***Лабораторная работа 6***

**Тема :Защита от несанкционированного доступа и сетевых хакерских атак**

***Цель работы:*** *Познакомиться с настройками встроенного* *брандмауэра и Центра обеспечения* *безопасности системы Microsoft* *Windows XP.*

**Задание 1. *Брандмауэр Windows***

Задачу защиты от несанкционированного доступа и сетевых атак домашнего компьютера успешно решает брандмауэр (или межсетевой экран). Он может быть как встроенным в операционную систему (например, брандмауэр Windows), так и устанавливаемым отдельно.

**Брандмауэр или межсетевой экран** — это программное или аппаратное обеспечение, которое помогает отражать атаки хакеров, вирусов и червей, пытающихся попасть на компьютер через Интернет. Брандмауэр является одним из наиболее популярных средств защиты.

Брандмауэр Windows контролирует входящий и исходящий сетевой трафик подключений. Брандмауэр следит за информацией, отправляемой с компьютера, и предотвращает попадание в него ненужных данных из сети. При необходимости брандмауэр динамически открывает порты и позволяет компьютеру принимать запрошенный трафик, например сайт, адрес которого Вы набрали в браузере.

**"Порт"** — это сетевой термин, обозначающий точку, через которую сетевой трафик поступает на компьютер. Открываемые порты зависят от типа трафика, который нужно отправить или получить.

Если вы не запрашивали входящий трафик, брандмауэр подключения к интернету блокирует его до того, как он достигнет компьютера. В некоторых случаях, таких как работа в сети, установка онлайновых игр или собственного сервера, можно открыть некоторые порты. Это позволит другим пользователям подключаться к компьютеру, но может также снизить уровень безопасности.

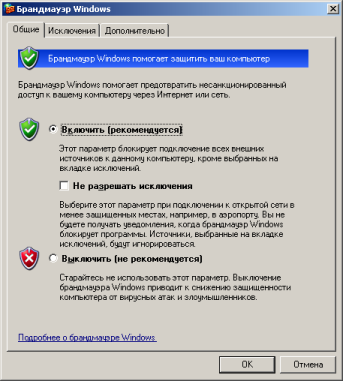
Ранние версии операционных систем Windows (до Windows XP) не содержали встроенный брандмауэр. Более поздние версии - Vista и Seven, 8 - содержат в себе дополнительные компоненты защиты от несанкционированного доступа и шпионских программ, например Windows Defender.

Встроенные брандмауэры, в отличие от брандмауэров сторонних производителей, отличаются скромной функциональностью, но при этом работают без конфликтов с операционной системой. Еще одним существенным преимуществом является их бесплатность.

1. Для того чтобы открыть брандмауэр Windows XP выполните следующие действия:Пуск –>Настройка->Панель управления –>Брандмауэр Windows

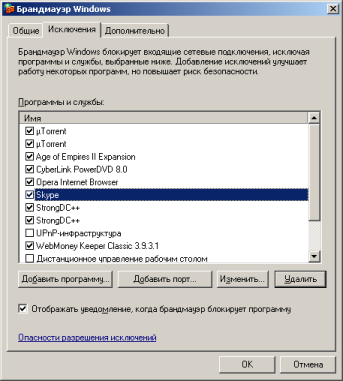
  
**Рис. 1.**

1. На экране появится меню Брандмауэр Windows

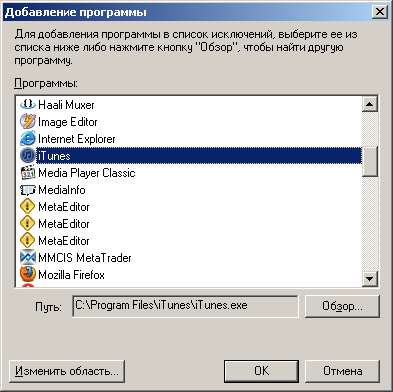


**Рис. 2.**

1. Вкладка **Общие** позволяет менять режим работы Брандмауэра Windows. Можно **Включить брандмауэр** или **Выключить** его. Отключите Брандмауэр Windows, а затем вновь включите его.
2. Вкладка **Исключения** позволяет создавать исключения для нужных служб и программ. Если Вы точно уверены в легитимности программы, например, игры, а брандмауэр заблокировал ей сетевой доступ, добавьте ее в список исключения. Для этого нажмите на кнопку **Добавить программу**http://www.intuit.ru/EDI/09_08_13_2/1375996704-20630/tutorial/428/objects/21/files/3_k1.jpg и в появившемся списке выберите любое приложение.



