**Практическое занятие №4**

**Тема «**Настройка Брандмауэра Windows**»**

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

**Теоретическое введение**

Брандмауэр (Межсетевой экран) - это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные (рис. 1).

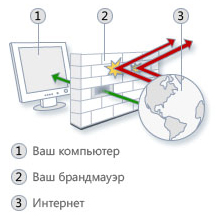


Рисунок 1 – Принцип действия Брандмауэра

Межсетевой экран является одним из основных компонентов защиты сетей. Наряду с Internet-протоколом межсетевого обмена (Internet Security Protocol — IPSec). Межсетевой экран является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от несанкционированного доступа. Отметим, что большая часть проблем с информационной безопасностью сетей связана с "прародительской" зависимостью коммуникационных решений от ОС UNIX – особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов (Transmission Control Protocol/Internet Protocol — TCP/IP) имеет "бреши" в защите.

К числу таких служб и протоколов относятся:

* служба сетевых имен (Domain Name Server — DNS);
* доступ к всемирной паутине WWW;
* программа электронной почты Send Mail;
* служба эмуляции удаленного терминала Telnet;
* простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP);
* протокол передачи файлов (File Transfer Protocol);
* графическая оконная система X Windows.

Настройки межсетевого экрана, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах – запрещать всё, что не разрешено в явной форме, и разрешать всё, что не запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жёстко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как она предоставляет пользователям больше возможностей "обойти" межсетевой экран и использовать запрещенные сервисы через нестандартные порты (User Data Protocol – UDP), которые не запрещены политикой безопасности.

**Создание правила по ограничению доступа программ к сети**

Для создания правила по ограничению доступа программ к сети необходимо открыть Панель управления в меню Пуск. В зависимости от версии операционной системы Windows может отображаться классический вид (рис. 2) панели управления или с разделениям по категориям (рис. 3).

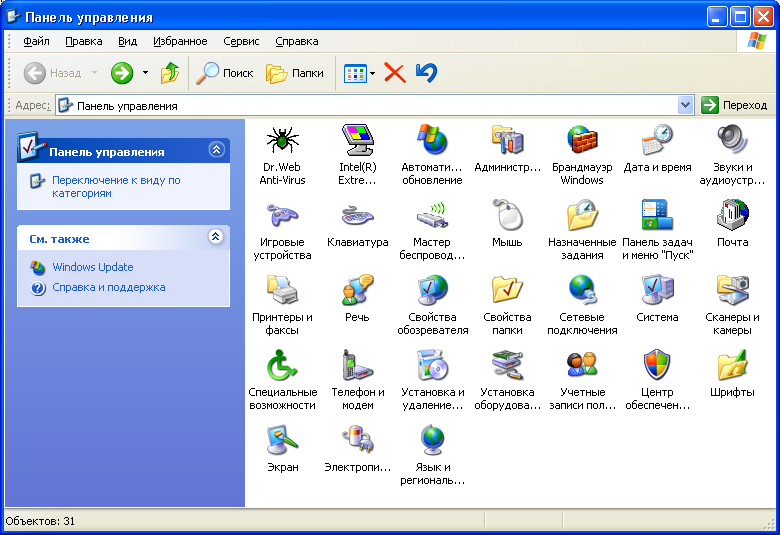


Рисунок 2 – Классический вид

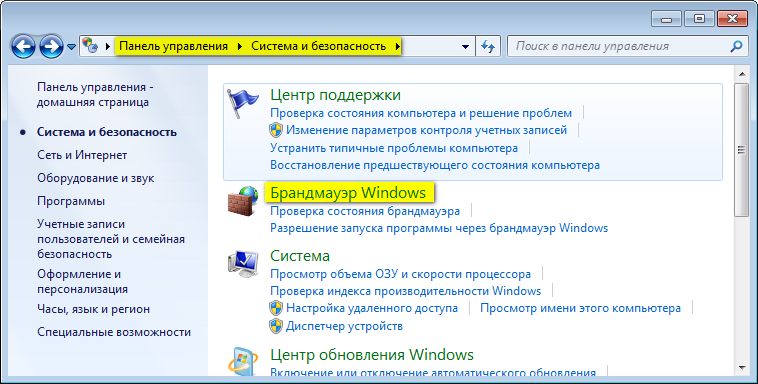


Рисунок 3 – Вид с разделением по категориям

Первым этапом необходимо включить брандмауэр, в случае, если он был ранее выключен. Необходимо выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows» (рис. 4).

