МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ  
Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ   
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных технологий

Кафедра Информационных систем и технологий

Специальность 1—98 01 03 «Программное обеспечение информационной

безопасности мобильных систем»

**Отчет**

по дисциплине «Основы информационной безопасности»

**Исполнитель**

студент(ка) 2 курса 7 группы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Банкузов М.О.

подпись, дата

**Руководитель**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ржеутская Н. В.

должность, ученая степень, ученое звание подпись, дата

**Практическое занятие №3**

**Тема «Настройка Брандмауэра Windows»**

Цель: разобраться в настройках и использовании Брандмауэра.

**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.

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.

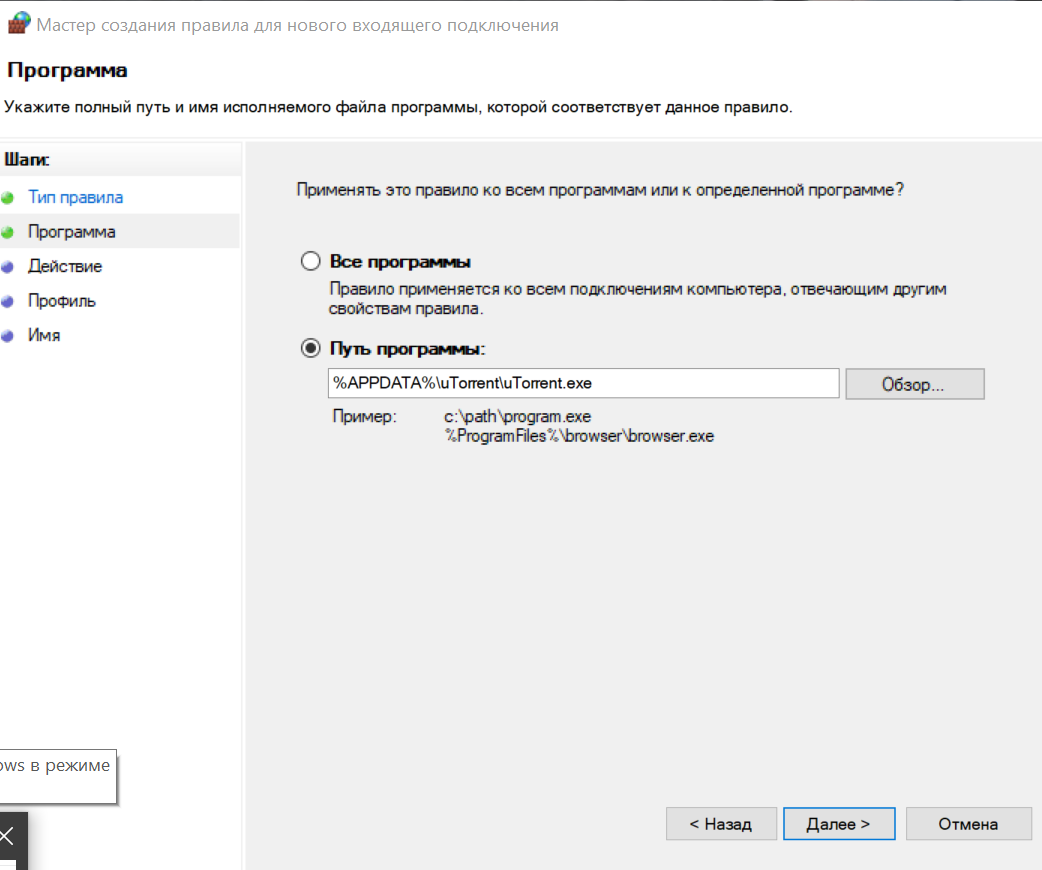
Настройки межсетевого экрана, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются 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.

