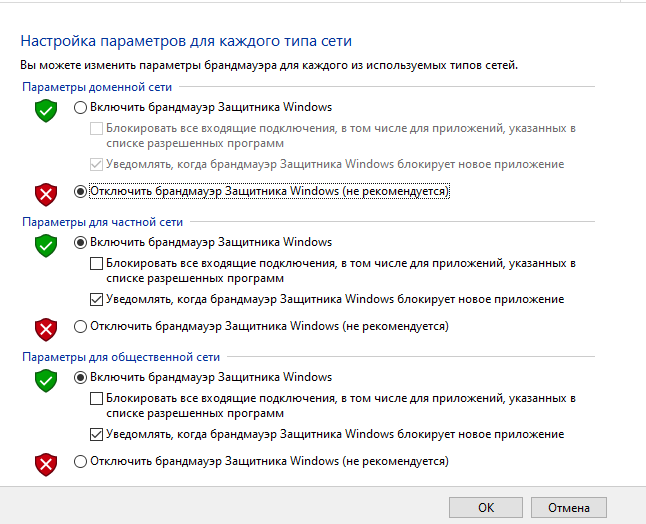
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название | Год выпуска | Версия | Стоимость | Производитель |
| Comodo Firewall | 2008 | 5.3.176757.1236 | Бесплатен | Comodo |
| Privatefirewall | 2008 | 7.0.25.4 | Бесплатен | PWI |
| Malware Defender | 2006 | 2.7.3.0002 | Бесплатен | Qihoo 360, Software |
| Kaspersky Internet Secuirity | 2000 | 12.0.0.374 | 1519 р/ год | Лаборатория Касперского |
| Avast Internet Security | 1988 | 13.12.2023 | 1200 р/ год | AVAST SOFTWARE |
| Norton 360 | 2006 | 22.22.11.12 | 2599 р/ год | Symantec Corporation |
| Outpost Security Suite Free | 2010 | 7.0.4.3418.520.1245.401 | Бесплатная | Agnitum |
| pFSense | 2001 | 2.5.2 | Бесплатная | FreeBSD |

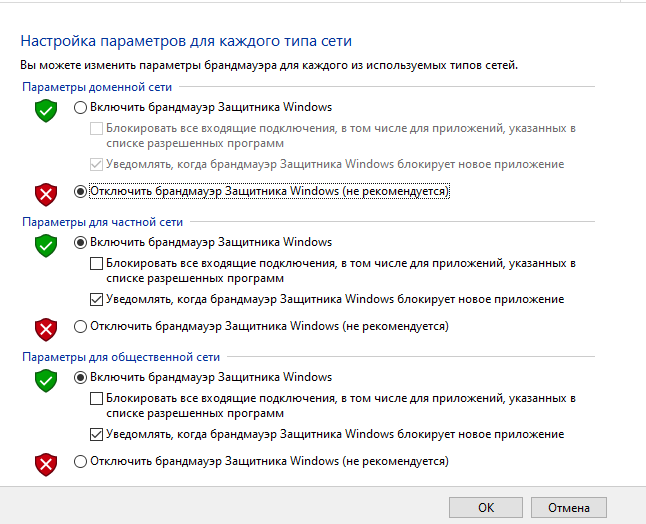
**Задание 4. Осуществить настройку брандмауэра.**

***Включение и отключение системного брандмауэра***

1. Проще всего найти брандмауэр в Windows — это воспользоваться поиском через меню Пуск. Для этого кликните по кнопке «Пуск» в левом нижнем углу экрана и в строку поиска вбейте Брандмауэр и кликните на появившемся значке «Брандмауэр Windows».

