Текущий контроль №5

1. Первое лабораторное задание
Включение и настройка Брандмауэра подключения к Интернету (ICF).

1. В меню **Пуск** (Start) щелкните **Мой компьютер** (My Computer), **Сетевое окружение** (My Network Places), затем — **Отобразить сетевые подключения**(View Network Connections). Откроется окно **Сетевые подключения** (Network Connections).
2. Щелкните значок подключения к Интернету (через модем, локальную сеть или высокоскоростного), которое требуется защитить с помощью брандмауэра.
3. В группе **Сетевые задачи** (Network Tasks) щелкните **Изменение настроек подключения** (Change Settings Of This Connection).
4. На вкладке **Дополнительно** (Advanced) нажмите клавишу **Параметры**(Settings) чтобы войти в меню Брандмауэра Windows. Для включения Брандмауэра подключения к Интернету (ICF) установите флажок**Включить (Рекомендуется).**
5. На вкладке **Исключения** добавьте флажок **Дистанционное управление рабочим столом** Рис. 6.3. (Что это изменяет в защите?)

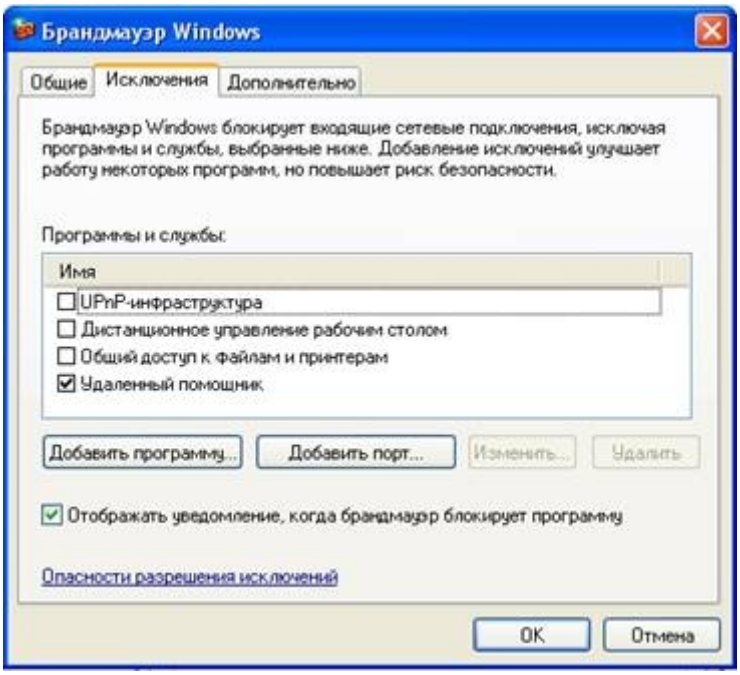

Рис. 6.3. Вкладка Исключение диалогового окна Брандмауэр Windows.

Если программа или служба, которую требуется разрешить, отсутствует в списке, выполните следующие действия.

- Нажмите кнопку **Добавить программу**.
- В диалоговом окне **Добавление программы** выберите программу, которую требуется добавить, и нажмите кнопку **OK**. Эта программа появится (с установленным флажком) на вкладке **Исключения** в группе **Программы и службы**.
- Нажмите кнопку **OK**.

Если программа или служба, которую требуется разрешить, не перечислена в диалоговом окне **Добавление программы**, выполните следующие действия.

- В диалоговом окне **Добавление программы** нажмите кнопку **Обзор**, найдите программу, которую требуется добавить, и дважды щелкните ее. (Программы обычно хранятся на компьютере в папке «Program Files».) Программа появится в группе **Программы** в диалоговом окне **Добавление программы**.
- Нажмите кнопку **OK**. Эта программа появится (с установленным флажком) на вкладке**Исключения** в группе **Программы и службы**.
- Нажмите кнопку **OK**.

6. На вкладке **Дополнительно** (Advanced) можно настроить **Параметры сетевого подключения**, параметры **Ведения журнала безопасности,**параметры **Протокола ICMP** или восстановить параметры по умолчанию Рис. 6.4**.**
7. Для изменения параметров сетевого подключения нажмите клавишу**Параметры** (Settings). Откроется диалоговое окно **Дополнительные параметры** (Advanced Settings) (рис. 6.5). Следует указать разрешенные службы к которым могут получать доступ пользователи допущенные к работе в Интернет.