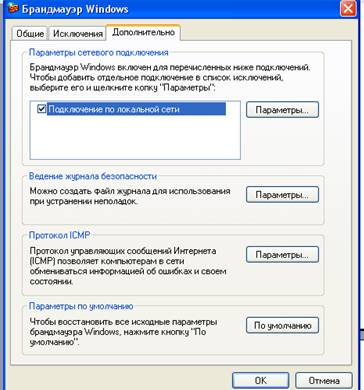
**Рис. 3.**



**Рис. 4.**

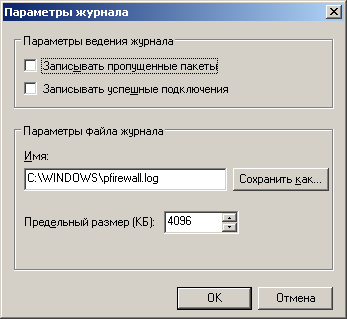
На [рис. 4](http://www.intuit.ru/studies/courses/2291/591/lecture/7622?page=1#image.21.4) в список будет добавлена программа iTunes для работы с плеером Ipod. После выбора программы нажмите на кнопку ОК.

1. Вкладка **Дополнительно** позволяет включить или отключить Брандмауэр Windows для конкретных сетевых подключений, заблокировать или разблокировать сетевые службы. Выберите нужное сетевое **Подключение** и нажмите кнопку **Параметры**http://www.intuit.ru/EDI/09_08_13_2/1375996704-20630/tutorial/428/objects/21/files/3_k2.jpg



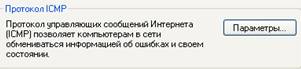
**Рис. 5.**

1. При устранении неполадок, можно воспользоваться **Журналом Безопасности**, для того, чтобы выяснить, когда произошла неполадка и при каких обстоятельствах. Нажмите кнопку **Параметры**http://www.intuit.ru/EDI/09_08_13_2/1375996704-20630/tutorial/428/objects/21/files/3_k2.jpg в блоке **Ведение журнала безопасности**. В появившемся окне произведите настройки, согласно предложенному [рис. 6](http://www.intuit.ru/studies/courses/2291/591/lecture/7622?page=1#image.21.6) и нажмите ОК.



**Рис. 6.**

1. Блок **Протокол ICMP** служит для приема и отправки сообщений об ошибках и состоянии компьютеров в сети. Так же этот протокол используют некоторые вредоносные программы, с периодичностью показывая различные сообщения о якобы произошедших ошибках в операционной системе.



**Рис. 7.**

1. Блок **Параметры по умолчанию** служит для восстановления исходных настроек Брандмауэра Windows.

http://www.intuit.ru/EDI/09_08_13_2/1375996704-20630/tutorial/428/objects/21/files/3_7.jpg

**Рис. 8.**

**Задание 2. *Центр Обеспечения безопасности Windows***

Для безопасной работы в сети Интернет, необходимо, что на компьютере постоянно функционировал межсетевой экран и антивирусная программа. Кроме того, необходимо чтобы все последние обновления ПО и ОС были установлены на Вашем компьютере. Отслеживание обновления антивирусных баз, программного обеспечения и т.п. является достаточно трудоемкой задачей, и пользователь не всегда компетентен в этих вопросах. Более того, это требует значительных временных затрат. Для решения вышеизложенных задач компания Microsoft включила в состав обновлений SP2 и SP3 для Windows XP инструмент под названием **Центр обеспечения безопасности Windows (Windows Security Center)**.