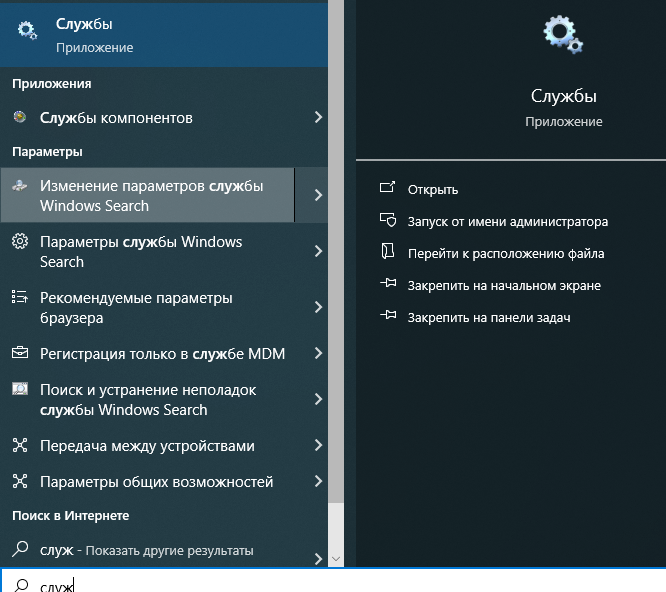
2. После того как откроется страница брандмауэра, выберите в левом меню пункт «Включение и отключение брандмауэра Windows»..

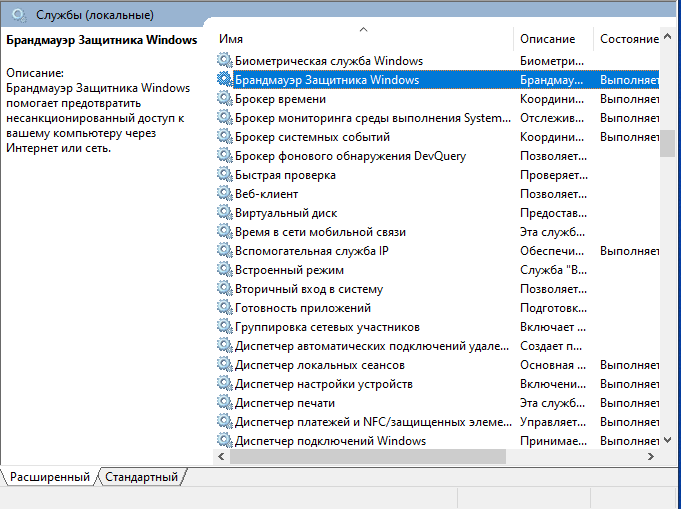
3. Кликнув по вкладке включение и отключение брандмауэра Windows, попадете на страницу, на которой можно как включить, так и отключить брандмауэр Windows, просто выбрав пункт меню «Отключить Брандмауэр (не рекомендуется)», причем можно выбрать отключение как только для своей домашней сети, так и для всех остальных.

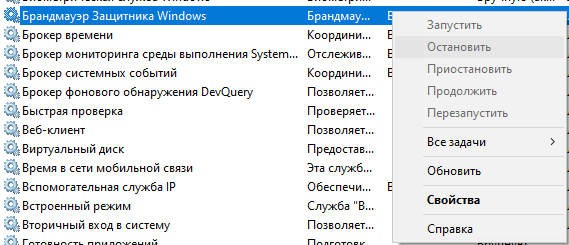
4. Как понимаете, включить брандмауэр Windows (если он выключен) можно точно так же, только лишь необходимо отметить пункт меню «Включение брандмауэра Windows». В этом же окошке можно снять галочки различных уведомлений, когда брандмауэр блокирует новые программы.

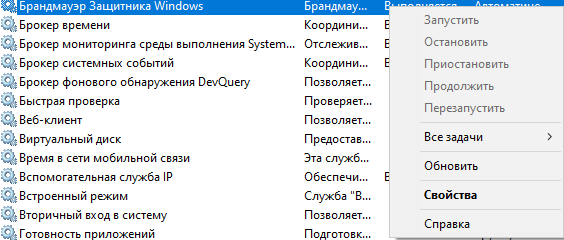
***Отключение службы Брандмауэр Windows***

1. Для оптимизации операционной системы, так же рекомендуется отключить службу Брандмауэра Windows. Проще всего опять использовать поиск в меню «Пуск». В строку поиска вбейте «Службы» и кликните по ним, для того что бы их открыть.



