Задание 9

1. Изучить лекцию.
2. Ответить на вопросы в конце лекции.
3. Прислать ответы по данной лекции на почтовый ящик vasilizhuk11@mail.ru
4. Законспектировать основные определения.

Что такое Firewall?

В переводе с английского языка слово **firewall** , переводится как «горящая стена». Многие пользователи называют его стеной или **брандмауэром** . В народе очень часто firewall называют просто стена или стенка.

Давайте разберёмся что такое firewall и зачем он нужен. Firewall обеспечивает как бы преграду между сетью и компьютером, или другими словами является фильтром. Эта программа отслеживает соединения компьютера, анализирует их и делает решение разрешать это соединение или нет. То есть программа пропускает только то, что разрешил сам пользователь. Понятное дело, что абсолютной гарантии ни кто не может дать, но если кто-то попытается взломать ваш компьютер, стена для него будет ощутимой преградой. Все еще будет зависеть от опытности хакера.

Простыми понятиями firewall можно сравнить с вашим домом. В доме есть двери. Все двери вы держите на замке, и вы бы наврятли хотели чтоб каждый желающий мог бы зайти к вам через открытую дверь. По аналогии, вам нужно быть быть заинтересованым в том, чтобы никто чужой не мог просто так зайти в ваш компьютер - управлять им иполучать различные данные с него. На дверях дома есть замки. Чтобы впустить знакомого вы открываете замок. Так же работает и firewall. Он может пропускать в интернет или запускать из интернета только те программы, которые вы ему разрешите. Все остальные программы будут заблокированы для доступа как на вход с интернета так и на выход.
Получаеться вы ставите сторожа между вашим компьютером и интернетом, который будет пропускать только нужное и важное для вас, все остальное он будет задерживать.

Для максимальной защиты компьютера необходимо правильно произвести

настройки. Рекомендуется разрешить подключение только программам, которые действительно в этом нуждаются. И при этом программа должна иметь **доступ только к тем портам** , по которым она работает. На первый взгляд это кажется сложным, но в брандмауэрах имеются помощники настройки, которые подсказками упрощают процесс настройки. Главное внимательно читайте сервисные сообщения, которые будут появляться в процессе работы.

Firewall имеет два вида стен – персональную и корпоративную. Персональная стена, это программа, которая устанавливается на персональном компьютере, а корпоративный файерволл устанавливается на шлюз между сетью интернет и локальной сетью.

В персональном файерволле имеется встроенный режим обучения, с помощью которого просто разобраться в работе программы и что допускать к соединению, а что запретить. Если программа, которая стоит на компьютере не подходит для файервола, тогда появится системное сообщение и пользователь сможет сам решать – дать разрешение на соединение или отказать. На сегодняшний день достаточное количество персональных файерволлов, и среди них просто подобрать самый подходящий. Они отличаются по видам, интерфейсу, платные и бесплатные, но по своей сущности практически не отличаются. То есть вы выбираете ту программу, которой вам будет удобней пользоваться.

Корпоративные firewall настраиваются системным администратором, что и защищает полностью всю сеть от атак.
Проверить работоспособность программы firewall можно с помощью утилиты LeakTest. Для этого необходимо запустить утилиту, нажать «Test» и тогда вам необходимо ответить на запрос файерволла, ответьте «Разрешить однократно». Программа должна вам сообщить - «Firewall Penetrated». Это необходимо для того что бы проверить соединение с интернетом и сервер который используется для тестирования. После чего нажимаем кнопку «Test» и на запрос программы файерволла дать ответ «Запретить однократно». Программа при этом должна дать сообщение «Unable to connect», что и будет означать, что firewall заблокировал соединение.

Затем следует EXE-файл программы LeakTest переименовать, что бы имя совпадало с именем браузера, если для Internet Explorer, то это