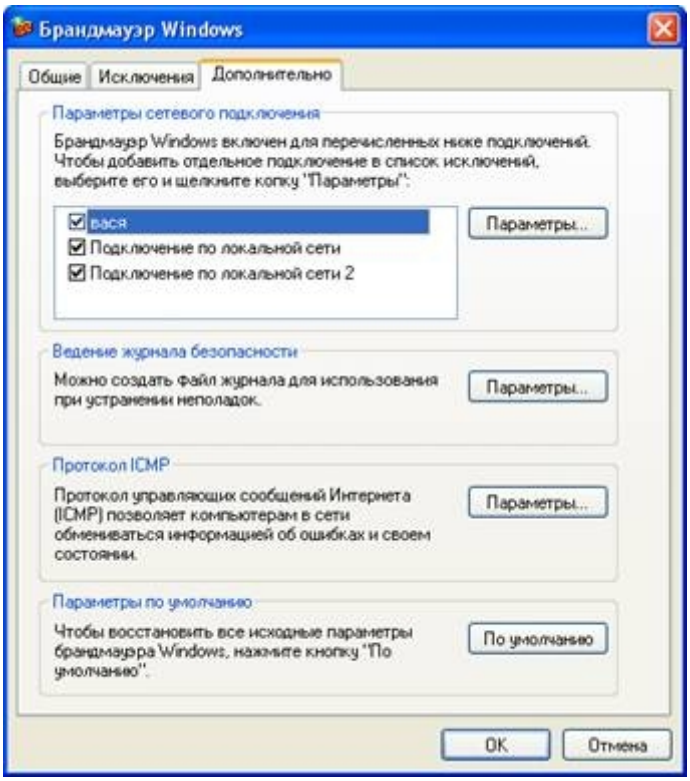

Рис. 6.4. Вкладка Дополнительно диалогового окна Брандмауэр Windows

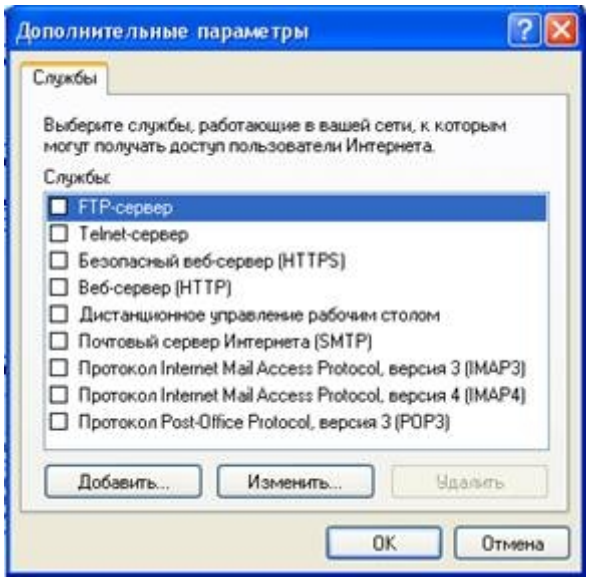

Рис. 6.5. Вкладка Службы (Services) диалогового окна параметры сетевого подключения

На вкладке **Ведение журнала безопасности** (Security Logging) следует определить, нужно ли регистрировать отброшенные (пропущенные) пакеты и успешные подключения. Здесь же задаются размер и размещение файла журнала. По умолчанию имя файл журнала **PFIREWALL.LOG**, а его размер ограничен 4096 кбайт.
Чтобы включить ведение журнала безопасности, выберите один из параметров**Записывать пропущенные пакеты** (Log Dropped Packets) или **Записывать успешные подключения** (Log Successful Connections) или оба сразу.
Ведение журнала безопасности
Чтобы включить параметры ведения журнала безопасности необходимо войти в систему с учетной записью «Администратор».