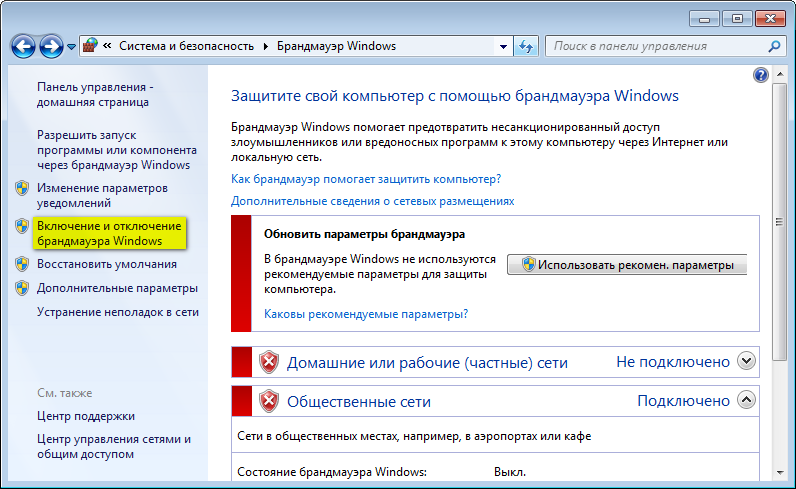


Рисунок 4 – Брандмауэр Windows

В появившемся окне переключаем параметры на значение «Включение брандмауэра Windows» (рис. 5).

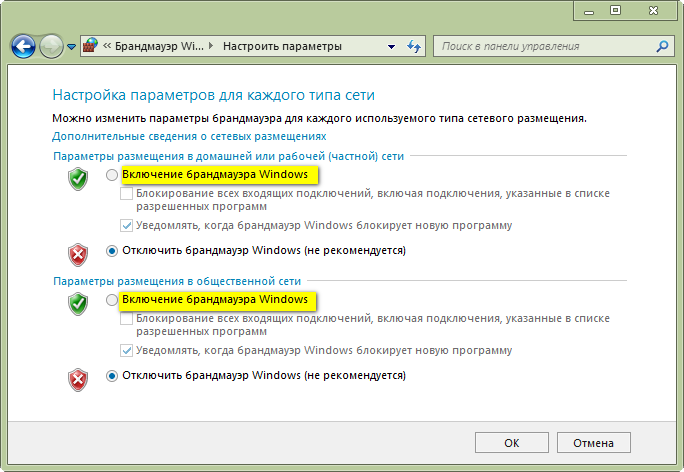


Рисунок 5 – Включение брандмауэра Windows

Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого во вкладке «Дополнительные параметры» (рис. 6).

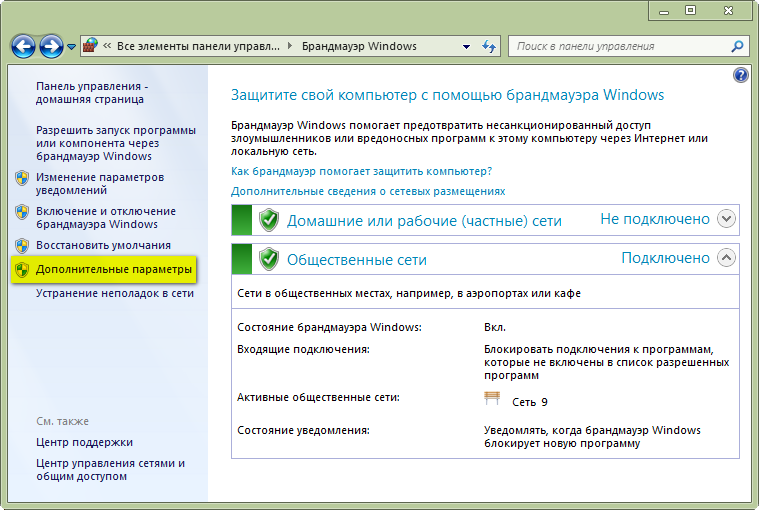


Рисунок 6 – Включенный брандмауэр

В открывшемся окне выбираем в левой панели правила для входящих подключений, затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели (рис. 7).