1. Для того чтобы открыть Центр обеспечения безопасности Windows нажмите Пуск –>Настройка->Панель управления –>Центр обеспечения безопасности



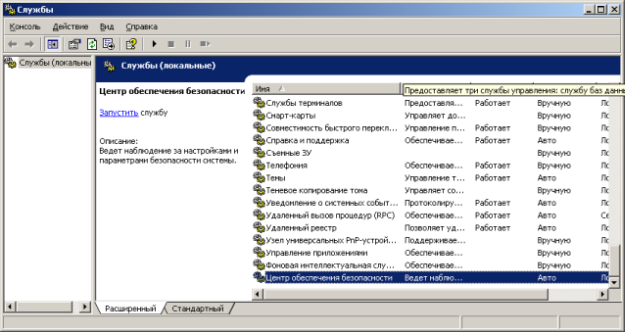
**Рис. 9.**

1. Для включения Центра обеспечения безопасности Windows нажмите Пуск –>Настройка->Панель управления –>Администрирование –>Службы.

http://www.intuit.ru/EDI/09_08_13_2/1375996704-20630/tutorial/428/objects/21/files/3_9.png

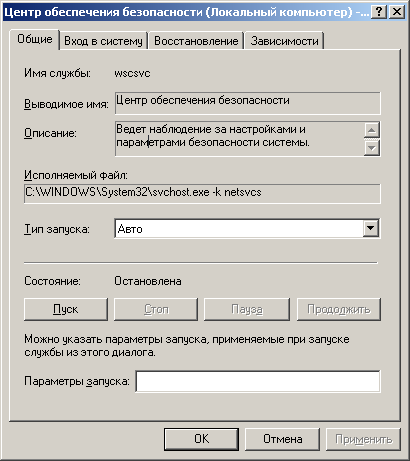
**Рис. 10.**

В открывшемся окне среди списка служб выберите **Центр обеспечения безопасности**.



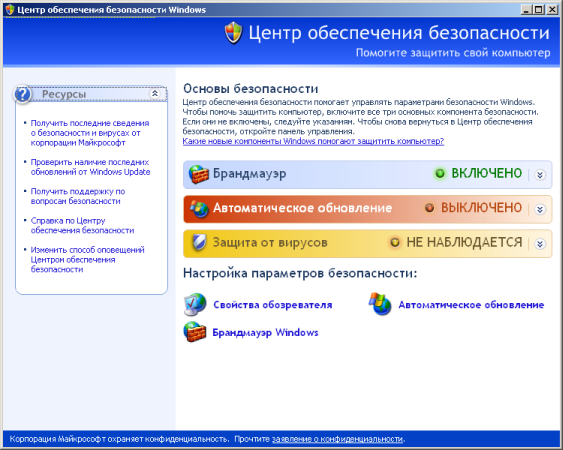
**Рис. 11.**

Кликните на службе мышью два раза. В открывшемся окне выберите тип запуска **Авто**. В строке **Состояние** указано состояние службы. Если она остановлена, нажмите на Пуск. После этого **Состояние** изменится на **Работает**. Нажмите на кнопки Применить и ОК и перезагрузите компьютер.



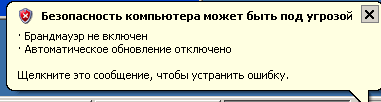
**Рис. 12.**

1. На экране появится меню **Центра обеспечения безопасности Windows.**



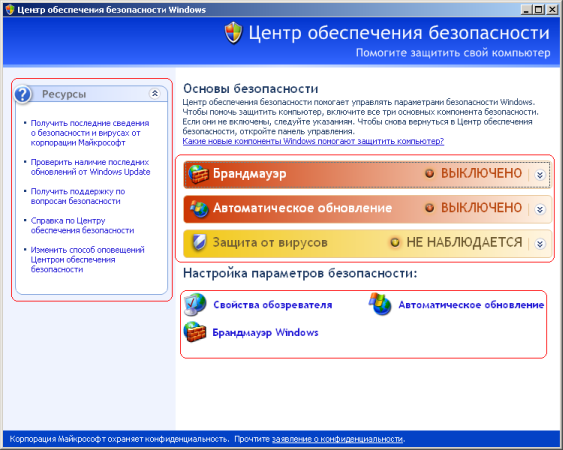
**Рис. 13.**

Как видно из рис. 12 **Центр обеспечения безопасности** контролирует три основные компонента для защиты – брандмауэр, антивирус и систему автоматического обновления. В случае, если компонент будет отключен или параметры одного из компонентов будут настроены не верно, система выдаст предупреждение пользователю ( рис. 13).



