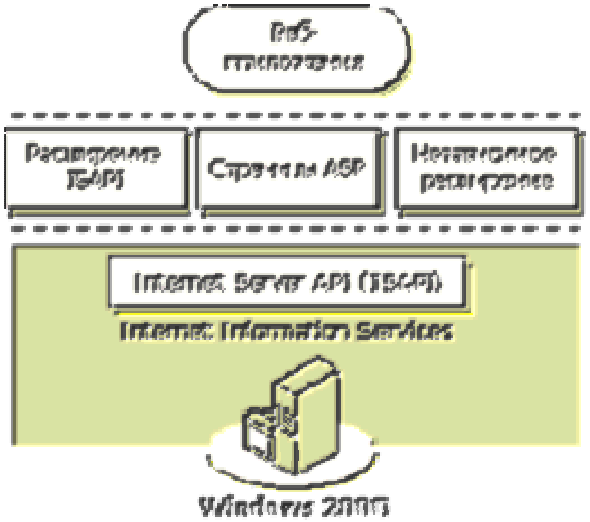
**В.К. Толстых**

УЧЕБНОЕ ПОСОБИЕ

# Администрирование сервера IIS 5




Донецк, ДонНУ 2004

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ

В.К. Толстых

УЧЕБНОЕ ПОСОБИЕ

# Администрирование сервера IIS 5

для студентов инженерных и математических специальностей

ИЗДАНИЕ ПЕРОВОЕ

Донецк, ДонНУ 2004

ББК 32 97
Т58
УДК 681.325.5

**Толстых В.К.**
Т58 Администрирование сервера IIS 5: учебное пособие – Донецк: ДонНУ, 2004. – 54 с.: ил.

Описывается архитектура сервера IIS 5 в составе Windows XP Professional, администрирование узлов Web и FTP, конфигурирование приложений, обеспечение защиты IIS, разрешения Web-сервера и NTFS, аутентификация.

Учебное пособие составлено на основе курса, читаемого на кафедре компьютерных технологий физического факультета Донецкого национального университета по специальности 8.080404 „Интеллектуальные системы принятия решений”.

Пособие предназначено для администраторов и программистов в области Internet-технологий.

Рецензент зав. кафедрой компьютерных технологий ДонНУ
д.т.н., проф. А.А. Каргин



странице, и затем выполняет их. Наиболее часто используемая директива SSI вставляет, или *включает*, содержимое файла в веб-страницу. Например, если на веб-странице требуется неоднократно обновлять рекламное объявление, можно использовать SSI для включения исходного HTML-текста объявления в веб-страницу. Чтобы обновить рекламу, требуется только изменить файл, содержащий исходный текст объявления. Чтобы использовать SSI, нет необходимости знать язык сценариев, достаточно придерживаться правильного синтаксиса директив.

Например, директива **#include** дает веб-серверу команду вставить содержимое файла в веб-страницу. Директивы нужно заключать в теги комментариев HTML:

```
<!-- #include file="myfile.html" -->
<!-- Включаемый файл находится в виртуальном
каталоге Scripts: -->
<!-- #include
virtual="/scripts/tools/global.html" -->
```

Директива **#exec** выполняет указанное приложение или команду оболочки и отправляет ее результаты в обозреватель клиента:

```
<!-- #exec
CGI="/testfolder/test.asp?test=Привет" -->
```

Файл, содержащий включения **#include** должен иметь расширения *.asp, *.inc, *.stm, *.shtm или *.shtml. Web-сервер по умолчанию производит разбор директив только в файлах указанных типов.

Чтобы перенаправить запросы на другой каталог или веб-узел

1. В оснастке IIS выберите веб-узел или каталог и откройте его окно свойств.
2. Выберите вкладку **Домашний каталог**, **Виртуальный каталог** или **Каталог**.
3. Выберите параметр **постоянный адрес URL**.
4. В поле **Адрес** введите адрес URL каталога назначения или веб-узла. Например, чтобы перенаправить все запросы на файлы в каталоге /Catalog на каталог /NewCatalog, введите **/NewCatalog**.

Чтобы перенаправить все запросы на один файл

1. В оснастке IIS выберите веб-узел или каталог и откройте окно его свойств.
2. Выберите вкладку **Домашний каталог**, **Виртуальный каталог** или **Каталог**.
3. Выберите параметр **постоянный адрес URL**.
4. В поле **Адрес** введите адрес URL файла назначения.
5. Установите флажок **на введенный выше адрес URL**, чтобы исключить добавление веб-сервером исходного имени файла к адресу назначения URL.

## Другие полезные средства

Часто бывает полезно динамически изменить содержимое после того, как оно было запрошено, но перед передачей его в обозреватель. IIS включает две возможности, обеспечивающие эти функции: включения на стороне сервера (SSI) и среда создания сценариев ASP.

С помощью SSI можно выполнить все множество задач управления веб-узлом, от добавления динамических штампов времени до запуска специальных команд при запросе файла. Команды SSI, называемые *директивами*, добавляются к веб-странице на этапе разработки. Когда страница запрашивается, веб-сервер производит разбор всех директив, найденных на веб-



# Содержание

файлы в домашний каталог узла. Если имеется сложный узел или требуется указать другие адреса URL для различных частей узла, следует добавить необходимые виртуальные каталоги через оснастку IIS:

1. В оснастке IIS выберите веб- или FTP-узел, к которому требуется добавить каталог.
2. В меню Действие укажите на команду Создать и выберите Виртуальный каталог.
3. Используйте окно Мастер создания виртуального каталога для выполнения этой задачи.

Если используется файловая система NTFS, виртуальный каталог также может быть создан следующим образом: щелкните правой кнопкой каталог в проводнике Windows, выберите команду Общий доступ и безопасность и откройте вкладку Доступ через веб.

## Документы каталога

Закладка Документы в свойствах каталога используется для определения используемой по умолчанию веб-страницы каталога и добавления примечаний к документам каталога.

## Изменение маршрутов запросов перенаправлением

Когда веб-обозреватель запрашивает страницу на веб-узле, веб-сервер обнаруживает страницу по адресу URL и возвращает ее в веб-обозреватель. При перемещении страницы на веб-узле не всегда удается исправить все ссылки на старый адрес URL. Для того чтобы веб-обозреватели могли находить страницу в ее новом положении, следует обеспечить предоставление веб-сервером нового адреса URL для веб-обозревателя. После этого веб-обозреватель использует новый адрес URL для повторного запроса страницы. Этот процесс называют «перенаправлением запроса веб-обозревателя» или «перенаправлением URL».

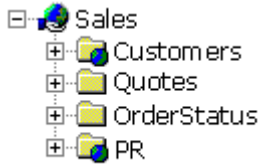
## Что такое виртуальный каталог?

Для публикации из любого каталога, не содержащегося в домашнем каталоге, следует создать виртуальный каталог. *Виртуальным каталогом* называют каталог, который физически не содержится в домашнем каталоге, но выводится в клиентских веб-обозревателях как его подкаталог.

Виртуальный каталог имеет *псевдоним*, т.е. имя, которое веб-обозреватели используют для доступа к этому каталогу. Поскольку псевдоним обычно оказывается более коротким, чем полное имя каталога, пользователям легче его запоминать и вводить. Применение псевдонимов является также более безопасным. Пользователи не знают, где ваши файлы физически размещаются на сервере, и не могут использовать эту информацию для изменения файлов. Псевдонимы также упрощают перемещение файлов в узле. Вместо того чтобы изменять адрес URL для каталога, достаточно изменить сопоставление псевдонима и физического адреса каталога.

Например, настраивается веб-узел группы маркетинга в интрасети компании. В приведенной ниже таблице показано соответствие физического расположения файлов и адресов URL для доступа к ним.

И виртуальные каталоги, и физические каталоги (каталоги без псевдонима) будут отображаться в оснастке IIS. Виртуальный каталог представляется значком папки с глобусом в углу. На следующем рисунке изображен веб-узел, описанный в примере выше. Каталоги /Customers и /PR являются виртуальными каталогами.




Для простого веб-узла добавление виртуальных каталогов может оказаться излишним. Достаточно просто поместить все



# Введение

Internet Information Services (IIS) является составной частью архитектуры Microsoft для Web-приложений. Роль IIS состоит в связывании клиентов, обращающихся к системе через протокол HTTP, с другими службами Windows.

Напоминаем, что IIS доступен в клиентской ОС Windows XP Professional после установки соответствующих компонент Windows. При стандартной установке Windows XP Professional сервер IIS не доступен.

# Терминология

**архитектура DNA**
Distributed interNet Application Architecture. Архитектура Microsoft для веб-приложений.

**архитектура клиент/сервер**
Модель компьютерной сети, в которой клиентские приложения, выполняющиеся на рабочих станциях или персональных компьютерах, получают доступ к информации на удаленных серверах или главных компьютерах. Клиентская часть приложения обычно оптимизируется для удобства взаимодействия с пользователем, тогда как серверная часть поддерживает централизованную многопользовательскую функциональность.

**веб-приложение**
Программное обеспечение, использующее HTTP как основной протокол связи и доставляющее информацию из Интернета пользователю на языке HTML. Такие приложения называют также основанными на вебе.

**веб-сервер**
В общем смысле, компьютер с программным обеспечением сервера, использующий протоколы Интернета, такие как HTTP и FTP, для ответов на запросы веб-клиентов по сети TCP/IP.

**веб-страница**
Веб-документ. Веб-страница обычно состоит из HTML-файла и связанными с ним файлами рисунков и сценариев, которые находятся в определенном каталоге на конкретном компьютере (и таким образом, определяются адресом URL).

**виртуальный каталог**
Используемое в адресе имя каталога, соответствующее физическому каталогу на сервере. Такое сопоставление иногда называют сопоставлением URL.

**виртуальный сервер**
Используется также термин «веб-узел». Виртуальный компьютер, находящийся на сервере HTTP, но выглядящий для пользователя как отдельный сервер HTTP. На одном компьютере могут размещаться несколько виртуальных серверов, каждый из которых способен выполнять собственные программы и самостоятельно осуществлять доступ к входным и периферийным устройствам. Каждый виртуальный сервер имеет собственное имя домена и IP-адрес и выглядит для пользователя как отдельный веб-узел или FTP-узел. Некоторые поставщики услуг Интернета предоставляют виртуальные серверы клиентам, которые хотят использовать собственные имена доменов.

