МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическая работа №3**

по дисциплине «Основы информационной безопасности»

на тему: Разработка политики информационной безопасности фабрики

Выполнил студент 2 курса 7 группы специальность ПОИБМС Володькин Никифор Дмитриевич

(Ф.И.О.)

Преподаватель Ржеутская Надежда Викентьевна

(Ф.И.О.)

**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).

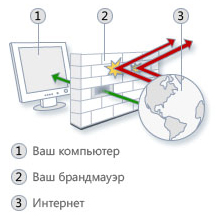


Рисунок 1 – Принцип действия Брандмауэра

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);

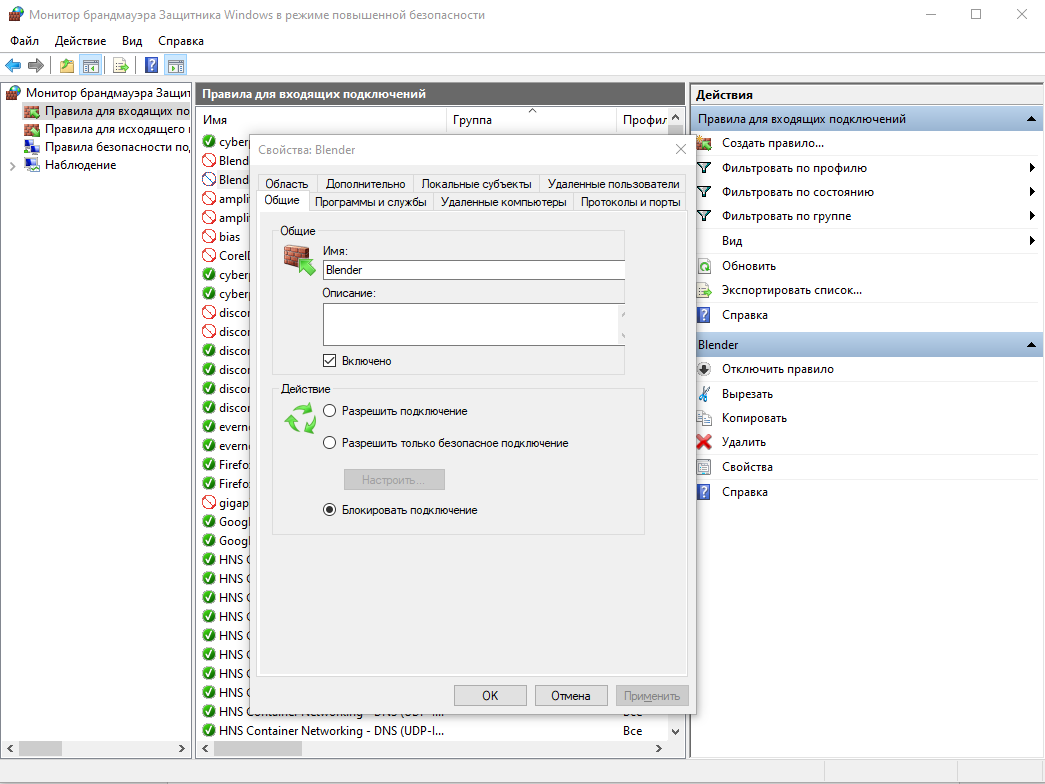
протокол передачи файлов (File Transfer Protocol);

