**Лекция №11: Учетные записи, аутентификация и политика безопасности**

**Цель:** ознакомить студентов с важностью правильного управления учетными записями и процессом аутентификации в системе безопасности. Рассмотреть принципы и методы применения политики безопасности, направленной на защиту информации и предотвращение несанкционированного доступа.

### Применение политики безопасности

Привилегии и ограничения, присваиваемые пользователям для работы с ресурсами системы, позволяют применять политику безопасности к управлению и *распределению информации*. Многие организации не уделяют достаточного внимания этой политике. Согласно требованиям современного информационного мира сначала необходимо ознакомиться с *ключевыми параметрами* безопасности ресурсов сервера (см. [табл](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=1" \l "table.4.1)[. 4.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=1" \l "table.4.1)).

|  |  |
| --- | --- |
| Таблица 4.1. Параметры политики безопасности веб-сервера | |
| **Параметр** | **Описание** |
| Правила безопасности IP | Установка фильтров IP-трафика. Определение причин и способов шифрования пакетов. |
| Присвоение/создание переданных (распределенных) полномочий администрирования | Назначение администратора, ответственного за содержимое и безопасность *сервера. Установка* псевдо-административных ролей, таких как операторы резервирования данных. |
| Присвоение/создание учетных записей пользователей | Установка анонимной и аутентифицируемой учетных записей. |
| Правила безопасности учетных записей | Указание групп, к которым принадлежат учетные записи. Использование блокировки при вводе неправильного пароля. Указание числа попыток ввода пароля перед блокировкой, а также длительность блокировки. Указание срока действия пользовательского билета Kerberos. |
| Правила безопасности групп | Указывают группы, членов групп, а также правила, примененные к группам. |
| Определение правил безопасности паролей | Установка минимальной длины паролей, разрешения/запрещения использования "пустых" паролей. Установка отказа на повторное использование паролей. Установка требований для численно-буквенных паролей. Установка правила периодической смены паролей пользователей (если такая возможность имеется). |
| Правила конфиденциальности данных | Установка разрешений на каталоги и файлы. |

*Список* этот довольно краткий, но все же дает необходимое *представление* о проблеме. Понятен ли каждый *пункт* таблицы? Вам предстоит обрабатывать эти параметры, так как они непосредственно связаны с управлением данными.

Перед началом работы необходимо ознакомится с концепциями безопасности *Windows* 2000 и соответствующей терминологией.

### Принципы безопасности Windows 2000 и IIS

*Сервер* *IIS* является встроенным компонентом *Windows* 2000, и *безопасность* *IIS* полностью зависит от безопасности этой операционной системы. *Управление безопасностью* *Windows* 2000 основано на следующих принципах.

* *Доверительные отношения*.
* Рабочие группы и домены (а также Active Directory).
* Аутентификация учетных записей и групп.
* Контроль доступа (права, разрешения и ограничения).
* Наследование.

Все аспекты безопасности *Windows* 2000 базируются на этих принципах. Они обеспечивают *безопасность* системы посредством запрета, ограничения и разрешения доступа к данным и ресурсам на веб-сайте *IIS*.

#### Доверительные отношения

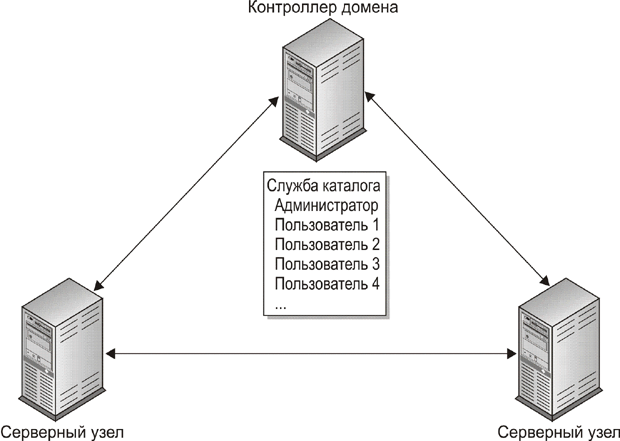
Безопасность Windows 2000/IIS основывается на правилах и параметрах, определяющих разрешенные и запрещенные действия в системе. Жизненно важной частью данной системы являются механизмы уникальной идентификации для отдельных пользователей, компьютеров и ресурсов. В Windows 2000 сетевые IP-адреса, имена *пользователя, сертификаты* (цифровые идентификаторы) и идентификационные данные Kerberos являются способами проведения идентификации. Между компьютерами и отдельными пользователями или другими компьютерами устанавливаются правила доверия, зависящие от *степени доверия*, имеющей место в процессе идентификации. В Windows 2000 при наивысшем уровне доверия на взаимодействующих компьютерах считается легальным любой вход в систему и обмен информацией.

#### Рабочие группы и домены

Рабочие группы и домены представляют собой наборы отдельных пользователей и ресурсов сети. Ресурсы состоят из устройств хранения данных, принтеров, файлов данных и прочих компонентов, связанных с серверами.

Рабочая группа отличается от домена тем, что в домене серверы при взаимодействии пользуются доверием и используют общую базу данных управления, а в рабочей группе каждый сервер обрабатывает свою собственную базу данных. Когда организации нужен более чем один сервер, несмотря на то, что сеть настроена на управление с помощью рабочих групп, целесообразно использовать домен. *Доверительные отношения* между серверами домена облегчают работу, как для пользователей, так и для администраторов. Пользователи, входящие в домен, осуществляют вход на все серверы одновременно, и им не нужно входить в систему каждого сервера по отдельности. Администраторам выгодно использовать такое решение, поскольку общая база данных доменов позволяет избежать создания и управления ненужными записями пользователей на каждом сервере.

На [рисунке 4.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=1" \l "image.4.1) изображена группа серверов в домене. Обратите внимание, что домен содержит систему, называемую контроллером домена, "владеющую" *базой данных пользователей*, которая является общей для всех остальных серверов.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_01.gif)

[увеличить изображение](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_01.gif)

**Рис. 4.1.**В домене Windows 2000 Server контроллер "владеет" базой данных пользователей.

Организации, в которых используются домены, часто используют службу Windows 2000 под названием Active Directory. Active Directory представляет собой базу данных, которая управляет пользователями и всеми сетевыми ресурсами в логической модели. Например, пользователь видит принтеры, расположенные к сети, независимо от того, к какому именно серверу они непосредственно подключены.

В интранет-сетях многих крупных организаций технология Active Directory пользуется большой популярностью, так как централизованное управление облегчает контроль над серверами, ресурсами, учетными записями, группами и другими объектами без повторения одних и тех же процедур в консолях каждого сервера. Active Directory позволяет физически конфигурировать сетевые ресурсы без изменения их представления в графическом пользовательском интерфейсе.

#### Аутентификация

Домены Windows (и Active Directory) облегчают работу пользователей при аутентификации. Аутентификация – это процесс подтверждения подлинности пользователя компьютера, осуществляемый посредством ввода имени пользователя и пароля. Централизованный контроль над учетными записями и паролями в домене Windows (в Active Directory) исключает необходимость входа пользователей на каждый сервер по отдельности.

#### Интранет против интернета

По иронии судьбы некоторые правила безопасности веб-сервера нередко конфликтуют с преимуществами, обеспечиваемыми доменами Windows и технологией Active Directory. Например, если веб-сервер расположен в интернете, он не должен иметь доверительных отношений с другими системами. В таком случае, стоит ли делать веб-сервер частью домена Windows? Да, при наличии соответствующих мер защиты. По другую сторону от брандмауэра, т.е. в сети интранет, организация может расположить веб-сервер в домене, если при входе на веб-сервер будет затребована аутентификация. Домен исключает повторный ввод на сервере идентификационных данных пользователей, паролей и т.д. (это очень существенно для крупных сетей), уже имеющихся в базе данных контроллера домена.

Каждый раз при создании доверительных отношений между системами повышается степень их уязвимости до уровня ошибки системы безопасности лишь в одном из компьютеров, поэтому управление веб-сервером интернета безопаснее всего осуществлять в отдельных системах. Веб-серверы настраиваются на специальный тип аутентификации, называемый анонимным входом, при котором не указывается уникальный идентификатор учетной записи. Использование анонимного входа в систему является различием в конфигурациях веб-серверов интернета и интранета. В остальном параметры безопасности довольно похожи.

**Совет**. Для любого правила можно найти исключения. На некоторых веб-серверах интранет используется анонимный вход без указания идентификатора и пароля. С другой стороны, некоторые веб-серверы интернета требуют аутентификацию. В этом случае, если управляющая сервером организация использует серверы FTP, серверы новостей и другие, она может объединить их в изолированный домен управления. Сейчас мы не будем рассматривать эти исключения.

#### Управление локальной безопасностью

Большинство аспектов безопасности, помимо управления аутентификацией, являются похожими для сайтов в интернете и интранете. Веб-серверы обоих типов имеют параметры, которые настраиваются отдельно на самом сервере. Даже если веб-сайт является частью домена Windows интранет-сети, к серверу необходимо применить меры безопасности, отличающиеся от остальных компьютеров домена. На веб-сервере требуется больший уровень защищенности, нежели на файловом сервере, так как веб-технологии содержат большее количество слабых мест. Основные параметры безопасности веб-сервера должны настраиваться с помощью управления параметрами его локальной безопасности. Параметры локальной безопасности на веб-сервере IIS или другом компьютере с Windows 2000 контролируют все аспекты безопасности, являющиеся уникальными для сервера.

#### Списки контроля доступа

Доступ к серверам Windows 2000 осуществляется через систему учетных записей пользователей и групп. После аутентификации на сервере пользователь может использовать ресурсы сервера согласно своим правам и разрешениям. Права и разрешения для учетных записей и групп хранятся в локальном списке Access Control List (ACL) (Список контроля доступа). Параметры списка ACL определяют то, какие действия учетная запись или группа может выполнять на сервере, эти параметры не являются общими с другими системами, даже если компьютер представляет собой часть домена Windows.

Права и разрешения определяются следующим образом.

* **Права**. Право – это возможность выполнения какого-либо действия, часто носящего административный или ограниченный характер, например запуск и *остановка системы* или создание новых учетных записей и групп пользователей.
* **Разрешения**. Альтернатива правам, позволяющая пользователям получать доступ к каталогам, файлам и принтерам. Для каталогов и файлов разрешения представляют собой любые комбинации возможностей просмотра, считывания, *изменения, записи* и выполнения файлов.

**Совет**. Если управление доменами осуществляется посредством Active Directory, ресурсы принадлежат сети, а не серверу, и авторизация осуществляется не локально, а при помощи контроллера домена.

Администрирование параметров безопасности веб-сайта влечет за собой изменения в локальных списках ACL для отказа, расширения или передачи прав и разрешений, присвоенных группам и учетным записям для доступа к ресурсам сервера. После этого определяются правила паролей, правила безопасности IP, правила аудита и ряд других дополнительных настроек (см. [табл. 4.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=1" \l "table.4.1)).

#### Фильтры

Фильтры представляют собой параметры, дополняющие списки ACL. Они усиливают ограничения на доступ. Хотя фильтры не очень распространены, они являются важной частью политики безопасности, так как устанавливают правила, не поддерживаемые списками ACL. Например, фильтр IP используется для ограничения доступа всех посетителей, пытающихся получить доступ к сайту с определенного IP-адреса или домена DNS. Ограничения, налагаемые фильтрами, представляют собой нечто, являющееся обратным разрешениям. Фильтры повсеместно используются в брандмауэрах, о которых пойдет речь в ["Особенности процесса разработки"](https://www.intuit.ru/studies/courses/1002/122/lecture/3527)и в ["Сторонние средства обеспечения безопасности"](https://www.intuit.ru/studies/courses/1002/122/lecture/3533). Например, одним из распространенных правил фильтрации является блокировка брандмауэром всего трафика, поступающего на веб-сервер, за исключением трафика HTTP через порт 80.