**интерфейс ISAPI**
Internet Server Application Programming Interface. Этот интерфейс программирования приложений Интернета размещается на сервере и предназначен для запуска программных служб, настроенных для работы с операционной системой Microsoft Windows. Интерфейс предназначен для разработки



стандартный домашний каталог C:\Inetpub\Wwwroot. Для FTP-узла следует скопировать файлы в каталог C:\Inetpub\Ftproot. Пользователи интрасети могут получить доступ к этим файлам, указав следующий адрес URL: http://*имя_сервера/имя_файла*.

## Указание домашних каталогов

Каждый веб- или FTP-узел должен иметь один домашний каталог. *Домашний каталог* является центральным расположением публикуемых страниц. Этот каталог содержит домашнюю страницу или файл указателя с приветствием посетителям и ссылками на другие страницы веб-узла. Домашний каталог сопоставляется с именем домена узла или именем сервера. Например, если узел имеет в Интернете имя домена www.microsoft.com и домашний каталог C:\Website\Microsoft, то веб-обозреватели будут использовать адрес URL http://www.microsoft.com/ для доступа к файлам в этом домашнем каталоге. В интрасети, в которой имеется сервер с именем AcctServer, веб-обозреватели будут использовать для доступа к файлам в домашнем каталоге адрес URL http://acctserver.

Стандартный домашний каталог создается при установке Internet Information Services и при создании нового веб-узла. Имеется возможность изменить домашний каталог:

1. В оснастке IIS выберите веб- или FTP-узел и откройте его окно свойств.
2. Выберите вкладку Домашний каталог и укажите, где расположен домашний каталог. Допускается выбор следующих параметров:
3. каталог данного компьютера;
4. общая папка другого компьютера;
5. постоянный адрес URL. Обозреватели, запрашивающие этот адрес URL, будут отправляться на другой адрес URL. Невозможно задать переадресацию для каталога FTP.
6. Введите в поле локальный путь, имя общего ресурса или адрес URL вашего каталога.

сертификатов также осуществляется агентством по выдаче сертификатов. Клиентский сертификат и общий ключ поддерживаются сервером, выступающим в роли *ключевой пары*, обеспечивающей защищенные коммуникации. Клиенты могут и не иметь клиентские сертификаты. При этом на сервере необходимо настроить разрешение на их игнорирование их сертификатов в свойствах узла: Безопасность каталога => Безопасные подключения => Изменить (доступно при установленном сертификате) => Игнорировать клиентские сертификаты.

Для использования SSL потребуется на сервере IIS установить серверный сертификат. Эти сертификаты можно получить в агентстве по выдаче сертификатов, таком как Verisign. На Web-узле фирмы Microsoft по адресу http://backoffice.microsoft.com/securitypartners можно найти список провайдеров сертификатов, отсортированных по именам и названиям их продуктов.

Если сертификат уже установлен на сервере, потребуется выполнить его настройку. На Web-узле может быть установлен только один сертификат.

## Об управлении веб-узлом

Первым делом при установке веб-узла необходимо указать, в каких каталогах будут содержаться публикуемые документы. Веб-сервер не сможет публиковать документы, не находящиеся в указанных каталогах. Поэтому при формировании веб-узла следует сначала определить, как файлы будут организованы. После этого с помощью оснастки IIS следует указать, какие каталоги являются частью узла.

Если веб-узел состоит только из файлов, расположенных на одном диске компьютера, на котором выполняется Internet Information Services, можно немедленно приступить к публикации документов без создания специальной структуры каталогов. Для этого достаточно скопировать файлы в



расширений для IIS и других серверов HTTP, поддерживающих интерфейс ISAPI.

**интерфейс общего шлюза (CGI)**
Интерфейс на стороне сервера для запуска программных служб. Спецификация, которая определяет связь между информационными службами (такими как служба HTTP) и ресурсами на сервере, такими как базы данных и другие программы. Например, когда пользователь отправляет форму через веб-обозреватель, служба HTTP выполняет программу (которую часто называют сценарием CGI) и передает введенные пользователем сведения в эту программу через CGI. Программа затем возвращает эти сведения в службу через CGI. Программой CGI может быть любая программа, обрабатывающая операции ввода и вывода согласно стандарту CGI. CGI-приложения всегда выполняются вне процесса.

**интрасеть**
Сеть, предназначенная для обработки информации в учреждении или организации. Обычными задачами таких сетей являются распространение документов, распространение программного обеспечения, доступ к базам данных и обучения. В интрасети обычно используются приложения, относящиеся к Интернету, такие как веб-страницы, веб-обозреватели, узлы FTP, электронная почта, группы новостей и списки рассылки, но при этом они остаются доступными только внутри учреждения или организации.

**компонентная модель объектов (COM)**
Component Object Model. Объектно-ориентированная модель программирования, определяющая взаимодействие объектов внутри одного приложения или между приложениями. В модели COM клиентское программное обеспечение осуществляет доступ к объекту через указатель на интерфейс объекта, т.е. на соответствующий набор функций, которые называют методами.

**кэш**
Специальная подсистема памяти, в которую для ускорения доступа копируются часто используемые данные. В кэш-памяти сохраняется содержимое часто используемых расположений в ОЗУ, а также адреса, в которых сохраняются элементы данных. Когда процессор получает ссылку на адрес в памяти, он проверяет, содержится ли это адрес в кэше. Если да, то данные возвращаются в процессор; если нет, осуществляется обычный доступ к памяти. Кэширование полезно, когда доступ к ОЗУ оказывается медленным по сравнению со скоростью микропроцессора; в этом случае кэш-память работает быстрее, чем основное ОЗУ.

**метабаза**
Структура, в которой сохраняются параметры настройки IIS. Метабаза выполняет некоторые из функций системного реестра, но занимает меньше места на диске.

**обработчик сценариев**
Программа, интерпретирующая и выполняющая сценарии.

**оснастка**
Программа для консоли MMC (Microsoft Management Console), которую администраторы используют для управления сетевыми службами. MMC предоставляет

общую среду для инструментов управления (оснасток); оснастки обеспечивают средства управления, необходимые для администрирования сетевых служб, таких как IIS.

**объекты IIS Admin**
Набор методов, предоставляемых IIS, которые позволяют приложениям получать доступ и изменять настройки конфигурации в метабазе.

**объекты данных ActiveX (ADO)**
Программный интерфейс высшего уровня для доступа к данным, работающий на основе технологии доступа к данным (например, OLE DB), который реализуется с помощью компонентной модели объектов (COM).

**поток**
Основная сущность, на которую операционная система выделяет процессорное время. Поток может выполнять любую часть кода приложения, включая часть, выполняемую в данное время другим потоком. Все потоки процесса используют общее виртуальное адресное пространство, глобальные переменные и ресурсы операционной системы процесса.

**процесс**
В Windows-объект, состоящий из исполняемой программы, набора адресов виртуальной памяти и потока.

**процесс сервера**
Процесс, содержащий компоненты COM. Компонент COM может быть загружен в суррогатный серверный процесс на компьютере клиента (локальном) или на другой компьютер (удаленный). Кроме того, допускается его загрузка в процесс приложения клиента (как внутренний компонент процесса).

**сервер**
Термин, имеющий следующие значения: компьютер в сети, отправляющий файлы на другие компьютеры или выполняющий приложения для других компьютеров в сети; программное обеспечение, выполняющееся на компьютере-сервере, ответственное за обслуживание файлов или выполнение приложений; в объектно-ориентированном программировании — программный блок, по запросу обменивающийся информацией с другим программным блоком.

**сценарий CGI**
Программа, обеспечивающая связь сервера с пользователями в Интернете. Например, когда пользователь вводит данные в форму на веб-странице, сценарий CGI интерпретирует эти данные и передает их в программу базы данных на сервере.

**технология внедрения и связывания объектов (OLE)**
Набор объединяющих стандартов передачи и совместного использования данных в клиентских приложениях. Технология OLE позволяет создавать составные документы, содержащие ссылки на другие приложения. При этом у пользователя нет необходимости переключаться на другие приложения при редактировании связанных объектов. OLE базируется на компонентной модели объектов (COM) и позволяет создавать допускающие многократное использование объекты, способные работать в различных приложениях. Эта техноло-



## Стойкость шифра

Стойкость шифра, используемого при осуществлении защищенных коммуникаций, определяется длиной ключа, заданной в битах. По умолчанию сервер IIS использует 40-битовый ключ шифрования. Можно выбрать 128-битовый ключ шифрования путем установки флажка Require 128-bit encryption (Требуется 128-битовое шифрование) в диалоговом окне Secure Communications.

Из-за экспортных ограничений 128-битовое шифрование доступно только в Канаде и в США. Имейте в виду, что при установке 128-битового шифрования для сервера каждый броузер, подключающийся к такому Web-серверу, нуждается в 128-битовом ключе шифрования. В этом случае доступ к вашему Web-узлу возможен только из США и Канады.

Банковские учреждения могут использовать расширение SSL, известное под названием Server-Gated Cryptography (SGC). Этот метод использует 128-битовое шифрование и может осуществлять откат к 40-битовому шифрованию. Для использования метода SGC необходимо связаться с агентством по выдаче сертификатов и запросить сертификат SGC.

## Сертификаты

При использовании сертификатов для броузера и сервера осуществляется проверка идентичности с помощью цифровой подписи. По существу, имеются два типа сертификатов: серверные и клиентские.

*Серверные сертификаты* размещены на сервере и выполняют три функции. При этом выполняется аутентификация пользователей на сервере, может проверяться содержимое Web либо устанавливаться защищенные коммуникации с использованием SSL или SGC.

*Клиентские сертификаты* размещаются на клиентском компьютере и могут использоваться для осуществления идентификации пользователей на сервере. Выдача клиентских

5. Расскажите всем пользователям, подключающимся к данному Web-узлу, о необходимости использования заголовка https:// вместо http://.


Настройки безопасности каталога



гия широко применяется в деловых приложениях, в которых становится возможным использование в архитектуре клиент/сервер распределенных данных в электронных таблицах, текстовых процессорах, финансовых пакетах и других программах.

**фильтр**
Средство ISAPI в IIS, делающее возможной на отдельном узле предварительную обработку запросов HTTP и обработку полученных ответов.

**фильтр по IP-адресу**
Разрешение или запрет на доступ на основании IP-адреса, с которого предпринимается попытка доступа в веб-обозревателе.