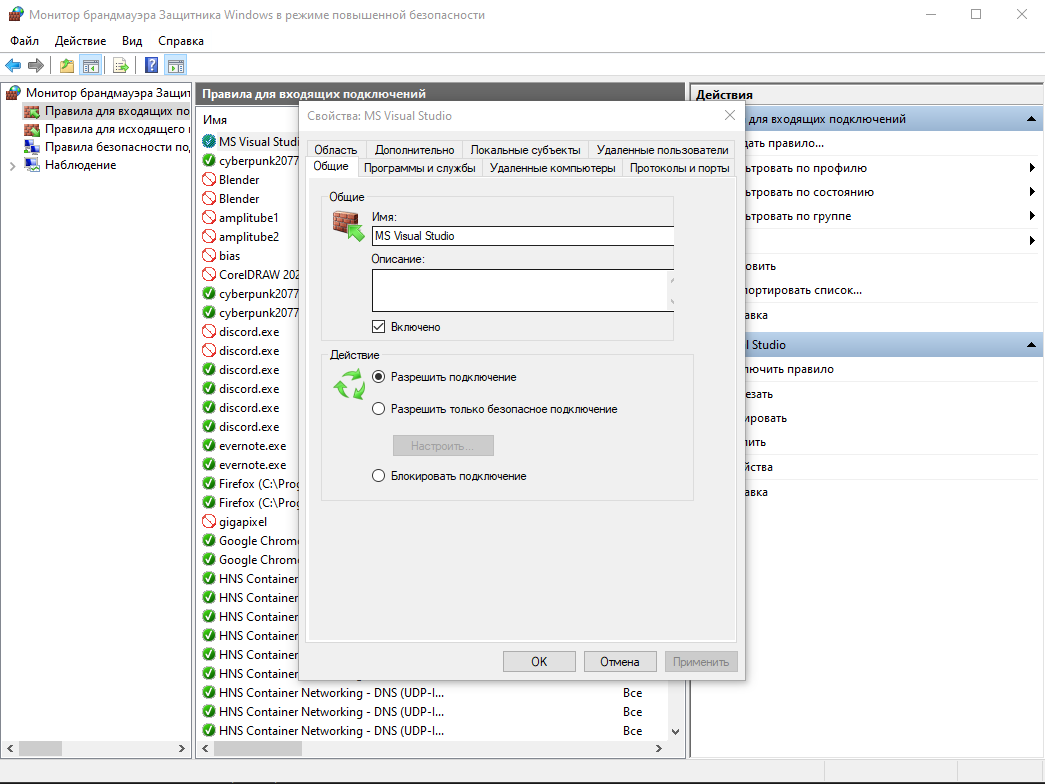
графическая оконная система X Windows.

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.