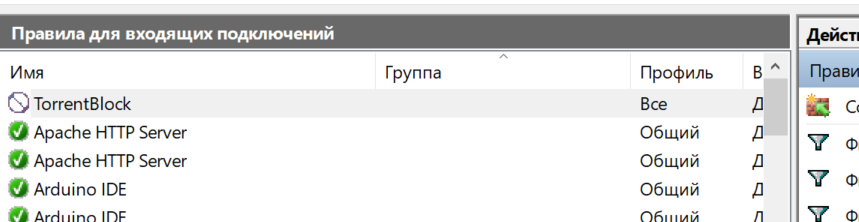
**Шпаргалка администратора ( Меню->Выполнить)**

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

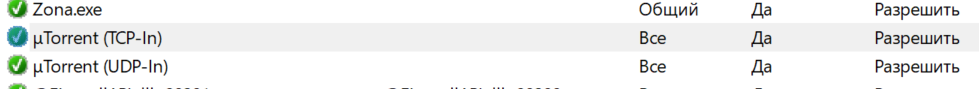
**Практическая часть**

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;

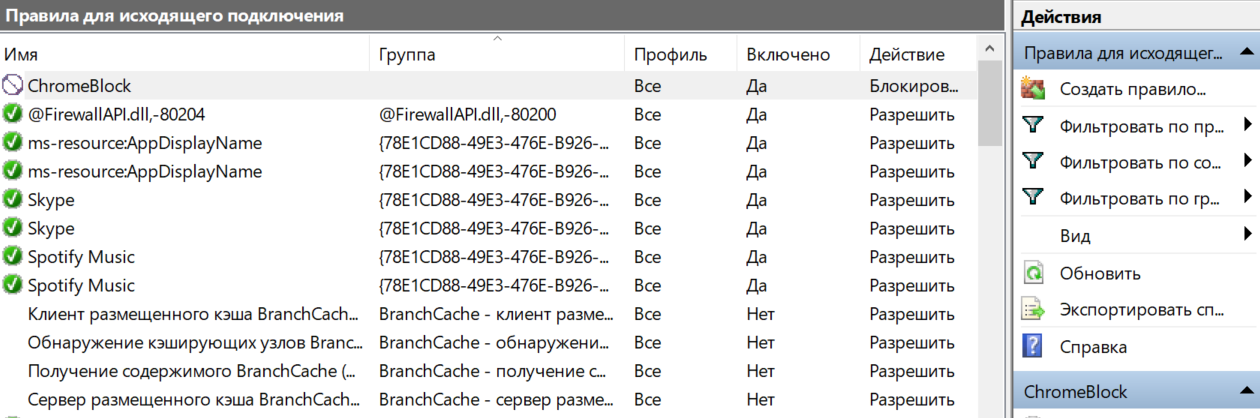