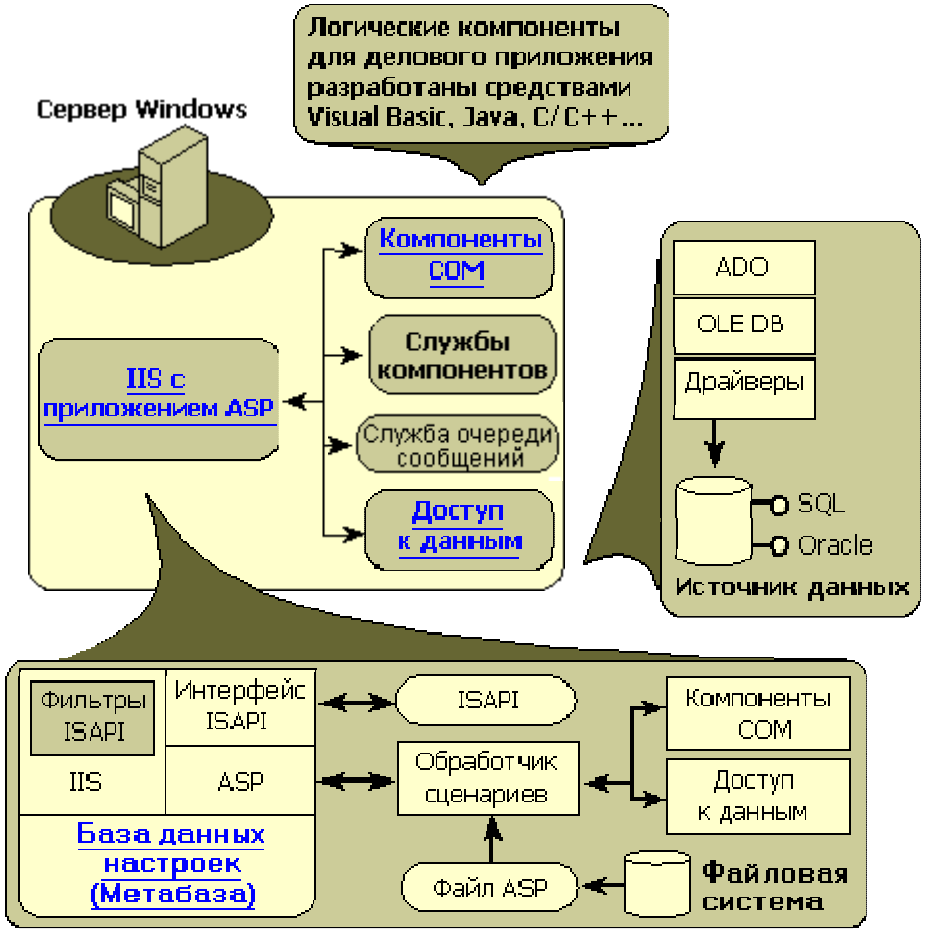
**элементы ActiveX**
Допускающие многократное использование компоненты программного обеспечения, включающие технологию ActiveX. Эти компоненты используются для расширения функциональности, например, для добавления анимацией или всплывающих меню на веб-страницы, в приложения для настольных компьютеров и в средства разработчиков программного обеспечения. Элементы ActiveX программируются на разных языках, в том числе C, C++, Object Pascal, Visual Basic и Java.

**элементы ActiveX разработчика**
Визуальные компоненты разработчика, помогающие создавать динамические веб-приложения путем автоматической генерации стандартных кодов HTML и сценариев. Эти компоненты являются аналогами мастеров. Элементы ActiveX разработчика существуют только во время разработки и не существуют во время выполнения.

**WebDAV (Web Distributed Authoring and Versioning)**
Позволяет авторам, работающим через удаленный доступ, создавать, перемещать или удалять файлы, свойства файлов, каталоги и свойства каталогов на сервере при HTTP-подключении.

# Архитектура Internet Information Services

IIS является составной частью архитектуры Windows DNA. Роль IIS состоит в связывании клиентов, обращающихся к системе через протокол HTTP, с другими службами Windows DNA, например DHTML, ASP и так далее. Кроме того, IIS включает базовый набор возможностей, который может быть расширен разработчиками систем для определения архитектуры настраиваемого приложения.






- **Чтение**. Пользователи могут просматривать содержимое файлов.
- **Запись**. Пользователи могут изменять содержимое файлов.
- **Запись в журнал**. Посещения этого каталога регистрируются в журнале.

# Шифрование

## Активизация шифрования

Активизация шифрования на сервере происходит после того, как клиент выполнит запрос с использованием в качестве заголовка URL броузера https://. Если для сервера не будет подключено шифрование, сеанс не будет его использовать. Для использования шифрования потребуется установить серверный сертификат на сервере.

Для включения шифрования используйте следующую процедуру.

1. **Получите** и **установите** серверный сертификат.
2. Откройте страницу Properties (Свойства) для Web-узла, каталога или файла, который будет защищаться с помощью шифрования.
3. Выберите вкладку Directory Security (Безопасность каталога), затем щелкните на кнопке Edit (Изменить), находящейся в разделе Secure Communications (Безопасные подключения). Если эта кнопка окрашена в серый цвет, значит, сертификат на сервере не установлен.
4. Установите в диалоговом окне Secure Communications флажок Require secure channel (SSL) (Требуется защищенный канал).

## Разрешения NTFS

IIS зависит от разрешений NTFS при обеспечении безопасности отдельных файлов и каталогов от несанкционированного доступа. В отличие от разрешений веб-сервера, которые применяются ко всем пользователям, разрешения NTFS позволяют точно указать, какие пользователи могут получать доступ к содержимому и как эти пользователи могут обрабатывать содержимое.

Уровни разрешений NTFS включают следующие.

- **Полный контроль**. Пользователи могут изменять, добавлять, перемещать и удалять файлы, свойства, связанные с ними, и каталоги. Кроме этого, можно изменить разрешения для всех файлов и подкаталогов.
- **Изменение**. Пользователи могут просматривать и изменять файлы и их свойства, включая удаление и добавление файлов в каталог или свойств файла к файлу.
- **Чтение и выполнение**. Пользователи могут запускать выполняемые файлы, включая сценарии.
- **Список содержимого папки**. Пользователи могут просматривать список содержимого папки.
- **Чтение**. Пользователи могут просматривать файлы и их свойства.
- **Запись**. Пользователи могут записывать файл.
- **Нет доступа**.Когда ни один из флажков не установлен, пользователи не имеют никакого доступа к ресурсу, даже если пользователь имеет доступ к каталогу более высокого уровня.

### Чтобы задать разрешения для содержимого FTP

1. В оснастке IIS выберите FTP-узел, виртуальный каталог или файл и откройте его окно свойств.
2. На вкладке **Домашний каталог**, **Виртуальный каталог** или **Файл** установите или снимите соответствующий флажок.

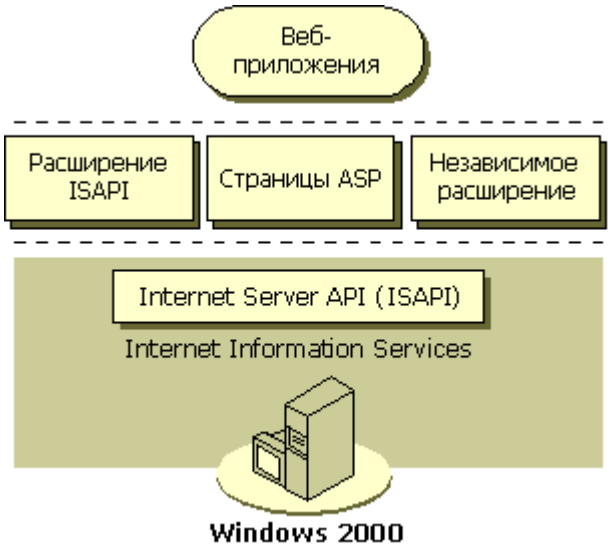


## Основные функциональные возможности IIS

IIS определяет функциональные возможности, которые можно использовать для построения веб-приложений. Основные возможности сервера доступны через интерфейс программирования приложений ISAPI (Internet Server Application Programming Interface). Основные функции, предоставляемые IIS, включают:

- Установление и поддержание HTTP-соединений.
- Чтение HTTP-запросов и запись HTTP-ответов.
- Изменение заголовков HTTP.
- Получение информации о клиентских сертификатах.
- Управление асинхронными соединениями.
- Сопоставление URL физическим путям.
- Управление приложениями и их выполнение.
- Передача файлов.

ASP расширяет основные функциональные возможности, предоставляя связь с архитектурой COM. Аналогично, можно расширить архитектуру IIS, определив настраиваемый набор функций с помощью ISAPI:



## IIS и службы компонентов

IIS и службы компонентов работают вместе для формирования базовой архитектуры для построения веб-приложений. IIS использует функциональные возможности, предоставляемые службами компонентов, для выполнения следующих задач.

- Изолирования приложений в отдельные процессы.
- Управления связью между компонентами COM (включая встроенные объекты ASP).
- Координации обработки транзакций в приложениях ASP, использующих транзакции.

## Обработка запросов IIS

Когда IIS получает HTTP-запрос, он оценивает URL для определения типа содержимого запроса: статическое (HTML) или динамическое (ASP или ISAPI).

**Действия по обработке запроса**

| Запрос | Файлы | Действие |
|---|---|---|
| Страница HTML | *.html | IIS возвращает HTML страницу. |
| Расширение ISAPI | *.dll | IIS загружает динамическую библиотеку ISAPI (если она еще не запущена) и запрос передается расширению. |
| Расширение файла, сопоставленное с определенным расширением ISAPI | *.asp, *php … ⇓ *.dll | IIS загружает файл соответствующей динамической библиотеки и представляет запрос. Расширение asp, например, сопоставлено файлу asp.dll, поэтому все запросы на файлы с расширением asp будут направлены asp.dll. |
| Приложение CGI | *.exe, *.cgi, … | IIS создает новый процесс, обеспечивает строку запроса и другие включаемые параметры с помощью запроса к среде и стандартного дескриптора ввода (STDIN) для процесса. |



## Разрешения веб-сервера

В конфигурации веб-сервера имеется возможность задать *разрешения* для конкретных узлов, каталогов и файлов. Эти разрешения будут действовать для всех пользователей, вне зависимости от имеющихся у них конкретных прав доступа. После включения разрешения «Чтение» все пользователи получат возможность просматривать веб-узел, за исключением случая, когда установлены ограничения файловой системы NTFS на просмотр узла пользователями.