**Рис. 14.**

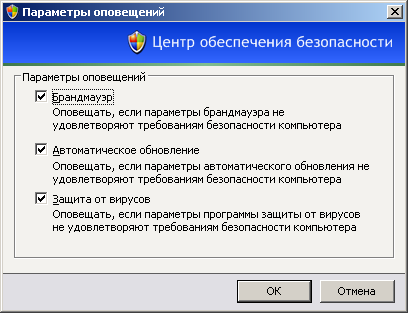
1. Основное окно Центра обеспечения безопасности Windows можно разделить на 3 части



**Рис. 15.**

* + **Ресурсы**. С помощью данной части меню можно получить доступ локальным и Интернет-ресурсам: последним сведениям о безопасности и вирусах от Microsoft, проверить наличие последних обновлений от Windows Update, вызвать справку о Центре обеспечения безопасности, получить поддержку по вопросам безопасности и изменить способ оповещения Центром обеспечения безопасности.
  + **Компоненты безопасности**. Здесь отображаются параметры настройки трех основных компонентов безопасности: брандмауэра, автоматического обновления, антивирусной защиты.
  + **Параметры безопасности**. Отсюда можно перейти к настройкам безопасности обозревателя Internet Explorer, автоматического обновления, брандмауэра Windows. Рассмотрим меню окна Центр обеспечения безопасности более подробно.

1. В меню **Ресурсы** первые три ссылки предназначены для перехода на соответствующие страницы на сайте Microsoft. Предпоследняя ссылка предназначена для открытия справочной службы Windows на странице "Общие сведения о центре обеспечения безопасности Windows". Последняя ссылка предназначена для открытия окна "Параметры оповещений". Нажмите на последнюю ссылку. Появится окно для настроек параметров системы оповещений.



**Рис. 16.**

Вы можете отключить любое из оповещений Центра обеспечения безопасности. В частности, если установлен антивирус, который Центр обеспечения безопасности не обнаруживает, удалите галочку напротив "Защита от вирусов".

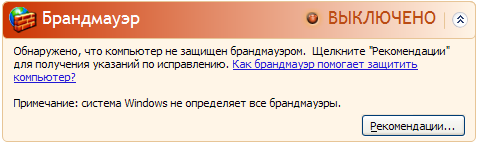
1. В меню **Компоненты безопасности** напротив каждого компонента отображается его текущее состояние. На рис. 16 представлены возможные состояния.



**Рис. 17.**

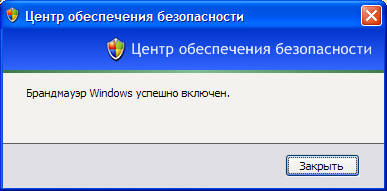
Состояния A-C понятны без комментариев. Состояние D - "Не найдено" - соответствует невозможности определить присутствие соответствующего ПО (например, антивирус или брандмауэр). Состояние E - "Срок истек" - возможно для антивирусной защиты, когда обновления антивирусных баз устарели. Состояние F - "Не наблюдается" - соответствует отключенному контролю над соответствующим компонентом.

1. Выключите один из компонентов защиты. Состояние этого компоненты примет вид, показанный на рис. 18 (например, если отключить Брандмауэр Windows).



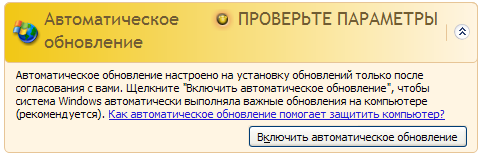
**Рис. 18.**

1. Включите отключенный компоненты защиты, на экране появится сообщение о том, что Ваш компонент успешно запущен.