- Откройте брандмауэр Windows.
- На вкладке **Дополнительно** в группе **Ведение журнала безопасности** нажмите кнопку**Параметры**.
- Выберите один из следующих параметров.
    - Чтобы включить регистрацию неудачных попыток установления входящего подключения, установите флажок **Записывать пропущенные пакеты**.

Примечания: Ведение журнала безопасности не включено по умолчанию, если брандмауэр Windows включен, однако брандмауэр работает независимо от того, включено ведение журнала безопасности или отключено. Ведение журнала доступно только для подключений, для которых включен брандмауэр Windows.

    - Чтобы включить регистрацию успешных исходящих подключений, установите флажок**Записывать успешные подключения**.

Чтобы просмотреть файл журнала безопасности

- Откройте брандмауэр Windows.
- На вкладке **Дополнительно** в группе **Ведение журнала безопасности** нажмите кнопку**Параметры**.
- Нажмите кнопку **Обзор**.
- Щелкните правой кнопкой мыши файл pfirewall.log, а затем нажмите кнопку **Открыть**.
- По умолчанию журнал безопасности имеет имя pfirewall.log и расположен в папке Windows.
- Чтобы файл pfirewall.log появился в папке Windows, необходимо установить флажок**Записывать пропущенные пакеты** или **Записывать успешные подключения**.
- Если превышен максимально допустимый размер журнала pfirewall.log (4096 килобайт), сведения, содержащиеся в файле, передаются в другой файл, который сохраняется с именем pfirewall.log.old. Новые сведения сохраняются в первом созданном файле с именем pfirewall.log.

4.2. Второе лабораторное задание

Настройка параметров безопасности и конфиденциальности подключения к Интернету.

Для доступа к параметрам Интернета выполните описанные далее действия.
1. Щелкните ***Пуск*** (Start), затем — ***Панель управления*** (Control Panel).
2. Щелкните категорию ***Сеть и подключения Интернета*** (Network And Internet Connections), затем щелкните значок ***Свойства обозревателя*** (Internet Options). Откроется диалоговое окно ***Свойства: Интернет*** (Internet Properties), показанное на рис. 6.6.

Вкладка Общие (General)

Раздел Домашняя страница (Home Page) на вкладке ***Общие*** (General) диалогового окна ***Свойства: Интернет*** (Internet Properties) позволяет изменить Web-страницу, которая будет использоваться вами как ***домашняя страница*** (home page), то есть страница, которая загружается каждый раз при запуске Internet Explorer. Вернуться к ней можно, щелкнув значок ***Домой*** (Home) на панели инструментов.

Раздел Временные файлы Интернета (Temporary Internet Files) на вкладке ***Общие***(General) позволяет удалить все файлы «cookies» и временные файлы Интернета, хранящиеся на вашем компьютере. Файлы «cookie» — это файлы, создаваемые Web-сайтом и сохраняющие вашу персональную информацию на вашем компьютере. Для удаления всех этих файлов щелкните кнопку ***Удалить «cookie»*** (Delete Cookies). В появившемся окне ***Удаление файлов «cookie»***(Delete Cookies) следует подтвердить, что вы действительно хотите удалить все файлы «cookie», сохраненные на вашем компьютере, щелкнув кнопку ОК, или отказаться от удаления, щелкнув кнопку **Отмена**(Cancel).