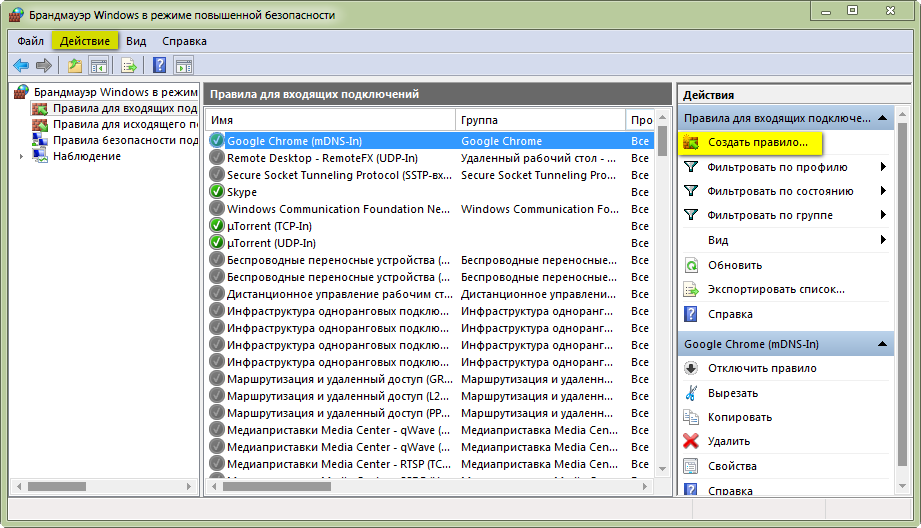


Рисунок 7 – Создание правила

В открывшемся мастере создания правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы) (рис. 8).

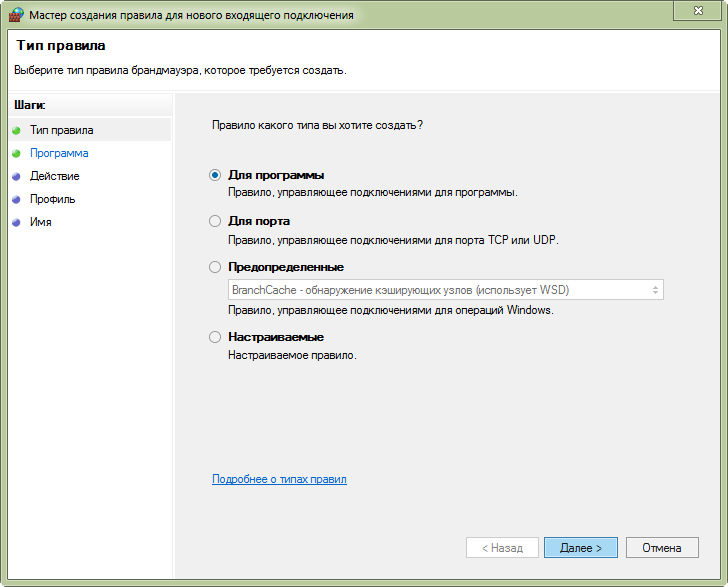


Рисунок 8 – Выбор типа правила

При ограничении работы программы, далее необходимо указать её путь, обязательно через папку в которой она установлена, а не через ярлыки! (Рис. 9).

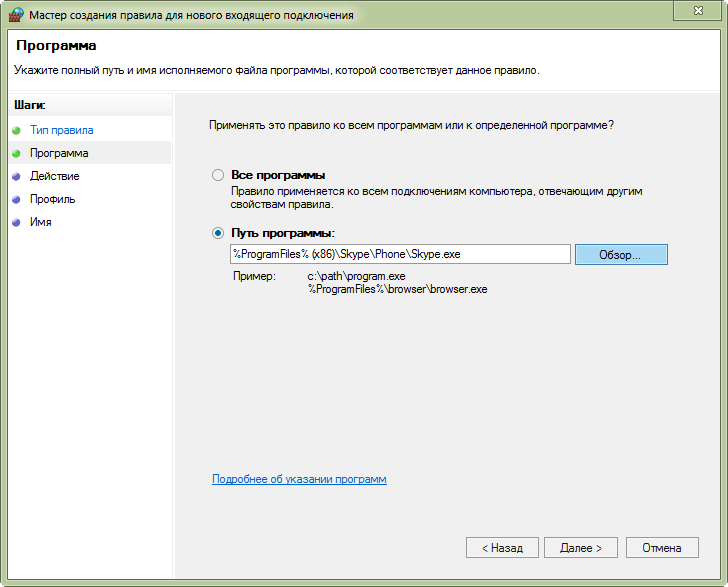


Рисунок 9 – Настройка пути программы

Далее указывается какое именно действие вы хотите применить. В данном случае необходимо блокировать подключение (рис. 10).