#### Наследование

После установки прав и разрешений для папки новые файлы и подпапки, созданные в ней, по умолчанию наследуют параметры ACL. Другими словами, новым файлам и папкам (именуемым дочерними объектами) присваиваются те же права и разрешения учетных записей и групп, что и для папки, в которой они созданы (эта папка называется родительской). Данное условие можно изменить при необходимости обхода параметров наследования. В процессе изучения материала вы узнаете, как это делается.

### Средства управления локальной безопасностью

Управление локальными параметрами и политикой не зависит от того, работаете вы с отдельным сервером или с сервером, являющимся частью домена интранет-сети или использующим технологию *Active* *Directory*. Локальные настройки и политика применяются к тому компьютеру, на котором они установлены. Даже если *компьютер* является частью домена, другим системам в домене неизвестны локальные настройки отдельных компьютеров и на них не распространяются.

*Windows* 2000 и *IIS* используют три основных набора инструментов для конфигурирования и управления локальными настройками безопасности сервера.

* Пакет средств Microsoft Management Console (MMC).
* IIS Lockdown (IIS Lock).
* Анализ и настройка безопасности MMC и шаблоны.

Набор средств *MMC* представляет собой пакет инструментов, предназначенных для конфигурирования безопасности и ее поддержки, включая настройку параметров аутентификации, создание пользователей и групп, управление *ACL* и т.д. Компоненты *IIS* Lockdown и *Security* *Configuration* *and* *Analysis* (*Анализ* и настройка безопасности) являются специализированными средствами. *IIS* Lock используется для автоматизации настройки параметров безопасности при начальной установке или при изменении конфигурации сервера. Оснастка *Security* *Configuration* *and* *Analysis* и связанные с ней шаблоны безопасности используются для построения и применения особых локальных политик безопасности.

В ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)вы познакомились с *MMC* и с *IIS* Lock и даже использовали эти компоненты для укрепления своего сервера. *IIS* Lock вновь потребуется при установке новых сервис-пакетов, служб *FTP*, *NNTP* и *SMTP*. *MMC* используется постоянно, причем не только для защиты, но и для поддержки сервера *IIS*.

#### Консоль Microsoft Management Console

Инструменты пакета MMC находятся в папке Administrative Tools (Администрирование) в меню Start (Пуск). На отдельном сервере все локальные учетные записи пользователей, группы, пароли и другие настройки управляются посредством MMC и хранятся локально в файле диспетчера безопасности учетных записей (SAM).

Некоторые средства управления безопасностью в Active Directory MMC несколько отличаются от аналогичных инструментов отдельного сервера. Например, для управления пользователями и группами на отдельном сервере используются папки Local Users (Локальные пользователи) и Groups (Группы) в компоненте MMC *Computer Management* (Управление компьютером). В среде домена/Active Directory используется компонент Active Drectory Users and Computers (Пользователи и компьютеры Active Directory). Active Directory хранит информацию о домене в отдельном файле, который называется *NTDS*.*DIT* и имеется на других контроллерах доменов.

Те читатели, чьи веб-сайты соединены только с интернетом, при выполнении рекомендаций (см. ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)) не должны были включать свои веб-серверы в домен и, следовательно, использовали локальные средства управления MMC для Windows 2000 и IIS. Обратите внимание, что большая часть параметров локальной безопасности веб-сайта, находящегося в домене, настраивается с помощью локальных инструментов управления MMC. Исключением является управление пользователями и группами интранет-сети, осуществляемое инструментами MMC Active Tools. Причина заключается в том, что пользователи и группы могут быть общими для всех серверов сети интранет. Однако в этой лекции мы не будем рассказывать о средствах Active Directory. В дальнейшем речь пойдет только об управлении локальной политикой безопасности сервера. [Таблица 4.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=3" \l "table.4.2) содержит перечень средств MMC, предназначенных для управления локальной безопасностью Windows 2000/IIS.

|  |  |
| --- | --- |
| Таблица 4.2. Инструменты управления локальной безопасностью для IIS | |
| **Средство** | **Функция** |
| *Computer Management* (Управление компьютером) | Управляет локальными или удаленными компьютерами. Содержит функции по управлению атрибутами сервера, такими как *системные события*, свойства хранилищ, пользователи и группы, параметры устройств и службы. |
| Internet Services Manager (Диспетчер служб интернета) | Управляет параметрами безопасности веб-сервера IIS, включая разрешения домашних каталогов, методы аутентификации, *анонимный доступ* и права оператора. |
| Local *Security Policy* (Локальная политика безопасности) | Управляет локальной политикой безопасности на сервере по отношению к таким параметрам, как свойства IPSec, свойства паролей, свойства группы и свойства блокировки. |
| Оснастка Security Configuration and Analysis (Анализ и настройка безопасности) | Осуществляет анализ и конфигурирование прав пользователя локального компьютера, ограниченных групп, реестра, файловой системы и *системных служб* с использованием шаблона политики безопасности. |
| Оснастка Security Templates (Шаблоны безопасности) | Определяет политику безопасности, применяемую к группе или компьютеру. |

#### Настройка политики безопасности с помощью шаблонов

Шаблоны безопасности представляют собой *централизованный метод* установки параметров безопасности при работе с оснастками MMC Security Configuration and Analysis (Анализ и настройка безопасности) и Security Template (Шаблон безопасности). На сайте Microsoft Technet находится шаблон безопасности Microsoft. Он содержит основные параметры безопасности для IIS, которые, по мнению Microsoft, должны применяться к защищаемым веб-сайтам. Шаблоном является файл с именем Hisecweb.inf, который можно загрузить с веб-сайта Microsoft по адресу [http://support.microsoft.com/support/misc/kblookup.asp?id =Q316347](http://support.microsoft.com/support/misc/kblookup.asp?id%20=Q316347" \t "_blank).

Шаблон безопасности представляет хорошую основу для реализации защиты сервера. При запуске программы IIS Lock (см. ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)) этот компонент применял к серверу настройки файла Hisecweb.inf.

С помощью шаблонов эффективно разрабатывается локальная политика безопасности. Шаблон Hisecweb.inf можно использовать в качестве базы, затем внести в него изменения, после чего сохранить под другим именем для создания собственной политики. Так можно просматривать, настраивать и применять к локальному компьютеру широкий спектр настроек безопасности. Этот метод используется для определения изменений, которые вносятся в настройки политики безопасности Microsoft IIS по умолчанию.

Политики безопасности в шаблоне Hisecweb.inf содержат настройки следующих параметров.

* **Account Policies** (Политики учетных записей). Защита паролей, блокировки учетных записей и аутентификации Kerberos.
* **Local Policies** (Локальные политики). Ведение журналов событий, связанных с безопасностью, а также учет присвоения прав пользователям и группам.
* **Restricted Groups** (Ограниченные группы). Администрирование членов локальной группы.
* **Registry** (Реестр). Безопасность параметров локального реестра.
* **System Services** (*Системные службы*). Режим запуска и безопасность локальных служб.
* **Security Options** (Параметры безопасности). Правила для других настроек безопасности.

Для получения полного представления о количестве рассматриваемых параметров нужно ознакомиться со всеми лекциями книги. На данном этапе работы необходимо настроить оснастки, так как они понадобятся в последующих лекциях. А сейчас мы создадим шаблоны, работу с которыми продолжим позже.

##### Установка оснасток Security Configuration и Security Template

Для использования шаблона необходимо скопировать его в системный раздел веб-сервера, после чего установить оснастки MMC Security Templates (Шаблоны безопасности) и Security Configuration and Analysis (Анализ и настройка безопасности). Выполните приведенные ниже процедуры.

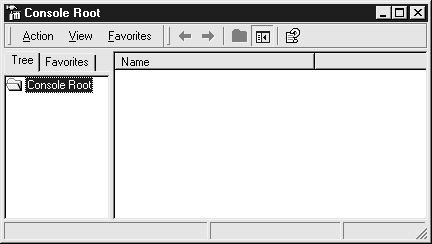
1. Скопируйте шаблон (файл Hisecweb.inf) в каталог шаблонов безопасности системного раздела веб-сервера c:\WINNT\security\templates.
2. Для установки оснастки откройте MMC в авторском режиме. Можно создать новую консоль MMC для оснасток или добавить оснастки в имеющуюся консоль *Computer Management* (Управление компьютером).

Для добавления оснастки в имеющуюся консоль выполните следующие действия.

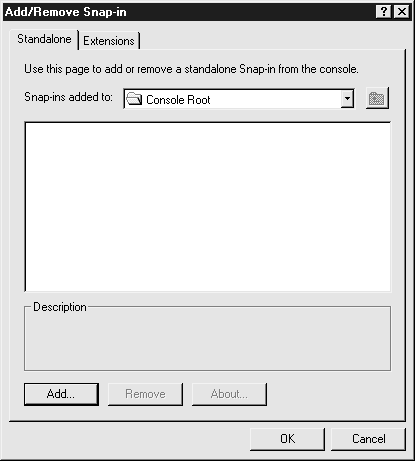
1. Откройте окно Administrative Tools (Администрирование) и найдите значок *Computer Management*.
2. Щелкните правой кнопкой мыши на значке *Computer Management* и выберите пункт Author (Авторский режим). Консоль *Computer Management* откроется в авторском режиме. Установите нужные средства в *Computer Management*, а не в Console Root (Корень консоли).

Для создания новой консоли выполните следующие действия.

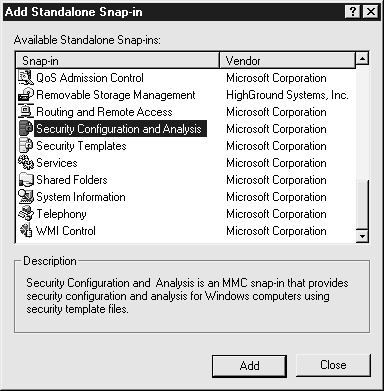
1. В меню Start (Пуск) выберите Run (Выполнить).
2. Запустите исполняемый файл MMC, напечатав mmc.exe в диалоговом окне Run. Откроется пустое окно консоли в авторском режиме (см. рисунок).



1. Откройте меню Console (Консоль) и выберите Add/Remove Snap-in (Добавить/удалить оснастку), чтобы открыть диалоговое окно, показанное на рисунке ниже. Нажмите на кнопку Add (Добавить). Откроется перечень Snap-in Selection (Выбор оснастки).



1. В списке, изображенном на рисунке ниже, выберите Security Configuration And Analysis (Анализ и настройка безопасности), после чего нажмите на кнопку Add (Добавить). Повторите процедуру для консольного средства Security Templates (Шаблоны безопасности). Закройте окно Snap-in (Оснастка), и оснастка будет добавлена в консоль.



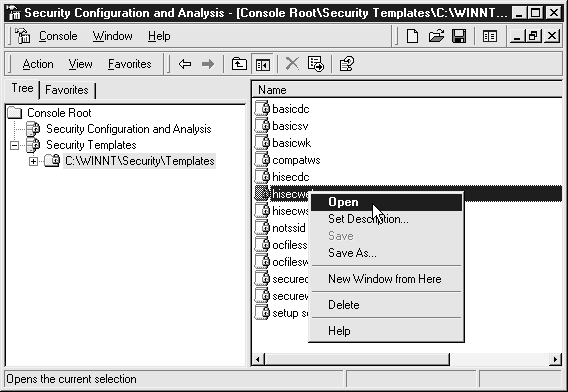
1. Нажмите на OK, чтобы закрыть диалоговое окно и сохранить изменения. Если вы создали новое консольное средство, сохраните его посредством присвоения имени при закрытии консоли. Оно будет добавлено в папку Administrative Tools (Администрирование) в меню Start (Пуск).

