

Федеральное агентство по образованию  
Государственное образовательное учреждение  
высшего профессионального образования  
Ивановский государственный химико-технологический университет

С.С.Алаева, С.П. Бобков, С.В. Ситанов

# **Администрирование в информационных сетях**

Учебное пособие

Иваново 2010

УДК 681.3

Алаева С.С., Бобков, С.П., Ситанов С.В. Администрирование в информационных системах: учеб. пособие / Иван. гос. хим.-технол. ун-т. Иваново, 2010. 52 с.

Учебное пособие посвящено изучению теоретических и практических основ администрирования в информационных системах, способов управления информационными сетями.

Подробно рассмотрены вопросы инсталляции, эксплуатации и сопровождения информационных систем. Большое внимание уделено изучению служб управления: конфигурацией и изменениями; контролем характеристик; ошибочными ситуациями; учетом и безопасностью; планирования и развития. Подробным образом освещены вопросы аудита информационных систем; функции, процедуры администрирования; объекты администрирования; методы администрирования; аппаратно-программные платформы администрирования.

Предназначено для самостоятельной работы студентов, обучающихся по направлению подготовки «Информационные системы и технологии». Кроме того, данный материал может быть полезным для студентов других специальностей и направлений.

Ил. 13. Библиогр.: 5 назв.

Печатается по решению редакционно-издательского совета Ивановского государственного химико-технологического университета.

Рецензенты:

кафедра математики, экономической теории и вычислительной техники Ивановского филиала Российского государственного торгово-экономического университета;

ст. преподаватель кафедры вычислительной и прикладной математики Ивановского государственного университета Д.В. Туртин.

Ситанов С.В., Алаева С.С., 2010  
© Ивановский государственный  
химико-технологический  
университет, 2010

## ВВЕДЕНИЕ

В настоящее время специалисты в области «Информационные системы в технике и технологиях» являются одними из наиболее востребованных на международном рынке труда, а среди категорий профессиональных работников в области информационных технологий - одними из наиболее высокооплачиваемых.

Потребность в таких специалистах возникла в связи с возрастающей ролью в современном мире информационных систем. Любая информационная система функционирует на конкретном уровне мирового хозяйства (микро-, мезо-, макро- и мегаэкономики) в муниципальных, государственных, негосударственных и международных организациях различного назначения, в органах управления, министерствах, ведомствах и подчиненных им организациях, в органах юрисдикции, юридических и адвокатских консультациях, судах, правоохранительных органах, экономических, банковских, налоговых учреждениях, учебных заведениях, общественных организациях, в ассоциациях и объединениях, на предприятиях различной организационно-правовой формы, в органах охраны природы, распределения природных ресурсов и энергоносителей, в различных отраслях хозяйства страны или региона. (Даже на небольших предприятиях ощущается потребность в информационной инфраструктуре, которая смогла бы обеспечить работу сотрудников в рамках единых информационных технологий.) Приведенный перечень и определяет потенциальное место работы выпускника этой новой специальности.

# 1. ЦЕЛИ И ЗАДАЧИ АДМИНИСТРИРОВАНИЯ ОБЪЕКТЫ АДМИНИСТРИРОВАНИЯ

Администрирование информационными системами – сложный процесс, основной целью которого является приведение информационной системы в соответствие целям и задачам предприятия или организации. Для достижения этой основной цели системное управление должно быть построено таким образом, чтобы минимизировать необходимое время и ресурсы, направляемые на управление системой и, в то же время, максимизировать доступность, производительность и продуктивность системы.

## 1.1. Обязанности системного администратора

**В обязанности системного администратора входят:**

- планирование системы;
- планирование нагрузки;
- установка и конфигурация аппаратных устройств;
- установка программного обеспечения;
- контроль защиты;
- архивирование (резервное копирование) информации;
- создание и управление счетами пользователей;
- определение и управление подсистемами;
- управление системными ресурсами;
- мониторинг производительности;
- управление лицензиями;
- документирование системной конфигурации и т.д.

