Практическая работа

Файрвол в Windows и как его настроить?

В любой операционной системе должна быть хоть какая-то защита. В Windows есть целых две защитных функции – фаервол (брандмауэр) и Защитник Windows. Само понятие «фаервол» имеет несколько значений, но в этом материале будет разобран вариант межсетевого экрана.

Что такое файрвол?

Файрвол (брандмауэр) – является межсетевым экраном в системе Windows, предотвращающим несанкционированный доступ к компьютеру из сети Интернет и локальных сетей, а также запрещающий или разрешающий приложениям соединение с сетью.

Простыми словами, брандмауэр является стеной или закрытой дверью, которая открывается только перед теми, кому это разрешено. В Windows ограничения обычно ставятся на программное обеспечение, которые связывается с Интернетом. Теперь мы разобрались с понятием «фаервол», но как же его правильно настроить, чтобы обеспечить компьютеру защиту?

Как настроить фаервол (брандмауэр) на Windows 10?

В офисах этим занимается системный администратор, поэтому будет не лишним иметь навыки настройки защитного программного обеспечения. В домашних условиях любой желающий может изменять параметры компьютера как захочет, но в пределах разумного.

Настройка файрвола [после установки Windows 10](http://remontkomputerovnovosibirsk.ru/pereustanovka-windows.html) происходит очень просто. Вначале нужно разобраться, как включить или отключить защиту, так как при проблемах с брандмауэром возникают различные критические ошибки, исправить которые можно простым отключением или включением защитной функции.

Один из способов зайти в настройки брандмауэра следующий:

Используем на клавиатуре такую комбинацию клавиш: Win+I. Затем идём в раздел «Обновления и безопасность»;

Перейдите слева в подраздел «Защитник Windows»;

Нажмите на кнопку справа «Открыть Центр безопасности Защитника Windows»;

В открытом окошке выбираем опцию «Брандмауэр и безопасность сети».

Здесь находится новый интерфейс, в котором настройки немного запутаны для новичка. Если вам не нравится расположение функций, можно вернуться, конечно же, к старому, привычному интерфейсу, какой демонстрируется Windows 7 и 8. Для этого нажимаем по поиску на панели задач и вводим «Брандмауэр», выбрав результат.

Находясь в окне брандмауэра, в десятой версии системы можно увидеть два пункта – «Частная сеть» и «Общественная сеть». В обоих этих пунктах находятся опции отключения брандмауэра для подключенной сети. Тут можно и блокировать все входящие подключения, отметив функцию галочкой.

Чтобы разрешить программам устанавливать соединение с сетью через брандмауэр, нужно найти ниже пункт «Разрешить работу с приложениями через брандмауэр». Откроется окошко, где изменения параметров будут осуществляться после нажатия по кнопке «Изменить параметры».

Если галочка стоит, то обмен ПО через сеть разрешен. Обычно разрешения ставятся только на приложения Microsoft. Если с брандмауэром возникли проблемы, для их разрешения есть опция «Устранения неполадок [при подключении к сети](http://remontkomputerovnovosibirsk.ru/nastroyka-seti.html)». По возможности используйте её.

Перейдя в раздел «Параметры уведомлений», можно увидеть параметры, позволяющие выводить в системе уведомления о заблокированных программах. Если вы настроили параметры неверно, настройки можно «Восстановить по умолчанию». Эта опция находится на главном экране.

Как добавить программу в исключение в брандмауэре?

В главном окне фаервола перейдите к пункту «Параметры уведомлений брандмауэра»;

Щелкните по опции «Параметры защиты от вирусов и угроз»;

Дойдите до раздела «Исключения» и нажмите на кнопку в пункте «Добавление и удаление исключений»;

Теперь жмём кнопку «Добавить исключение» и выбираем тот элемент, который не является вредоносным по вашему мнению. Можно добавлять файлы, целые папки, конкретные типы файлов и процессы.

Дополнительные функции файрвола

В параметрах защиты от нежелательных и вредоносных программ можно активировать или отключить следующие функции:

Защита в режиме реального времени – если отключить эту защиту, это может привести к активной работе тех программ, которые были заблокированы.

Облачная защита – позволяет защищать данные в облаке.

Автоматическая отправка образцов – на сервера Microsoft отправляются данные о найденных вредоносных компонентах.

Остальные настройки уже были разобраны выше.

Настройка фаервола на Windows 7 и 8

При наличии устаревших версий операционных систем, настройка брандмауэра происходит немного по-другому:

Откройте брандмауэр из панели управления.

Необходимые настройки находятся с левой стороны окна, и доступ к ним осуществляется быстрее, чем в ОС Windows 10.

Для включения фаервола нажмите на кнопку параметра «Включение и отключение брандмауэра Windows». Сразу после этого отметьте флажки «Включить…».

Также вы можете сразу сбросить параметры по умолчанию, осуществить взаимодействие приложений в брандмауэре, и настроить уведомления.

Правила безопасности брандмауэра

В окошке слева переходим по опции «Дополнительные параметры». Сразу откроется окошко, где для приложений можно настроить правила по входящим и исходящим подключениям.

Здесь можно полноценно управлять приложениями, соединяющимися с сетью и создавать свои правила. Если вы добавите в запрет браузер, то не сможете выходить с помощью него в Интернет. Также доступ к приложениям можно ограничивать для компьютеров, подключенных по локальной сети или удалённо.