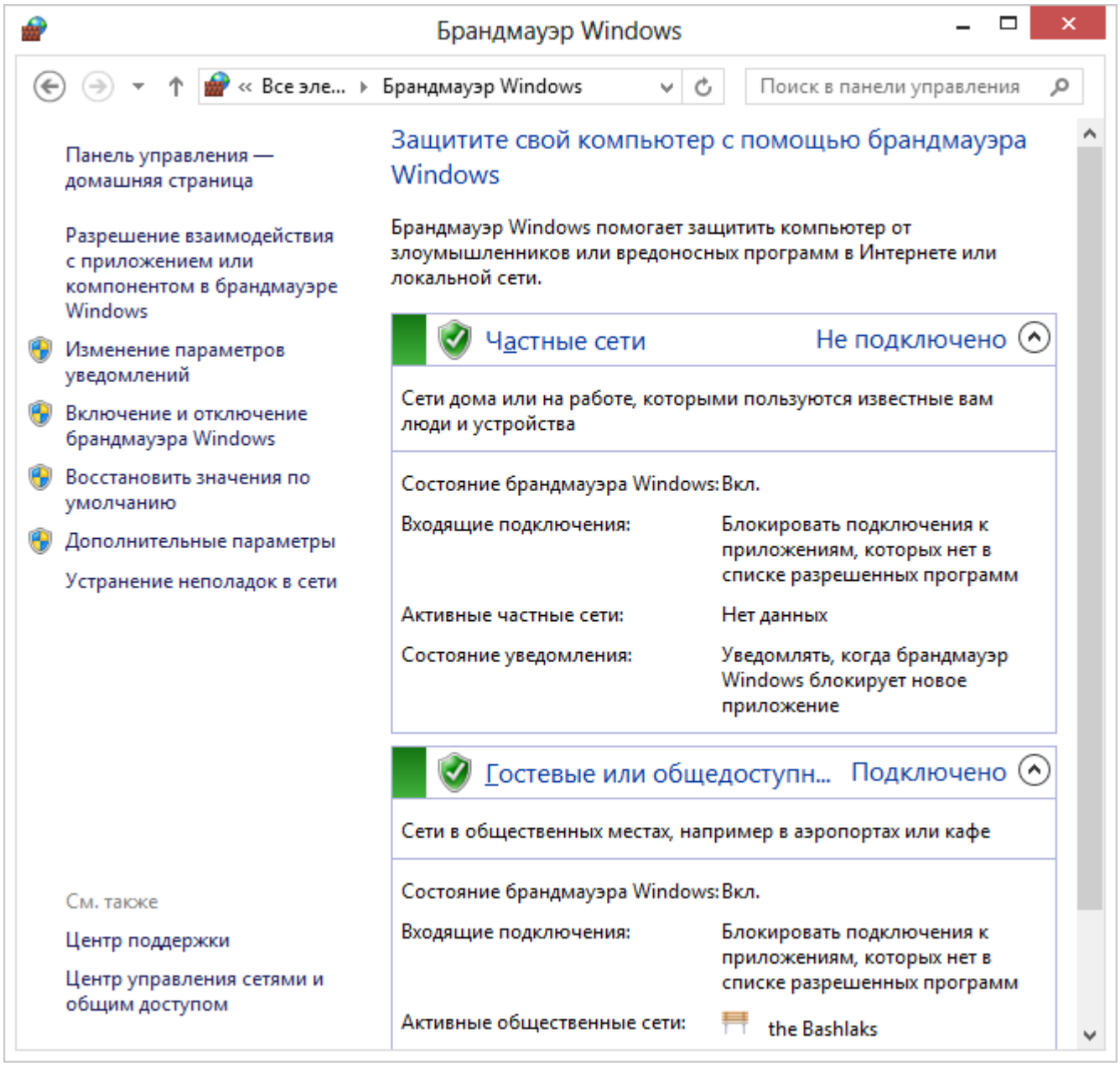
IEXPLORE.EXE, а для Opera – OPERA.EXE, а для других браузеров посмотрите имя в свойствах ярлыка в «Пуск». И при попытке запуска или при установке соединения firewall выдаст вам предупреждение, что программа не та, для которой было создано правило. Если такого предупреждения не будет и соединение будет установлено, то есть появится сообщение «Firewall Penetrated», значит и любой вирус обойдет файерволл, просто переименовав файл, а это значит, что данный файерволл необходимо срочно сменить на другой.

Зачем нужен брандмауэр или фаервол

Вы, наверное, слышали, что брандмауэр Windows 10, 8.1 или Windows 7 (как, впрочем и другой любой другой операционной системы для компьютера) является важным элементом защиты системы. Но знаете ли вы точно, что это такое и что он делает? Многие люди не знают. В этот статье постараюсь популярно рассказать о том что такое брандмауэр (его также называют фаервол), зачем он нужен и еще о некоторых вещах, имеющих отношение к теме. Статья предназначена для начинающих пользователей.

Суть брандмауэра состоит в том, что он контролирует или фильтрует весь трафик (данные, передаваемые по сети) между компьютером (или локальной сетью) и другими сетями, например сетью Интернет, что наиболее типично. Без использования фаервола, может проходить любой тип трафика. Когда брандмауэр включен, проходит только тот сетевой трафик, который разрешен правилами брандмауэра.