##### Изменение и применение шаблонов безопасности

Добавленные в консоли MMC оснастки Security Templates и Security Configuration and Analysis используются для изменения и применения параметров шаблона к серверу.

Для проверки и изменения настроек шаблона откройте его с помощью оснастки Security Templates. Выполните следующие процедуры.

1. Откройте консоль MMC, содержащую оснастку Security Templates (Шаблоны безопасности).
2. Щелкните на оснастке для отображения вложенных элементов. Щелкните на папке Security Templates для отображения шаблонов, находящихся в папке. Дважды щелкните на шаблоне с именем hisecweb (или щелкните на нем правой кнопкой мыши и выберите Open), чтобы открыть его.

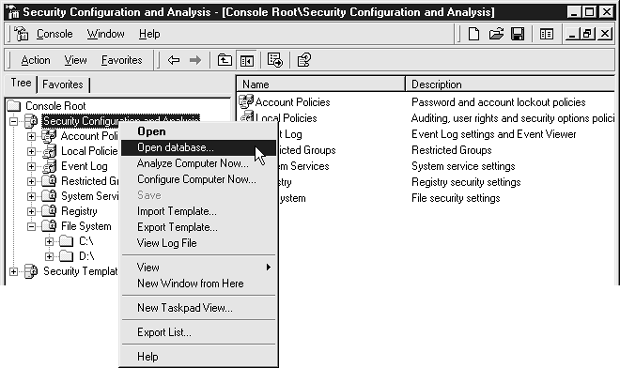


1. Сохраните шаблон под новым именем, чтобы можно было изменять его параметры. Щелкните правой кнопкой мыши на значке hisecweb и выберите Save As (Сохранить как). Укажите нужное имя и нажмите на кнопку Save (Сохранить). После этого в папке шаблонов появится файл новой политики безопасности.

Для просмотра и редактирования новой политики безопасности найдите соответствующий файл, щелкните на нем правой кнопкой мыши и выберите команду Open (Открыть), чтобы отобразить параметры политики в правой области окна MMC. Щелкните правой кнопкой мыши на любой политике, которую необходимо изменить, и выберите команду Change (Изменить). Таким способом изменяются любые параметры шаблонов.

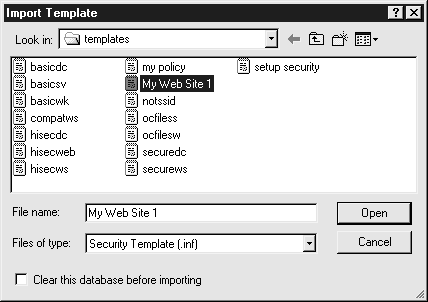
Теперь можно работать с шаблоном. Перед запуском средства конфигурирования проведите сопоставление созданных настроек шаблонов и текущих параметров сервера для выяснения различий. Для этого используйте средство Security Configuration and Analysis (Анализ и настройка безопасности), которое запишет результирующие данные в файл журнала (в контексте оснастки используется термин "база данных"). Ниже приведены соответствующие инструкции.

1. В консоли MMC, содержащей оснастку Security Configuration and Analysis, щелкните правой кнопкой мыши на оснастке и выберите команду Open Database (Открыть базу данных), как показано на рисунке.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_06.gif)

[увеличить изображение](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_06.gif)

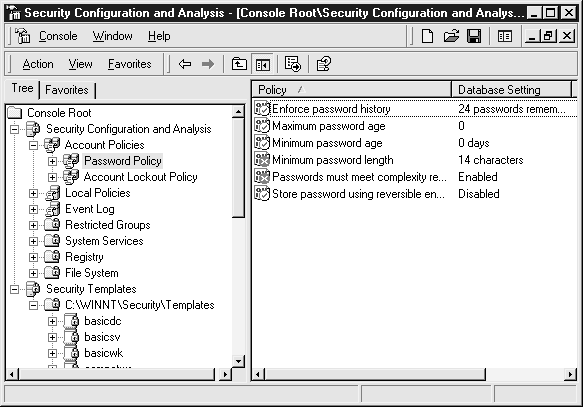
1. Откроется диалоговое окно Open Database, в котором укажите название базы данных для сохранения результатов сравнения. Введите любое предпочитаемое имя. Если в окне присутствуют файлы баз данных, созданные в результате предыдущих сравнений, их можно проигнорировать. В данном случае подойдет имя "test" (файлу базы данных будет присвоено расширение .sdb). После этого нажмите на кнопку Open.
2. Появится диалоговое окно Import Template (Импорт шаблона) (см. рисунок). В центральном окне отобразится список шаблонов. Выделите созданный шаблон и нажмите на кнопку Open, чтобы вернуться в консоль MMC. На первый взгляд никаких изменений не произойдет, однако, если новый шаблон теперь находится среди шаблонов Microsoft по умолчанию, то можно провести процедуру сравнения.



1. Откройте меню Action (Действие) в консоли MMC и выберите команду Analyze Computer Now (Анализировать компьютер). Запустится сравнение параметров шаблонов с текущими параметрами сервера, результат которого сохранится в созданной базе данных. Результирующие данные появятся в правом окне консоли. Все настройки сервера, отличные от настроек в шаблоне, отобразятся с символами "X" на своих значках (см. рисунок вверху следующей страницы) на примере политики Password Policy (Политика паролей).

**Совет**. При выполнении анализа появится запрос на расположение файла *журнала ошибок*. Этот журнал поможет в отслеживании изменений настроек. Самостоятельно выберите его место расположения.

**Совет**. При выполнении конфигурирования без всяких предупреждений изменяются параметры конфигурации, а также отключаются ненужные службы (см. ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)). Редактор данной книги сконфигурировал сетевой сервер, в результате чего отключился клиентский процесс DHCP, а это совершенно не требовалось. Поэтому внимательно просмотрите шаблон, если система не является изолированным компьютером с минимальной конфигурацией (согласно рекомендациям ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)), а потом выполняйте настройку.



1. Выполните конфигурацию. Щелкните правой кнопкой мыши на оснастке Security Configuration and Analysis в левом окне консоли MMC и выберите команду Configure Computer Now (Настроить компьютер). Начнется процедура настройки, по окончании которой конфигурация будет завершена.

Если повторно запустить сравнение, приводимое в шаге 4, на значках параметров исчезнут красные кресты, так как задействуются все настройки шаблона.

### Настройка контроля доступа к веб-серверу в Windows 2000

При просмотре настроек в шаблоне безопасности Hisecweb.inf видно, что параметры контроля доступа по большей части не определены. Необходимо самостоятельно настроить эти параметры. В списке *ACL* каждой группе или учетной записи пользователя можно присвоить любую комбинацию прав и разрешений. Это свойство делает систему защиты *Windows* 2000 очень гибкой и мощной, однако в случае неправильной настройки прав и разрешений возможно появление слабого места

#### Настройка групп и параметров администратора по умолчанию

Первое, что необходимо сделать для управления списками ACL на веб-сервере, – заблокировать возможность управления ресурсами хранилищ данных. Иными словами, следует определить, кто имеет право на доступ к хранилищу.

В Windows 2000 устанавливается набор учетных записей администраторов, групп и пользователей по умолчанию. При установке IIS эти параметры не изменяются. В [таблице 4.3](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=6" \l "table.4.3) приведены учетные записи и группы по умолчанию при установке на изолированный компьютер.

Спектр прав и разрешений администраторов очень широк (см. [табл. 4.4](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=6" \l "table.4.4)). Администратор имеет полный набор прав по управлению системой и осуществляет всесторонний контроль над ней.

|  |  |  |
| --- | --- | --- |
| Таблица 4.3. Учетные записи и группы Windows 2000 по умолчанию | | |
| **Группы по умолчанию, отображаемые в ACL** | **Группы по умолчанию, не отображаемые в ACL** | **Учетные записи по умолчанию, отображаемые в ACL** |
| Administrators (Администраторы)  Backup Operators (Операторы резервного копирования)  Guests (Гости)  *Power Users* (Опытные пользователи)  Replicator (Репликатор)  Users (Пользователи)  Everyone (Все пользователи)  Web *Anonymous Users* (Анонимные пользователи интернета)  Web Applications (При-ложения интернета) | SYSTEM (Система)  CREATOR OWNER (Владелец-создатель)  *AUTHENTICATED USERS* (Авторизованные пользователи)  ANONYMOUS LOG-IN (Анонимный вход)  BATCH (Пакетный файл)  Service (Служба)  CREATOR GROUP (Группа создателя)  *DIALUP* (Удаленный доступ)  INTERACTIVE NETWORK  TERMINAL SERVICE USERS (Пользователи службы терминала) | Administrator (Администратор).  Guest (Гость).  IUSR\_computername (IUSR\_имя\_компьютера).  IWAM\_computername (IWAM\_имя\_компьютера).  TsInternetUser. |

|  |  |
| --- | --- |
| Таблица 4.4. Полный набор прав и разрешений Windows 2000 | |
| **Право или разрешение** | **Описание** |
| *Traverse* Folder/*Execute File* (Проход по каталогам/запуск файла) | *Traverse* Folder позволяет открывать каталог для доступа к другим файлам и каталогам, независимо от разрешений, имеющихся у пользователя относительно данной папки (только для каталогов). Используется только в том случае, если у пользователя нет права *Bypass* *Traverse* Checking (Обход проверки прохода). *Execute File* позволяет запускать файлы программ (только для файлов). |
| List Folder/Read Data (Просмотр каталога/чтение данных) | List Folder позволяет просматривать имена файлов и подкаталога (только для каталогов). Read Data позволяет осуществлять считывание файлов (только для файлов). |
| Read Attributes (Считывание атрибутов) | Позволяет просматривать NTFS-*атрибуты файла*. |
| Read Extended Attributes (Считывание расширенных атрибутов) | Позволяет просматривать расширенные *атрибуты файла*, определяемые разными программами. |
| Create Files/Write Data (Создание файлов/запись данных) | Create Files позволяет создавать файлы в каталоге (только для каталогов). Write Data позволяет изменять и/или перезаписывать файлы (только для файлов). |
| Create Folders/Append data (*Создание каталогов*/присоединение данных) | Create Folders позволяет создавать папки внутри папки (только для каталогов). Append data позволяет вносить изменения в конец файла (только для файлов). |
| Write Attributes (Запись атрибутов) | Позволяет изменять атрибуты NTFS файлов (например, "только чтение" или "скрытый"). |
| Write Extended Attributes (Запись расширенных атрибутов) | Позволяет изменять расширенные *атрибуты файла*, специфичные для определенной программы. |
| Delete *Subfolders* and Files (Удаление подкаталогов и файлов) | Позволяет удалять подкаталоги и файлы независимо от присвоения подкаталогу или файлу разрешения Delete (Удаление). |
| Delete (Удаление) | Позволяет удалять файл или каталог. |
| Read Permissions (Чтение разрешений) | Позволяет просматривать разрешения, установленные для каталога или файла. |
| Change Permissions (Изменение разрешений) | Позволяет изменять разрешения для файла или каталога. |
| Take Ownership (Присвоение права собственности) | Позволяет присваивать право собственности для файла или каталога. |

Как правило, во всех учетных записях отсутствует возможность полного управления списками ACL веб-сервера, если только пользователь не наделяется полномочиями администратора. Даже в этом случае его полномочия ограничиваются некоторым неполным набором администраторских привилегий и ресурсов. Например, веб-менеджер наделяется следующими разрешениями в корневом каталоге диска с содержимым веб-сервера (но только для этого каталога и только на этом диске).