2. Для того что бы быстро найти службу Брандмауэр Windows, кликните на любой службе одни раз и нажмите на клавиатуре букву Б, сразу же найдете нужную службу и уже на ней кликните двойным щелчком, для того что бы ее открыть.

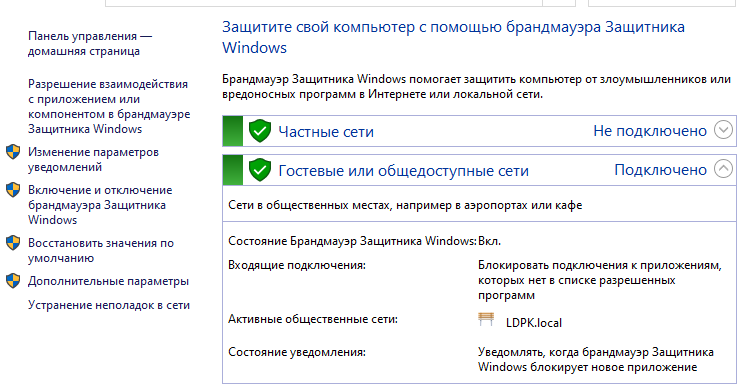
3. В строке Состояние — нажмите Остановить. Откройте выпадающее меню Тип запуска и выберите Отключена и нажмите ОК. Появится диалоговое окно с предложением перезагрузить компьютер прямо сейчас или вы можете выйти без перезагрузки, выполнив ее чуть позже.

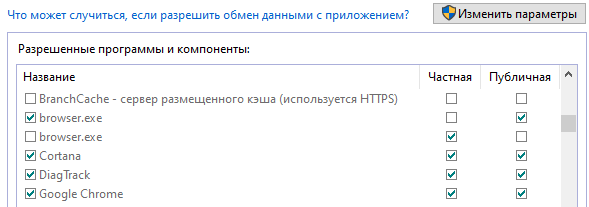
4. Для того что бы включить брандмауэр Windows, выполните те же действия в обратном порядке: Настройка брандмауэра Windows-> Исключения брандмауэра Windows.

***Снятие блокировки программ в Брандмауэре Windows***

1. Когда брандмауэр блокирует приложения или например брандмауэр порой блокирует доступ к интернет сети для некоторых игр, существует достаточно простой способ снять это ограничение и дать полный доступ на выход в интернет для этого приложения, в этой сети, к которой подключены.

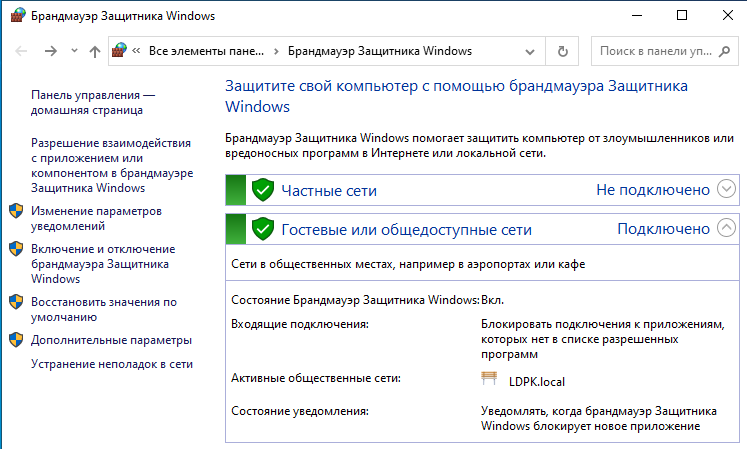
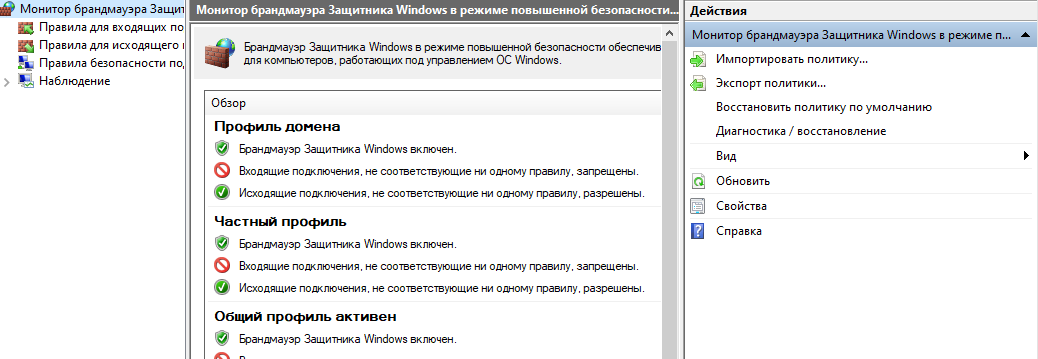
Для этого на странице межсетевого экрана (брандмауэра) выберите в левом меню пункт меню: Разрешить запуск программ через брандмауэр Windows.