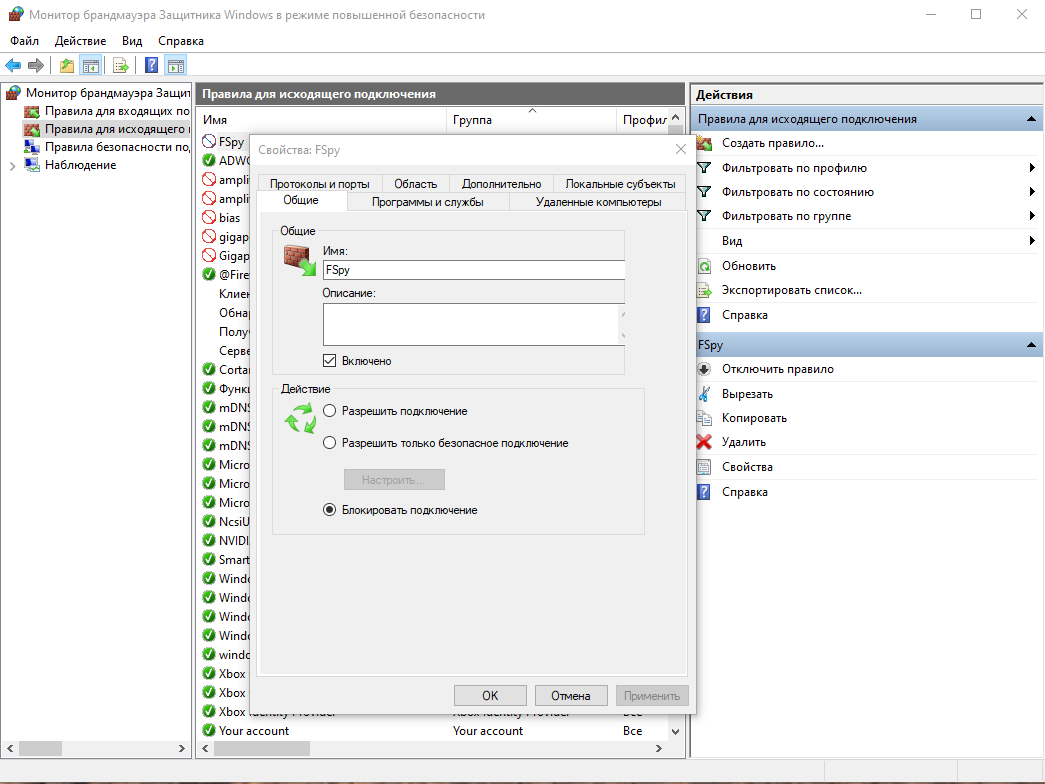
**Выполнение работы**

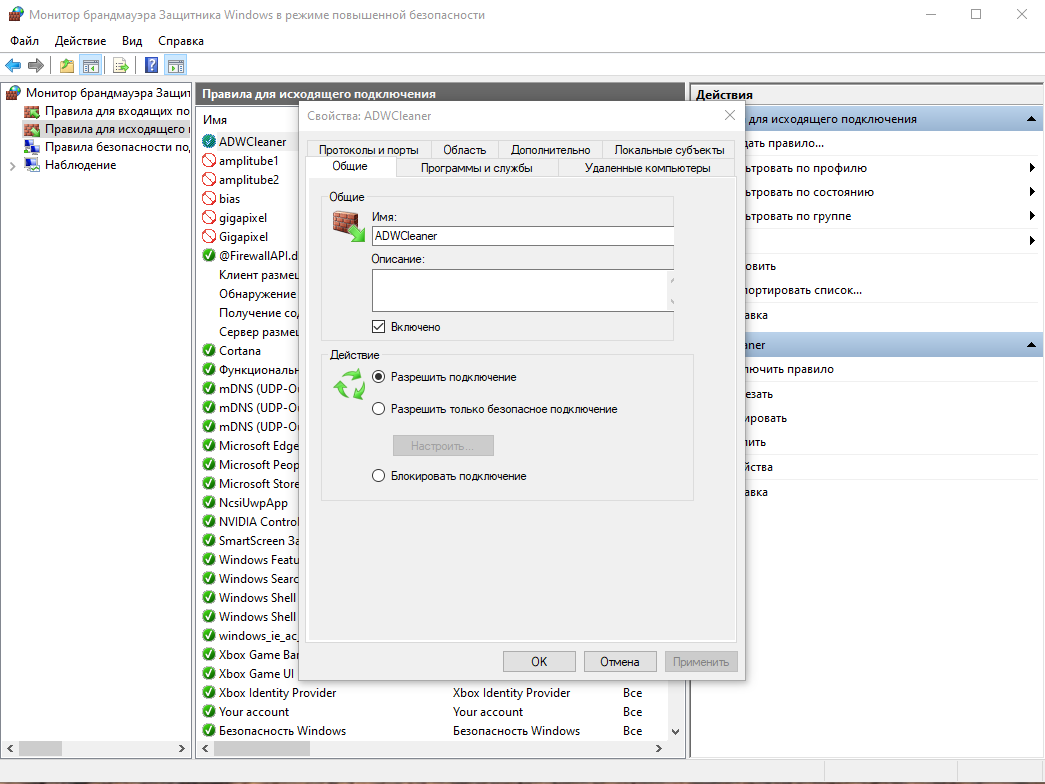
После включения брэндмауэра Windows были созданы правила для входящих подключений. В мониторе брэндмауэра была выбрана опция для создания правила входящего подключения. В появившемся окне был выбран тип правила для программы, после чего был указан путь программы. Были выбраны типы действий (запретить подключения для Blender и разрешить подключения для Visual Studio), после чего был выбран тип профиля (доменный, частный и публичный). После правилу были даны соответствующие имена:



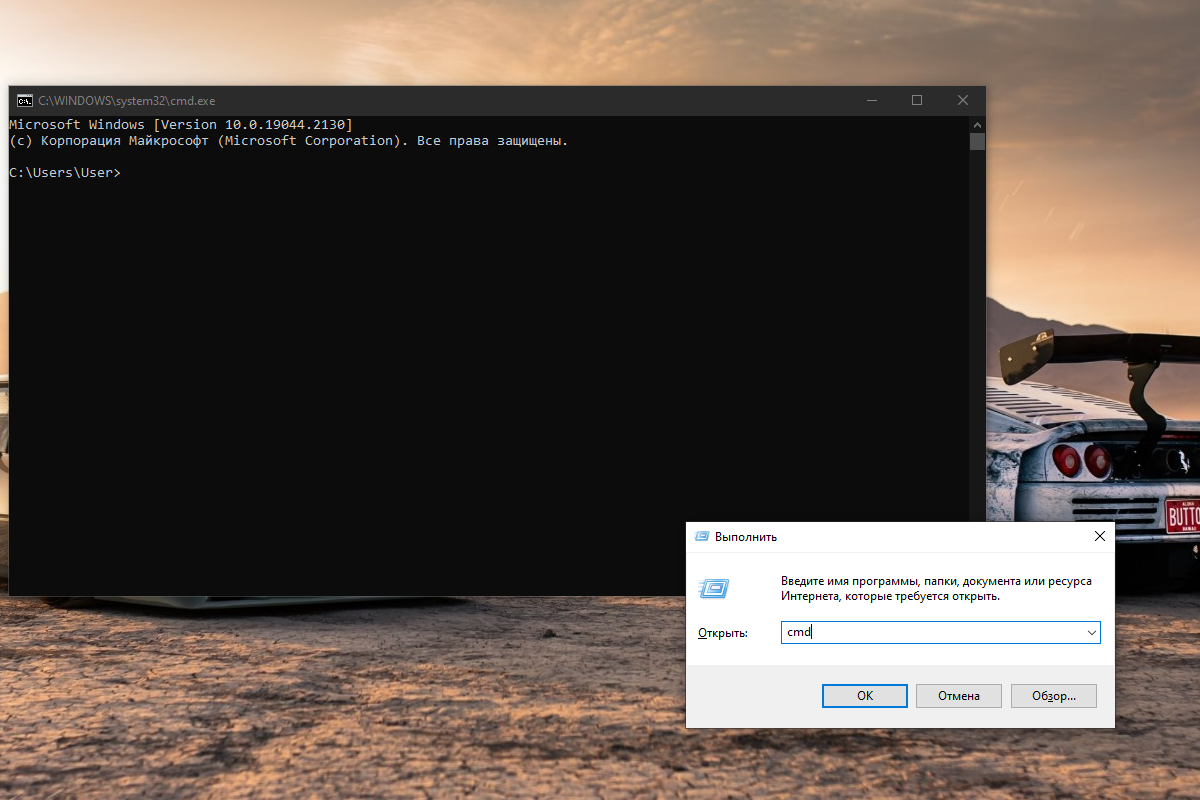


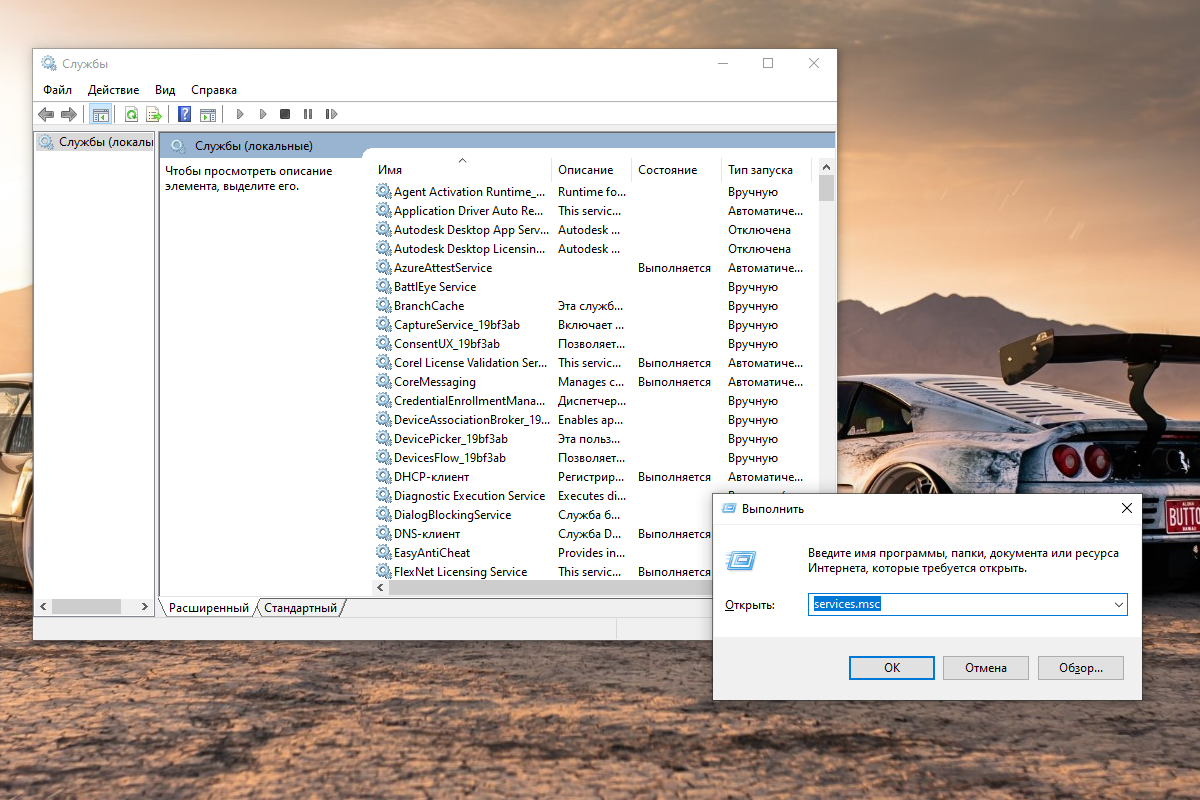
После включения брэндмауэра Windows были созданы правила для исходящих подключений. В мониторе брэндмауэра была выбрана опция для создания правила исходящего подключения. В появившемся окне был выбран тип правила для программы, после чего был указан путь программы. Были выбраны типы действий (запретить подключения для FSpy и разрешить подключения для ADWCleaner), после чего был выбран тип профиля (доменный, частный и публичный). После правилу были даны соответствующие имена:

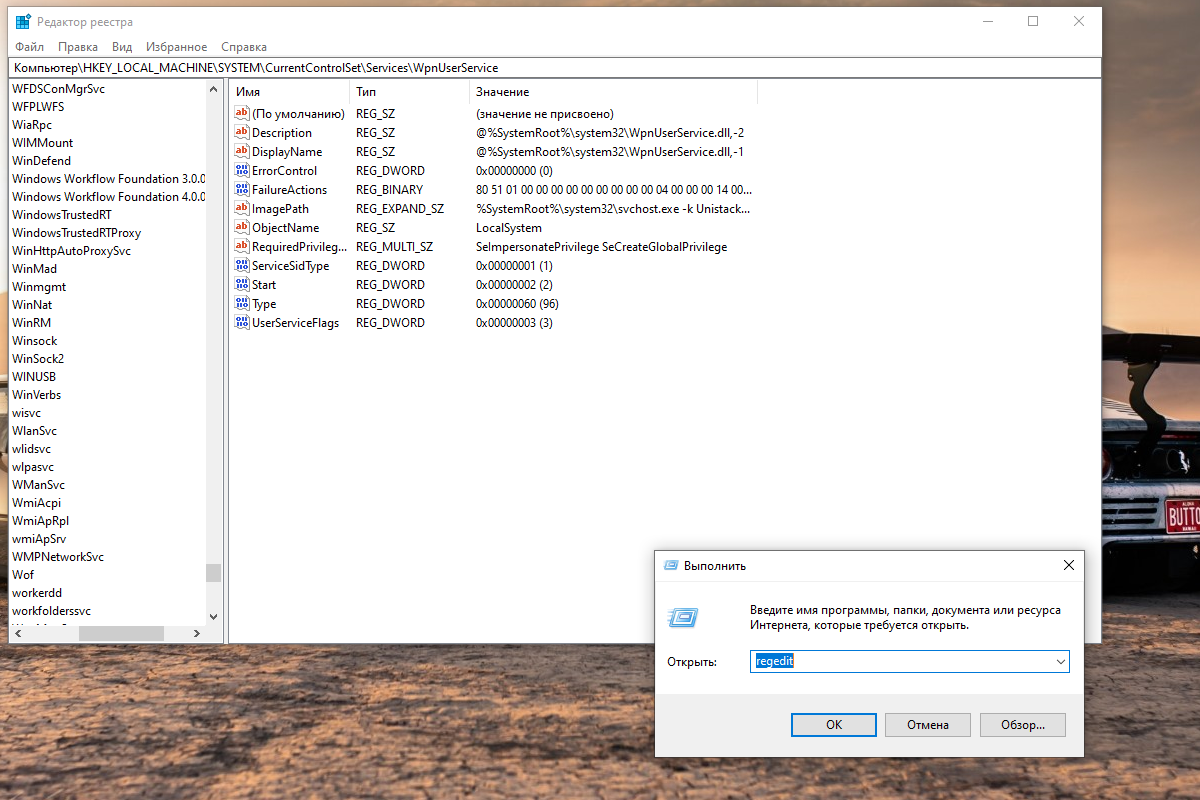




Настройки брэндмауэра были возвращены в изначальное состояние. После этого с помощью сочетания клавиш Win + R (альтернативно можно воспользоваться меню пуск) было открыто окно выполнить, в котором при введении соответствующей команды запускается определенная программа:







**Вывод: были получены навыки настройки и использования Брандмауэра Windows.**