**1. Цель работы**

Изучить принципы работы защитных межсетевых экранов на примере программы Kaspersky Anti-Hacker.

**2. Порядок проведения работы**

2.1. Изучить лекционный материал (раздел [5](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\chapter5_1.html))

2.2. Изучить теоретический материал по лабораторной работе

2.3. Выполнить задание на лабораторную работу.

2.4. Ответить на контрольные вопросы.

**3. Задание на лабораторную работу**

3.1. Создать и настроить правило, разрешающее работу в сети для любого приложения (по выбору студента), после чего проверить функционирование этого приложения.

3.2. Изменить правило на запрет работы в сети для этого приложения и проверить его функционирование с помощью того же приложения.

3.3. Создать и настроить правило, разрешающее работу в сети для любого протокола (рекомендуется ICMP) и проверить работоспособность данного правила с помощью приложений, использующих этот протокол.

3.4. Изменить правило на запрет работы в сети для этого протокола и проверить его функционирование.

3.5. Просмотреть и проанализировать данные о текущих сетевых соединениях. Запустить любое другое сетевое приложение, дать ему задание на получение или отправку данных в Интернет и проверить, как изменится список соединений. Разорвать это соединение и проверить реакцию приложения на разрыв соединения.

**4. Теоретический материал и практические аспекты**

Для выполнения данной лабораторной работы необходимо знание учебного материала в объеме главы [5](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\chapter5_1.html). Для защиты от компьютерных атак извне и изнутри необходимо применение различных защитных экранов.

Они анализируют входящий трафик на предмет нахождения в нем шаблонов атак, предотвращают сканирование портов, благодаря контролю за приложениями позволяют обезвредить троянские кони. Рассмотрим наиболее распространенные возможности таких программ на примере Kaspersky Anti-Hacker.

Загрузить пробную версию программы Kaspersky Anti-Hacker: [kantihacker\_rus.exe](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\soft\kantihacker_rus.exe)

**ОСНОВНЫЕ СВЕДЕНИЯ О ПРОГРАММЕ**

Функционально Kaspersky Anti-Hacker выполняет свою задачу при помощи фильтрации всего входящего и исходящего трафика на уровне сетевого протокола. Такой подход обеспечивает максимальную надежность, отсекая все опасные действия еще до обработки данных другими приложениями.

Фильтрация трафика проводится тремя путями.

Во-первых, с помощью контроля над приложениями. Можно разрешить или запретить тем или иным программам выходить в Интернет, а также установить параметры их работы (используемые порты, адреса, протоколы и пр.). Как только Kaspersky Anti-Hacker засечет попытку неавторизованного приложения (например, троянца-шпиона) пробраться в сеть, он сообщит об этом.

Дезинфекция трафика на уровне приложений - вещь необходимая, но для надежной защиты компьютера недостаточная, поскольку троянские программы могут подсоединиться к приложениям, которые работают с внешней сетью, и рассылать пакеты через них. Так работают многие современные сетевые черви типа Melissa или LoveLetter. Для исключения таких инцидентов в программе имеется функция контроля над сетевыми пакетами. Здесь программа проверяет атрибуты всех пакетов данных и не позволяет им уходить на запрещенные адреса, через запрещенные порты и протоколы.

Кроме того, в программу встроена система обнаружения атак (IDS - Intrusion Detection System), которая анализирует входящий трафик и предотвращает все наиболее распространенные хакерские нападения, такие как DoS-атаки, сканирование портов и пр.

Точкой входа для хакеров, пытающихся получить доступ к информации, являются порты. Их обилие и неопределенный статус создают ситуацию, подходящую для успешной хакерской атаки. Именно поэтому любой современный брандмауэр должен иметь в своем арсенале механизм надежной защиты портов. Именно за это и отвечает четвертый защитный слой Kaspersky Anti-Hacker.

В программе имеется встроенная технология SmartStealth для контроля над портами компьютера. Согласно сведениям разработчика, благодаря ей защищенный компьютер становится полностью невидимым для нежелательных лиц из внешнего окружения. Для пользователя при этом сохраняется обычная прозрачность сети, а для злоумышленника компьютер исчезает из сети. Если же установить наивысший уровень защиты, то компьютер просто перестает реагировать на все входящие запросы (как бы выпадает из виртуального мира), за исключением тех, которые разрешены.