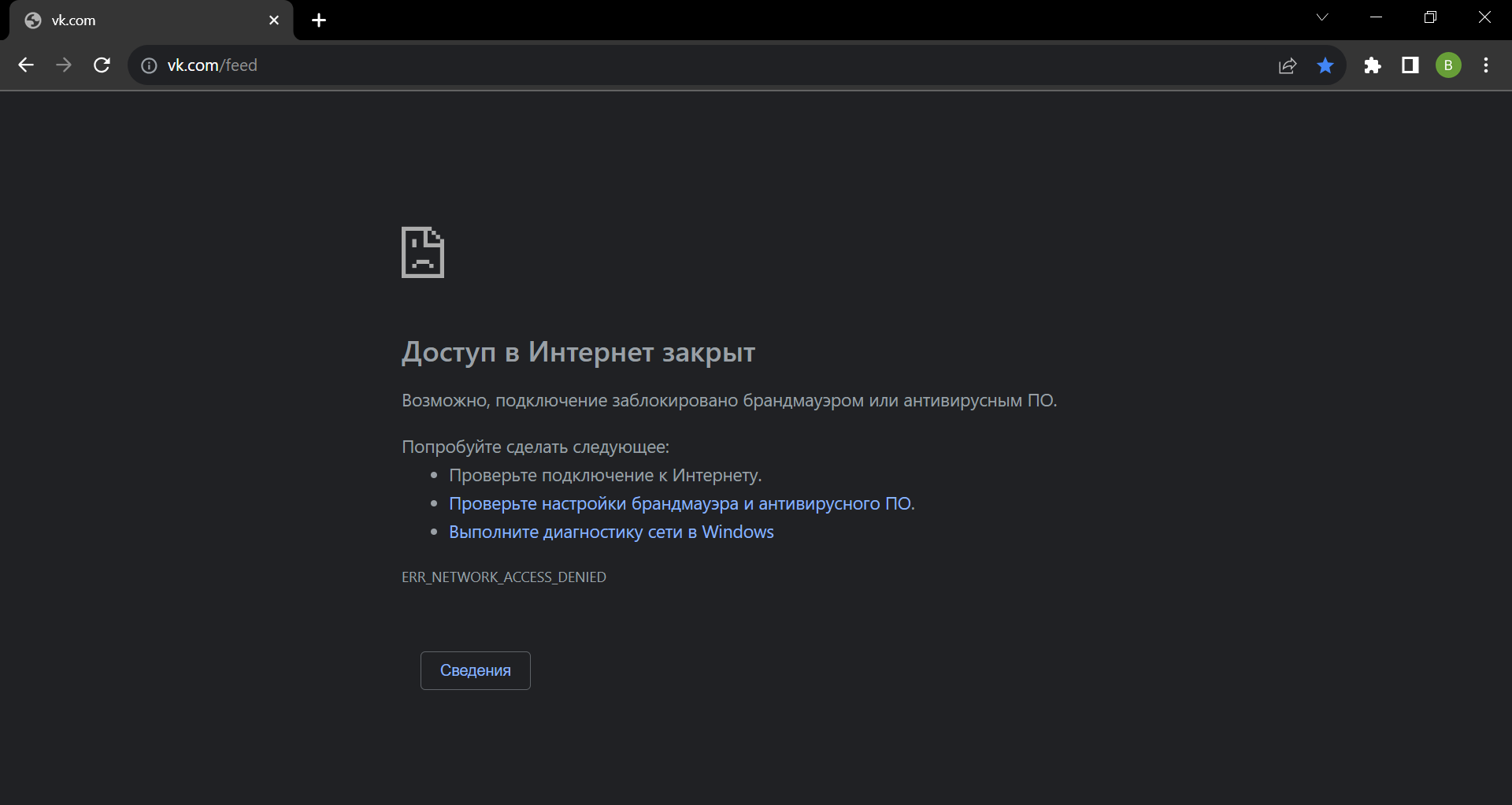


* 1. Для 1 программы (по выбору) на разрешение подключения;

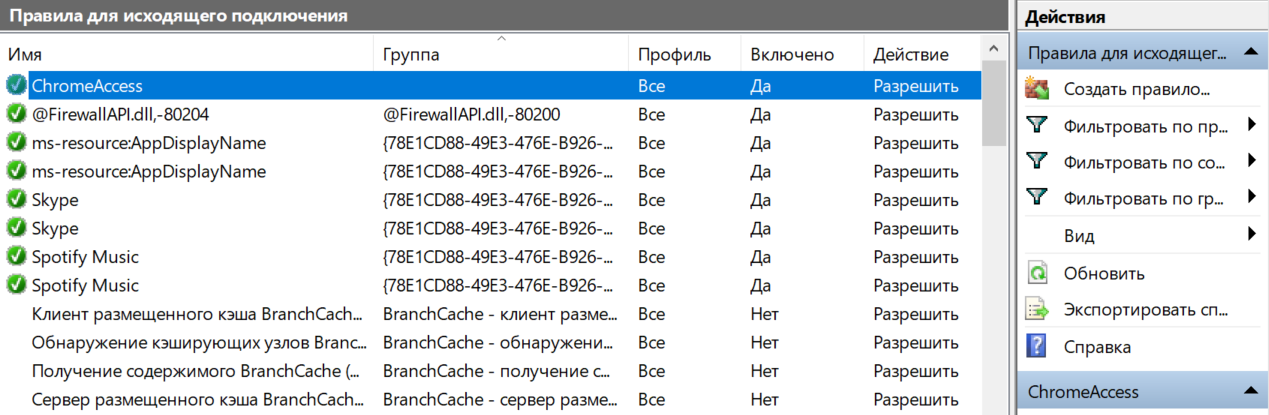


1. Создать правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий):
   1. Для 1 программы (по выбору) на блокировку подключения;