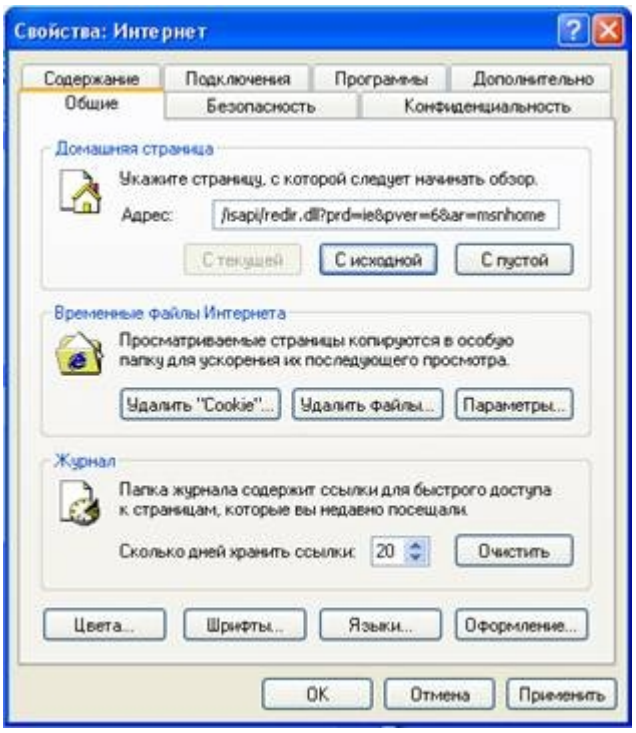

Рис. 6.6. Вкладка Общие (General) диалогового окна Свойства: Интернет

Временные файлы Интернета (temporary Internet file) - это файлы, загруженные с Web-сайта и сохраненные на вашем компьютере с целью уменьшения времени доступа к сайту при следующих обращениях. Чтобы

удалить все временные файлы Интернета, щелкните кнопку ***Удалить файлы***(Delete Files). Будет выведено окно сообщений, в котором вас просят подтвердить необходимость удаления всех временных файлов Интернета на вашем компьютере. Установка флажка ***Удалить это содержимое*** (Delete All Offline Content) приведет к удалению содержания любых сайтов, которые вы сделали доступными в автономном режиме. Щелкните ОК для удаления всех временных файлов Интернета на вашем компьютере. Чтобы определить, когда ваша система должна осуществлять проверку наличия новых версий сохраненных файлов и задать местоположение и размер папки для хранения временных файлов Интернета, щелкните кнопку ***Параметры*** (Settings).
Раздел Журнал(History) позволяет установить время хранения ссылок на посещенные вами страницы или удалить все сохраненные ссылки. Кроме того, вкладка ***Общие*** (General) позволяет настроить параметры используемых при просмотре цветов, шрифтов, языков и оформления.

Вкладка Безопасность (Security) диалогового окна ***Свойства: Интернет***(Internet Properties) позволяет разделить Web-сайты на зоны, чтобы настроить параметры безопасности для каждой зоны.
Первая зона, называемая ***Интернет*** (Internet) включает все Web-сайты, не входящие в другие зоны (рис. 6.7).
Вторая зона представляет местную интрасеть. Третья зона предназначена для надежных узлов, а четвертая - для ограниченных узлов. Чтобы добавить Web-сайт в одну из этих зон, щелкните значок зоны, а затем щелкните кнопку ***Узлы***(Sites).

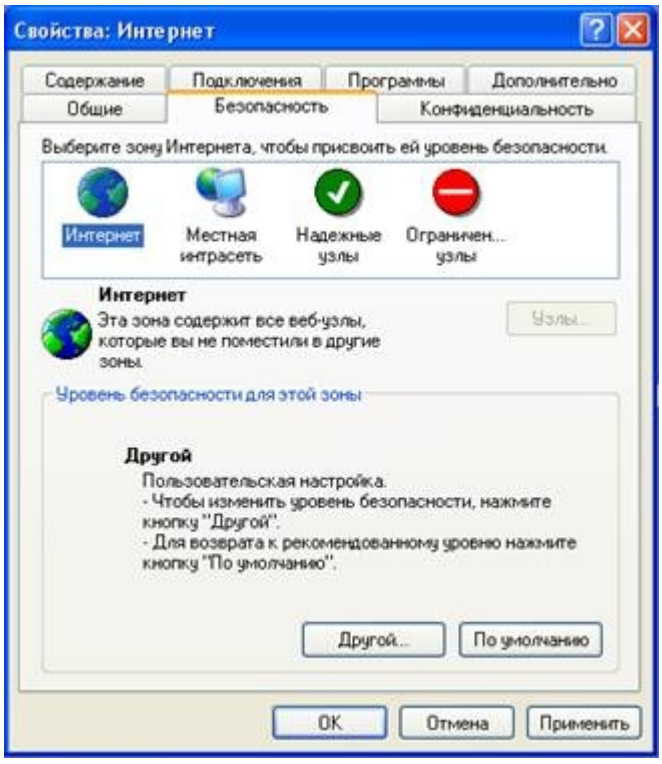

Рис. 6.7. Вкладка Безопасность (Security) диалогового окна Свойства: Интернет

Раздел Уровень безопасности для этой зоны (Security Level For This Zone) позволяет настроить параметры безопасности для каждой из этих зон. Для