* Modify (Изменение). Внесение изменений в каталог.
* Read & Execute (Чтение и выполнение). Запуск исполняемых программ.
* List Folder Contents (Просмотр содержимого каталога). Просмотр перечня файлов в каталогах.
* Read (Чтение). Просмотр файлов данных в каталоге.
* Write (Запись). Сохранение новых файлов в каталоге.

Этот набор разрешений включает практически все функции всестороннего контроля над системой, за исключением некоторых. В [таблице 4.5](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=6" \l "table.4.5), взятой из документации Microsoft по IIS, отражены отличия прав и разрешений веб-менеджера от полномочий, позволяющих полностью управлять системой.

Учетные записи других пользователей веб-сервера (не являющихся менеджерами или администраторами), как правило, являются довольно ограниченными и обычно соответствуют лишь разрешениям на чтение (как при *анонимном доступе*).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Таблица 4.5. Подкатегории разрешений в сравнении с полным контролем | | | | | |
| **Разрешения полного контроля** | **Изменение** | **Чтение и выполнение** | **Просмотр содержимого папки** | **Чтение** | **Запись** |
| Проход по папкам/Выполнение файла | Описание: \surd | Описание: \surd | Описание: \surd |  |  |
| Просмотр папки/Чтение данных | Описание: \surd | Описание: \surd | Описание: \surd | Описание: \surd |  |
| Чтение атрибутов | Описание: \surd | Описание: \surd | Описание: \surd | Описание: \surd |  |
| Чтение расширенных атрибутов | Описание: \surd | Описание: \surd | Описание: \surd | Описание: \surd |  |
| Создание файлов/Запись данных | Описание: \surd |  |  |  | Описание: \surd |
| Создание папок/Присоединение данных | Описание: \surd |  |  |  | Описание: \surd |
| Запись атрибутов | Описание: \surd |  |  |  | Описание: \surd |
| Запись расширенных атрибутов | Описание: \surd |  |  |  | Описание: \surd |
| Удаление подпапок и файлов |  |  |  |  |  |
| Удаление | Описание: \surd | Описание: \surd |  |  |  |
| Чтение разрешений | Описание: \surd |  | Описание: \surd | Описание: \surd | Описание: \surd |
| Изменение разрешений |  |  |  |  |  |
| Присвоение прав владения |  |  |  |  |  |

##### Отключение прав на администрирование хранилища для группы Everyone

Один из параметров безопасности по умолчанию в Windows 2000 и IIS создает уязвимое место в настройках устройств хранения данных, так как группе Everyone (Все пользователи) при установке присваиваются права полного контроля по умолчанию. Следует отключить для этой группы права полного контроля и управления устройствами сервера.

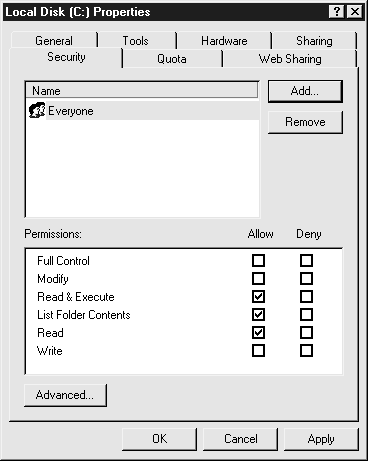
Группа Everyone состоит из множества пользователей, включая анонимных, поэтому данный параметр предоставляет полномочия слишком большому кругу пользователей. Такими правами на доступ к серверу обладают только администраторы или пользователи, ответственные за работу сервера.

Если вы создали отдельный раздел для веб-содержимого, то придется выполнить процедуру отключения прав для группы Everyone на нескольких дисках. Ниже приведены соответствующие инструкции.

1. Откройте Windows Explorer (Start\Accessories\Windows Explorer –Пуск\Программы\Проводник Windows) или дважды щелкните на значке My Computer (Мой компьютер) на рабочем столе и найдите устройства, с которыми будете работать.

**Совет**. Для установки разрешений на доступ и управление в корневом каталоге устройства используется консоль MMC *Computer Management* (Управление компьютером). Однако функции консоли не настолько гибки для выполнения этой задачи, как возможности Проводника Windows.

1. Щелкните правой кнопкой мыши на нужном устройстве и выберите Properties (Свойства). Появится окно *Local Disk* Properties (Свойства локального диска). Откройте вкладку Security (Безопасность).



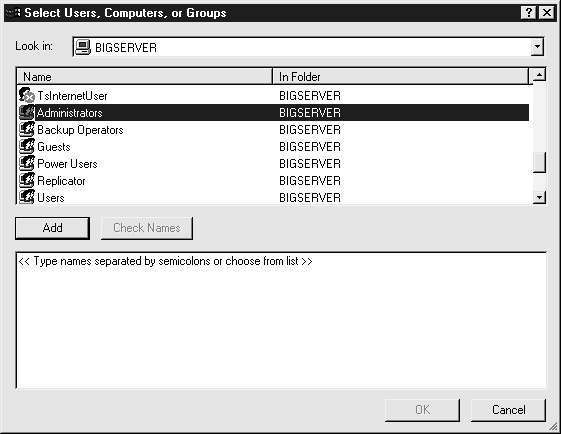
1. Удалите группу Everyone (Все пользователи), выделив ее и нажав на кнопку Remove (Удалить). Если параметры накопителей сервера изменились в процессе работы после создания групп и учетных записей в списках ACL, то их также следует удалить. После этого нажмите на кнопку Apply (Применить) для сохранения изменений в системе.
2. Повторите шаги 1 – 3 по отношению к остальным устройствам.

##### Присвоение прав полного доступа группам Administrators и System

После исключения ненужных групп из списков ACL накопителей можно добавить нужные группы и учетные записи и установить для них права и разрешения. Группы по умолчанию Administrators (Администраторы) и System (Система) добавляются в обязательном порядке. Группа System представляет операционную систему, которой, естественно, требуется доступ ко всем ресурсам компьютера. Члены группы Administrators осуществляют управление сервером. Можно добавить и другие группы, если стратегия управления и политика безопасности организации предусматривает использование вспомогательных ролей с некоторыми наборами администраторских полномочий.

Для добавления нужных групп выполните следующие шаги.

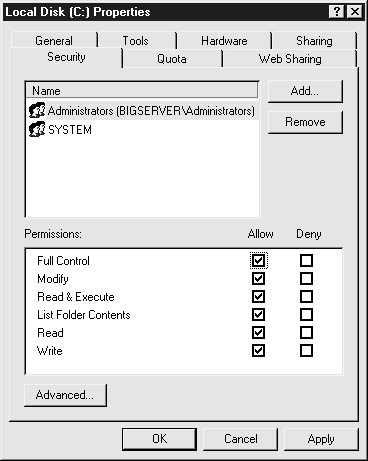
1. Откройте окно Start\Administration Tools\*Computer Management* (Пуск\Администрирование\Управление компьютером) и найдите диски компьютера в дереве ресурсов консоли или перейдите к соответствующему устройству с помощью Проводника Windows.
2. Щелкните правой кнопкой на нужном диске и в появившемся меню выберите Properties для открытия окна *Local Disk* Properties (Свойства локального диска). Откройте вкладку Security (Безопасность) и нажмите на кнопку Add (Добавить) для добавления новых групп в ACL.
3. Выделите группы Administrators и System и нажмите на кнопку Add для внесения изменения. Нажмите на OK для сохранения изменений и возврата в окно *Local Disk* Properties.



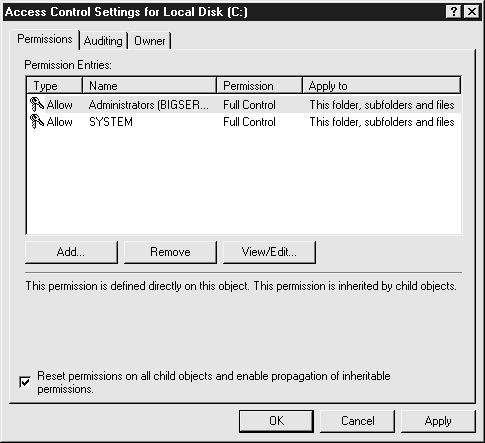
После добавления групп и учетных записей установите права и разрешения. Группам Administrators и System следует присвоить права полного доступа к устройству и настроить устройство на наследование разрешений при создании новых директорий на диске.

Ниже приведены инструкции по установке разрешений для каждой группы или учетной записи, добавленной в список ACL.

1. На вкладке Security (Безопасность) окна *Local Disk* Properties (Свойства локального диска) выделите группу Administrators в верхнем окне, чтобы отобразить права и разрешения групп в нижнем окне, как показано на рисунке.



1. Отметьте опцию Full Control Allow (Разрешить полный доступ) для включения всех разрешений для группы, затем нажмите на Apply (Применить) для сохранения изменений. Для новой учетной записи нужно включить наследование для рассматриваемого объекта.
2. Нажмите на кнопку Advanced (Дополнительно), расположенную внизу диалогового окна, чтобы отобразить окно Access Control Settings for *Local Disk* (Параметры контроля доступа для локального диска) (см. рисунок).



1. На вкладке Permissions (Разрешения) отметьте опцию *Reset Permissions On All Child Objects And Enable Propagation Of Inheritable Permissions* (Сброс разрешений на всех дочерних объектах и передача наследуемых разрешений). Нажмите на OK, чтобы сервер обновил реестр Windows 2000, записав в него новые настройки. В запросе на подтверждение нажмите на кнопку Yes (Да) для продолжения работы.

**Совет**. При выполнении процедуры может появиться сообщение об ошибке, информирующее о том, что разрешения в файле Pagefile.sys не могут быть обновлены, так как файл занят. Этот файл используется процессом виртуальной памяти компьютера, и сообщение об этой ошибке всегда отображается при включенной виртуальной памяти. Проигнорируйте эту ошибку.

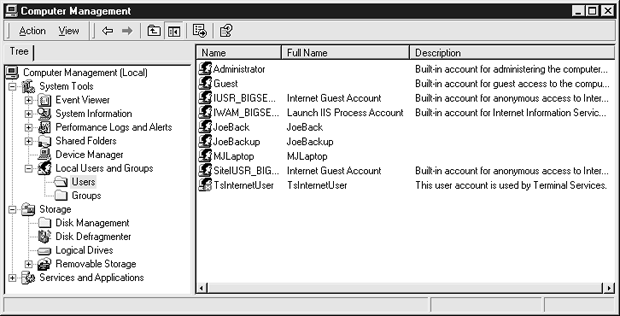
1. Повторите шаги 1 – 4 для каждого носителя информации.

**Совет**. Перед нажатием на кнопку OK для переустановки разрешений для всех объектов убедитесь, что все остальные приложения и файлы закрыты, иначе при обновлении реестра появятся сообщения об ошибках.

##### Изменение имени учетной записи Administrator и создание устойчивого пароля

Поскольку Administrator является учетной записью по умолчанию, она часто используется при проведении атак, так как о ней известно большинству хакеров. Вы будете сильно удивлены, когда узнаете о том, насколько часто эти атаки заканчивались успехом в случае недостаточно стойких паролей. Одним из способов защиты является переименование учетной записи. Следует делать пароль администратора устойчивым (т.е. пароль должен представлять собой комбинацию букв, цифр и знаков препинания длиной не менее восьми символов) для противостояния атакам грубой силы и словарным атакам, направленным на взлом парольной защиты. Обе процедуры выполнить достаточно легко.

