Тема: Настройка межсетевого экрана в Windows 10

Цель: Ознакомиться с встроенным в Windows межсетевым экраном.

Межсетевой экран (брандмауэр, файервол) предназначен для повышения безопасности системы при работе в сети, он ограждает сеть от внешних вредоносных атак, не пропускает «опасный» входящий и исходящий трафик и блокирует подозрительную активность.

- Межсетевой экран (МСЭ) — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решение: пропустить или блокировать конкретный трафик.

- Межсетевые экраны используются в качестве первой линии защиты сетей уже более 25 лет.

- Они ставят барьер между защищенными, контролируемыми внутренними сетями, которым можно доверять, и ненадежными внешними сетями, такими как Интернет.

- Межсетевой экран может быть аппаратным, программным или смешанного типа.

Типы межсетевых экранов

Межсетевой экран на прокси-сервере
Это один из первых типов МСЭ. Межсетевой экран на прокси-сервере служит шлюзом между сетями для конкретного приложения. Прокси-серверы могут выполнять дополнительные функции, например кеширование контента и его защиту путем предотвращения прямых подключений из-за пределов сети. Однако это может отрицательно сказаться на пропускной способности и производительности поддерживаемых приложений.

Межсетевой экран с контролем состояния сеансов
Он пропускает или блокирует трафик с учетом состояния, порта и протокола. Он отслеживает все действия с момента открытия соединения до его закрытия. Решения о фильтрации принимаются на основании как правил, определяемых администратором, так и контекста. Под контекстом понимается информация, полученная из предыдущих соединений и пакетов, принадлежащих данному соединению.

Межсетевой экран нового поколения (NGFW)
Современные межсетевые экраны не ограничиваются фильтрацией пакетов и контролем за состоянием сеансов. Большинство компаний внедряет межсетевые экраны нового поколения, чтобы противостоять

современным угрозам, таким как сложное вредоносное ПО и атаки на уровне приложений.

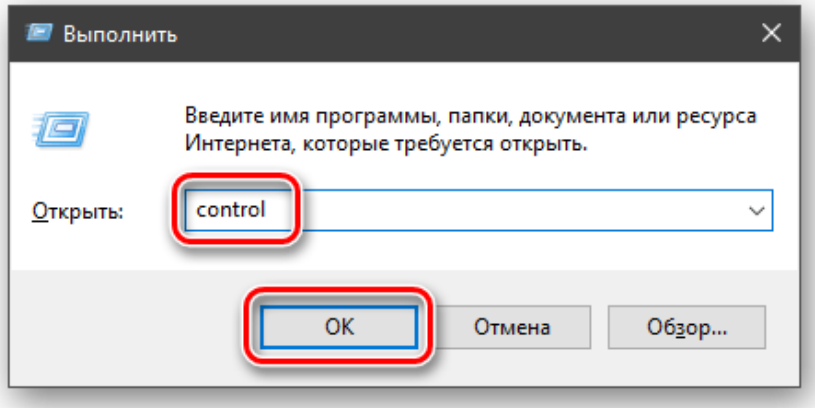
Настройка брандмауэра в Windows 10

В отличие от сторонних (особенно бесплатных) программ, брандмауэр Windows довольно легок в управлении, имеет дружественный интерфейс и понятные настройки.

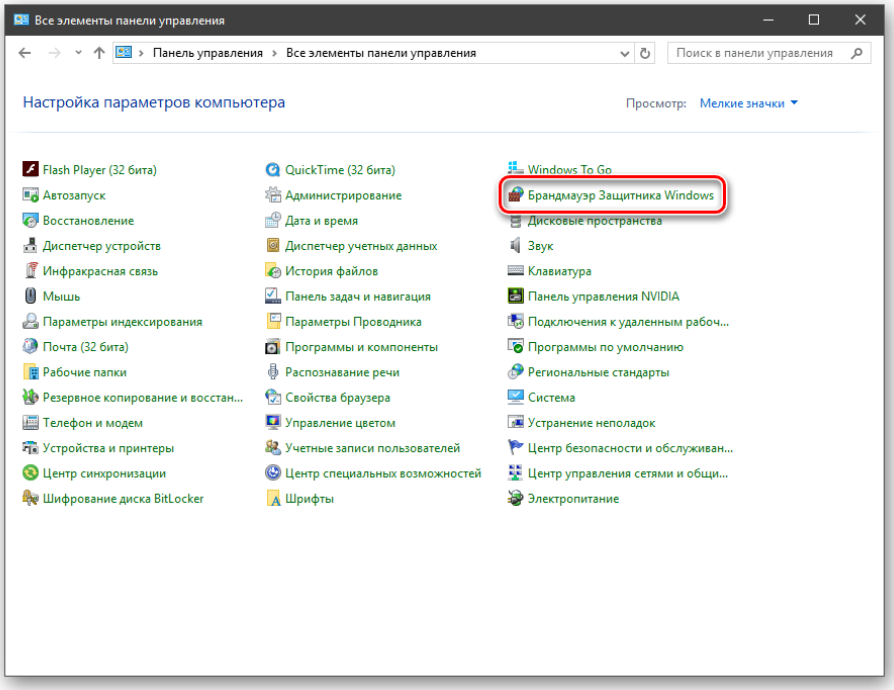
Встроенный брандмауэр не имеет рекламы и не требует платной активации. Брандмауэр работает в фоновом режиме беспрерывно и не может отключиться без команды пользователя. В случае если приложению потребуется доступ к определённым параметрам компьютера, придёт запрос от файервола, который нужно будет подтвердить.