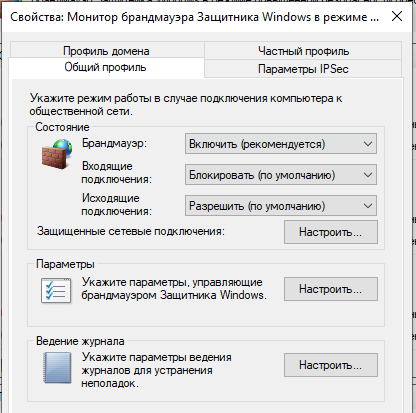
2. Найдите в списке программу и дайте ей доступ в нужной сети или сразу во всех, где нет галочек, таким образом можно добавлять Исключения брандмауэра Windows.

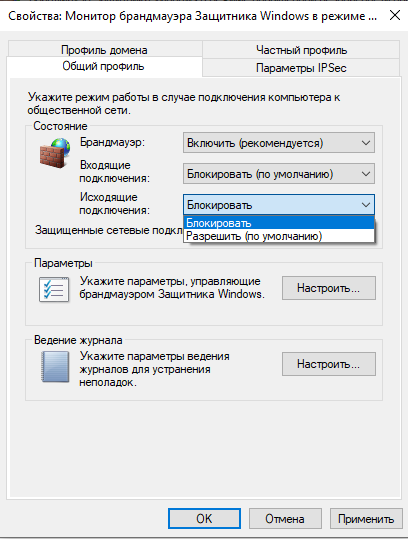
***Настройка брандмауэра Windows***

1. Для настройки брандмауэра Windows, необходимо перейти на вкладку Дополнительные параметры в окне Брандмауэра. Выберите Брандмауэр Windows в режиме повышенной безопасности в левом меню, после чего в правой колонке, кликните по пункту «Свойства».