настройки уровня безопасности зоны щелкните значок зоны, а затем — кнопку***Другой*** (Custom Level). Откроется диалоговое окно ***Параметры безопасности***(Security Settings) (рис. 6.8). Оно позволяет контролировать, какая информация будет загружаться на ваш компьютер из Интернета.
Например, для параметра ***Загрузка подписанных элементов ActiveX*** (Download Signed ActiveX Controls) можно задать одно из трех значений:
• ***Разрешить*** (Enable). Позволяет загружать подписанные элементы управления ActiveX;
• ***Отключить*** (Disable). Запрещает загрузку подписанных элементов управления ActiveX;
• ***Предлагать*** (Prompt). Для каждого подписанного элемента управления ActiveX система выводит окно, позволяющее указать, загружать этот элемент или нет.

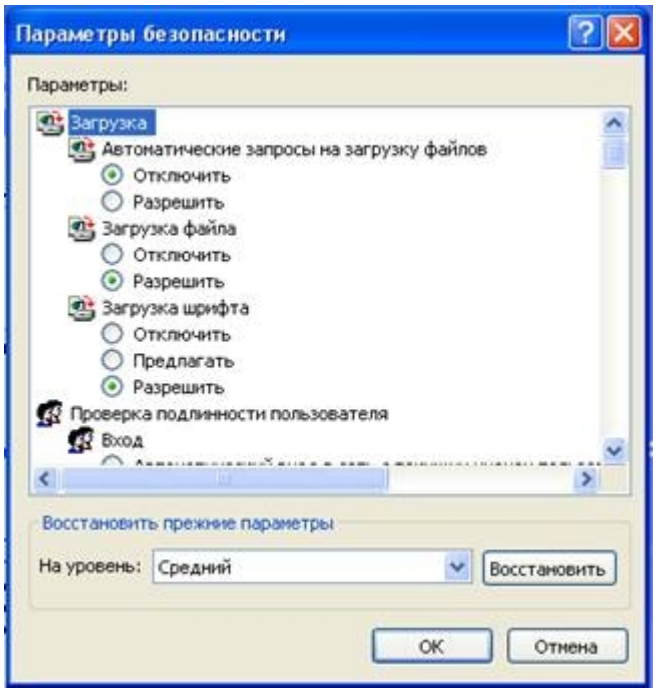

Рис. 6.8. Диалоговое окно Параметры безопасности (Security Settings)

• ***Разрешить метаобновление*** (Allow META REFRESH);
• ***Отображение разнородного содержимого*** (Display Mixed Content);
• ***Не запрашиватьсертификатклиента, когдаонотсутствуетилиимеетсятолькоодин*** (Don't Prompt For Client Certificate Selection When No Certificates Or Only One Certificate Exists);
• ***Перетаскивание или копирование и вставка файлов*** (Drag And Drop Or Copy And Paste Files);
• ***Установка элементов рабочего стола*** (Installation Of Desktop Items);
• ***Запускпрограммифайловвокне I FRAME*** (Launching Programs And Files In An I FRAME);
• ***Переходмеждукадрамичерезразныедомены*** (Navigate Subframes Across Different Domains);
• ***Передачанезашифрованныхданныхформ*** (Submit Nonencrypted Form Data);
• ***Устойчивость данных пользователя*** (User Data Persistence);
• ***Активные сценарии*** (Active Scripting);
• ***Разрешить операции вставки из сценария*** (Allow Paste Operations Via Script);
• ***Выполнять сценарии приложений Java*** (Scripting Of Java Applets);