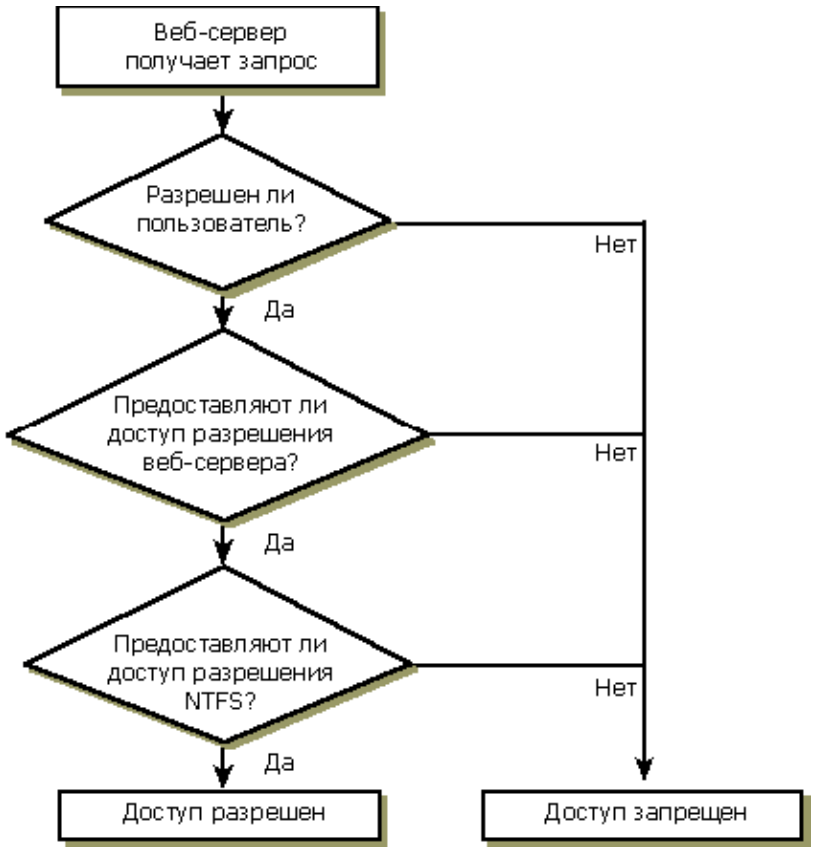
Уровни веб-разрешений включают следующие.

- **Чтение** (выбирается по умолчанию). Пользователи могут просматривать содержимое файла и его свойства.
- **Запись**. Пользователи могут изменять содержимое файла и его свойства через броузер.
- **Доступ к источнику сценария**. Пользователи получают доступ к исходным файлам. Если выбрано разрешение «Чтение», исходный текст может быть прочитан. Если установлено разрешение «Запись», можно производить запись и в исходные тексты. «Доступ к источнику сценария» разрешает доступ к исходным текстам для файлов, например сценариям в приложении ASP. Эта возможность доступна только при установленных разрешениях «Чтение» или «Запись».
- **Обзор каталогов**. Пользователи могут просматривать списки файлов и семейства
- **Запись в журнал**. Запись в журнал делается для каждого посещения веб-узла.
- **Индексация каталога**. Позволяет службе индексации создать индекс для ресурса.

Установки разрешений web-сервера определяют команды HTTP, которые могут быть использованы для узла, виртуального каталога или файла.

пользователь получает сообщение об ошибке «403: Отказ в доступе».

5. Любые модули безопасности от независимых разработчиков, добавленные администратором веб-узла, используются на этом этапе.
6. IIS проверяет разрешения NTFS для ресурса. Если пользователь не имеет разрешений NTFS для ресурса, запрос не выполняется и пользователь получает сообщение об ошибке «403: Отказ в доступе».
7. Если пользователь имеет разрешение NTFS, запрос выполняется.






# Установка дополнительных компонентов

Службы IIS содержат дополнительные компоненты, которые пользователь может включать и отключать в любое время. Ниже приводится описание этих компонентов и их влияние на текущие настройки IIS.

## Общие файлы

Параметр IIS «Общие файлы» выбирается по умолчанию при установке IIS. Для повышения безопасности в среде сервера пользователь имеет возможность отказаться от некоторых общих файлов (снять соответствующие флажки). Однако если отключить параметр «Общие файлы», все общие файлы становятся не выбранными и IIS не будет установлен на компьютер. Таким образом, для установки IIS на компьютере следует оставить этот флажок установленным. Если требуется ограничить службы и компоненты, устанавливаемые с IIS, снимайте флажки отдельных компонентов, перечисленных под компонентом «Общие файлы».

## Документация

Параметр «Документация» выбирается по умолчанию при установке IIS. Электронная документация IIS содержит полные руководства «Приступая к работе», «Администрирование» и «Руководство по Active Server Pages», в каждом из которых обсуждаются основные понятия, помогающие понимать различные возможности, средства и параметры администрирования IIS. Документация также включает пошаговое описание процедур, помогающее выполнять администрирование и наблюдение, а также повышать производительность веб-сервера IIS.

После установки этого дополнительного компонента достаточно для просмотра электронной документации IIS ввести

http://localhost/iisHelp/ в адресную строку обозревателя и нажать клавишу ENTER.

## FTP-сервер

Протокол FTP (File Transfer Protocol, отключен по умолчанию) используется для копирования файлов с и на удаленный сетевой компьютер с использованием одного из протоколов пакета TCP/IP, например протокола IP. Кроме того, протокол FTP позволяет пользователям использовать команды FTP для работы с файлами, например, для создания списка файлов и каталогов на удаленном компьютере. Для IIS включение FTP означает, что появляется возможность передавать файлы через веб-обозреватель.

## Серверные расширения FrontPage

Серверные расширения FrontPage обеспечивают просмотр и управление веб-узлами в графическом интерфейсе с использованием FrontPage в качестве среды разработки. FrontPage позволяет быстро создавать веб-узлы на сервере, а также создавать, изменять и отправлять веб-страницы в IIS с удаленного компьютера. Когда пользователь создает собственный веб-узел, FrontPage держит открытым подключение к IIS, сохраняет и изменяет веб-файлы, что дает возможность просматривать собственный узел. Если отказаться от установки серверных расширений FrontPage, придется выполнять копирование всего содержимого веб-узла вручную, задавать настройки и в некоторых случаях вручную регистрировать приложения, уже зарегистрированные в FrontPage.

## Оснастка IIS в консоли MMC

Диспетчер служб Интернета называется «оснастка Internet Information Services». Оснастка IIS представляет графический интерфейс пользователя для администрирования собственного веб-узла. Оснастка IIS в консоли MMC (Microsoft Management



Для входа всех пользователей на web-сервер по умолчанию используется анонимная учетная запись. При установке сервера создается специальная учетная запись анонимного пользователя (Гостевая учетная запись Интернета – Встроенная запись для анонимного доступа к IIS) с именем IUSR_имяКомпьютера. Например, для компьютера с именем TOLSTYKH учетная запись анонимного пользователя получит имя **IUSR_TOLSTYKH**. Каждый web-узел на сервере может использовать для входа анонимных пользователей либо одну и ту же, либо разные учетные записи. С помощью оснастки Windows «Локальные пользователи и группы» можно создать учетную запись для «анонимного входа».

Например, учетная запись для запуска процессов IIS – это **IWAM_TOLSTYKH**.

## Как работает управление доступом

Для того чтобы управлять доступом пользователей к содержимому web-сервера, следует задать правильную конфигурацию средств безопасности Windows и web-сервера. Когда пользователь пытается получить доступ к web-серверу, сервер выполняет ряд операций по проверке пользователя и определению разрешенного уровня доступа.

Ниже приведена структура процесса:

1. Клиент запрашивает ресурс на сервере.
2. Сервер, если его конфигурация предполагает это, запросит у клиента сведения для проверки подлинности. Обозреватель или предложит пользователю ввести имя пользователя и пароль, или передаст эти сведения автоматически.
3. IIS проверяет допустимость учетной записи пользователя. Если пользователь не имеет соответствующих разрешений, запрос не выполняется и пользователь получает сообщение об ошибке «403: Отказ в доступе».
4. IIS проверяет наличие у пользователя веб-разрешений для запрашиваемого ресурса. Если пользователь не имеет соответствующих разрешений, запрос не выполняется и

Сервер FTP может использовать методы аутентификации Anonymous и Basic, рассмотренные ранее. С сервером FTP связано одно обстоятельство: если установлен метод доступа Anonymous и тип аутентификации Basic, сервер предпримет попытку первым использовать метод Anonymous. Учитывайте этот момент при установке системы защиты для сервера FTP!

## Задание разрешений веб и FTP

Важно понимать различие между разрешениями web или FTP и разрешениями NTFS. Разрешения NTFS применяются к конкретным пользователям или группам пользователей, для которых существуют действительные учетные записи Windows. NTFS управляет доступом к физическим каталогам на сервере.

В отличие от разрешений NTFS, разрешения веб и FTP действуют для всех пользователей, получающих доступ к веб- и FTP-узлам. Разрешения web и FTP управляют доступом к виртуальным каталогам на узле веб или FTP.

Разрешения на доступ к узлам веб и FTP по умолчанию используют учетную запись Windows IUSR_*ИмяКомпьютера*. Эта учетная запись применяется, когда пользователи осуществляют доступ к узлу с использованием анонимной проверки подлинности. По умолчанию учетная запись IUSR_*ИмяКомпьютера* получает от IIS разрешения NTFS на физические каталоги, включающие узел web или FTP. Вы можете, однако, изменить эти разрешения для любого каталога или файла на вашем узле. Например, имеется возможность с помощью web-разрешений указать, разрешается ли посетителям web-узла просматривать определенную страницу, загружать данные или выполнять сценарии на узле.

## Анонимный доступ

Анонимный доступ, который является наиболее широко используемым методом доступа к web-узлам, позволяет любому пользователю посетить общие области на web-узле.



Console) означает, что приложение присоединяется к программе MMC и отображается в окне MMC так же, как и другие средства администрирования в консоли MMC. Имеется возможность управлять сервером без оснастки IIS, но при этом для создания веб-узлов, приложений, виртуальных каталогов и настроек безопасности приходится писать сценарии типа inetpub\adminscripts\adsutil.vbs или собственные сценарии, вызывающие интерфейсы API IIS. Оснастка IIS является необходимой для службы и службы FTP.