1. В консоли MMC *Computer Management* (Управление компьютером) найдите папку Local Users and Groups (Локальные пользователи и папки) в дереве ресурсов консоли и откройте ее, чтобы отобразить показанный на рисунке список.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_13.gif)

[увеличить изображение](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_13.gif)

1. Щелкните на пункте Users (Пользователи) для отображения списка учетных записей пользователей сервера в правом окне.
2. Щелкните правой кнопкой мыши на учетной записи Administrator и выберите команду Rename (Переименовать). Присвойте учетной записи предпочитаемое имя.
3. Если применен шаблон Hisec.web, то сервер предъявит повышенные требования к стойкости парольной защиты. Даже при отсутствии принудительной политики в учетной записи Administrator следует использовать пароль с высокой степенью устойчивости. Щелкните правой кнопкой мыши на переименованной учетной записи Administrator и выберите команду Set Password (Установить пароль), чтобы изменить текущий пароль на более устойчивый. Нажмите на OK для сохранения изменений.

#### Передача прав на администрирование

Можно наделить пользователя полномочиями для выполнения операций с веб-сайтом, такими как управление содержимым или поддержка FTP-каталогов. Например, поручить ежедневную поддержку сайта веб-менеджеру, для чего создать учетную запись с правами более широкими, нежели права обычного пользователя, но все же более ограниченными, чем полномочия системного администратора. Разрешения веб-менеджера в папке содержимого веб-сервера должны позволять ему чтение, изменение и запись файлов. В IIS имеется роль по умолчанию с именем Operator, позволящая устанавливать разрешения на доступ, вести журнал, настраивать безопасность каталога и изменять документ по умолчанию.

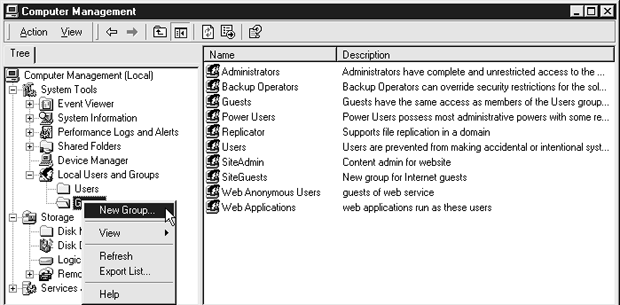
Для пользователей, выполняющих администрирование содержимого, рекомендуется создать специальную группу с учетными записями этих пользователей. С точки зрения безопасности не нужно наделять их полными правами администратора, так как столь широкие полномочия не требуются для управления содержимым сайта.

Польза от разделения процесса администрирования сайта становится видна, когда один и тот же сервер используется для управления несколькими веб-сайтами. Это позволяет организациям распределять работу по управлению сайтами, не предоставляя ни одной группе пользователей полного контроля над всеми сайтами сервера и не наделяя их без особой надобности всесторонними полномочиями.

##### Создание группы распределенного администрирования

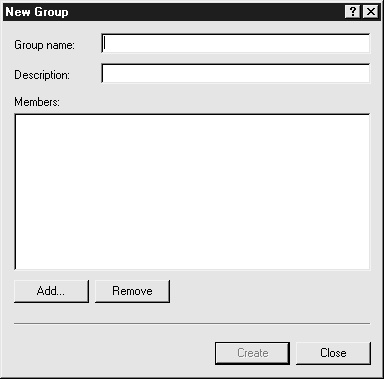
Для создания группы распределенного администрирования выполните следующие шаги.

1. Откройте консоль MMC *Computer Management* (Управление компьютером) и в дереве ресурсов консоли найдите папку Local Users and Groups (Локальные пользователи и группы), после чего откройте ее, чтобы развернуть список, как показано на рисунке. Щелкните правой кнопкой мыши на папке Groups (Группы) и выберите команду New Group (Создать группу).

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_14.gif)

[увеличить изображение](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_14.gif)

1. В появившемся диалоговом окне New Group (Создание группы) (см. рисунок) присвойте группе имя. Укажите любое желаемое имя. Введите требуемое описание (например, описание "Siteadmin" говорит о том, что группа предназначена для администрирования сайта на сервере с одним сайтом). Если на сервере работают несколько сайтов, в названии группы укажите имя сайта.



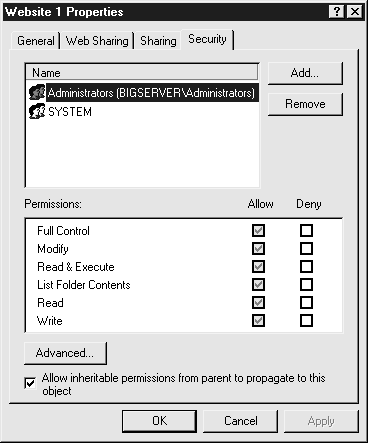
1. В окне Members (Члены) укажите пользователей, которые будут обладать полномочиями управления. Если сервер находится в сети интранет, то в одном из доменов выберите *имя учетной записи* пользователя в списке учетных записей, отображаемом в этом окне. В этом списке имена учетных записей будут отсутствовать, если сервер изолирован. Ничего страшного в этом нет, так как при создании учетных записей можно присвоить учетную запись созданной группе.
2. Нажмите на кнопку Create (Создать) и закройте окно.

##### Присвоение прав и разрешений группе распределенного администрирования

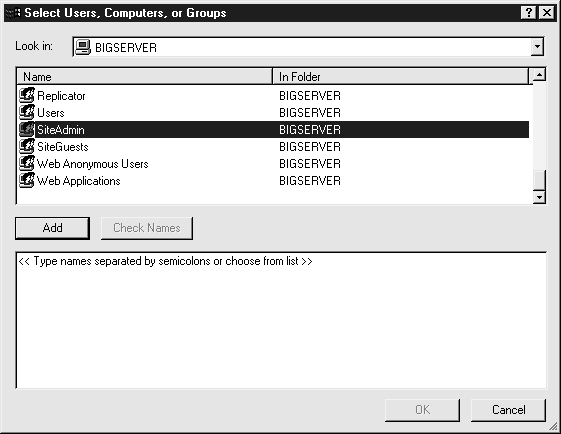
Минимальный набор прав для менеджера сайта – это разрешения на доступ к каталогу для изменения папок с информацией веб-сайта. Вероятно, нужно наделить некоторыми полномочиями и пользователей, работающих под контролем менеджера. Если членам группы распределенного администрирования нужны полные права операторов IIS по умолчанию, используйте MMC Interent Services Manager (Диспетчер служб интернета) для добавления группы в список ACL Operators (Операторы). Для более ограниченного набора прав настройте их непосредственно в списках ACL Windows 2000.

Выполните следующие процедуры для присвоения прав и разрешений в локальном списке ACL сервера.

1. С помощью Проводника Windows найдите корневой каталог содержимого веб-сайта в окне My Computer (Мой компьютер).
2. Щелкните на нем правой кнопкой мыши, выберите Properties (Свойства), чтобы открыть диалоговое окно, откройте вкладку Security (Безопасность), после чего появится окно настроек Properties (см. рисунок).



1. На вкладке Security (Безопасность) отображены группы Admini-strators и System, которым ранее были присвоены полные разрешения на доступ ко всему жесткому диску. Теперь, находясь в корневом каталоге папок содержимого, добавьте новую группу с правами на доступ к ним.
2. Нажмите на кнопку Add (Добавить), чтобы открыть диалоговое окно Select Users, Computers, or Groups (Выбор пользователей, компьютеров или групп) (см. рисунок). Прокрутите вниз список групп, чтобы отобразить новую группу администрирования, созданную для управления содержимым сайта. Выберите эту группу и нажмите на кнопку Add (Добавить).



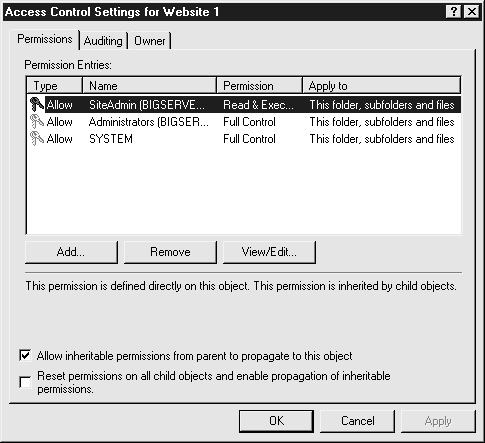
1. Нажмите на OK, чтобы сохранить изменения и закрыть окно. Вы вернетесь в диалоговое окно Properties для корневого каталога веб-сайта.
2. В окне Properties корневого каталога в списке ACL появилась новая группа администрирования. При ее выделении отобразятся свойства, приписанные этой группе по умолчанию (убедитесь, что выделена нужная группа). Этих разрешений, по умолчанию установленных в IIS, недостаточно для управления содержимым сайта, поэтому расширьте их.
3. Для добавления возможности изменения и записи данных отметьте опции разрешений Modify (Изменение) и Write (Запись). Нажмите на кнопку Apply (Применить) для сохранения изменений.

**Предупреждение**. В левом нижнем углу диалогового окна Properties корневого каталога веб-сайта (см. шаг 2) находится опция Allow Inheritable Permissions From Parent To *Propagate* To This Object (Разрешить наследование этим объектом разрешений от *родительских объектов*). Убедитесь, что она отмечена. Данный параметр не относится к учетным записям; он влияет на всю директорию в целом. При отключении наследуемых разрешений все учетные записи в *родительских каталогах* будут игнорироваться. Также будут игнорироваться права учетных записей Administrators и System, с помощью которых присваиваются права полного доступа к *разделу диска*. Отменять эти права сейчас не требуется.

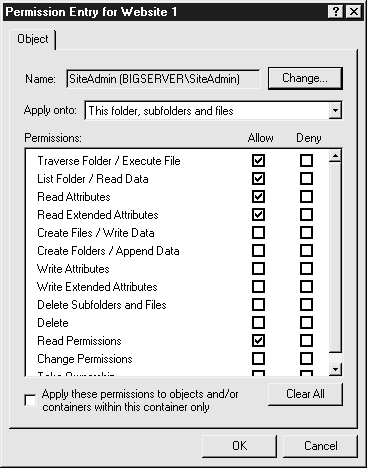
Повторите указанные шаги для домашнего каталога каждого из веб-сайтов сервера, если эти процедуры соответствуют тем полномочиям, которыми наделяются менеджеры веб-содержимого. В зависимости от политики безопасности можно присваивать дополнительные права и разрешения профилям менеджеров. В таблицах [4.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=1" \l "table.4.1), [4.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=3" \l "table.4.2) представлен перечень остальных разрешений, присваиваемых или отключаемых в группах распределенного администрирования.

Ниже приведены процедуры для изменения подкатегорий разрешений Windows.

1. Нажмите на кнопку Advanced (Дополнительно) внизу вкладки Security (Безопасность) окна домашнего каталога веб-сайта (см. шаг 2 предыдущей процедуры). Откроется новое диалоговое окно Access Control Settings (Параметры контроля доступа), показанное на рисунке. Внесите изменения в настройки на вкладке Permissions (Разрешения) данного окна.



1. В левом нижнем углу находятся две опции, относящиеся ко всем учетным записям в данном каталоге. Выполните следующие действия, если они *соответствуют политике безопасности* организации.
   * Отметьте опцию Allow Inheritable Permissions From Parent To *Propagate* To This Object (Разрешить наследование этим объектом разрешений от *родительских объектов*), чтобы учетные записи, содержащие права на *родительские каталоги* данной учетной записи, передавали по наследству свои права этой учетной записи.
   * Отметьте опцию Reset Permissions On All Child Objects And Enable Propagation Of Inheritable Permissions (Сброс разрешений на всех дочерних объектах и передача наследуемых разрешений). Это обеспечит применение ко всем *вложенным каталогам* разрешений, присвоенных учетной записи в данном каталоге.
2. В списке ACL выберите группу, для которой нужно изменить параметры прав доступа, после чего нажмите на кнопку View/Edit (Просмотр/Изменение).
3. Отобразится полный список прав и разрешений Windows 2000, как показано на рисунке ниже. Выберите нужные права и разрешения, отметив соответствующие опции. После этого нажмите на OK, чтобы сохранить изменения и выйти из окна.