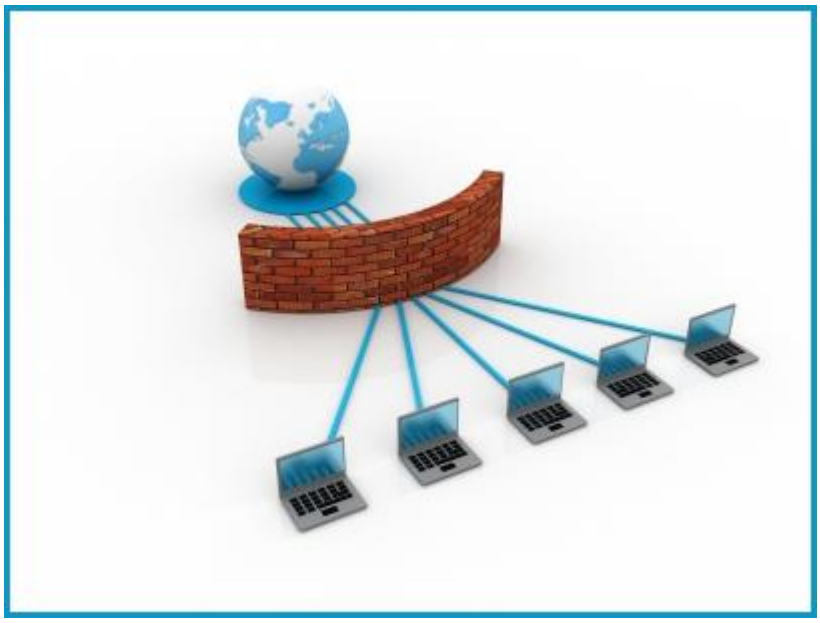
Почему в Windows 7 и более новых версиях брандмауэр является частью системы



Очень многие пользователи сегодня используют роутеры для доступа к Интернету сразу с нескольких устройств, что, по сути тоже является своеобразным фаерволом. При использовании прямого Интернет-подключения через кабель или DSL модем, компьютеру присваивается публичный IP-адрес, обратиться к которому можно с любого другого компьютера в сети. Любые сетевые службы, которые работают на Вашем компьютере, например сервисы Windows для совместного использования принтеров или файлов, удаленного рабочего стола могут быть доступны для других компьютеров. При этом, даже когда Вы отключаете удаленный доступ к определенным службам, угроза злонамеренного подключения все равно остается — прежде всего, потому что рядовой пользователь мало задумывается о том, что в его ОС Windows запущено и ожидает входящего подключения, а во вторых — по причине различного рода дыр в безопасности, которые позволяют подключиться к удаленной службе в тех случаях, когда она просто запущена, даже если входящие подключения в ней запрещены. Брандмауэр попросту не дает отправить службе запрос, использующий уязвимость.

Первая версия Windows XP, а также предыдущих версий Windows не содержали встроенного брандмауэра. А как раз с выходом Windows XP и совпало повсеместное распространение сети Интернет. Отсутствие фаервола в поставке, а также малая грамотность пользователей в плане Интернет-безопасности, привела к тому, что любой компьютер, подключенный к Интернет с Windows XP мог быть заражен в течение пары минут в случае целенаправленных действий.