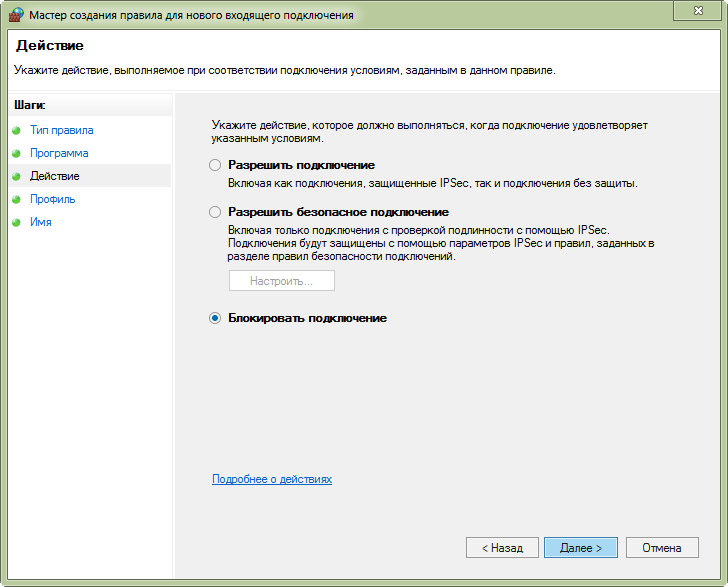


Рисунок 10 – Выбор действия

В следующем окне указывается имя правила (рис. 11).

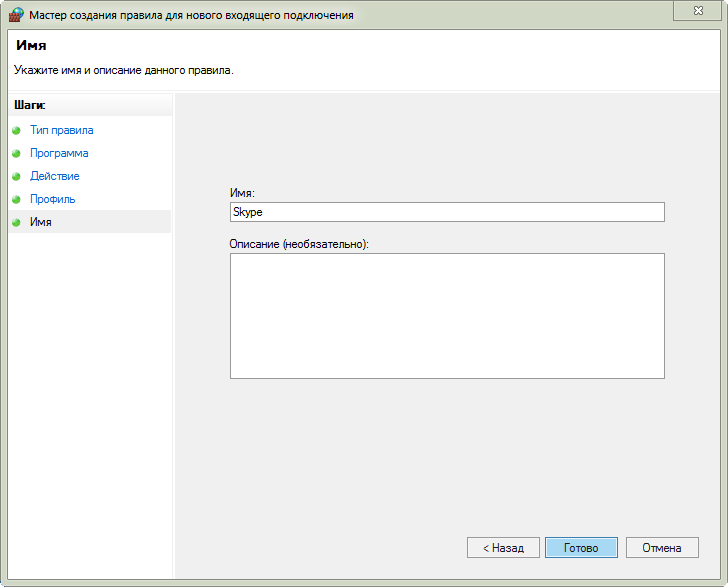


Рисунок 11 – Окно ввода имени

В общем списке появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели (рис. 12).