**Совет**. Обратите внимание на опцию Apply These Permissions To Objects And/Or Containers With This Container Only (Применять эти разрешения к объектам и/или приложениям только внутри данного родительского приложения). В терминологии Windows 2000 эта опция сохраняет вносимые изменения в группу администрирования только в рамках приложения Active Directory, если сервер находится в домене Windows. При отсутствии в сети доменов данную опцию использовать нельзя.

1. Нажмите на OK, чтобы сохранить изменения и закрыть окно. Подтвердите действия в появившемся диалоговом окне, нажав на кнопку Yes (Да) для продолжения работы.

#### Изменение настроек по умолчанию для учетных записей пользователей

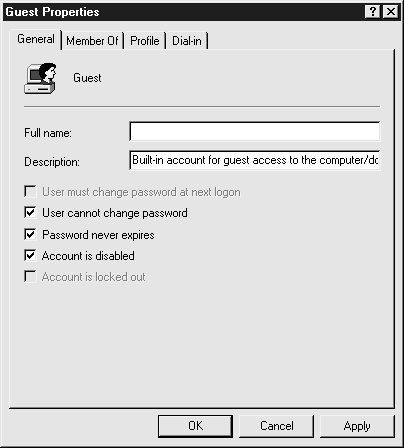
Учетные записи по умолчанию, устанавливаемые при инсталляции Windows 2000 и IIS, следует проверить на соответствие политике безопасности и адаптировать при необходимости. Ниже приведены соответствующие рекомендации.

##### Отключение и игнорирование прав и разрешений учетной записи Guest Windows 2000

Windows 2000 всегда устанавливает учетную запись Guest (Гость) по умолчанию. При правильной установке IIS учетная запись Guest должна быть отключена. Убедитесь, что это так, если вы обновили систему с Windows NT или преобразовали имевшийся сервер Windows 2000 в веб-сервер.

Для проверки состояния учетной записи Guest выполните следующие шаги.

1. В консоли *Computer Management* (Управление компьютером) найдите папку Local Users and Groups (Локальные пользователи и группы) в дереве ресурсов. Откройте ее, затем откройте папку Users (Пользователи) для отображения имен всех учетных записей пользователей в правом окне.
2. Если гостевая учетная запись отключена, то на ее значке будет изображен красный крестик.
3. Если учетная запись Guest не отключена, щелкните на ней правой кнопкой мыши и выберите пункт Properties (Свойства). Откроется диалоговое окно, показанное ниже. Отметьте опцию Account Is Disabled (Учетная запись отключена), после чего нажмите на OK для сохранения изменений и закрытия окна.



##### Обеспечение безопасности группы Guest в Windows 2000

Группа Guest (Гость) по умолчанию устанавливается и в Windows 2000. Следует внимательно следить за настройками гостевых учетных записей. Учетная запись Windows 2000 Guest всегда входит в группу Guest, как и некоторые другие учетные записи по умолчанию.

Как и учетная запись Guest, группа Guest часто подвергается атакам хакеров, знающих о ее существовании. Атаки хакеров обычно основаны на возможности проникновения в систему, так как права и разрешения группы Guest по умолчанию настроены некорректно с точки зрения безопасности и позволяют использовать одну из учетных записей для получения доступа.

Высокоэффективная защита против атак через учетную запись Guest заключается в ее удалении из группы Guest. Но не удаляйте ее сразу. Учетная запись Internet Guest (IUSR\_ *%имя компьютера%* ) необходима для реализации анонимного входа. Вместо удаления ее следует переименовать и переместить. Перед тем как предпринимать дальнейшие действия, прочтите два следующих раздела.

##### Обеспечение безопасности учетной записи Internet Guest для анонимного входа в систему

На большей части сайтов в интернете, используемых для маркетинга и распространения информации, не нужна аутентификация пользователей, так как все посетители считаются легальными. Вместо аутентификации используется анонимный вход, о котором вкратце говорилось в ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521). Анонимный вход представляет собой автоматическую аутентификацию пользователей при помощи общей учетной записи с именем IUSR. (В списке ACL сервера она значится как IUSR\_ *%имя компьютера%*.) Эту учетную запись называют гостевой записью интернета.

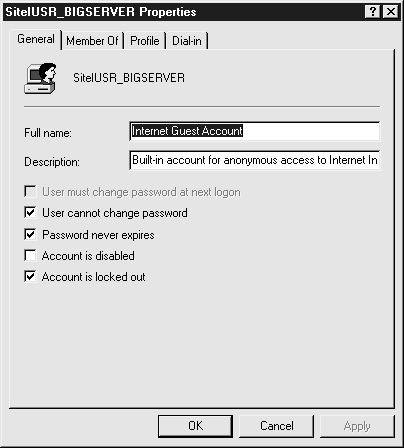
**Важно**. При использовании анонимного входа (например, если веб-сайт находится во внутренней сети, и нужна аутентификация всех пользователей без исключения) убедитесь, что учетная запись AnonymousGuest (Анонимный гость) не выбрана на вкладке IIS *Directory Service* (Служба каталогов IIS), и отключите ее.

Учетная запись Internet Guest (Гостевая учетная запись интернета) имеет ограниченные разрешения, которыми можно смело наделять всех посетителей сайта. Для обеспечения максимальной безопасности учетные записи должны содержать только разрешение Read (Чтение) в некоторых каталогах веб-сайта.

Рекомендуется создать новую учетную запись Internet Guest. Во-первых, уменьшается опасность использования учетной записи по умолчанию при попытке атаки. Во-вторых, на данном этапе при перезагрузке Windows 2000/IIS сбрасываются некоторые настройки, о которых вы узнаете далее. В случае изменения учетной записи Internet Guest внесенные изменения сбрасываться не будут.

Для создания новой учетной записи Internet Guest выполните следующее.

1. Создайте новую группу, которой будет принадлежать учетная запись. Откройте консоль MMC *Computer Management* (Управление компьютером).
2. Найдите папку Local Users and Groups (Локальные пользователи и группы) в дереве ресурсов и откройте ее, чтобы развернуть вложенный список. Щелкните правой кнопкой мыши на папке Groups (Группы) и выберите New Group (Создать группу).
3. В диалоговом окне New Group присвойте группе название. Укажите любое желаемое имя. Имя "Siteguests" будет достаточно информативным. Нажмите на кнопку Create (Создать) для сохранения новых настроек группы.
4. Переименуйте учетную запись IUSR. Вернитесь в консоль MMC *Computer Management*, щелкните на папке Users (Пользователи) и найдите учетную запись IUSR в правом окне консоли. Щелкните на ней правой кнопкой мыши и выберите команду Rename (Переименовать). Присвойте учетной записи имя, например, SiteIUSR\_ *%имя сервера%*.
5. Настройте параметры учетной записи и включите ее в только что созданную группы Guest. Щелкните правой кнопкой мыши на учетной записи и выберите команду Properties.
6. Убедитесь, что на вкладке General (Общие) диалогового окна Properties отмечены следующие опции: User Cannot Change Password (Пользователь не может сменить пароль) и Password Never Expires (Срок действия пароля не ограничен) (см. рисунок).



1. Откройте вкладку Member Of (Член группы) и удалите учетную запись из группы Guests. Затем добавьте ее в новую группу "Siteguests". Не допускайте, чтобы эта учетная запись являлась членом какой-либо другой группы.

**Совет**. При необходимости можно удалить группу Web Anonymous (Анонимные пользователи интернета). Специалисты в области информационной безопасности, как правило, оставляют ее в качестве обманного маневра (убедитесь, что отключены все разрешения для данной группы).

1. Нажмите на OK, чтобы сохранить изменения и закрыть диалоговое окно.

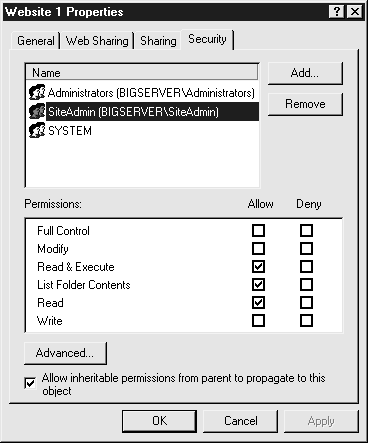
##### Права на доступ к каталогу для записи Internet Guest

После переименования Internet Guest (Гостевой учетной записи интернета) и включения ее в новую группу убедитесь, что у нее есть доступ к домашнему каталогу веб-сайта, и дважды проверьте ее разрешения насоответствие гостевой учетной записи интернета. Необходимо, чтобы все было максимально корректно. Если у записи Internet Guest нет прав доступа, веб-браузеры (и, соответственно, пользователи) не смогут открывать страницы для просмотра. Если ей присвоено слишком много разрешений, то считайте, что создано потенциально уязвимое место.

Основным разрешением для Internet Guest на сайте со статическими веб-страницами является разрешение на чтение корневого каталога, в котором они расположены. При использовании на сайте *динамических страниц* и сценариев включите разрешение Read & Execute (Чтение и выполнение) в каталоге сценариев. Ни в коем случае нельзя включать разрешение Write (Запись) в каком бы то ни было месте системы!

С точки зрения безопасности учетных записей Internet Guest рекомендуется вернуться в корневой каталог раздела, содержащего веб-сайт, запретить все разрешения, после чего по отдельности включить нужные разрешения. Ниже приведены инструкции для запрета всех разрешений.

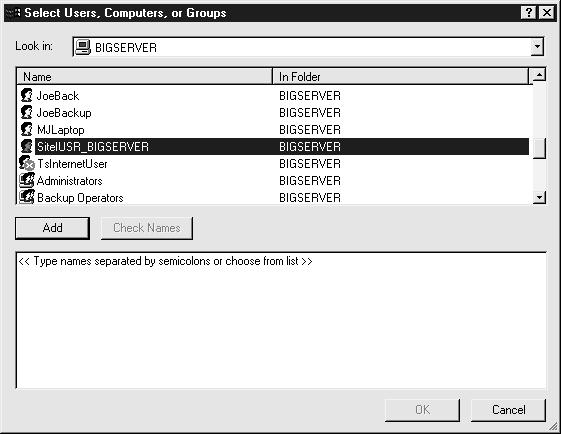
1. С помощью Проводника Windows или окна My Computer (Мой компьютер) найдите нужные дисковые устройства.
2. Щелкните правой кнопкой мыши на нужном диске и выберите команду Properties (Свойства). Появится окно *Local Disk* Properties (Свойства локального диска).
3. Откройте вкладку Security (Безопасность), чтобы отобразить учетные записи в ACL (см. рисунок). Нажмите на кнопку Add (Добавить) и добавьте переименованную учетную запись Internet Guest, которую вы только что создали.



1. Отметьте поля Deny (Запретить) для всех разрешений доступа. По завершении работы появится диалоговое окно подтверждения, в котором следует нажать на кнопку Yes (Да) для продолжения работы.
2. Повторите эти шаги для всех разделов накопителей веб-сервера.

Для присвоения учетной записи Internet Guest разрешений на отдельные каталоги сайта выполните следующие шаги.

1. Перейдите к корневому каталогу веб-сайта, содержащему статические веб-страницы, щелкните на нем правой кнопкой мыши, после чего выберите команду Properties (Свойства).
2. В окне Properties откройте вкладку Security (Безопасность).
3. В списке ACL должны находиться только следующие группы и учетные записи: Administrators (Администраторы), SYSTEM (Система) и созданная группа распределенного администрирования (это зависит от того, какие права имеются на сервере после изменений конфигурации прав). Нажмите на кнопку Add (Добавить), чтобы включить переименованную учетную запись Internet Guest в список ACL, если ее там еще нет.
4. В появившемся списке учетных записей (см. рисунок) выберите переименованную учетную запись. Нажмите на OK, чтобы сохранить изменения и закрыть список.