Работа по настройке начинается из классической **«Панели управления»** Windows.

1. Вызываем меню **«Выполнить»** комбинацией клавиш **Windows+R** и вводим команду
   control
   Жмем **«ОК»**.

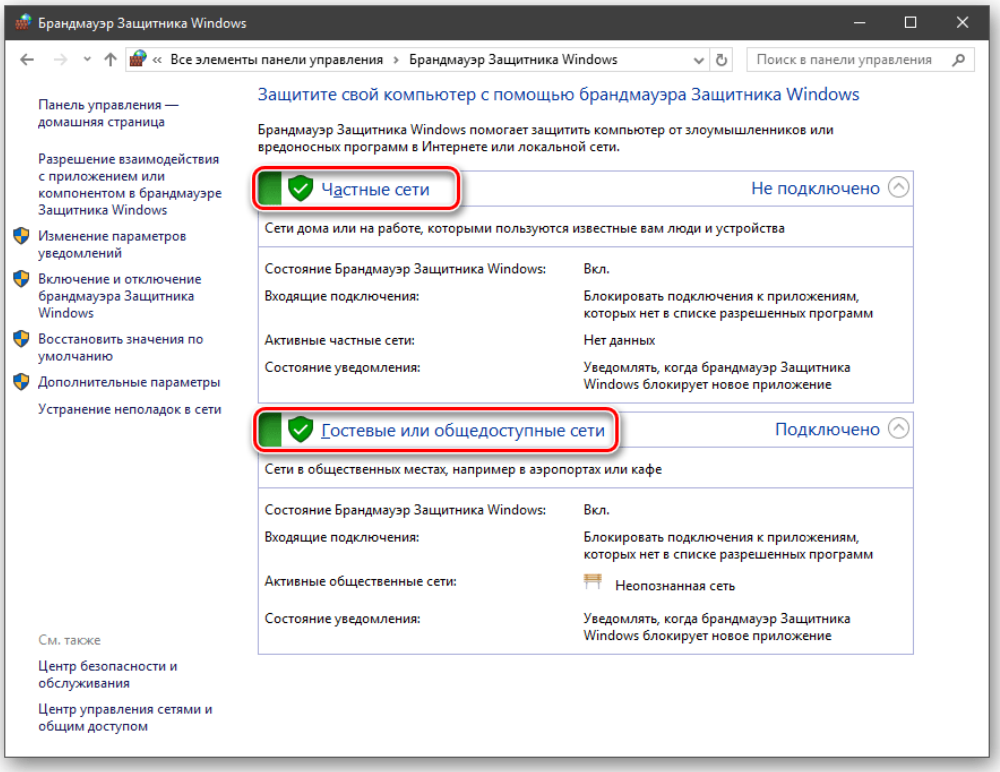


2. Переключаемся на режим просмотра **«Мелкие значки»** и находим апплет **«Брандмауэр защитника Windows»**.



Типы сетей

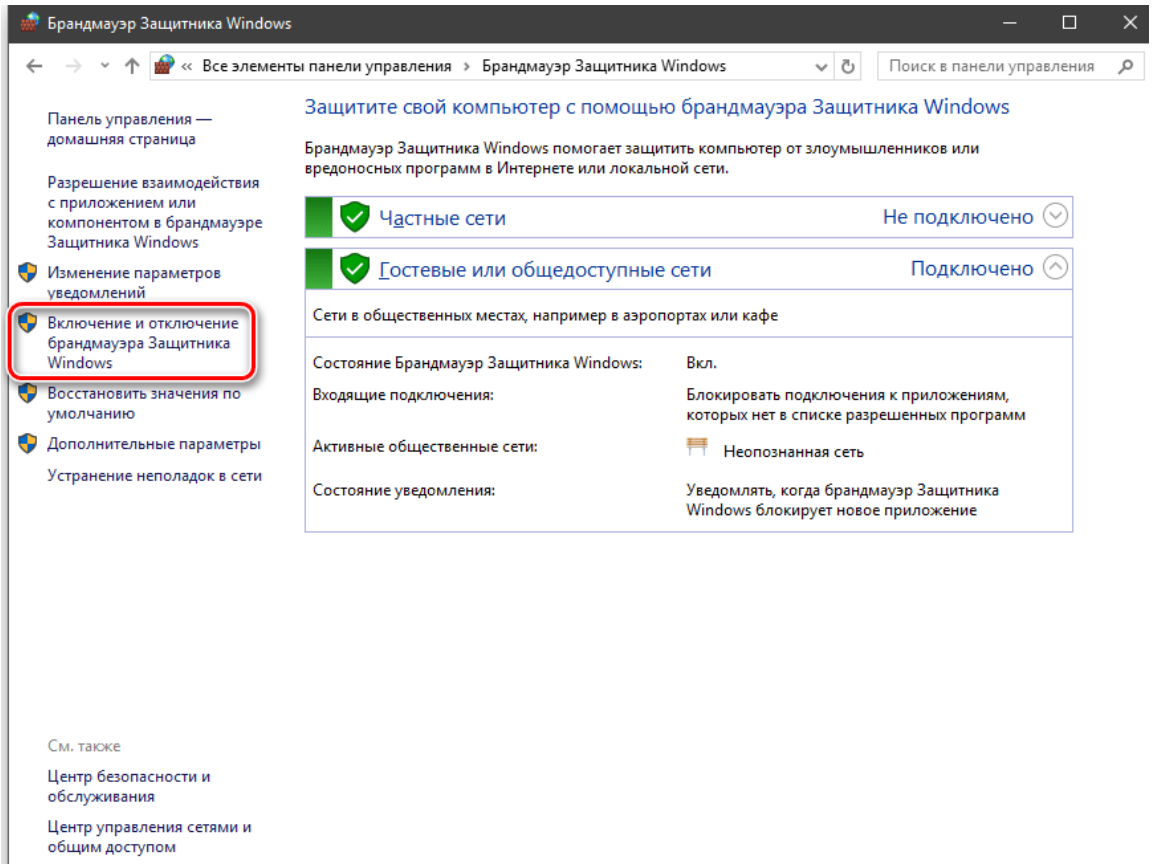
Различают два типа сетей: частные и общественные. Первыми считаются доверенные подключения к устройствам, например, дома или в офисе, когда все узлы известны и безопасны. Вторыми – соединения с внешними источниками через проводные или беспроводные адаптеры. По умолчанию общественные сети считаются небезопасными,
и к ним применяются более строгие правила.