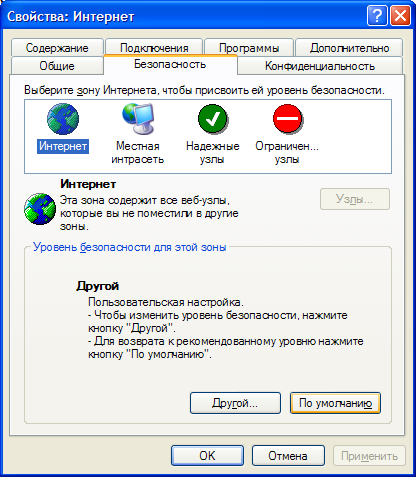
**Рис. 19.**

1. Если один из компонентов не может выполнить нужное действие (например, автоматические обновления устанавливаются по выбору пользователя), статус компонента примет вид, показанный на рис. 20.



**Рис. 20.**

1. Как уже отмечалось ранее, в меню Параметры безопасности расположены кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows, нажав на кнопку **Свойства обозревателя**, вы попадете на закладку **Безопасность** в окне настроек обозревателя Internet Explorer.



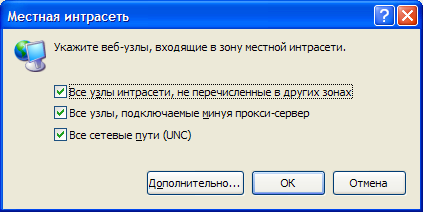
**Рис. 21.**

Рассмотрим параметры, доступные на этой закладке. В верхней части расположены четыре зоны: Интернет, Местная интрасеть, Надежные узлы, Ограниченные узлы. В табл.1 дано описание для каждой зоны.

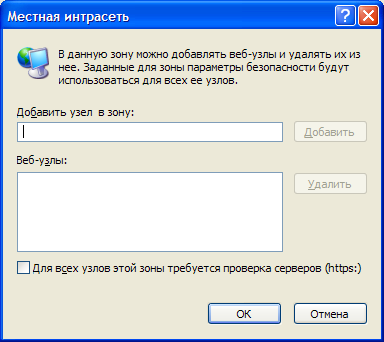
**Таблица 1. Описание зон**

|  |  |
| --- | --- |
| **Зона** | **Какие узлы может содержать зона** |
| **Интернет** | Содержит все веб-узлы, которые не помещены в другие зоны |
| **Местная интрасеть** | Может содержать указанные вами узлы. Может содержать все узлы интрасети, не перечисленные в других зонах, все узлы, подключаемые минуя прокси-сервер, все сетевые пути (UNC) |
| **Надежные узлы** | Может содержать указанные вами узлы |
| **Ограниченные узлы** | Может содержать указанные вами узлы |

Для всех зон, кроме зоны "Интернет", вы можете определить входящие в зону узлы. Для этого необходимо выбрать нужную зону и нажать кнопку "Узлы...". Для зоны "Местная интрасеть" в этом случае откроется окно, представленное на рис.23. Если вы хотите указать конкретные узлы, нажмите кнопку "Дополнительно…". В результате появится окно, представленное на рис.24. Аналогичное окно будет открыто, если вы будете определять узлы, входящие в зоны "Надежные узлы" и "Ограниченные узлы". Только для зоны "Ограниченные узлы" будет отсутствовать параметр "Для всех узлов этой зоны требуется проверка серверов (https:)".