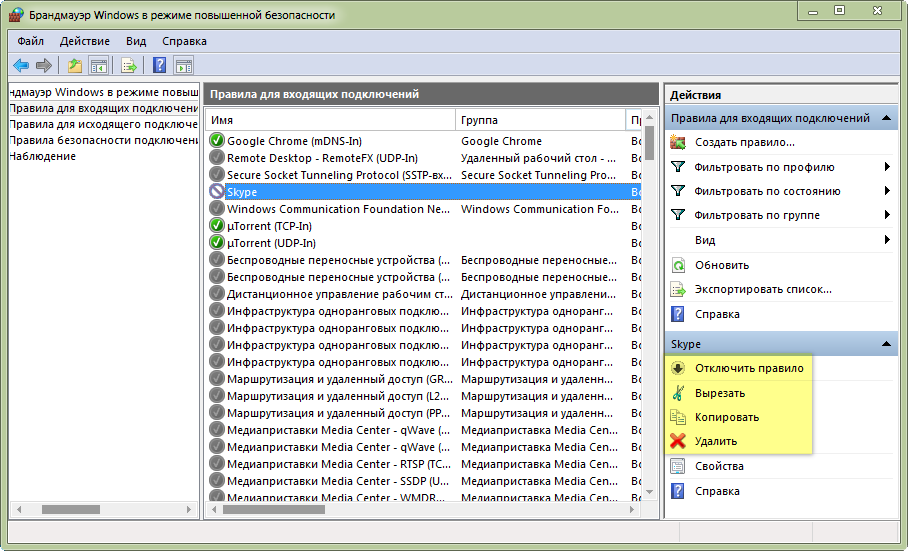


Рисунок 12 – Созданное правило

При двойном нажатии на правило отображаются его свойства.

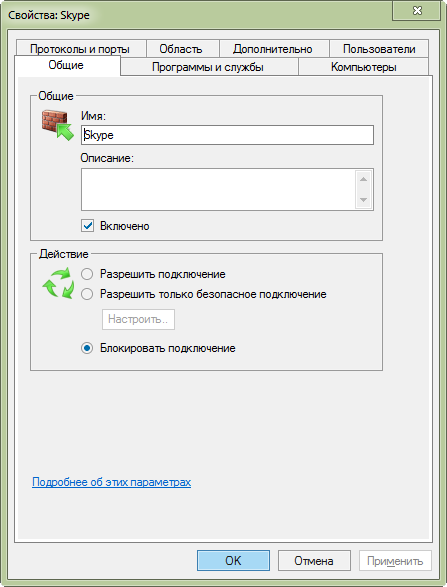


Рисунок 12 – Свойства правила

Таким же образом создаются и правила для исходящих подключений.

**Шпаргалка администратора ( Меню->Выполнить)**

Администрирование-control admintools  
Администратор источников данных-odbccp32.cpl  
Восстановление системных файлов-sfc /scannow  
Дефрагментация дисков-dfrg.msc  
Диспетчер проверки драйверов-verifier  
Дисптчер служебных программ-utilman  
Групповая политика-gpedit.msc  
Dr. Watson-drwtsn32  
Запросы операторов съемных ОЗУ-ntmsoprq.msc  
Защита БД учетных записей-syskey  
IExpress-iexpress  
Инфраструктура управления-wmimgmt.msc  
Проверка дисков-chkdsk  
Калькулятор-calc  
Командная строка-cmd  
Консоль управления-dcomcnfg  
Локальные параметры безопасности-secpol.msc  
Локальные пользователи и группы-lusrmgr.msc  
Мастер передачи файлов Bluetooth-fsquirt  
Настройка системы-msconfig  
Назначенные задания-control schedtasks  
Общие папки-fsmgmt.msc  
Общие ресурсы DDE-ddeshare  
Папка обмена-clipbrd  
Проверка подписи файла-sigverif  
Программа сетевого клиента SQL-cliconfg  
Производительность-perfmon.msc  
Просмотр событий-eventvwr.msc  
Подключение к рабочему столу-mstsc  
Результатирующая политика-rsop.msc  
Редактор системных файлов-sysedit  
Реестр-regedit  
Редактор личных символов-eudcedit  
Сертификаты-certmgr.msc  
Служба диагностики DirectX-dxdiag  
Службы-services.msc  
Службы компонентов-dcomcnfg  
Служба индексирования-ciadv.msc  
Съемные ЗУ-ntmsmgr.msc  
Телнет-telnet  
Управление дисками-diskmgmt.msc  
Управление рабочим столом-mstscoo  
Управление компьютером-compmgmt.msc  
Удаление вредоносных программ-mrt.exe

**Устранение возможных ошибок системы при включении Брандмауэра**

При возникновении ошибок при попытке включить Брандмауэр, например, как на рисунке 13, необходимо включить Брандмауэр в соответствующих службах Windows (рис 14-16).