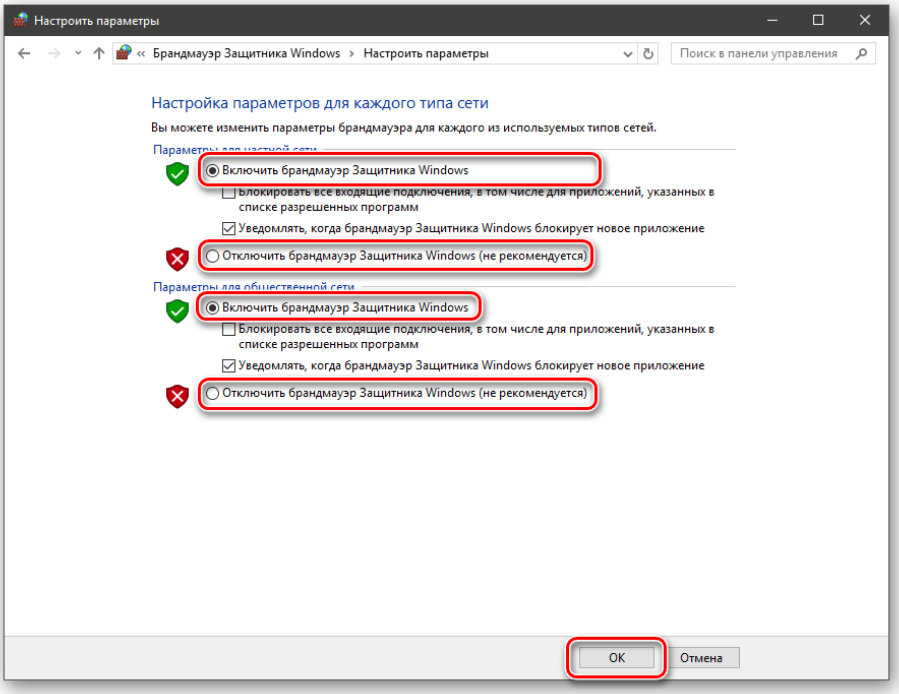
Включение и отключение, блокировка, уведомления

Активировать брандмауэр или отключить его можно, перейдя по соответствующей ссылке

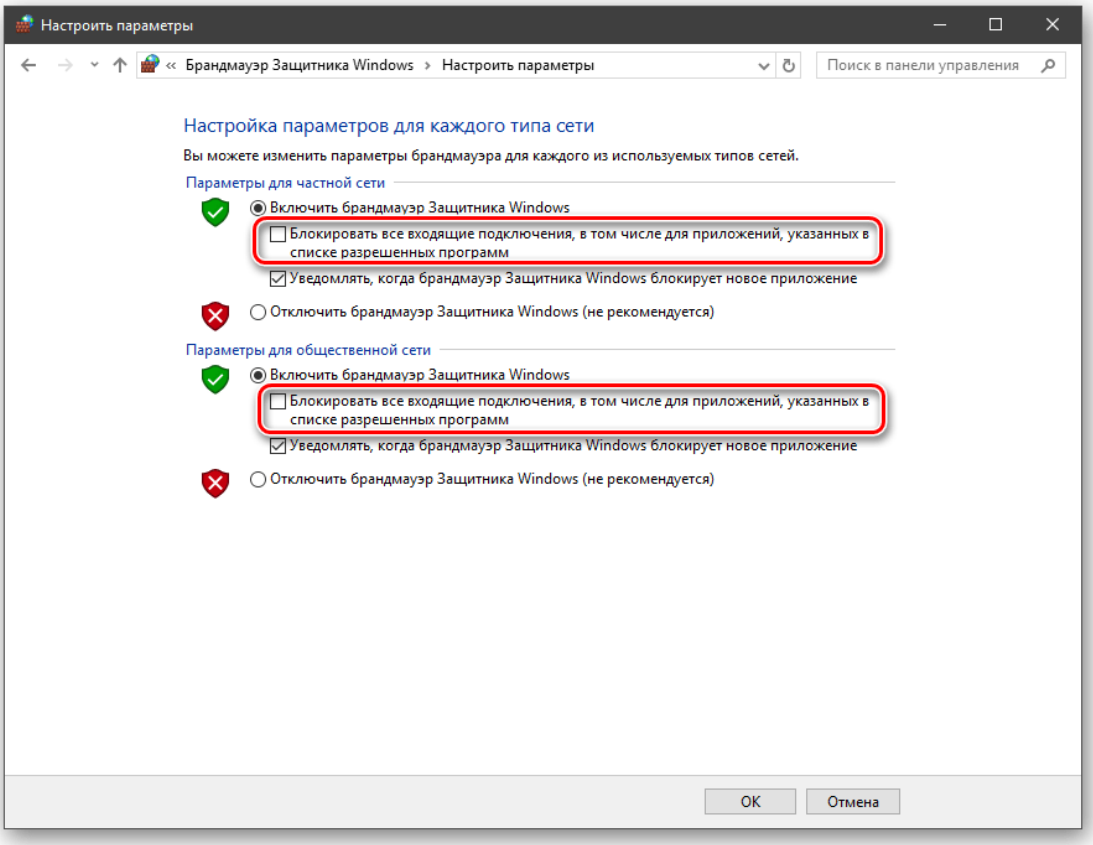
в разделе настроек:



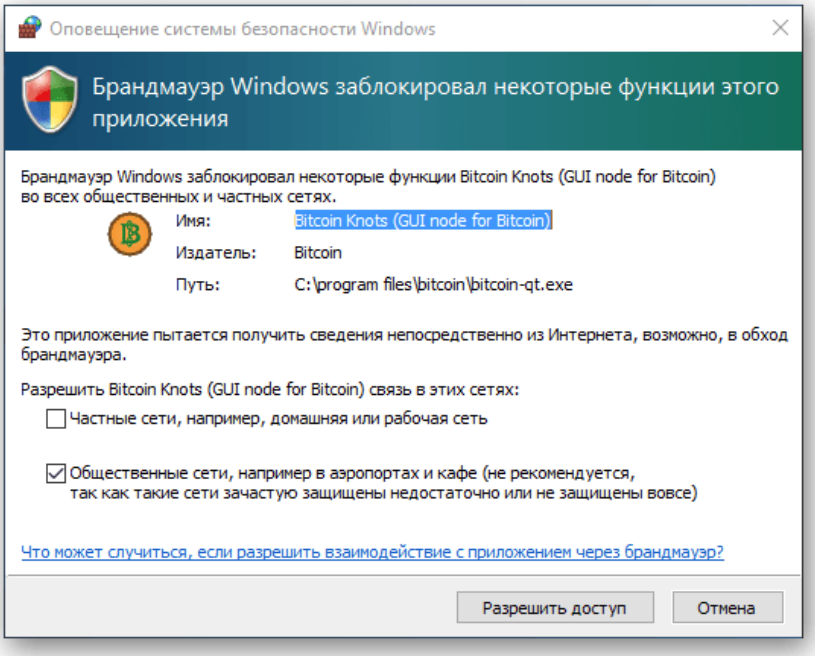
Здесь достаточно поставить переключатель в нужное положение и нажать **ОК**.



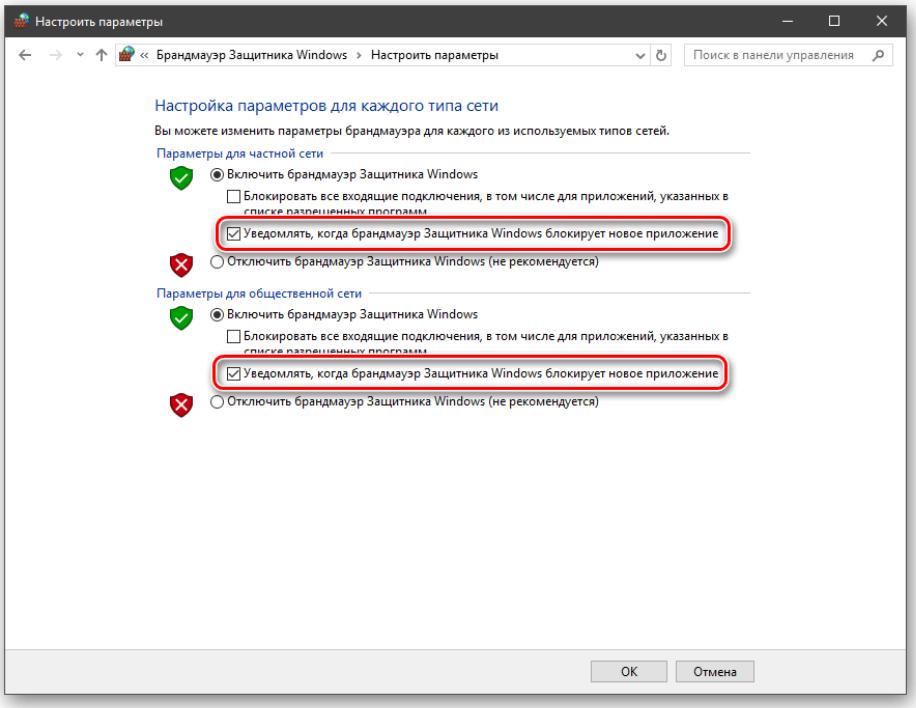
Блокировка подразумевает запрет всех входящих подключений, то есть любые приложения, в том числе и браузер, не смогут загружать данные из сети.



Уведомления представляют собой особые окна, возникающие при попытках подозрительных программ выйти в интернет или локальную сеть.