• ***Проверка подлинности пользователя*** (User Authentication Logon).
Также в диалоговом окне ***Параметры безопасности*** (Security Settings) доступен параметр ***Разрешения канала программного обеспечения*** (Software Channel Permissions), который может принимать следующие значения:
• ***Низкий уровень безопасности*** (Low Safety). Позволяет программному обеспечению из канала программного обеспечения автоматически загружаться и устанавливаться без уведомления пользователя.
• ***Средний уровень безопасности*** (Medium Safety). Позволяет программному обеспечению из канала программного обеспечения автоматически загружаться без уведомления пользователя, но не разрешает автоматическую установку.
• ***Высокий уровень безопасности*** (High Safety). Разрешает уведомление пользователя, но не разрешает автоматическую загрузку и установку программного обеспечения из канала программного обеспечения.
Вкладка ***Конфиденциальность*** *(Privacy)*
Вкладка Конфиденциальность (Privacy) позволяет определить параметры сохранения на вашем компьютере файлов «cookie» для всех Web-сайтов заданной зоны Интернета. Доступные параметры описаны в таблице 6.4.

Параметры на вкладке Конфиденциальность (Privacy). Таблица 6.4

Параметр	Описание
Блокировать все «cookies» (Block All Cookies)	Блокируются файлы «cookie» от всех Web-сайтов. Существующие на вашем компьютере файлы «cookie» становятся недоступны для Web-сайтов
Высокий (High)	Блокируются все файлы «cookie», не соответствующие политике конфиденциальности, и те, которые используют вашу личную информацию без вашего явного согласия
Умеренно высокий (Medium High)	Блокируются все сторонние файлы «cookie», не соответствующие политике конфиденциальности, и те, которые используют вашу личную информацию без вашего явного согласия
Средний (Medium)	Блокируются все сторонние файлы «cookie», не соответствующие политике конфиденциальности, и те, которые используют вашу личную информацию без вашего явного согласия. Ограничиваются основные файлы «cookie», использующие личную информацию без вашего явного согласия
Низкий (Low)	Ограничиваются все сторонние файлы «cookie», не соответствующие политике конфиденциальности, и те, которые используют вашу личную информацию без вашего явного согласия
Принимать все «cookie» (Accept All Cookies)	На компьютере сохраняются любые файлы «cookie». Все существующие файлы «cookie» доступны для создавших их Web-сайтов

Вкладка Содержание (Content) обеспечивает доступ к компоненту ***Управление содержанием*** (Content Advisor), позволяющему контролировать, какая информация будет вам доступна в Интернете. Это полезное инструментальное средство для родителей, желающих защитить своих детей от посещения областей Интернета, предназначенных только для взрослых. Вы можете контролировать доступ, основываясь на наличии ненормативной лексики, насилия, обнаженной натуры и сексуальных сцен. Также можно создать список Web-сайтов, которые будут всегда доступны для просмотра, либо никогда не будут доступны для просмотра независимо от их содержания.

Примечание Вкладка ***Подключения*** (Connections) поможет установить подключение к Интернету, а вкладка ***Программы*** (Programs) — определить, какие программы Windows XP Professional автоматически использует для каждой из служб Интернета.

Вкладка Дополнительно (Advanced) позволяет выполнить точную настройку специальных возможностей, параметров просмотра, параметров настройки протокола HTTP 1.1, мультимедийных функций и системы безопасности. Группа параметров ***Специальные возможности*** (Accessibility) включает два флажка:
• ***Всегда расширять текст для изображений*** (Always Expand ALT Text For Images). Определяет, необходимо ли расширять окно изображения по размеру альтернативного текста, когда флажок ***Отображать рисунки*** (Show Pictures) снят.
• ***Перемещать системную каретку вслед за фокусом и выделением*** (Move System Caret With Focus/Selection Changes). Указывает на необходимость перемещения системной каретки в случае изменения фокуса или выделения. Некоторые специальные возможности, такие как функция чтения экрана или экранная лупа, используют системную каретку, чтобы определить, какая часть экрана должна быть прочитана или увеличена.
В группу *Обзор* (Browsing) входит много параметров, управляющих обзором Интернета, включая следующие:
• ***Всегда отправлять URL-адреса как UTF-8*** (Always Send URLs As UTF-8). Задает использование стандарта UTF-8, определяющего символы, которые будут читаемыми в любом языке. Это позволяет вам обмениваться адресами Интернета (URL), содержащими символы других алфавитов. Параметр установлен по умолчанию;
• ***Включить вид папки для FTP-сайтов*** (Enable Folder View For FTP Sites). Разрешает отображать содержимое FTP-сайтов в виде папок. Эта функция может не работать при использовании некоторых видов подключений через прокси-сервер. Если вы снимете этот флажок, содержимое FTP-сайтов будет отображаться в виде HTML-страницы. Параметр установлен по умолчанию;
• ***Включить установку по запросу (прочие компоненты)*** (Enable Install On Demand (Other). Разрешает автоматическую загрузку и установку Web-компонентов, необходимых для правильного отображения Web-страницы или выполнения определенных задач. Параметр установлен по умолчанию.
Параметры в группе Настройка HTTP 1.1 (HTTP 1.1) определяют, в каких случаях вы хотите использовать протокол HTTP 1.1. Многие Web-сайты все еще используют протокол HTTP 1.0, таким образом, если у вас возникают трудности при подключении к некоторым Web-сайтам, вы можете отказаться от