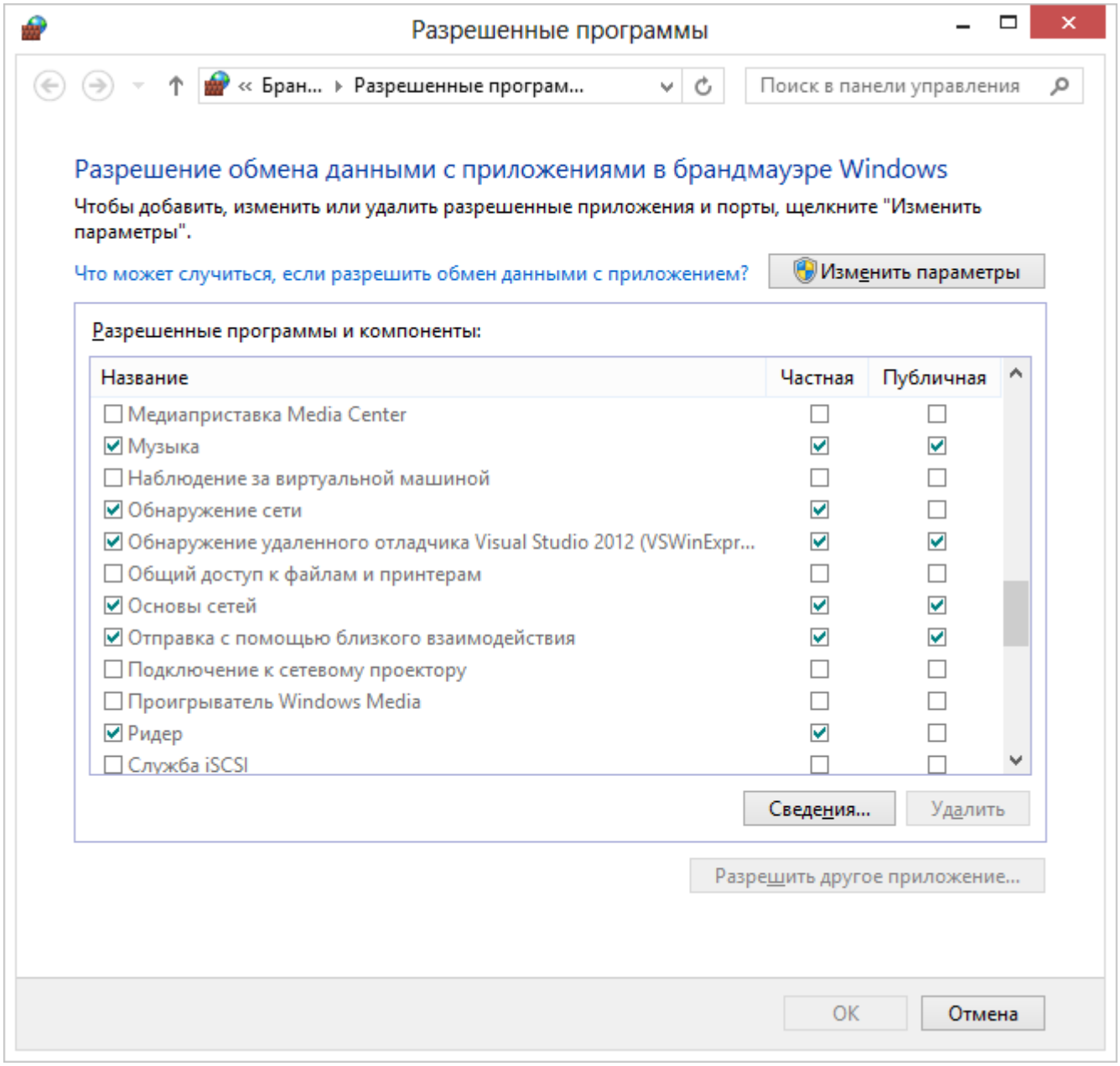
Первый брандмауэр Windows был представлен в Windows XP Service Pack 2 и с тех пор фаервол по умолчанию включено во всех версиях операционной системы. И те службы, о которых мы говорили выше, ныне изолированы от внешних сетей, а брандмауэр запрещает все входящие соединения за исключением тех случаев, когда это прямо разрешено в настройках брандмауэра.



Это предотвращает подключение других компьютеров из сети Интернет к локальным службам на вашем компьютере и, кроме этого, контролирует доступ к сетевым службам из Вашей локальной сети. Именно по этой причине, всякий раз при подключении к новой сети Windows спрашивает о том, домашняя это сеть, рабочая или же общественная. При подключении к домашней сети, брандмауэр Windows разрешает доступ к этим службам, а при подключении к общественной — запрещает.

Другие функции брандмауэра

Брандмауэр представляет собой барьер (отсюда название фаервол — с англ. «Огненная стена») между внешней сетью и компьютером (или локальной сетью), которая находится под его защитой. Главная защитная функция брандмауэра для домашнего использования — блокировка всего нежелательного входящего Интернет-трафика. Однако, это далеко не все, что может фаервол. Учитывая то, что фаервол «находится между» сетью и компьютером, он может использоваться для анализа всего входящего и исходящего сетевого трафика и решать, что с ним делать. Например, брандмауэр моет быть настроен для блокировки определенного типа исходящего трафика, вести журнал подозрительной сетевой активности или всех сетевых подключений.



В брандмауэре Windows вы можете настроить разнообразные правила, которые будут разрешать или запрещать определенные типы трафика. Например, могут быть разрешены входящие подключения только с сервера с определенным IP адресом, а все остальные запросы будут отклоняться (это может пригодиться, когда Вам требуется подключаться к программе на компьютере с рабочего компьютера, хотя лучше использовать VPN).

Фаервол — это не всегда программное обеспечение, как всем известный брандмауэр Windows. В корпоративном секторе могут использоваться тонко настроенные программно-аппаратные комплексы, выполняющие функции фаервола.

Если вы имеете дома Wi-Fi роутер (или просто роутер), он также действует в роли своего рода аппаратного брандмауэра, благодаря своей функции NAT, которая предотвращает доступ извне к компьютерам и другим устройствам, подключенным к роутеру.

Вопросы к лекции:

1. Что такое фаервол?
2. Что такое брандмауэр?
3. Зачем нужен фаервол?
4. Можно ли настроить брандмауэр?
5. Что может заменить брандмауэр?