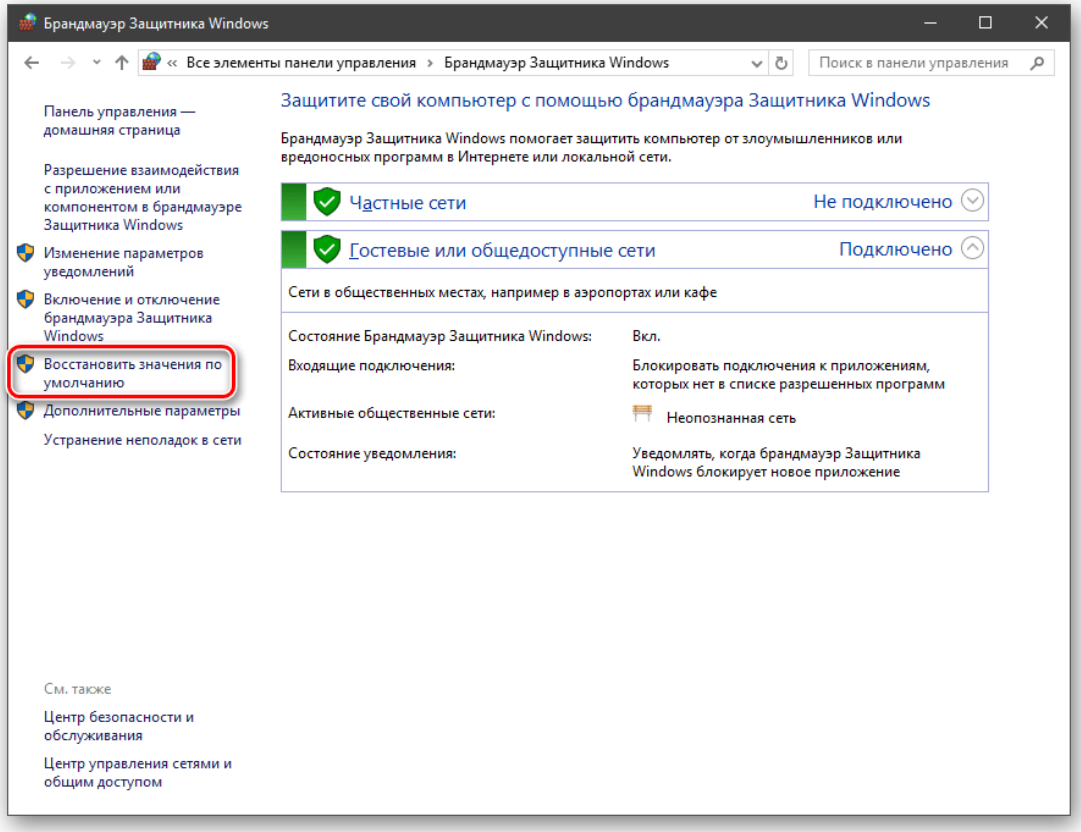


Функция отключается снятием флажков в указанных чекбоксах.

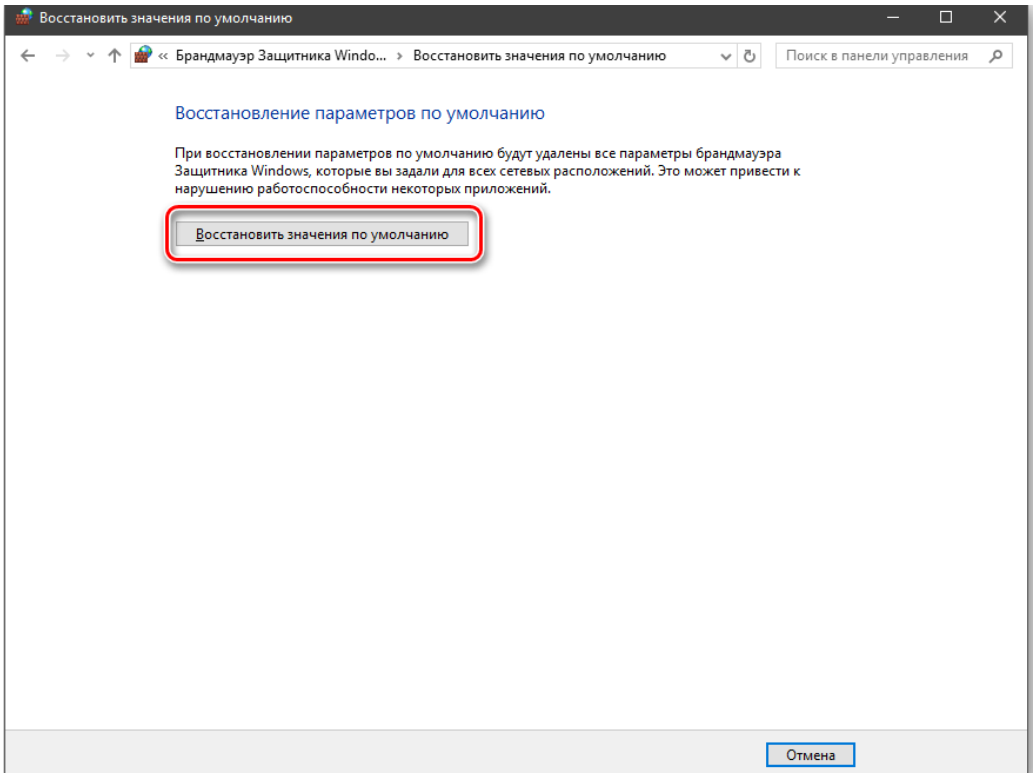


Сброс настроек

Данная процедура удаляет все пользовательские правила и приводит параметры к значениям по умолчанию.