## SMTP

Протокол SMTP (Simple Mail Transfer Protocol, отключен по умолчанию) можно использовать для установки почтовых служб интрасети, работающих вместе с IIS. Протокол SMTP является протоколом TCP/IP для отправки сообщений по сети с одного компьютера на другой. Если протокол SMTP установлен, то для просмотра документации по продукту достаточно ввести file:\\%systemroot%\help\mail.chm в адресную строку обозревателя и нажать клавишу ENTER.

## Веб-сервер

Обеспечивает страницы в Интернете и на веб-узлах. Этот компонент является обязательным для выполнения основной службы IIS. Снятие этого флажка приведет к отключению Internet Information Services. Веб-сервер включает следующие виртуальные каталоги.

### Виртуальный каталог MSADC

Этот каталог содержит объекты доступа к данным ADO (ActiveX Data Objects), которые включаются в веб-страницы для доступа к данным на стороне клиента. Эти файлы не требуются для доступа к объектам ADO из страниц ASP на стороне сервера (Active Server Pages). Этот каталог также называют службой удаленных данных MSRDS (Microsoft Remote Data Service).

### Виртуальный каталог принтеров

Windows XP динамически обновляет список всех принтеров на сервере на легко доступном веб-узле (http://localhost/printers/). Возможно отслеживание принтеров этого узла и выполнения их заданий печати. К принтерам также можно подключиться через этот узел с любого компьютера с Windows.

### Виртуальный каталог сценариев

Этот каталог является центральным местом хранения сценариев.

### Виртуальный каталог Интернет-подключения к удаленному рабочему столу служб терминала

Службы терминалов является средством Windows XP, обеспечивающим совместное использование рабочего стола на другом компьютере (удаленны рабочий стол) или множественное управление приложениями (сервер терминалов). Удаленный рабочий стол служб терминалов (включается по умолчанию в Windows XP) обеспечивает удаленное администрирование служб Windows XP, таких как IIS, аналогичное работе через консоль сервера. Службы терминалов не требуют установки консоли MMC (Microsoft Management Console) или оснастки IIS на удаленном компьютере.

Клиентское программное обеспечение служб терминалов доступно для старых компьютеров типа ПК и не ПК (таких как рабочие станции UNIX). (Для клиентских компьютеров, не использующих Windows, требуется программное обеспечение независимых изготовителей.) Встроенное программное обеспечение подключения к удаленному рабочему столу в Windows XP обеспечивает подключения по локальной сети, по протоколу PPTP или через удаленный доступ).

Интернет-подключение к удаленному рабочему столу обеспечивает элемент управления и страницы примеров для



Сервер IIS использует пять типов аутентификации.

• **Anonymous (Анонимный).** Этот основной тип аутентификации используется большинством Web-узлов, а также некоторыми каталогами FTP-серверов. При этом пользователям не требуется указывать комбинации из имен пользователей и паролей за исключением случаев применения FTP. В последнем случае в качестве имени пользователя применяется слово anonymous, а в качестве пароля указывается электронный адрес пользователя.

• **Basic Authentication (Базовая аутентификация).** Применяется комбинация имени пользователя и пароля для выполнения аутентификации пользователей. Однако при использовании этого метода проявляется один недостаток: пароль передается по сети в виде обычного текста. Такого рода пароли можно легко перехватить, а затем применить для получения доступа к ресурсам, защищенным данным паролем.

• **Digest Authentication (Справочная аутентификация).** Это свойство появилось в IIS 5.0 и предлагает различные возможности для выполнения аутентификации. При использовании этого вида аутентификации удостоверения пользователя передаются с помощью одностороннего процесса хеширования. Этот процесс необратим и никогда не повторяется.

• **Integrated Windows Authentication (Интегрированная аутентификация Windows).** Этот метод известен как метод NTLM (метод Windows Challenge/Response—Windows Вызов/Отклик).

• **Certificate Authentication (Сертификатная аутентификация).** Этот метод применяет протокол Secure Sockets Layer (SSL) для аутентификации при использовании сертификатов клиентами и сервером. Клиентские сертификаты применяются для обработки запросов со стороны клиентских броузеров, в то время как серверные сертификаты могут применяться для установки защищенного способа передачи информации в сети с помощью шифрования.

| | |
|---|---|
| | наиболее ограничительные права доступа |
| Ограничение IP-адресов | Проверьте, что при выполнении удаленного администрирования или удаленного доступа имеются только корректные IP-адреса |
| Обеспечение физической защиты | Проверьте, что для сервера обеспечена физическая защита либо установлены хранители экрана, защищенные паролями |
| Учетная запись администратора | Переименуйте учетную запись администратора, что позволит избежать ее использование хакерами |

Приведенная таблица — хорошее руководство, используемое при установке системы защиты. На практике применяются дополнительные меры защиты, а некоторые пункты таблицы могут не использоваться.

## Аутентификация

Аутентификация применяется в том случае, когда требуется проверить, что пользователи или клиенты сервера являются теми, за кого себя выдают. Эта проверка осуществляется при использовании комбинации имени пользователя и пароля. В будущем могут появиться другие методы аутентификации, например распознавание голоса, либо при обеспечении доступа к серверу — биометрические методы. Таким образом, доступ к серверу возможен только по завершении процесса аутентификации.

При работе с IIS можно определить выполнение аутентификации на уровне Web-узла, каталога или файла. Таким образом, можно устанавливать доступ к общедоступному разделу Web-узла, а затем требовать выполнения аутентификации для специфических каталогов либо файлов, содержащих важную информацию.



развертывания клиентских подключений служб терминалов через Интернет. Когда Интернет-подключение к удаленному рабочему столу развертывается на веб-сервере, клиентские компьютеры могут установить подключения к серверам терминалов и другим удаленным рабочим столам только через Internet Explorer и подключения TCP/IP.

# Администрирование узлов Web и FTP

Администрирование IIS является важной задачей при использовании его в качестве Web-платформы для хостинга множества виртуальных узлов Web и FTP. Сравнительно легко можно контролировать сервер, на котором выполняется хостинг Web-узла с одним IP-адресом и доменным именем. Однако задача значительно усложняется, если на сервере устанавливается несколько Web-узлов.

В этом случае одной сетевой карте назначается несколько IP-адресов и доменных имен. При этом используются заголовочные имена хоста (доменное имя в Internet или имя в локальной сети). Выбор узлов осуществляется на основе информации, передаваемой серверу из заголовка, и используется для определения требуемого хоста. При этом каждый Web-узел, установленный подобным образом, "ведет" себя так, как будто весь сервер находится в его распоряжении.

Работа с сервером IIS и его компонентами преимущественно осуществляется с помощью диспетчера Internet Services Maneger, выполняющегося в консоли MMC.

## Установка узлов на сервере Windows 2000

Данные установки целесообразно делать для Internet-клиентов, имеющих собственные доменные имена, зарегистрированные в InterNIC или в локальной Intranet-сети, где вы сами можете дать имена клиентам.

Изначально Internet Information Server сконфигурирован с учетом поддержки одного Web-узла, FTP-узла, SMTP-узла и NNTP-узла. При создании нескольких узлов на сервере Windows сначала устанавливаются начальные каталоги, заданные по умолчанию. Они могут размещаться на любом локальном диске либо в любом сетевом местоположении. Предположим, что будет создан Web-узел для отдела Marketing. Используя Windows Explorer или My Computer, создайте каталог и присвойте ему имя Marketing. Запомните, где был создан каталог. Автор присвоил начальному каталогу имя **InetPub\wwwroot**, благодаря чему облегчается его поиск в дальнейшем.

Затем запустите диспетчер Internet Services Manager (если он еще не запущен) и выберите пиктограмму сервера на вашем компьютере в левой панели. На рисунке – это компьютер TOLSTYKH. В меню Action (Действие) выберите команду New => WebSite (Создать => Web-узел). В результате произойдет запуск мастера Web Site.

Введите описание, соответствующее назначению узла, и щелкните на кнопке Next (Далее). Указанное описание идентифицирует Web-узел для вас и других администраторов и отображается в левой панели консоли MMC.

На экране появится диалоговое окно IP Address and Port Settings (Настройка IP-адреса и порта). Введем один из назначенных ранее IP-адресов, например, IP-адрес 1**92.168.5.1**, в качестве порта оставим порт 80, а в качестве заголовочного имени хоста используем имя **Marketing**.

Теперь узел доступен для просмотра Web-броузером. В строке Адрес указывается адрес **http://Marketing**. Используя его, а также заголовочное имя хоста, сервер IIS реализует направление пользовательского запроса. Для выполнения указанных выше действий потребуется определить заголовочную информацию хоста в настройках вашего сервера DNS либо в файле **HOSTS**. Например, в файл **HOSTS** можно добавить запись 192.168.5.1 Marketing. Подробнее читайте в разделе «Определение имен в IIS».



| | |
|---|---|
| IIS | сервере IIS. Запускайте только те службы, которые абсолютно необходимы |
| Доменные контроллеры | НЕ запускайте сервер IIS на доменных контроллерах |
| Аудит | Задействуйте подходящие свойства аудита с целью мониторинга нарушений системы защиты |
| Шифрование | Используйте по возможности шифрование файлов, а также применяйте сети VPN или другие методы обеспечения безопасности |
| Настройка системы резервирования | Установите службы резервирования для всех важных и чувствительных данных, а затем храните данные в защищенной области |
| Проверка на наличие вирусов | Планируйте автоматическое сканирование на предмет наличия вирусов, а также обновляйте вирусные базы |
| Привязки служб | Просмотр служб, привязанных к сетевым платам. Убедитесь в том, что при подключении к Internet не включена служба File and Printer sharing (Совместное использование файлов и принтеров) |
| Аутентификация IIS | Проверьте, что для клиентов и сервера используются максимально строгие методы аутентификации |
| Отображение сертификатов | Выберите отображение для сертификатов типа "один-к-одному" или "многие-к-одному". |
| Синхронизация прав доступа Web и NTFS | Убедитесь в том, что права доступа Web совпадают с правами доступа NTFS. Необходимо применять |

# Обеспечение защиты сервера IIS

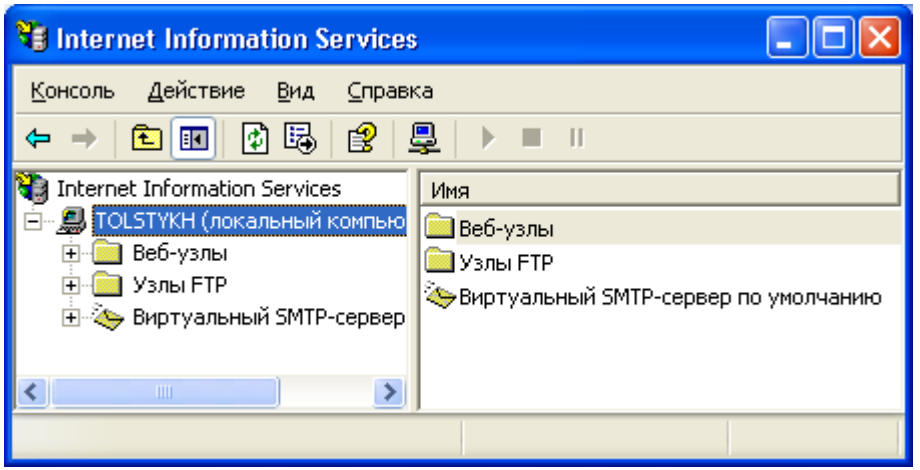
Большая часть механизмов обеспечения безопасности функционируют исключительно с использованием томов NTFS.