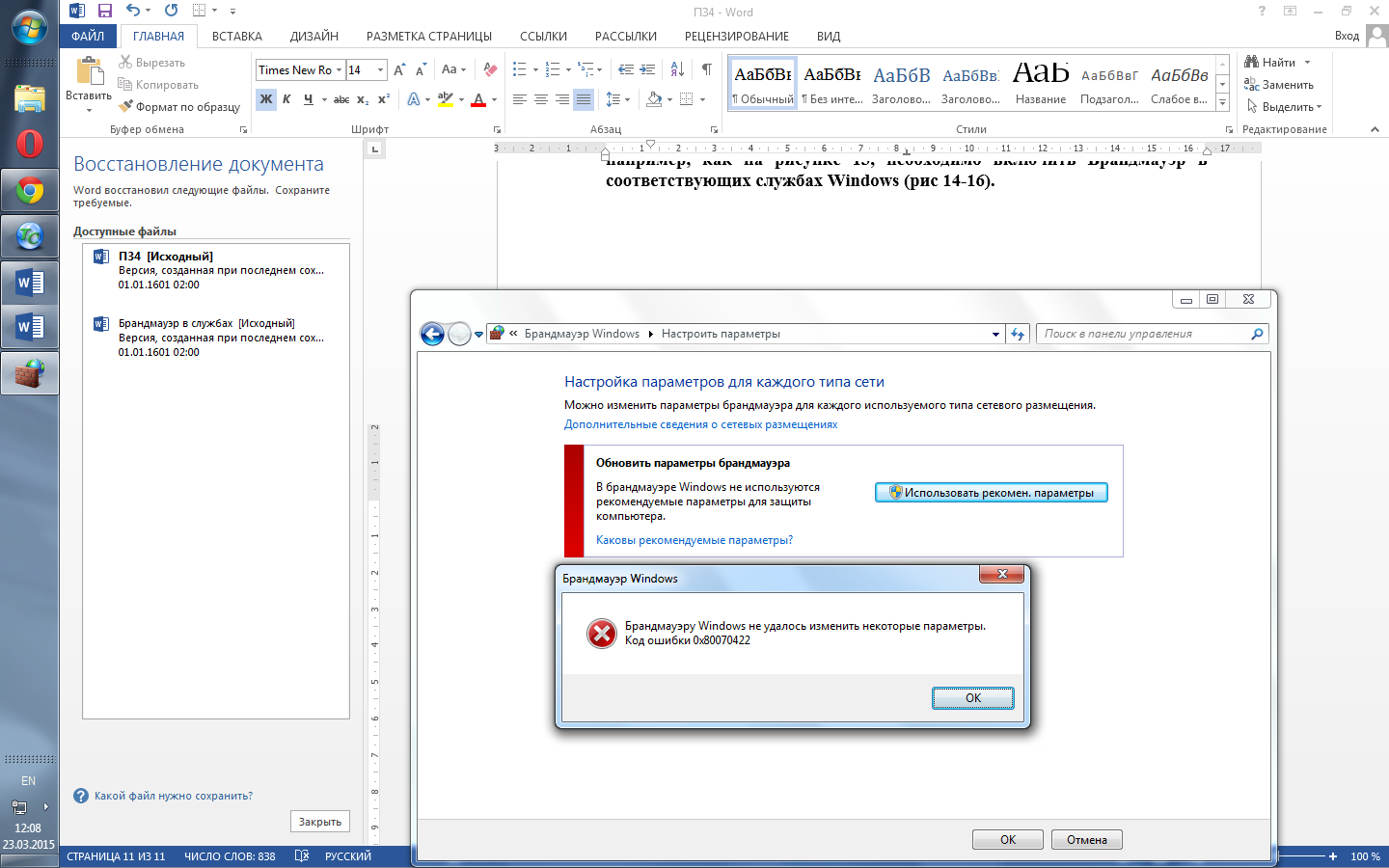


Рисунок 13. Ошибка при попытке включить Брандмауэр

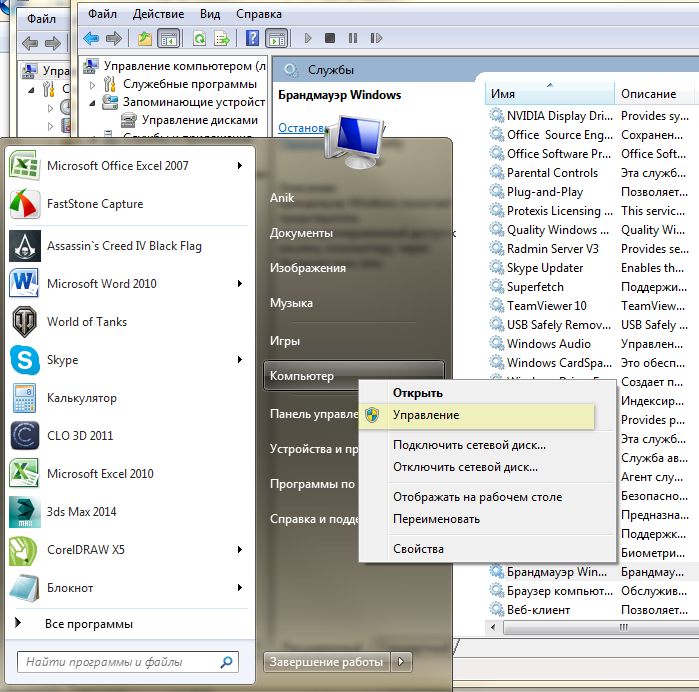


Рисунок 14. Открытие окна «Управление»

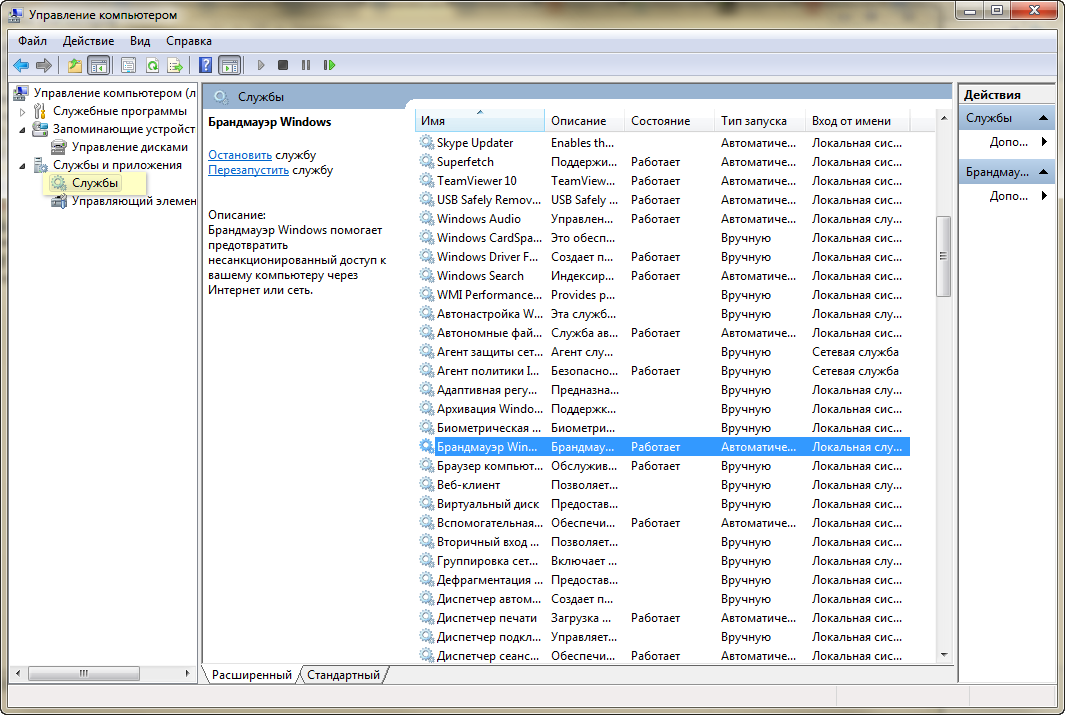


Рисунок 15. Доступ к службе Брандмауэр

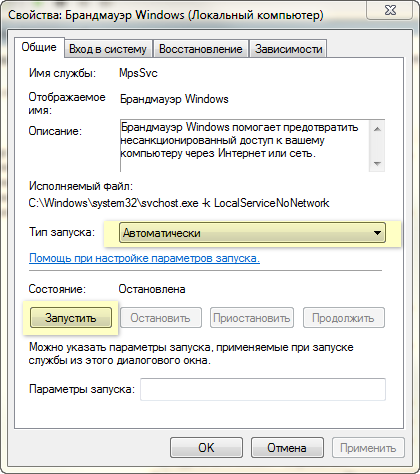


Рисунок 16. Запуск Брандмауэра

**Задание к выполнению**

1. Создать правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий):
   1. Для 1 программы (по выбору) на блокировку подключения;
   2. Для 1 программы (по выбору) на разрешение подключения;
2. Создать правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий):
   1. Для 1 программы (по выбору) на блокировку подключения;
   2. Для 1 программы (по выбору) на разрешение подключения;
3. Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.
4. Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).