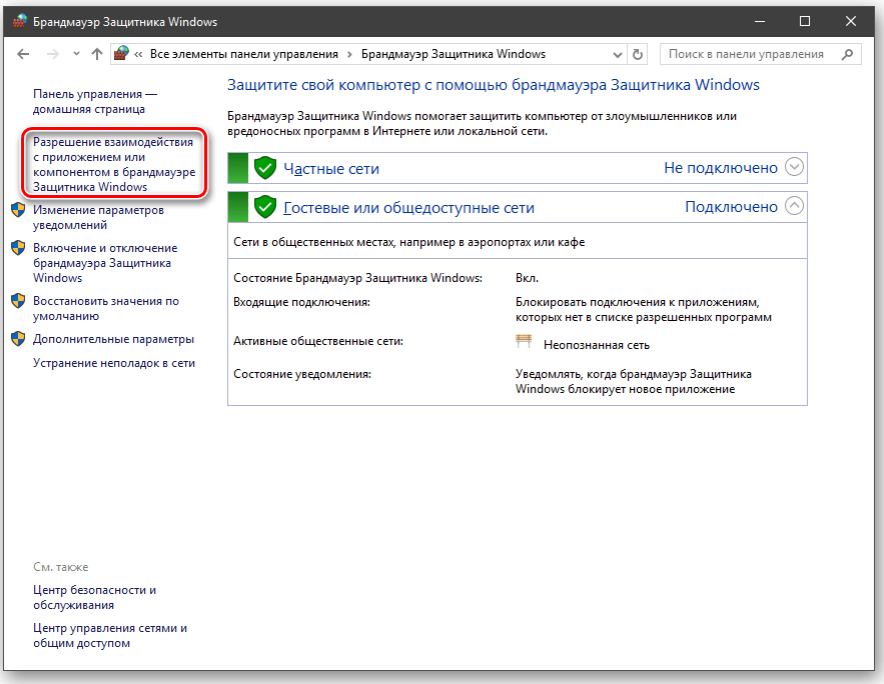


Сброс обычно производится при сбоях в работе брандмауэра в силу различных причин, а также после неудачных экспериментов с настройками безопасности. Следует понимать, что и «правильные» опции также будут сброшены, что может привести к неработоспособности приложений, требующих подключения к сети.

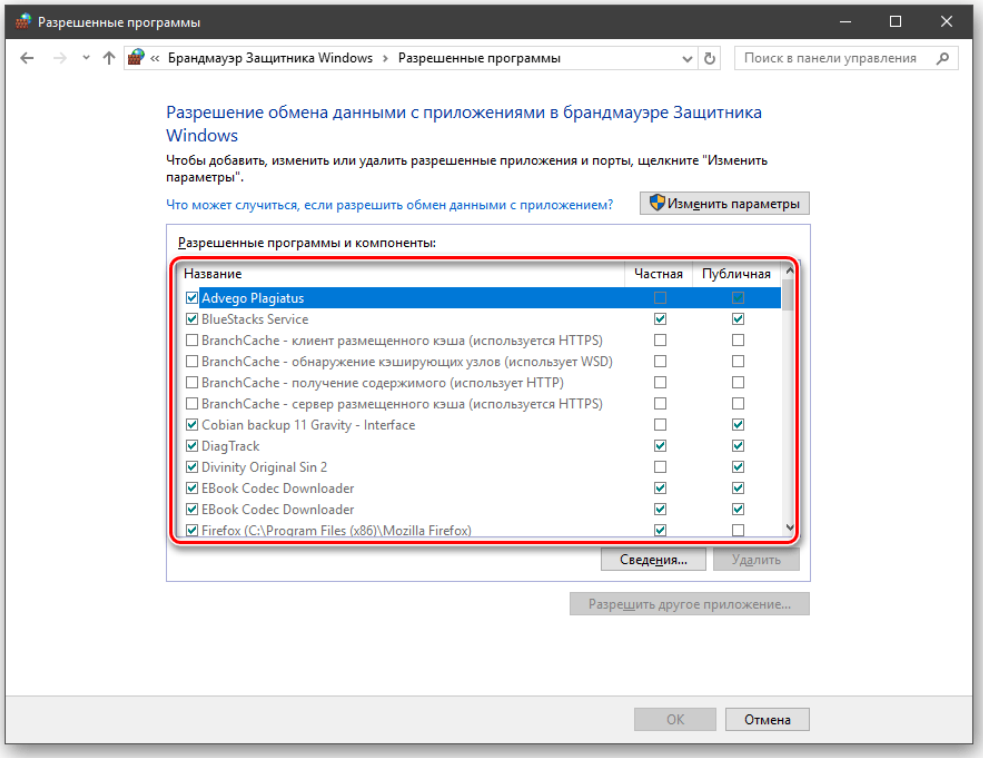


Взаимодействие с программами

Данная функция позволяет разрешить определенным программам подключение к сети для обмена данными.