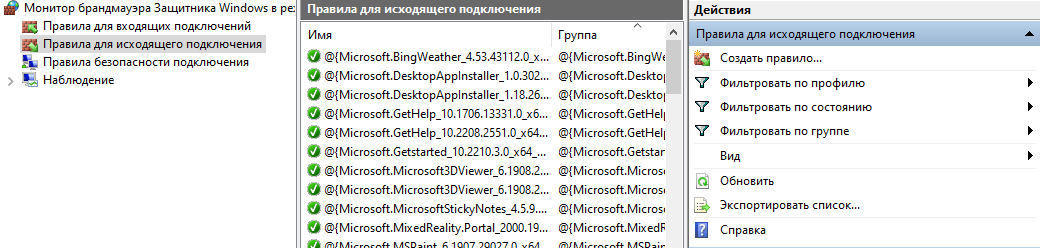


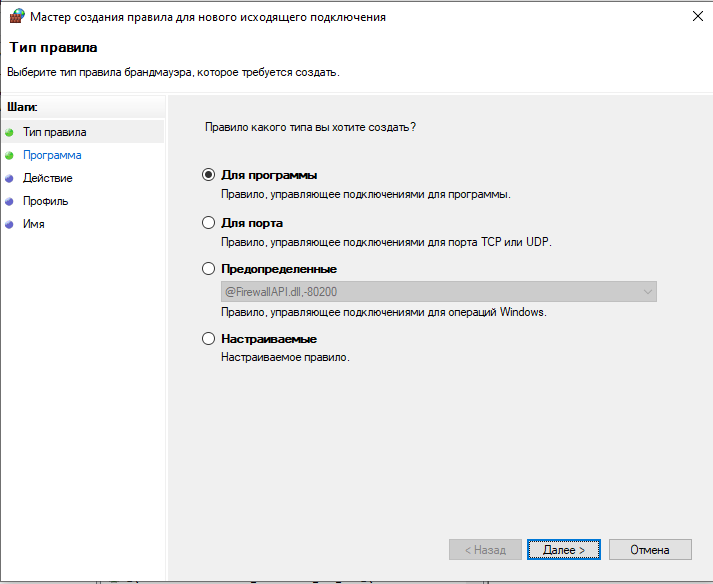
2. Откроется меню Свойства Брандмауэра, в котором можно заблокировать весь исходящий трафик, на вкладке Исходящие подключения.

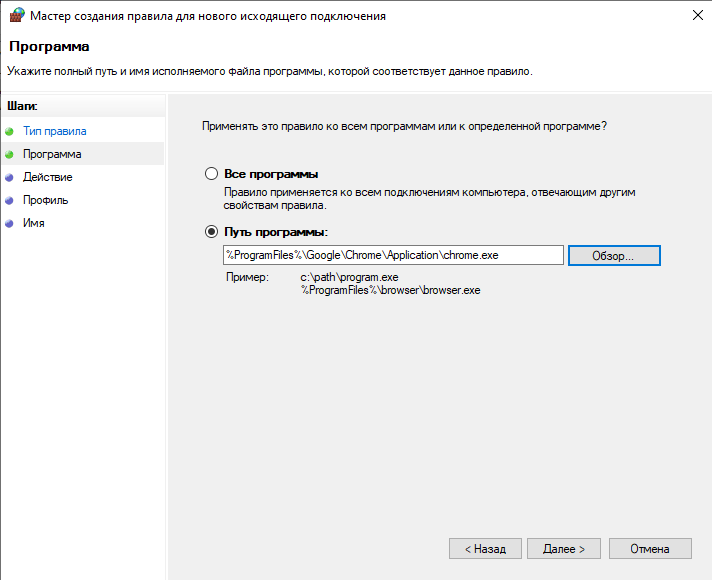


3. В выпадающем меню выберите «Блокировать» и нажмите Ок.

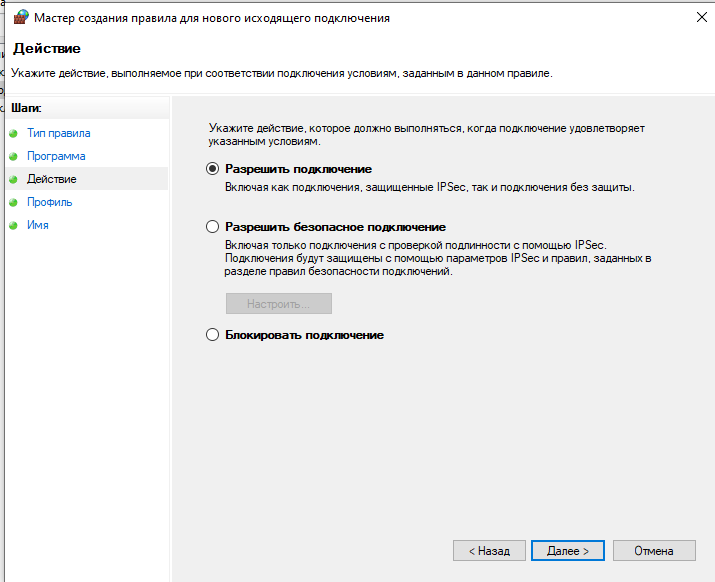
4. После того как были заблокированы все исходящие подключения к Интернет, можно создать правило, которое позволит подключаться к интернету некоторым программам. Давайте для примера создадим правило разрешающее браузеру Google Chrome подключаться к сети интернет.