1. Вернитесь в окно Properties каталога, в списке ACL которого теперь присутствует учетная запись Internet Guest. Выделите ее и отметьте опцию Read (Чтение) для включения соответствующего разрешения. Отключите все остальные опции без исключения. Нажмите на кнопку Apply (Применить), чтобы сохранить изменения.

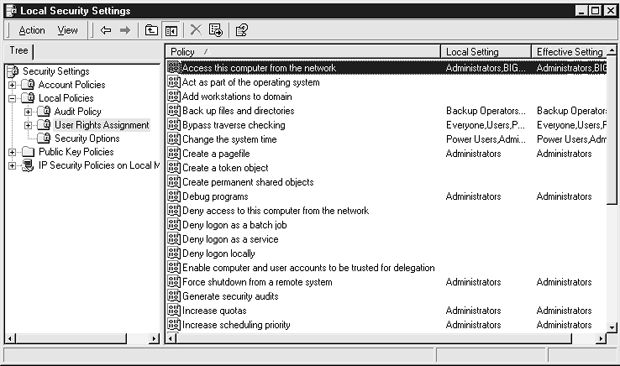
При использовании на сайте *динамических страниц* и сценариев повторите эти процедуры для каталога сценариев и установите разрешения Read & Execute (Чтение и выполнение). При этом автоматически отметятся опции Read (Чтение) и List Folder Contents (Просмотр содержимого каталога), но все остальные опции следует отключить.

##### Удаление записи Internet Guest из локальной политики безопасности

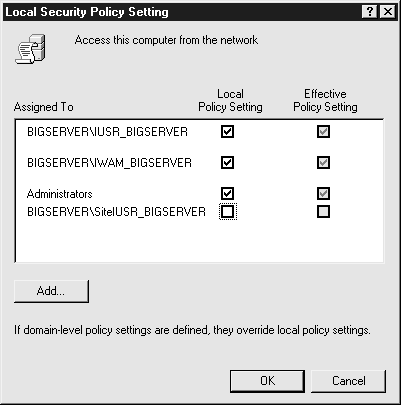
По умолчанию при создании учетная запись Internet Guest наделяется правами "доступ к данному компьютеру из сети" и "вход в систему в качестве пакетного задания". Однако эти права присваиваются только администраторам или выполняемым ими сценариям. Теперь учетная запись Internet Guest используется для анонимного входа, поэтому следует удалить эти права из локальной политики безопасности Windows 2000.

Выполните следующие действия.

1. Откройте окно My Computer\Control Panel\Administrative Tools (Мой компьютер\Панель управления\Администрирование), затем дважды щелкните на значке Local *Security Policy* (Локальная политика безопасности).
2. Разверните список в элементе Local Policies (Локальные политики) дерева Console (Консоль), щелкните правой кнопкой мыши на папке User Rights Assignment (Присвоение прав пользователей), выберите команду Open (Открыть) (или дважды щелкните на элементе, чтобы открыть его). В правом окне консоли отобразятся параметры политик присвоения прав, как показано на рисунке.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_24.gif)

1. Щелкните правой кнопкой мыши на параметре, который необходимо изменить, и выберите Security (Безопасность). Откроется диалоговое окно Local *Security Policy* (см. рисунок) с параметрами для выбранной политики. Права включаются и выключаются при помощи соответствующих опций. Отключите опцию для переименованной учетной записи Internet Guest и для любых ссылок на прежние гостевые учетные записи интернета.



1. Нажмите на OK для сохранения изменений и выхода из диалогового окна.

### Настройка атрибутов и параметров сайта IIS

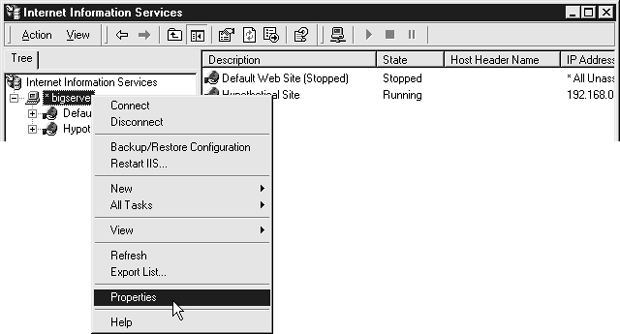
Поздравляем! Работа почти закончена! Самое сложное уже позади. Вы повысили степень защищенности учетной записи *Administrator*, усилили *контроль доступа* на жестких дисках сервера, осуществили распределение полномочий администрирования на веб-менеджеров, обеспечили защиту учетной записи *Internet* *Guest*. Теперь нужно настроить дополнительные параметры в свойствах безопасности *IIS* перед развертыванием веб-сайта.

#### Параметры безопасности IIS

Настройка дополнительных параметров сайта (или сайтов) IIS осуществляется через консоль MMC Internet Services Manager (Диспетчер служб интернета). Эта процедура выполняется последовательно для каждого сайта или одновременно для всех сайтов сервера через настройки Master Properties (Главные свойства). Если параметры каждого сайта настраиваются по очереди, следует повторить каждую процедуру для всех имеющихся сайтов.

##### Главные свойства

Откройте вкладку Security Properties Master (Главные параметры безопасности) консоли MMC Internet Services Manager (Диспетчер служб интернета) окна Adinistration Tools (Администрирование). Затем в дереве консоли щелкните правой кнопкой мыши на сайте сервера (не на веб-сайте), который необходимо настроить, и в появившемся меню выберите Properties (Свойства) (см. рисунок).

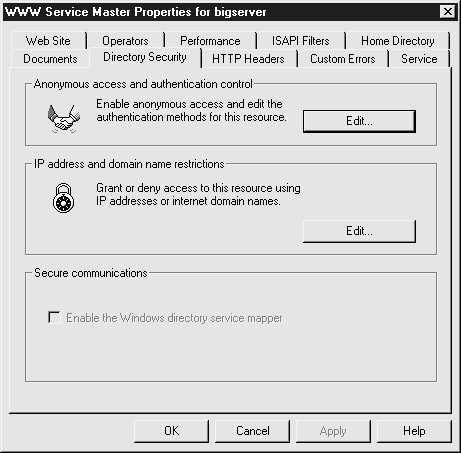
[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_26.gif)

Окно Master Properties (Главные свойства) содержит десять вкладок, предназначенных для изменения различных параметров сайта. Для нескольких сайтов придется настроить параметры каждого отдельно.

##### Настройка параметров анонимного доступа на веб-сайте IIS

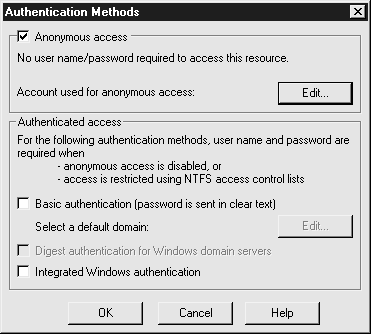
Настройки для учетной записи Internet Guest подготовили ее для среды интернета. Теперь укажите в IIS необходимость *анонимного доступа*. Это можно было сделать при укреплении сервера, однако рекомендуется еще раз проверить соответствующие настройки. Кроме того, если учетная запись переименована, следует указать новое имя.

Для включения *анонимного доступа* откройте вкладку Directory Security (Безопасность папки) (см. рисунок), позволяющую настраивать *анонимный доступ*, контроль аутентификации, ограничения по IP-адресу и имени домена. В этой вкладке имеется затемненная область *Secure Communications* (Безопасные соединения). Она используется для настройки шифруемого соединения между сервером и веб-клиентами, осуществляемого с помощью VPN или SSL. На изолированном сервере шифрование настраивается для каждого сайта в отдельности, а не через окно Master Properties (Главные свойства). Процесс шифрования рассмотрен в ["Применение шифрования"](https://www.intuit.ru/studies/courses/1002/122/lecture/3531).



Выполните следующие процедуры.

1. Нажмите на кнопку Edit (Изменить) в панели Anonymous Access and Authentication Control (Контроль *анонимного доступа* и аутентификации) вкладки Directory Security (Безопасность папки), чтобы открыть диалоговое окно *Authentication Methods* (Методы аутентификации), показанное на рисунке. Отметьте опцию Anonymous Access (*Анонимный доступ*).



**Совет**. Другие параметры методов аутентификации используются во внутренней сети, содержащей только клиентов Windows. В среде со смешанным набором операционных систем эти параметры имеют несколько принципиальных ограничений. Альтернативные методы аутентификации приведены в ["Приложение D. Методы аутентификации Microsoft IIS"](https://www.intuit.ru/studies/courses/1002/122/lecture/24710).

1. Нажмите на кнопку Edit (Изменить) в верхней части диалогового окна, чтобы открыть окно *Anonymous User* Account (Учетная запись анонимных пользователей) и выбрать учетную запись для использования в качестве гостевой учетной записи интернета. Нажмите на кнопку Browse (Обзор), чтобы отобразить список ACL сервера и выбрать нужную учетную запись.
2. Опция Allow IIS To Control Password (Разрешить *управление паролями* IIS) используется, если нужно применить несколько методов аутентификации с использованием служб IIS (см. ["Безопасность FTP, NNTP и других служб IIS"](https://www.intuit.ru/studies/courses/1002/122/lecture/3535)). Сейчас следует оставить эту опцию неотмеченной.
3. Нажмите на OK для сохранения изменений и выхода из диалогового окна.

##### Фильтры IP-адресов и доменов

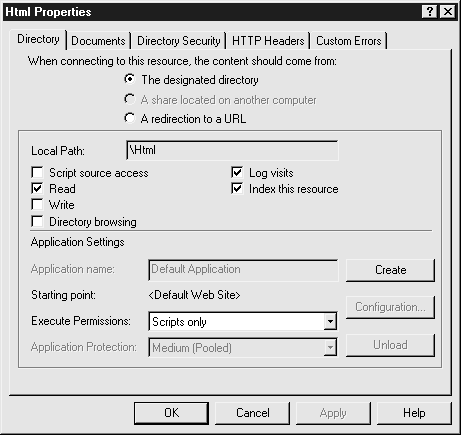
На вкладке Directory Security (Безопасность папки) присутствуют еще две категории параметров безопасности. Область *Secure Communications* (Безопасные соединения) позволяет настраивать сертификаты, используемые в технологиях VPN и SSL (см. ["Применение шифрования"](https://www.intuit.ru/studies/courses/1002/122/lecture/3531)). Ограничения IP-адресов и доменов устанавливают правила фильтрации, налагающие запрет на доступ к сайту с определенных IP-адресов или доменов DNS (см. ["Особенности процесса разработки"](https://www.intuit.ru/studies/courses/1002/122/lecture/3527)).

##### Разрешения на доступ IIS

На вкладке Home Directory (Домашний каталог) диалогового окна IIS Security Properties (Параметры безопасности IIS) имеется набор разрешений для контроля доступа к веб-сайтам, каталогам и отдельным файлам. Это разрешениями на доступ IIS, а не Windows 2000! IIS имеет инструменты для контроля доступа поверх операционной системы Windows 2000. Эти разрешения являются глобальными и не привязаны к конкретной учетной записи или группе.

Для включения разрешений на доступ IIS щелкните правой кнопкой мыши на названии веб-сайта, каталога или файла в консоли MMC Internet Service Manager (Диспетчер служб интернета) и выберите команду Properties (Свойства).

Эти права устанавливаются при создании сайта с помощью Site Creation Wizard (Мастер создания сайта). Для изменения прав всех сайтов сервера откройте вкладку Home Directory (Домашний каталог) в окне Master Security Properties (Главные свойства безопасности) на уровне веб-сайта. Или откройте вкладку Directory (Каталог) окна Properties файла (папки) (см. рисунок), выделив узел нижнего уровня в дереве консоли Internet Services Manager (Диспетчер служб интернета).