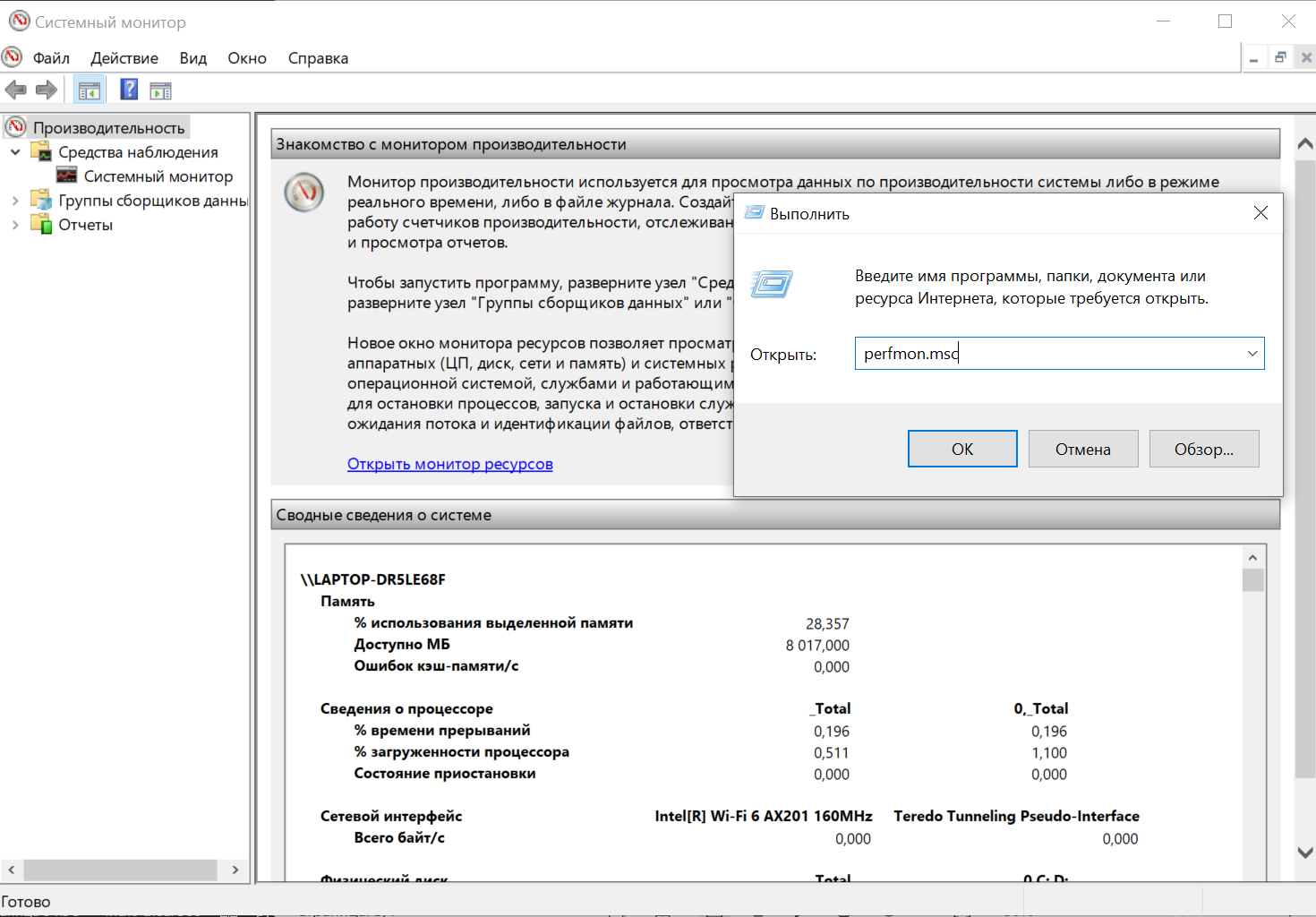




* 1. Для 1 программы (по выбору) на разрешение подключения;



1. Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.
2. Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).
   1. Производительность



* 1. Управление дисками