## Перечень мер безопасности

При конфигурировании системы защиты сервера IIS следует придерживаться мер безопасности, описанных в следующей таблице.

| Параметр сервера | Настройка |
|---|---|
| Файловая система | Используйте файловую систему NTFS для всех томов |
| Права доступа к каталогу | Проверьте права доступа каталогов. Удостоверьтесь в том, что если каталоги содержат только сценарии и приложения, для них установлены права доступа Script и Execute |
| Проверка прав доступа учетной записи IUSR_Computername | Назначаются корректные права доступа |
| Проверка каталогов исполняемых файлов и сценариев | Копируйте приложения и сценарии в каталоги, отделенные от других файлов |
| Просмотр учетных записей пользователей | Сетевой администратор должен проверять все списки ACL для пользователей и групп |
| Пароли | Проверить, применяют ли пользователи, требующие аутентификации, длинные и трудные для угадывания пароли |
| Политики учетных записей | Проверка политик групп и учетных записей |
| Службы компьютера | Просмотр всех служб, выполняемых на |






Диспетчер Internet Services Manager

После щелчка на кнопке Next (Далее) в диалоговом окне IP Address and Port Settings отобразится диалоговое окно Web Site Home Directory (Начальный каталог Web узла).Укажите путь либо воспользуйтесь кнопкой Browse (Просмотр) для нахождения пути, указывающего размещение Web-узла. В данном случае путь указывается для созданного ранее начального каталога. Оставьте установленным флажок Allow anonymous access this Web Site (Разрешить анонимный доступ к данному Web-узлу), чтобы любые Web-клиенты могли посещать ваш узел. Затем щелкните на кнопке Next (Далее).

На этом этапе отображается диалоговое окно Web Site Access Permissions (Права доступ к Web-узлу). Для клиентов, получающих NTFS-доступ к Web-узлу, можно назначить соответствующие права доступа:

- Read (Считывание). Разрешает клиентам просмотр страниц для данного узла.
- Run scripts (such as ASP) (Запуск сценариев (таких как ASP)). Разрешает клиентам запрашивать страницы, содержащие код ASP, а также вызывающие этот код.

- Execute (such as ISAPI and CGI apps) (Выполнение (например, приложений ISAPI и CGI)). Обеспечивает вызов приложений CGI и ISAPI для данного узла.
- Write (Запись). Обеспечивает операции выгрузки, удаления или передачи файлов клиента для данного каталога.
- Browse (Просмотр). Обеспечивает просмотр каталогов и коллекций.

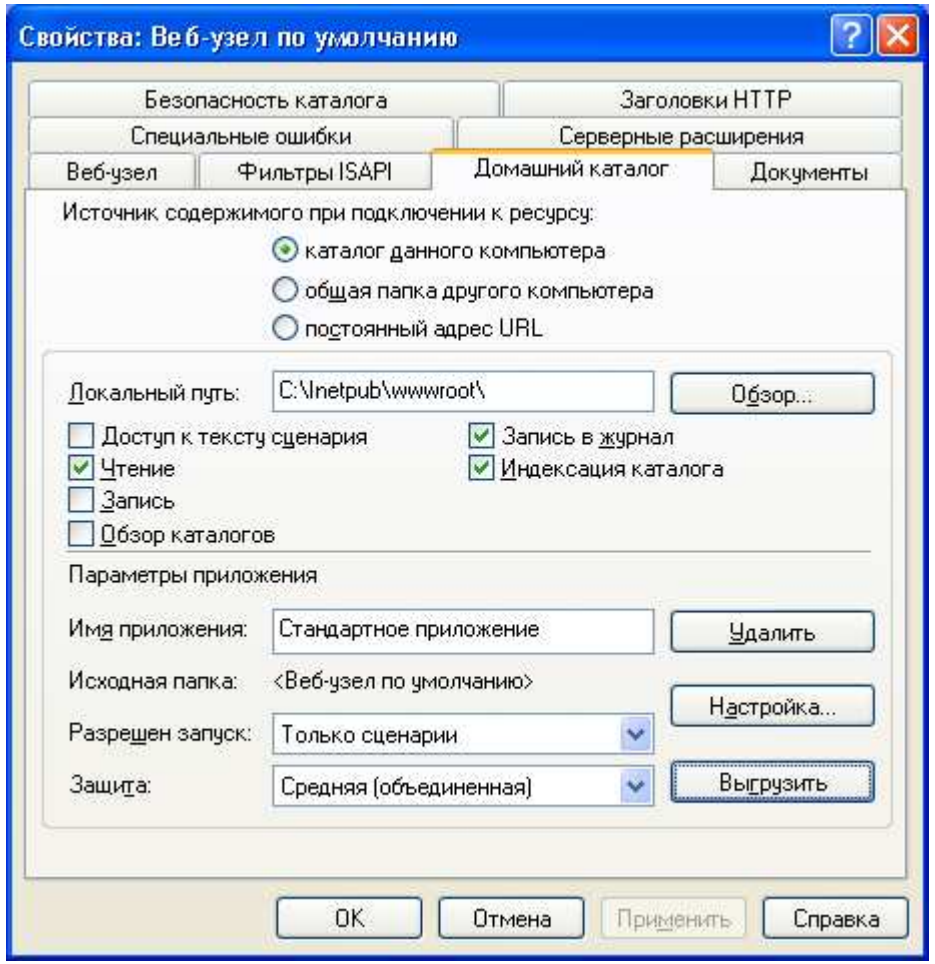
## Определение имен в IIS

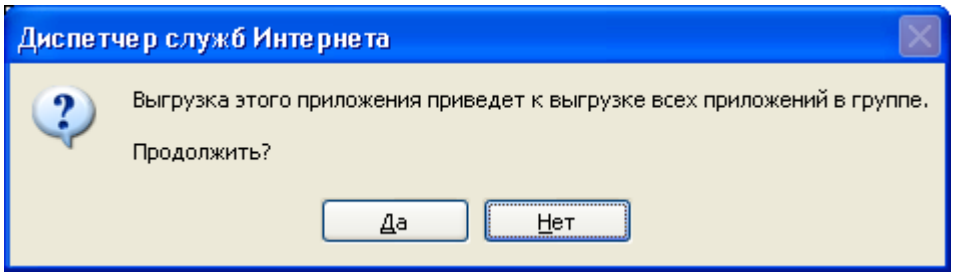
Определение IP-адресов в Windows 2000 производится с использованием двух методов: статическое присвоение имени и с использованием DHCP. Сконфигурируйте сервер IIS с применением статического IP-адреса.

Для того чтобы позволить клиентам использовать доменные имена необходимо иметь метод, который позволит сопоставить IP-адрес с конкретным доменным именем. Этот метод известен под названием Domain Name System (DNS). При его использовании применяются файлы **HOSTS:**

```
# Пример файла HOSTS, используемого Microsoft TCP/IP for Windows.
#
# Файл содержит соответствия между IP-адресами и именами
# узлов сети. Каждая запись должна находиться в отдельной строке.
# В первой колонке должен помещаться
# IP-адрес, за ним следует имя соответствующего
# узла сети. Между IP-адресом и именем
# узла сети должен находиться, как минимум, один пробел.
#
# Комментарии (подобные указанным здесь ) могут
# помещаться в отдельных строках либо следовать
# за именем компьютера. Комментарии вводятся с помощью
# символа '#'.
#
```






Выгрузка приложений web-узла

настройку повторного запуска процессов. Параметры приложения, в том числе, его уровень защиты, можно задавать на разных уровнях метабазы. Уровень защиты определяет, откуда приложение получает свои параметры повторного запуска процессов.

| Защита приложения | Параметры метабазы |
|---|---|
| **Низкая (процесс IIS)** | AppIsolated = 0 |
| **Средняя (объединенная)** | AppIsolated = 2 |
| **Высокая (изолированная)** | AppIsolated = 1 |

## Выгрузка приложений отдельных узлов

Если приложения на севере нуждаются в отладке либо требуется остановить выполнение приложения, особенно ISAPI-приложения в виде dll-библиотеки, на определенный период времени, сервер IIS позволяет выполнить это путем останова выполнения приложений конкретного узла, а не всей службы IIS. Это делается через Домашний каталог в Свойствах требуемого web-узла (см. рис.)



```
# Например:
#
# 102.54.94/97 rhino.acme.com   #  исходный сервер
# 38.25.63.10 x.acme.com        # x клиент узла сети

127.0.0.1 localhost
192.168.5.1 Marketing
127.0.0.1 www.donnu.edu.ua            # и не использовать в прокси
```