использования протокола HTTP 1.1.
Раздел *Мультимедиа* (Multimedia) содержит много параметров, включая следующие:
• ***Воспроизводить анимацию на Web-страницах*** (Play Animations In Web Pages). Параметр определяет, будет ли воспроизводиться анимация на показываемой Web-странице. Страницы, содержщие анимацию, могут загружаться очень медленно. Чтобы ускорить отображение таких страниц, снимите этот флажок. Анимационные ролики можно воспроизводить даже при снятом флажке, щелкнув правой кнопкой мыши значок, отображаемый вместо анимации, а затем щелкнув пункт ***Показать изображение*** (Show Picture) в контекстом меню. Параметр установлен по умолчанию;
• ***Воспроизводить звуки на Web-страницах*** (Play Sounds In Web Pages). Определяет, будет ли при просмотре страниц воспроизводиться музыка и другие звуки. Некоторые страницы, содержащие звуковое оформление, загружаются очень медленно. Снимите этот флажок, чтобы ускорить загрузку таких страниц. Если на вашем компьютере установлен компонент RealNetworks RealAudio или воспроизводится видеоклип, звук будет воспроизводиться даже при снятом флажке. Параметр установлен по умолчанию;
• ***Отображать рисунки*** (Show Pictures). Определяет, будут ли выводиться графические изображения при выводе страницы. Страницы, содержащие много графических изображений, могут загружаться очень медленно. Снимите флажок для ускорения загрузки таких страниц. Отдельные изображения можно просматривать, даже если флажок снят, щелкнув правой кнопкой мыши значок, выводимый вместо изображения, а затем щелкнув пункт меню ***Показать рисунок*** (Show Picture). Параметр установлен по умолчанию. Раздел параметров***Печать*** (Printing) устанавливает печать цветов фона и фоновых изображений.
Группа параметров ***Безопасность*** (Security) (рис. 6.9) позволяет произвести точную настройку системы безопасности.
Раздел ***Безопасность*** (Security) предоставляет доступ к ряду параметров и включает флажки, описанные далее.
• ***Удалять все файлы из папки временных файлов Интернета при закрытии обозревателя*** (Empty Temporary Internet Files Folder When Browser Is Closed). Определяет необходимость удаления всех файлов из папки ***Временные файлы Интернета*** (Internet Temporary Files) при закрытии браузера. По умолчанию флажок снят.
• **SSL 2.0 (Use SSL 2.0).** Контролирует возможность передачи и приема защищенной информации через протокол Secure Sockets Layer Level 2 (SSL 2.0), стандартный протокол защиты данных. Все Web-сайты поддерживают этот протокол. Параметр установлен по умолчанию.
• **SSL 3.0 (Use SSL 3.0).** Определяет необходимость использования для передачи и приема информации протокола Secure Sockets Layer Level 3 (SSL 3.0), обеспечивающего более высокий уровень безопасности, чем SSL 2.O. Некоторые Web-сайты не поддерживают протокол SSL 3.0. Параметр устанавливается по умолчанию.
• ***Предупреждать о недействительных сертификатах узлов*** (Warn About Invalid Site Certificates). Определяет, должен ли Internet Explorer предупреждать

вас, если URL-адрес сертификата безопасности Web-сайта неверен. Параметр установлен по умолчанию.