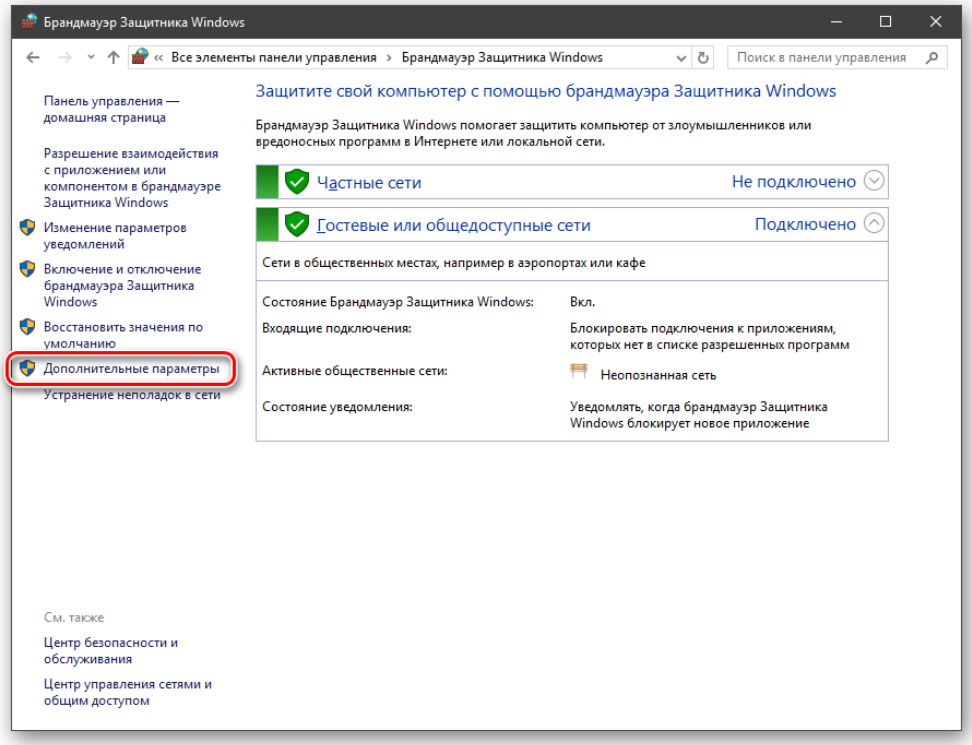


Этот список еще называют «исключениями».

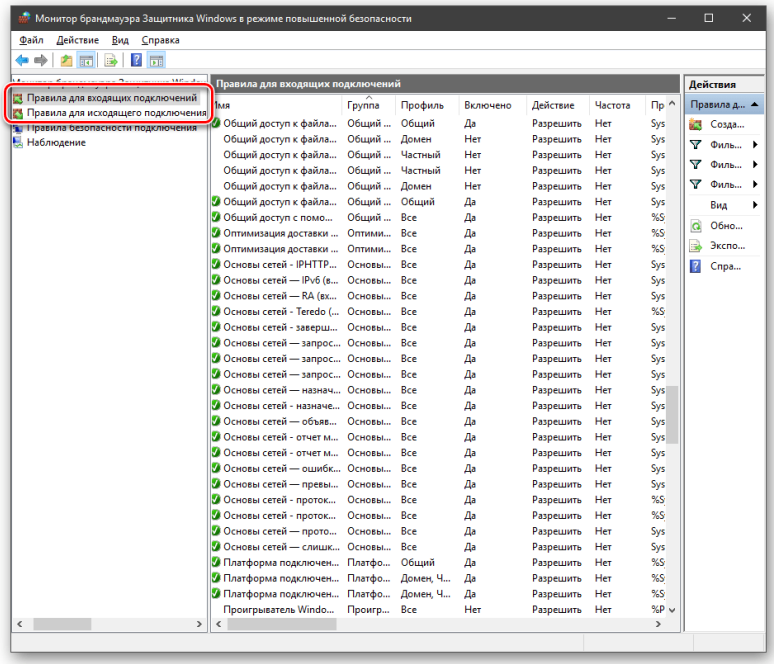


Правила

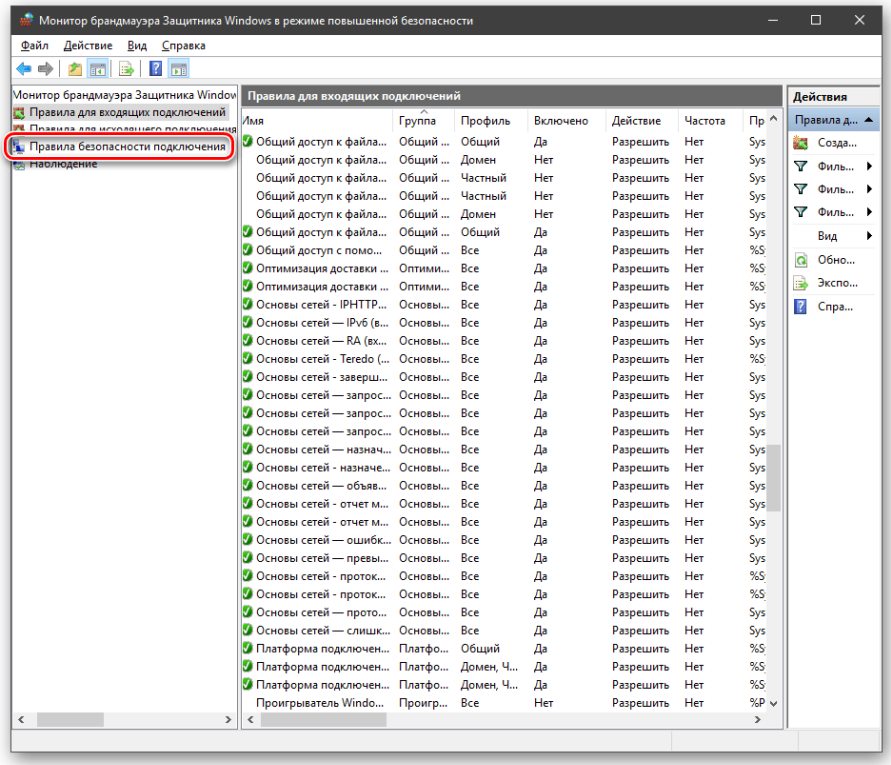
Правила – это основной инструмент брандмауэра для обеспечения безопасности. С их помощью можно запрещать или разрешать сетевые подключения. Эти опции располагаются в разделе дополнительных параметров.