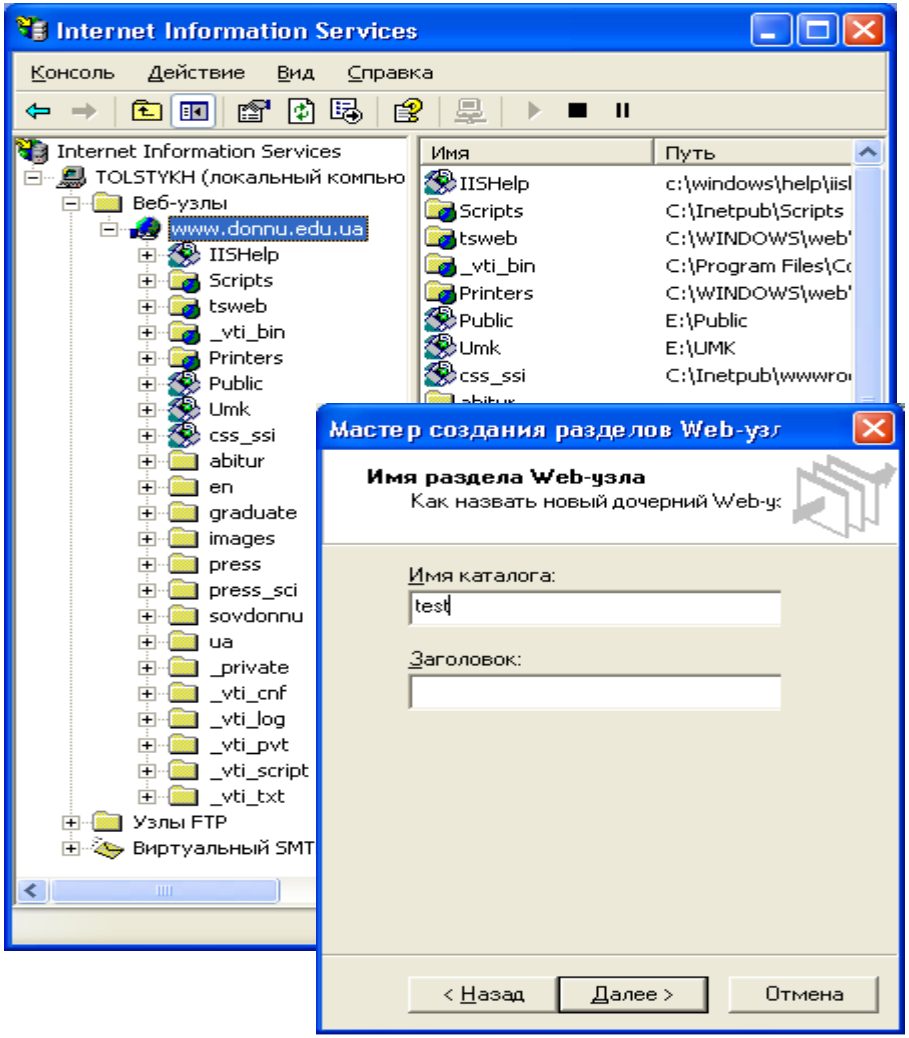
Этот файл должен находиться в каталоге systeinrpot\ system32\drivers\etc, где systemroot обозначает каталог, где устанавливается Windows 2000. Если этот метод используется для определения соответствия между хост-именами и IP-адресами, то этот файл должен размещаться на каждом компьютере, подключенном к сети. Причем конфигурация этих файлов должна быть идентичной. При работе с клиентами Windows 9x модифицируется и используется файл **Hosts.sam**, размещенный в каталоге Windows.

Как можно видеть, этот метод является быстрым и простым при использовании в малых сетях. Не требуется вводить IP-адреса сервера DNS для конфигурации TCP/IP в случае, если системы используются только во внутренней корпоративной сети и в этой сети требуется определять хост-имена. Однако при использовании Internet применение файлов **HOSTS** практически неоправданно. Слишком трудно администратору отслеживать новые узлы сети, добавляемые и изменяемые ежедневно.

В этом случае требуется воспользоваться сервером DNS. ОС Windows 2000 поставляется вместе со службой DNS, которая может быть установлена и сконфигурирована для выполнения определения хост-имени по IP-адресу и выполнения обратной операции. Помните, что доменные хост-имена в Internet должны быть зарегистрированы (куплены) в InterNIC.

## Установка web-узлов без заголовочных имен – web-узел серверных расширений

Данные установки целесообразно делать для Internet-клиентов, не имеющих собственных доменных имен. Здесь на сетевой карте IIS будет один IP-адрес. Все участники сети будут использовать заголовочное имя вашего узла с указанием пути к своим дочерним узлам (под-сайтам).




Создание дочернего Web-узла серверных расширений



Для настройки повторного запуска процессов используются четыре уникальных раздела метабазы. Первые три раздела, перечисленные ниже, можно задавать через интерфейс пользователя. Четвертый раздел ShutdownTimeLimit задается только непосредственно в метабазе.

- **PeriodicRestartRequests**
  Это свойство задает число запросов, которые должны быть обработаны приложением. После этого выполняется повторный запуск приложения. Дополнительные сведения см. в разделе PeriodicRestartRequests.
- **PeriodicRestartTime**
  Это свойство задает в минутах промежуток времени, в течение которого приложение обслуживает запросы. После этого IIS выполняет повторный запуск изолированного приложения. Дополнительные сведения см. в разделе PeriodicRestartTime.
- **PeriodicRestartSchedule**
  Это свойство задает значение времени в 24-часовом формате. В это время выполняется повторный запуск приложения. Дополнительные сведения см. в разделе PeriodicRestartSchedule.
- **ShutdownTimeLimit**
  Это свойство задает в секундах промежуток времени, в течение которого после достижения времени повторного запуска приложения IIS ожидает выполнения запросов старого приложения в старом процессе DLLHost.exe. По исчерпании периода ожидания ShutdownTimeLimit IIS закрывает старый процесс DLLHost. Дополнительные сведения см. в разделе ShutdownTimeLimit.

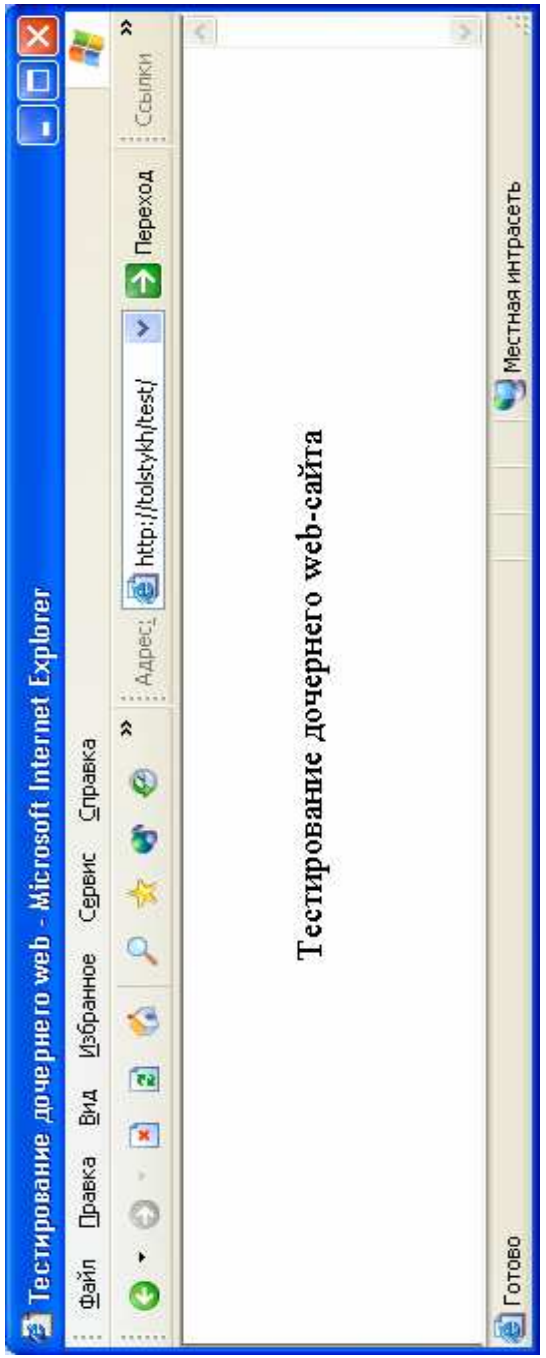
При настройке повторного запуска процессов без интерфейса пользователя необходимо иметь представление о разделе метабазы **AppIsolated**, поскольку значение параметра AppIsolated определяет уровень защиты приложения. С помощью этой информации следует решить, где выполнять

- **Низкая (процесс IIS)**. Приложения могут выполняться в основном процессе IIS **inetinfo.exe**, который также называют внутренним процессом. В процессе IIS следует выполнять только тщательно проверенные приложения. Сбой приложения, выполняющегося в этом процессе, приводит к сбою IIS и всех других внутренних приложений. Повторный запуск приложений, выполняющихся как внутренние, не выполняется.
- **Средняя (объединенная)**. Сгруппированные приложения выполняются как внешние в общем процессе **DLLHost.exe**. Повторный запуск процессов настраивается на уровне W3SVC в метабазе и все сгруппированные приложения повторно запускаются совместно.
- **Высокая (изолированная)**. Сгруппированные приложения выполняются как внешние и каждое приложение выполняется в отдельном процессе **DLLHost.exe**. Повторный запуск изолированных приложений осуществляется отдельно от любых других приложений. Настройка повторного запуска процессов может задаваться на любом уровне метабазы, на котором существует изолированное приложение.

Выполнять настройку событий повторного запуска процессов можно на различных уровнях метабазы IIS либо через интерфейс пользователя, либо непосредственно в метабазе. Все свойства, определяющие повторный запуск процессов, наследуются нижними уровнями метабазы IIS, за исключением случаев, когда свойство на нижнем уровне уже задано в явном виде.

- Настройка сгруппированных приложений задается на уровне W3SVC аналогично любым другим сгруппированным внешним приложениям.
- Настройка изолированных приложений выполняется на уровне AppRoot соответствующего веб-узла.






Просмотр файла, загружаемого по умолчанию, в дочернем сайте

Данные установки также целесообразно делать на локальных компьютерах клиентов для тестирования работоспособности их сайтов. Напоминаем, что IIS доступен в клиентской ОС Windows XP Professional после установки соответствующих компонент Windows. При стандартной установке Windows XP Professional сервер IIS не доступен.

Запустите диспетчер Internet Services Manager и выберите пиктограмму Web-узел по умолчанию. В меню Действие выберите команду Создать => Web-узел серверных расширений. В результате произойдет запуск мастера Web Site. Введите имя каталога дочернего узла и нажмите Далее. После завершения работы мастера, чтобы увидеть изменения, потребуется обновить панели MMC (кнопка Обновление на панели инструментов).