Программа предлагает два универсальных механизма настройки абсолютно всех параметров межсетевого экрана. Первый - система предопределенных уровней безопасности. Второй - шаблоны всех используемых приложений.

Kaspersky Anti-Hacker предоставляет пять встроенных режимов работы:

Разрешить все - данный вариант равносилен отсутствию Kaspersky Anti-Hacker на компьютере. Он бывает полезен для режима тестирования сети, когда, достаточно ненадолго переключиться в режим бездействия, а потом вернуться обратно без выгрузки системного сервиса из памяти.

Низкий (разрешить все, что не запрещено) - брандмауэр блокирует только те приложения, для которых созданы специальные правила. Все остальные программы работают беспрепятственно. Пользоваться этим режимом целесообразно только в том случае, если вы уверены, что внутренняя угроза доступа к конфиденциальным данным отсутствует.

Высокий (запретить все, что не разрешено) - брандмауэр разрешает доступ к сети только тем программам, которые указаны в правилах. В этом режиме окно обучения не появляется, и все попытки несанкционированных соединений отклоняются. Этот вариант следует использовать после того, как вы уже проработали достаточно долгий срок в режиме обучения и настроили все нужные правила.

Запретить все - Kaspersky Anti-Hacker полностью блокирует доступ вашей машины к сети. Компьютер изолируется от любого внешнего и внутреннего воздействия. Этот режим особенно полезен, если вам необходимо провести некую сверхсекретную операцию, а в случае подозрения на атаку позволяет временно отключиться от Интернета, чтобы спокойно разобраться в ситуации.

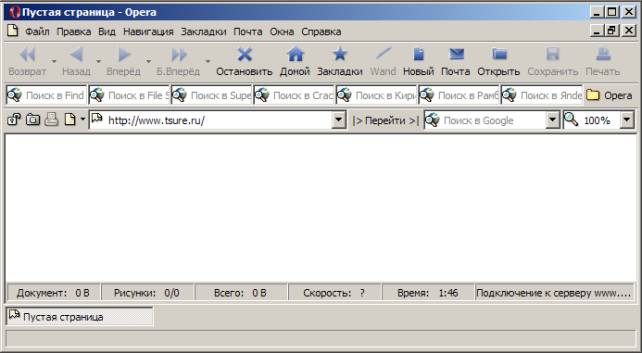
Средний уровень безопасности состоит в том, что брандмауэр уведомляет о сетевой активности всех приложений. Это хороший способ сконфигурировать систему безопасности наиболее рационально.

Уведомление представляет собой окошко с кнопочками: разрешить или блокировать данное событие однократно, запретить активность приложения полностью, разрешить активность приложения в соответствии с указанным.

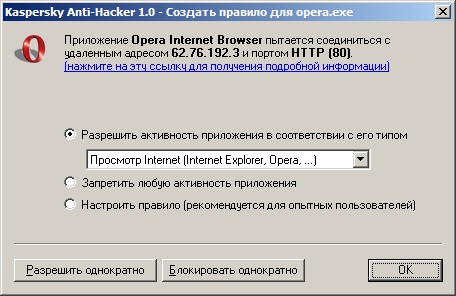
Самой важной частью режима самообучения являются шаблоны правил, с помощью которых конфигурируются правила для любого приложения.

**НАСТРОЙКА ПРАВИЛА ПО ДОСТУПУ К СЕТИ ДЛЯ ПРИЛОЖЕНИЯ**

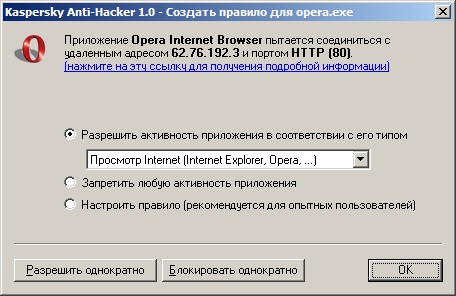
Запустим программу-броузер и попытаемся соединиться с какой-нибудь страницей в Интернет:



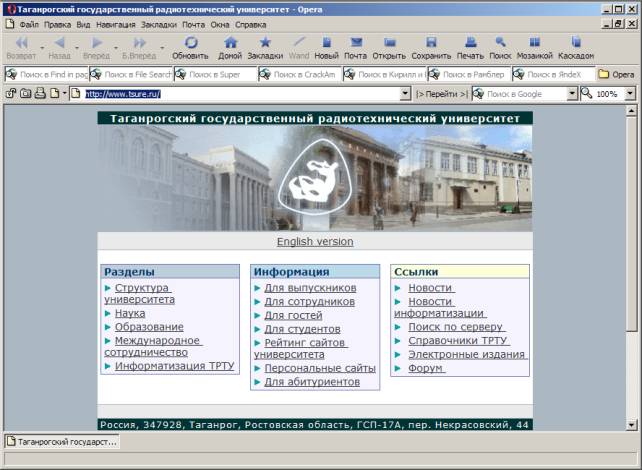
Защитный экран перехватит это обращение и выдаст запрос на соединение:



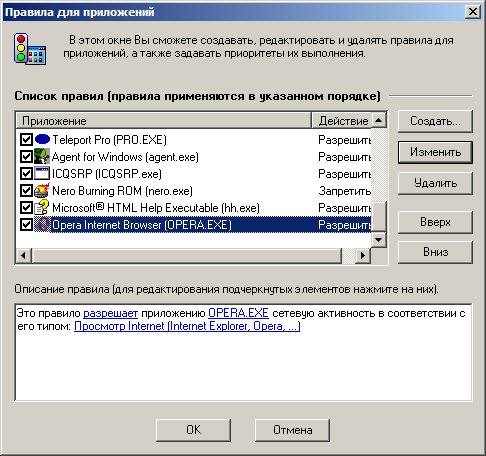
Можно сразу разрешить активность приложения (постоянно или однократно), а можно просмотреть, какое правило предлагает программа:



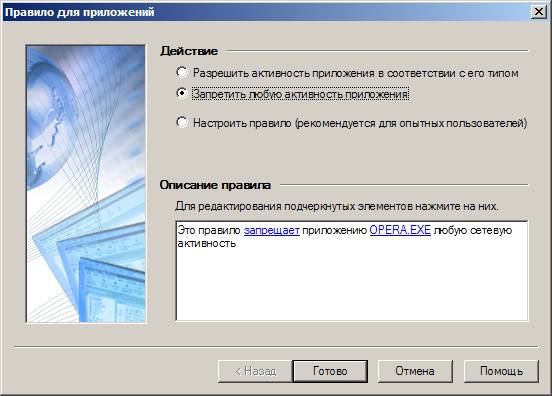
После этого браузер сможет получить доступ в Интернет:



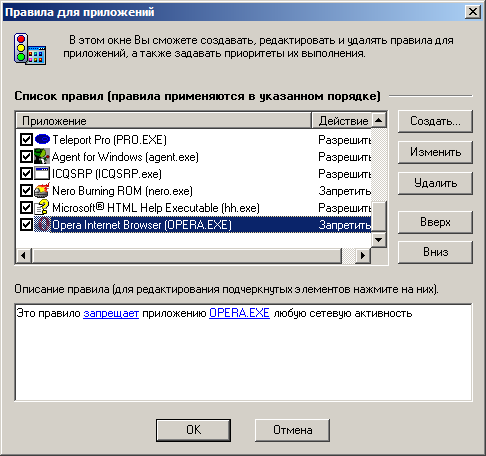
Посмотрим теперь, как выглядит список правил для приложений в окне "Правила для приложений":



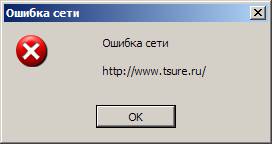
Теперь запретим активность этого приложения



Теперь список правил будет выглядеть следующим образом:



Теперь опять постараемся просмотреть сайт с помощью браузера и получим отказ:

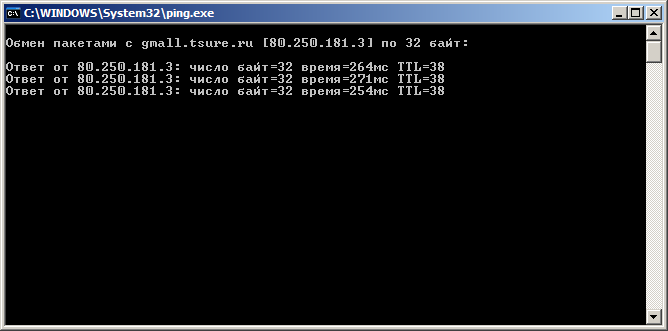


Просмотреть видеозапись процесса настройки правила по доступу к сети для приложения: [opera-1.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\opera-1.avi), [opera-2.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\opera-2.avi), [opera-3.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\opera-3.avi)

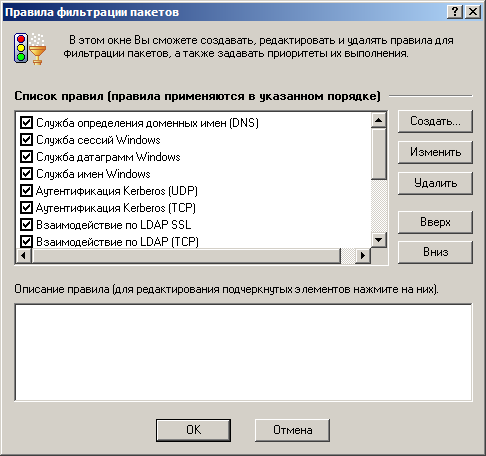
**НАСТРОЙКА ПРАВИЛА ФИЛЬТРАЦИИ ПАКЕТОВ**

Настроим нашу систему так, чтобы не пропускались пакеты по протоколу ICMP. Проверить работоспособность нашего правила мы сможем с помощью программы ping.

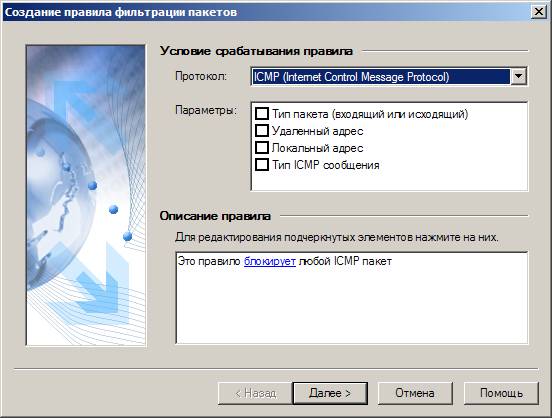
Запустим программу ping для проверки достижимости любого сетевого адреса:



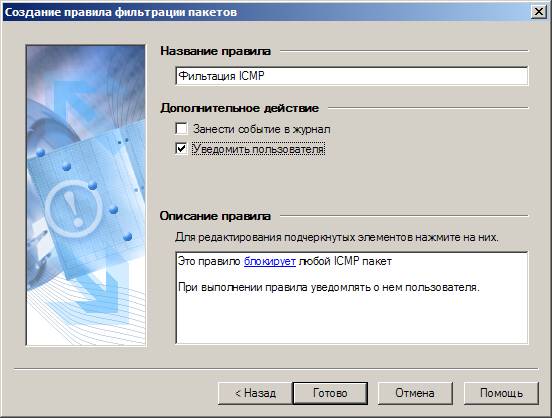
Теперь вызовем программу настройки защитного экрана и создадим новое правило:



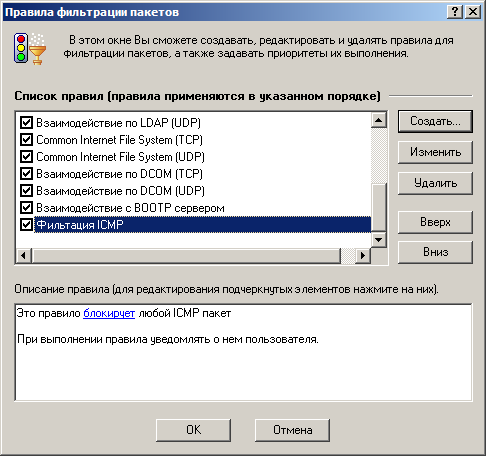
И создадим новое правило. Выберем нужный нам тип протокола:



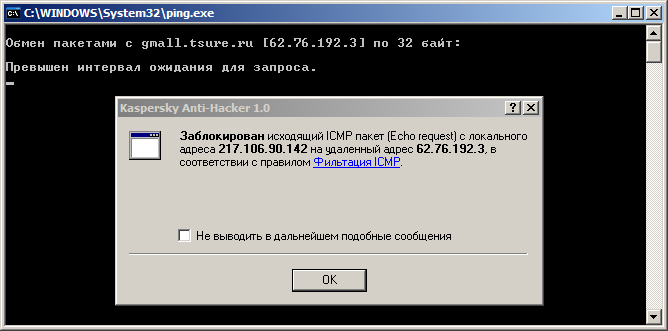
Дадим пакету название и потребуем уведомлять пользователя каждый раз, когда будет совершена попытка соединения по протоколу ICMP:



Теперь новое правило появилось в общем списке:

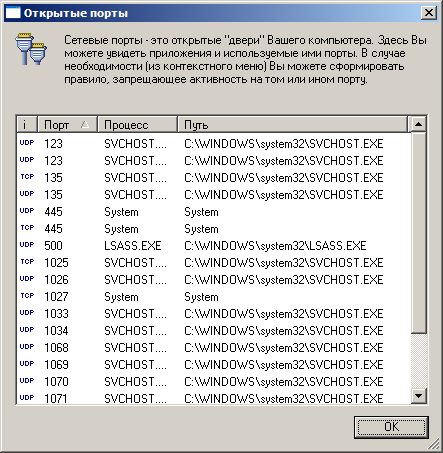


Попытаемся теперь опять выполнить команду ping. Получим сообщение о событии от межсетевого экрана и ошибки самой команды ping:

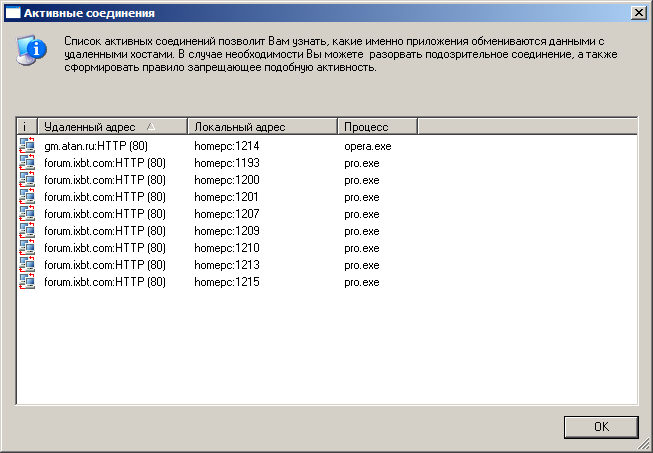


**ПРОСМОТР ДАННЫХ О ТЕКУЩИХ СОЕДИНЕНИЯХ**

Для просмотра информации об открытых портах необходимо выполнить команду "Вид/Показать/Открытые порты":

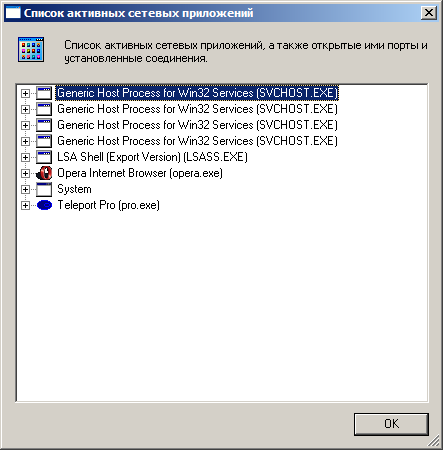


Для просмотра текущих соединений необходимо выполнить команду "Вид/Показать/Активные соединения":



Любое соединение можно разорвать.

Для просмотра приложений, которые в данный момент обмениваются данными с сетью, используем команду "Вид/Показать/Активные сетевые приложения":



Просмотреть видеозапись процесса настройки правила фильтрации пакетов: [ping\_1.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\ping_1.avi), [ping\_2.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\ping_2.avi), [ping\_3.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\ping_3.avi)