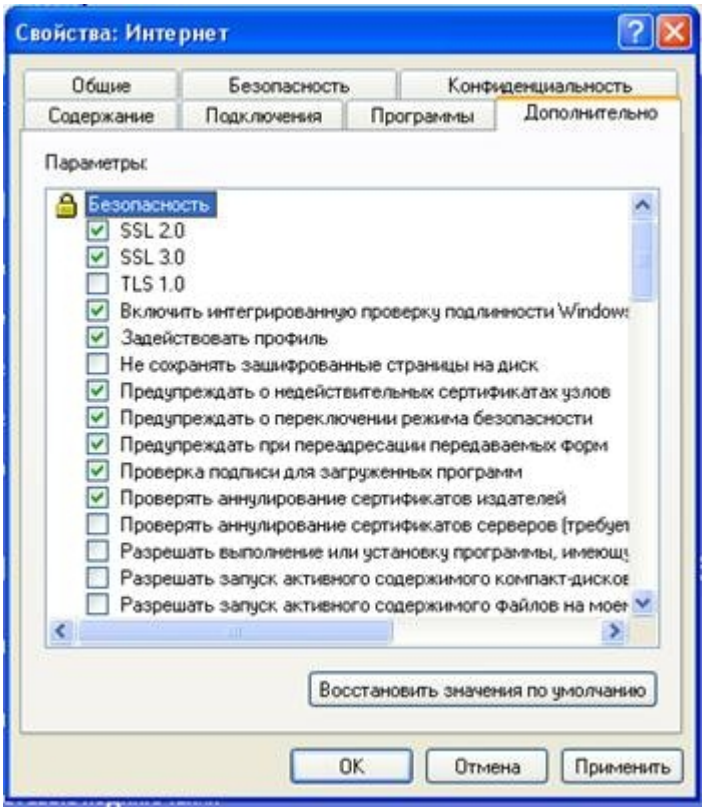

Рис. 6.9. Вкладка Дополнительно (Advanced) диалогового окна Свойства: Интернет (Internet Properties)

• ***Предупреждатьопереключениирежимабезопасности*** (Warn If Changing Between Secure And Not Secure Mode). Определяет, должен ли Internet Explorer выводить предупреждение при переходе между сайтами, использующими безопасное подключение, и обычными сайтами.

Примечание Для получения информации о назначении других флажков, расположенных на вкладке***Дополнительно*** (Advanced) диалогового окна ***Свойства: Интернет*** (Internet Properties), щелкните кнопку с изображением знака вопроса в правом верхнем углу диалогового окна, а затем выберите требуемый флажок.

5. УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ОТЧЕТА.

Отчет должен содержать:

- название работы;
- цель работы;
- назначение и функциональные возможности программы;
- порядок действий по выполнению лабораторной работы;
- устанавливаемые в процессе работы параметры;
- выводы по результатам проделанной работы.

6. КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ВЫПОЛНЕННОЙ РАБОТЕ.

- Что такое ICF?
- По умолчанию файл журнала безопасности ICF называется _____и имеет максимальный размер_____.
- Как включить для настройки Брандмауэр подключения к Интернету?
- Для чего нужны исключения?
- Как добавить программу если программа или служба, которую требуется разрешить, отсутствует в списке?
- Что нужно сделать для изменения параметров сетевого подключения?
- Какие параметры можно настроить?
- Какие параметры позволяет настраивать вкладка Ведение журнала безопасности?
- Как включить журнал безопасности?
- Как получить доступ к настройке параметров безопасности и конфиденциальности подключения к Интернету?
- Как удалить временные файлы Интернета
- Как влияет на безопасность личной информации время хранения ссылок на посещенные вами страницы?
- Как разделить Web-сайты на зоны для настройки параметров безопасности?
- Какие параметры безопасности можно настроить для каждой из этих зон?
- Какие параметры позволяет устанавливать вкладка Конфиденциальность?
- Какие параметры позволяет устанавливать вкладка Содержание?
- Какие возможности дают изменения параметров раздела Мультимедиа?
- Что позволяет произвести группа параметров Безопасность?