## Резервирование и восстановление конфигурации

Если вы имеете дело с производственным сервером, следует рассматривать создание сценариев резервирования и восстановления. Это высказывание в полной мере относится к серверу IIS. Представьте себе, что может случиться, если вы серьезно измените конфигурацию сервера IIS, а затем эту же операцию проделает ваш коллега или, что значительно хуже, какой-нибудь хакер? Будет потрачена масса времени на выяснение сути происходящего и восстановление нужной конфигурации.

Для резервирования текущей конфигурации воспользуйтесь следующей технологией.

1. Используя интегрируемый модуль IIS, выберите пиктограмму компьютера в левой панели.
2. В меню Action выберите опцию Backup/Restore Configuration (Резервирование/Восстановление конфигурации).
3. Щелкните на кнопке Create Backup (Создать резервную копию), в результате отобразится диалоговое окно Configuration Backup (Резервирование конфигурации), в котором можно указать имя файла резервной копии, введите имя файла резервной копии и щелкните на кнопке <OK>.



- **None (Нет).** Предотвращает выполнение приложений в указанном каталоге. С точки зрения обеспечения безопасности выбор этой опции — наилучшее решение, однако при этом невозможно выполнение приложений либо сценариев.
- **Scripts only (Только сценарии).** Возможно выполнение сценариев (ASP, Java и т.д.). При установке этой опции невозможно выполнение приложений. Она представляет своего рода компромисс, обеспечивающий безопасный метод для конфигурирования сервера при сохранении некоторых возможностей для выполнения.
- **Scripts and Executables (Сценарии и исполняемые приложения).** Обеспечивает выполнение из каталога любых сценариев и приложений. При этом может создаваться угроза для безопасности, поскольку в этом случае могут запускаться на выполнение приложения, которым соответствуют двоичные файлы Windows, такие как **.dll и .exe.** В этом случае враждебно настроенные пользователи могут запускать на сервере вирусы либо троянские программы. Используйте эту опцию осторожно, ознакомившись с вопросами обеспечения безопасности в IIS.

После установки необходимых прав доступа выполнения потребуется определить процесс, с помощью которого будут запускаться приложения выбранного узла. Выбор нужного процесса осуществляется из раскрывающегося комбинированного списка Application Protection (Защита приложений).

## Изоляция (защита) приложений

Приложения можно настраивать на выполнение одним из трех способов. Эти возможности в IIS 5.0 описываются в терминах «уровней изоляции». Три уровня изоляции приложений выбираются в оснастке IIS в окне свойств на вкладке «Домашний каталог» в поле со списком «Защита».

## Конфигурирование приложений в IIS

Web-приложение IIS является сценарием или исполняемой программой, которые вызываются на сервере в результате запроса со стороны клиента иди самого сервера IIS. Эти приложения могут принадлежать к одному из следующих типов:

ASP, CGI, ISAPI, SSI

В IIS 4.0 была возможность выполнения приложений в том же пространстве процесса, где выполняется сервер IIS. Эта опция получила название **Inetinfo.exe** (изолированное приложение). Приложения также может выполняться в отдельном процессе — **DLLhost.exe** (процесс). Сервер IIS 5.0 поддерживает описанные два метода, а также дополнительно осуществляет поддержку третьего метода, называемого объединенным процессом.

Рекомендуемым подходом при назначении защиты приложений для сохранения заданного уровня производительности является запуск сервера IIS в своем собственном процессе, выполнение важных приложений в их собственном процессе и выполнение всех остальных приложений в объединенном процессе. Можно иметь более 10 критических приложений, выполняющихся одновременно на одном сервере. Для выполнения конфигурирования можно воспользоваться лучшим решением, либо рассматривать возможность добавления второго сервера IIS и распределения приложений среди двух серверов.

После создания приложения можно начинать определение прав доступа, системы защиты приложений, а также выполнять конфигурирование отображения.

Сначала нужно решить, будет ли каталог приложения содержать сценарии, исполняемые файлы, комбинации сценариев и исполняемых файлов. Размещение описанных выше структурных элементов определяется с помощью раскрывающегося меню Execute Permissions (Права доступа выполнения). При этом доступны три типа прав доступа.



По умолчанию резервный файл хранится в каталоге <Системный корневой каталог>\ System32\inetsrv\Metaback.

Для восстановления конфигурации выполните следующее.

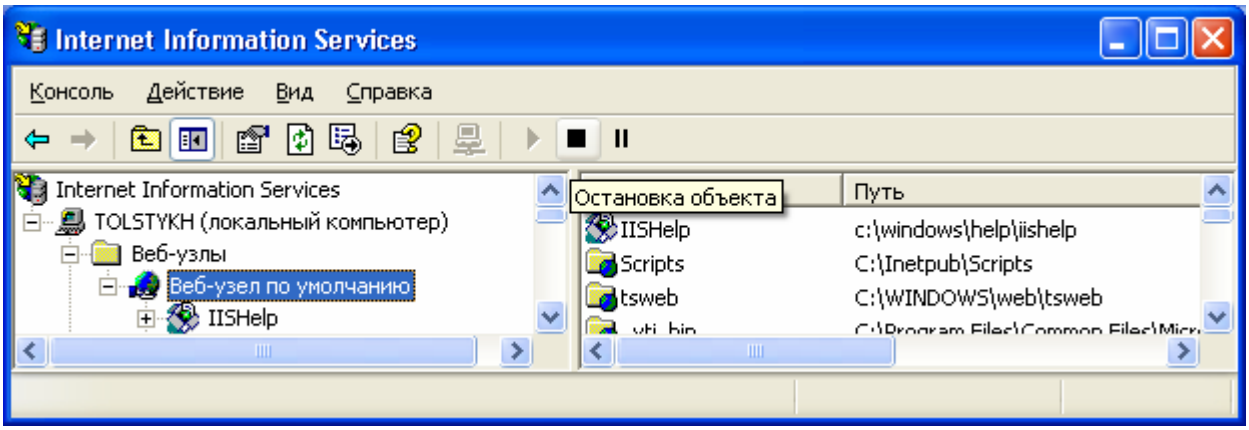
1. Выберите пиктограмму компьютера в левой панели.
2. В меню Action выберите опцию Backup/Restore Configuration в разделе Previous Backups (Предыдущие резервные копии) выберете файл созданной резервной копии.
3. Щелкните на кнопке Restore (Восстановить).

## Запуск и остановка узлов

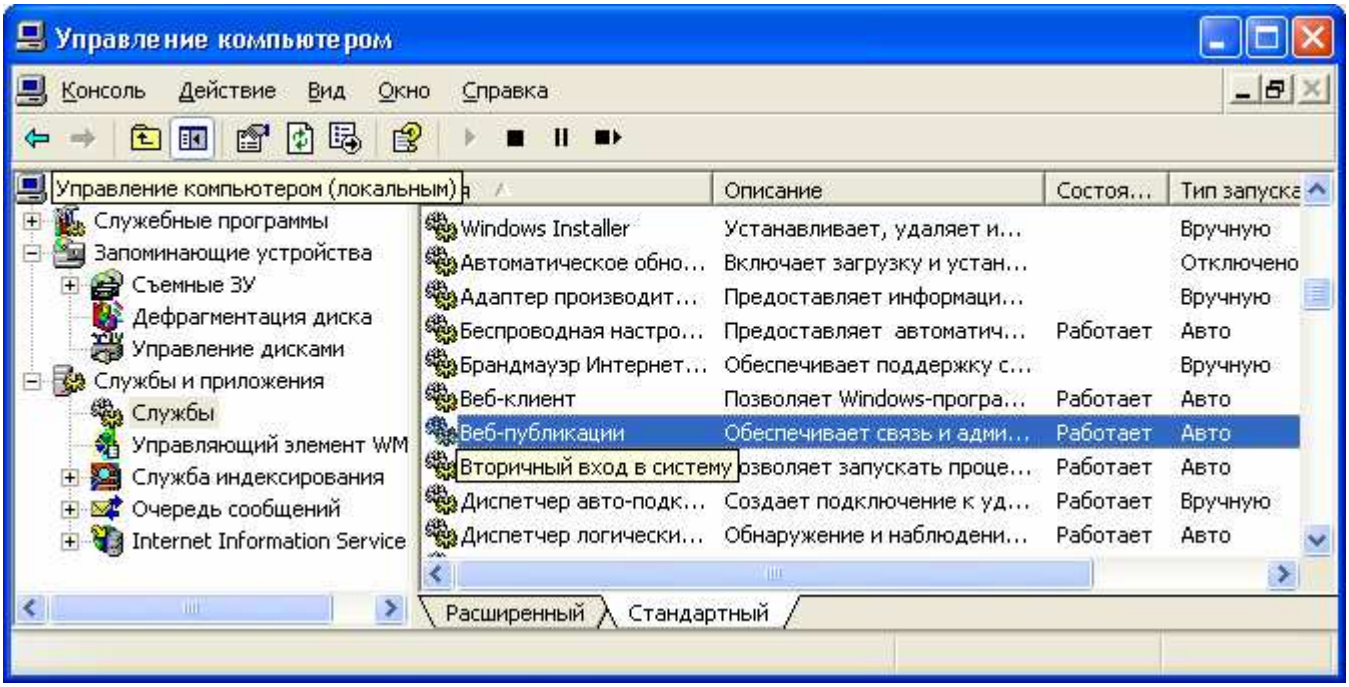
Работу любого web-узла IIS можно останавливать и возобновлять. После остановки он не будет доступен для просмотра клиентскими web-браузерами. Нельзя отдельно остановить дочерний узел без остановки основного узла. Остановка IIS также бывает необходима при программировании и тестировании ISAPI-приложений в виде dll-библиотек.

Для останова любого из выполняющихся узлов щелкните на имени узла в навигационной панели (левая панель) с целью его выделения, затем щелкните на кнопке Stop (Остановка объекта) в панели инструментов MMC (помечена сплошным черным квадратиком).

Для запуска, останова и приостановки узлов может также применяться апплет Services (Службы). Он находится в окне Control Panel (Панель управления) в разделе Administrative (Администрирование). После запуска апплета отобразится окно, показанное на рисунке. На этом рисунке выбрана служба World Wide Web Publishing Service (Веб-публикации). На правой панели отображается статус службы и тип запуска.




Остановка web-узла




Остановка IIS на компьютере