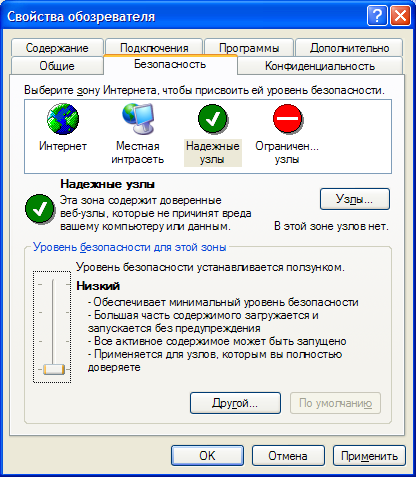
**Рис. 22.** Местная интрасеть



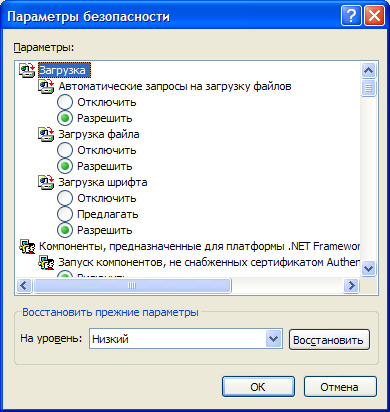
**Рис. 23.** Задание конкретных узлов

Каждой зоне можно присвоить нужный уровень безопасности: высокий, средний, ниже среднего, низкий. Низкий уровень безопасности соответствует минимальной защите и применяется для узлов, которым вы полностью доверяете.

Выберите нужную зону (см.рис.24) и нажмите кнопку "По умолчанию". Закладка "Безопасность" изменит свой вид (рис.25). В нижней части окна вы можете определить нужный уровень безопасности. Если вы не хотите использовать предлагаемые уровни безопасности, вы можете нажать кнопку "Другой…" и определить все параметры безопасности самостоятельно (рис.25).



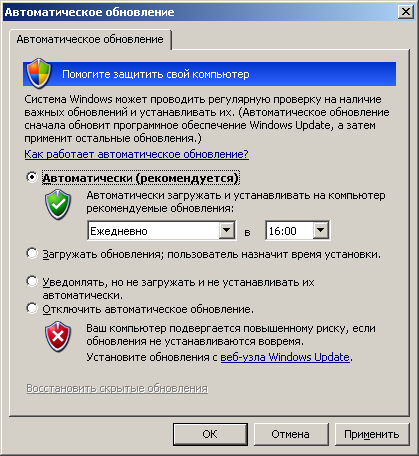
**Рис. 24.** Настройки безопасности Internet Explorer



**Рис. 25.** Параметры безопасности

Описанные выше настройки безопасности обозревателя Internet Explorer также доступны через групповую политику (Конфигурация компьютера, Административные шаблоны, Компоненты Windows, Internet Explorer, Панель управления обозревателем, Страница безопасности).

1. Нажав кнопку **Автоматическое обновление** , вы откроете окно настроек "Автоматического обновления".



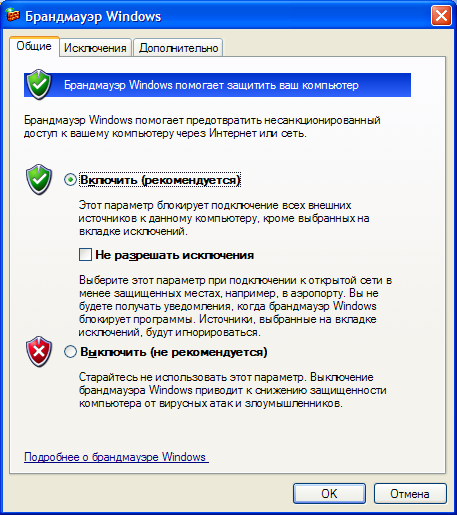
**Рис. 26.**

Здесь возможны несколько вариантов настройки обновлений:

* + **автоматически**. Операционная система будет в указанное время загружать обновления и самостоятельно устанавливать их. Это рекомендуемый режим.
  + **загружать обновления, пользователь сам назначает время установки**. В данном варианте обновления загружаются, выводится соответствующее сообщение. Далее пользователь сам решает, когда их нужно установить.
  + **уведомлять, но не загружать и не устанавливать их автоматически**. Операционная система проверяет наличие уведомлений и оповещает пользователя в случае, если таковые имеются. Пользователь вручную загружает их и устанавливает.
  + **отключение автоматических обновлений**.

Поставьте автоматическую установку обновлений каждый день в 16:00.

1. Нажав кнопку **Брандмауэр Windows**, вы попадете в окно настроек брандмауэра Windows, рассмотренное нами ранее.



**Рис. 27.**