Входящие правила содержат условия для получения данных извне, то есть загрузки информации из сети (download). Позиции можно создавать для любых программ, компонентов системы и портов. Настройка исходящих правил подразумевает запрет или разрешение отправки запросов на сервера и контроль процесса «отдачи» (upload).

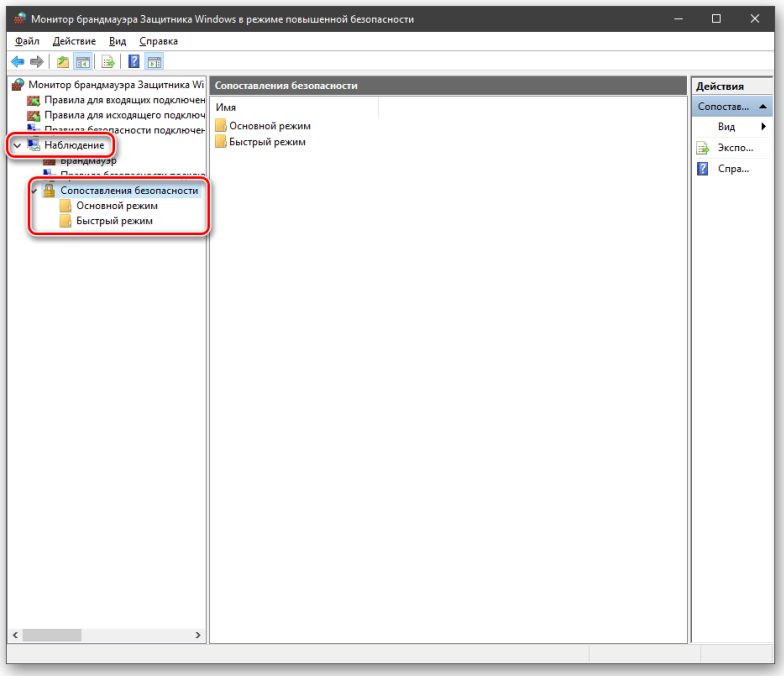


Правила безопасности позволяют производить подключения с использованием IPSec – набора специальных протоколов, согласно которым проводится



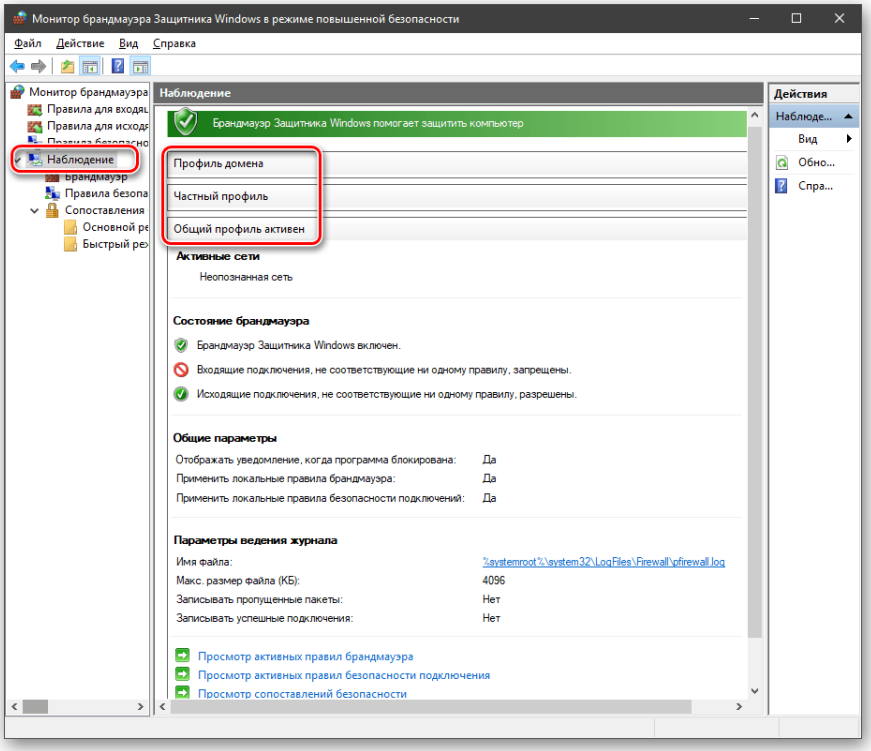
аутентификация, получение и проверка целостности полученных данных и их шифрование, а также защищенная передача ключей через глобальную сеть.

В ветке **«Наблюдение»**, в разделе сопоставления, можно просматривать информацию о тех подключениях, для которых настроены правила безопасности.



Профили

Профили представляют собой набор параметров для разных типов подключений. Существуют три их типа: **«Общий»**, **«Частный»** и **«Профиль домена»**.



При обычной работе эти наборы активируются автоматически при соединении с определенным типом сети (выбирается при создании нового подключения или подсоединении адаптера – сетевой карты).

Задание:

1. Ознакомиться с настройками встроенного брандмауэра Windows;
2. Используя интернет-ресурс https://lumpics.ru/firewall-settings-in-windows-10/ самостоятельно изучить вопросы создания правил для программ, работу с исключениями, правила для портов.
3. Ответить на вопросы:
   - что такое межсетевой экран?
   - какие типы межсетевых экранов существуют?
   - как настроить межсетевой экран в Windows 10?