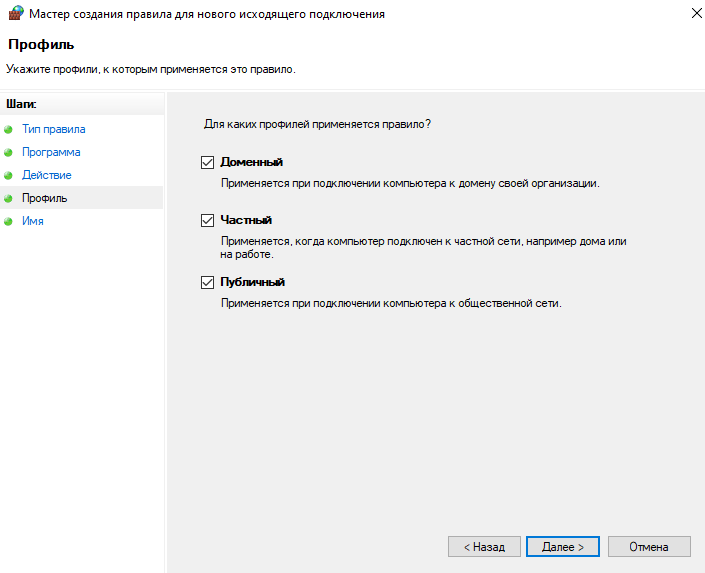
4.1. Для того что бы создать правило исходящего подключения, выберите «Правила для исходящего подключения», а в колонке действия выберите «Создать правило».

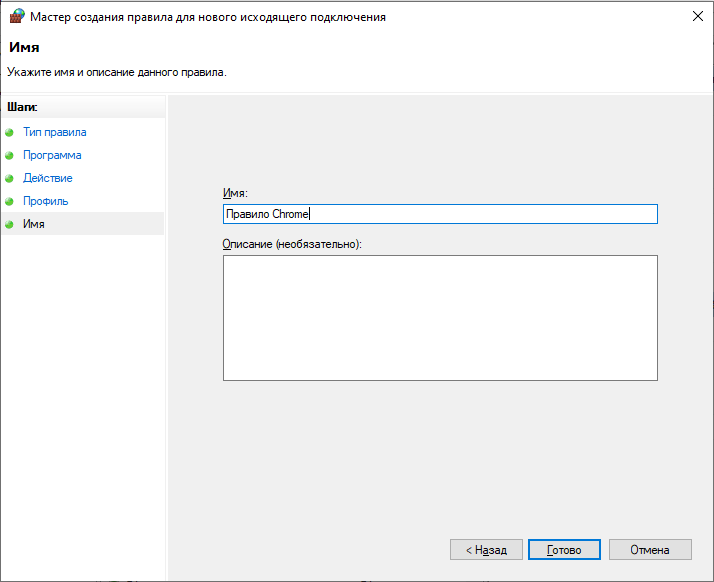
4.2. Появится мастер добавления нового правила, в котором необходимо нажать Далее.

4.3. На следующей странице, используя кнопку Обзор добавляете путь к приложению, в нашем случае к браузеру Google Chrome.

4.4. Для поиска пути расположения нужного ехе файла, можно воспользоваться поиском или посмотреть в свойствах ярлыка, там всегда указан путь к приложению.

4.5. Нажимаете далее —>на следующем шаге отмечаете Разрешить подключение и опять Далее.

4.6. Отмечаете, для каких профилей применяется правила и нажимаете «Далее».

4.7. На следующем шаге необходимо ввести имя для правила и если необходимо, то и его описание.

4.8. Новое правило для брандмауэра успешно создано и работает, о чем свидетельствует зеленая галочка напротив правила.