В [таблице 4.6](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=11" \l "table.4.6) приведено описание разрешений IIS (за исключением разрешений ведения журнала, о которых пойдет речь в ["Аудит и журналы безопасности"](https://www.intuit.ru/studies/courses/1002/122/lecture/3525)). Эти элементы IIS дополняют управление доступом NTFS и в совокупности образуют сложный набор разрешений. Например, пользователь, которому запрещен просмотр домашнего каталога веб-сайта, но имеющий разрешения List (Просмотр) Windows 2000, работает в рамках наиболее ограничивающего набора разрешений (т.е. ему будет отказано в просмотре файлов в папке).

С точки зрения безопасности рекомендуется использовать наиболее ограничивающие параметры, которые, тем не менее, позволят сайту нормально функционировать.

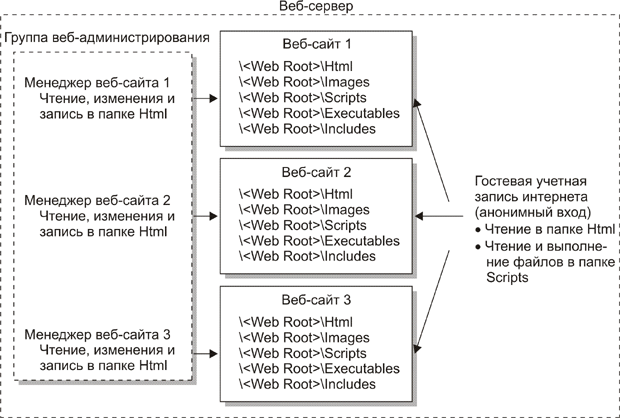
|  |  |
| --- | --- |
| Таблица 4.6. Разрешения на доступ IIS | |
| **Тип доступа** | **Описание** |
| Доступ к исходным файлам сценария | Позволяет осуществлять доступ к исходным файлам. При разрешении Read (Чтение) исходный код можно прочитать, при разрешении Write (Запись) исходный код можно записать. Под доступом к исходным файлам сценариев подразумевается доступ к коду сценариев, таких как сценарии приложения ASP. Опция недоступна, если не выбрано ни одно разрешение из пары Read (Чтение) и Write (Запись). |
| Разрешение на чтение | Позволяет осуществлять просмотр и передачу содержимого браузеру-клиенту для отображения. |
| Разрешение на запись | Позволяет клиентам с браузерами, поддерживающими возможность "PUT" стандарта HTTP 1.1, отгружать файлы на сервер или изменять содержимое файла, запись которого разрешена. "PUT" обычно не предоставляется, если администратор не включает данный тип доступа. |
| Просмотр каталогов | Позволяет клиенту просматривать все файлы каталога. Если сервер не является общим сервером FTP, опция должна быть отключена. |

#### Управление несколькими веб-сайтами

В IIS можно работать с несколькими сайтами на одном и том же компьютере. Такие сайты называются виртуальными серверами. Виртуальные серверы полезны в случае разделения информации для различных категорий пользователей. С точки зрения безопасности нужно использовать отдельный раздел диска для каждого сайта, чтобы успешный взлом хакером одного сайта не позволил ему получить доступ к информации на всех других.

При использовании виртуальных серверов поддержка учетных записей веб-менеджеров и записей анонимного входа осуществляется различными способами. Простейший и самый безопасный способ – это использование уникальной учетной записи с распределенными полномочиями Administration (Администрирование) для каждого сайта и общей учетной записи Internet Guest для всех сайтов.

Если последовать данной рекомендации, то при использовании отдельного домашнего каталога и папки с содержимым для каждого сайта за каждый набор папок будет отвечать свой веб-менеджер (см. [рис. 4.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3523?page=12" \l "image.4.2)).

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/4/files/04_30.gif)

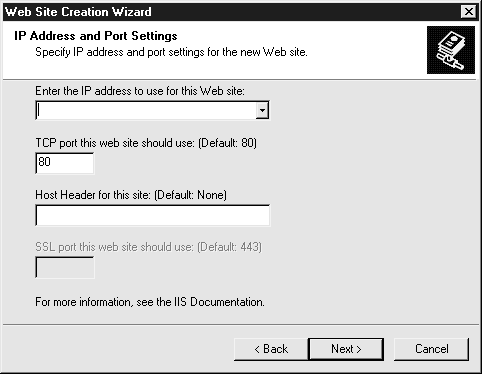
**Рис. 4.2.**Используйте общую для всех сайтов учетную запись анонимного доступа и отдельные учетные записи для управления сайтом

Такая конфигурация учетной записи позволит контролировать доступ веб-менеджеров к содержимому веб-сайта. Если всем менеджерам нужен один и тот же уровень доступа, настройте разрешения Windows 2000 на уровне группы или отдельно для каждого менеджера в соответствующих каталогах. А наличие одной учетной записи Internet Guest для всех сайтов уменьшит вероятность ошибок.

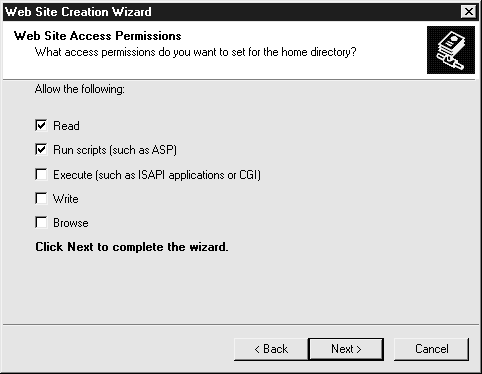
Виртуальный сервер создается при помощи консоли MMC Internet Server Manager (Диспетчер сервера интернета). В ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)говорилось, как это делается, при создании нового сайта и отключении сайта по умолчанию. Для одновременной работы нескольких сайтов создайте уникальный идентификатор для каждого сайта; с его помощью система DNS будет отправлять браузеры на соответствующие виртуальные серверы IIS. Уникальным идентификатором является альтернативное имя DNS или IP-адрес.

Процедура создания виртуального сервера состоит из следующих шагов.

1. Откройте консоль MMC Internet Services Manager (Диспетчер служб интернета).
2. Щелкните правой кнопкой мыши на сервере в дереве консоли и в появившемся меню выберите New Web Site (Создать веб-сайт). Откроется мастер для создания нового сайта.
3. Присвойте сайту название в первом окне мастера, затем нажмите на кнопку Next (Далее). В следующем окне укажите IP-адрес, номер порта



или заголовок узла. Любого из этих значений достаточно для создания уникального идентификатора сайта. При использовании уникального IP-адреса или доменного имени DNS скоординируйте свои действия с агентством интернета или администратором внутренней сети для обновления баз данных DNS.



1. В следующих окнах мастера укажите расположение домашнего каталога и присвойте разрешения доступа (см. рисунок). Укажите минимальный набор разрешений. При необходимости их можно будет изменить позже.
2. Нажмите на кнопку Finish (Готово) для создания сайта.

#### Работа с виртуальными каталогами

IIS позволяет использовать псевдонимы для реальных путей каталогов с веб-содержимым. Эти псевдонимы называются *виртуальными каталогами*. Виртуальные каталоги IIS скрывают от веб-браузеров расположение информации посредством отображения в адресах URL псевдонимов вместо реальных каталогов. Браузер воспринимает виртуальные каталоги как подкаталоги в корневом каталоге /wwwroot.

Виртуальные каталоги повышают уровень безопасности, скрывая реальные физические параметры сервера. При создании виртуального каталога для домашнего каталога сайта (для другого каталога) выполните следующее.

1. В консоли MMC Internet Services Manager (Диспетчер служб интернета) щелкните правой кнопкой на сайте, для которого создается виртуальный каталог, затем выберите команду New\Virtual Directory(Создать\Виртуальный каталог).
2. Мастер поможет создать каталог. В первом окне мастера введите нужное имя псевдонима и нажмите на кнопку Next (Далее).
3. В следующем окне введите путь к каталогу – перейдите к реальному каталогу, нажав на кнопку Browse (Обзор), затем нажмите на Next.
4. В последнем окне укажите разрешения IIS для создаваемого сайта. Еще раз нажмите на Next.
5. По окончании работы нажмите на кнопку Finish (Готово), и виртуальный каталог будет создан.

##### ПРОБЛЕМА

Виртуальные каталоги помогают защитить сайт, но они все же не защищают от атак с декодированием URL. С помощью нескольких известных эксплоитов были успешно реализованы атаки на сайты IIS с виртуальными каталогами, и злоумышленники получили доступ к структуре каталогов веб-сайта. Единственной защитой от атак с применением декодирования является обновление сервера сервис-пакетами и надстройками безопасности.

Не следует переоценивать безопасность каталогов. Применяйте к ним все способы защиты, обсуждаемые в книге, не полагайтесь на какое-то одно средство. Помните о том, что папки веб-сервера связаны с другими серверами с помощью виртуальных каталогов и создают для этих серверов потенциальные угрозы. При нарушении безопасности сервера пользователь перейдет в корневой каталог без ограничений на доступ и откроет в нем любую папку. Он сможет загрузить или удалить (изменить) любой файл или папку, псевдонимы которых находятся на веб-сайте.

Предотвратить эту опасность можно с помощью полного запрета на использование виртуальных каталогов, связанных с другими серверами. При установке связи веб-сервера с другими системами используйте методы, описанные в третьей части.

### Сводный перечень действий по настройке аутентификации учетных записей

* Отключите права администрирования накопителей для группы Everyone (Все пользователи).
* Обеспечьте полный контроль над ресурсами для групп Administrators (Администраторы) и System (Система).
* Переименуйте учетную запись Administrator (Администратор) и создайте устойчивый пароль.
* Создайте группу с распределенными полномочиями Administration (Администрирование) для управления веб-содержимым (не обязательно).
* Отключите гостевую учетную запись Windows 2000 Guest (Гость) по умолчанию и отключите права на доступ.
* Переименуйте гостевую учетную запись по умолчанию.
* Удалите права по умолчанию для учетной записи Internet Guest (Гостевая учетная запись интернета) из локальной политики безопасности.
* Установите для учетной записи Internet Guest разрешения на доступ Read Only (Только чтение).

### Перечень действий по настройке параметров сайта IIS

* Настройте сайт на разрешение *анонимного доступа* или встроенной аутентификации Windows.
* Установите разрешения контроля доступа IIS на Read Only (Только чтение) для папок с содержимым и на Read and Execute (Чтение и выполнение) для сценариев.
* Отключите возможность просмотра каталогов броузером.
* Используйте виртуальные каталоги для обеспечения дополнительной защиты сайта.

### Вопросы для закрепления

1. В чём заключается основная цель политики безопасности на веб-сервере?
2. Какие существуют ключевые параметры политики безопасности веб-сервера?
3. Какую роль играет фильтрация IP-адресов в обеспечении безопасности?
4. В чём отличие прав и разрешений в списках контроля доступа (ACL)?
5. Что такое наследование прав и разрешений, и как оно работает?
6. Чем отличаются рабочие группы от доменов в Windows 2000?
7. Как работает аутентификация в домене Windows?
8. Какие преимущества предоставляет использование Active Directory?
9. Почему важно разграничивать доступ к ресурсам с помощью прав и разрешений?
10. Что такое доверительные отношения между системами, и почему они важны?
11. Когда целесообразно использовать анонимную аутентификацию?
12. Какие инструменты Windows 2000 применяются для управления локальной безопасностью?
13. Как работает MMC и какие функции она выполняет?
14. В чём назначение утилиты IIS Lockdown?
15. Как осуществляется управление локальной безопасностью на сервере, являющемся частью домена?