## 1.2. Направления работы администраторов

Для снижения расходов на управление информационной системой и поддержку его качества обычно создают **три различные направления работы администраторов**, каждое из которых отвечает за определенные задачи управления и удовлетворение определенных потребностей пользователей.

### 1.2.1. Управление рабочими местами

Цель управления: обеспечить пользователей необходимыми вычислительными ресурсами.

Управление рабочими местами, как правило, включает в себя однообразную работу — установку и обновление приложений, перемещение пользователей и т. д. Из-за того, что пользователи могут находиться на значительном расстоянии, специалисты, выполняющие поддержку рабочих мест, пытаются решить максимальное количество проблем, не подходя к каждому рабочему месту в отдельности. Это создает потребность в средствах администрирования, которые хорошо работают в режиме удаленного доступа. Средства управления рабочим местом должны поддерживать широкий

диапазон настроек и служб рассылки, включая рассылку приложений, средства измерения и средства управления групповой политикой.

### **1.2.2. Управление центром обработки данных**

Цель управления: обеспечить доступность служб и достоверность данных.

Специфика работы диспетчеров центра обработки данных заключается в поставке большим группам пользователей большого количества централизованно предоставляемых служб работы с приложениями. Отсюда весьма жесткие требования к надежности работы этих диспетчеров и к достоверности рассылаемых пользователям приложений

### **1.2.3. Управление сетью**

Цель управления: обеспечить штатную работу сети.

Управление сетью имеет первоочередной задачей обеспечить передачу максимально возможного объема данных при хорошей достоверности, доступности и безопасности. Управление сетью в большей степени, чем центр обработки данных и управление рабочими местами, связано с текущим контролем состояния огромного числа сетевых устройств. На этом направлении весьма полезно использование диагностических средств контроля, которые предупреждают о возникновении проблем, автоматически фиксируя их по мере появления и выдавая при необходимости предупреждения.

## **1.3. Объекты администрирования**

Под объектами администрирования понимают те компоненты системы, которые нуждаются во внимании со стороны администратора. В зависимости от направления работы администратора объектами администрирования могут быть как отдельные пользователи, так и их более крупные объединения, различные сетевые устройства, а также базы данных. Рассмотрим рабочие группы и сети как объекты администрирования.

### **1.3.1. Рабочая группа**

Рабочая группа представляет собой логическое объединение компьютеров нескольких пользователей, чьи информационные потребности или деятельность взаимосвязаны, в результате чего возникает необходимость совместного использования файловых ресурсов. Обычно все компьютеры рабочей группы равноправны, в группе нет центрального компьютера, на котором сосредоточены ресурсы. Поэтому такая организация называется **одноранговой** сетью.

Сети рабочих групп существуют благодаря легкости установки и простоте обслуживания. Каждый пользователь сам управляет совместным доступом к ресурсам на своем компьютере, определяя, что будет предоставлено в общее пользование (принтер, устройство чтения компакт-дисков, жесткий диск или только отдельные файлы и каталоги) и у кого будет доступ к этому ресурсу. С

ростом сети появляются трудности- пользователей становится слишком много, соответственно возрастает количество совместно используемых ресурсов, возникают сложности с поиском нужного ресурса или с необходимостью установить разный режим доступа для разных членов рабочей группы.

Кроме того, неформальная структура рабочих групп означает отсутствие централизованного управления и администрирования. В большой рабочей группе затраты на поддержание ее работоспособности и администрирование становятся громадными, так как все действия по настройке приходится выполнять последовательно на всех компьютерах.

Для ограничения доступа используются пароли. Но с ростом одноранговой сети пароли множатся, запомнить их становится трудно, а сама система становится все более сложной. Пользователи, которым для доступа к различным ресурсам системы необходимо помнить множество паролей, начинают регулярно пользоваться одним и тем же паролем или выбирают такие, которые легко запомнить и, как следствие, легко угадать. Безопасность такой системы нарушается. Кроме того, если в системе используется удаленный доступ к сети и кто-то увольняется, переходя на работу в конкурирующую фирму, все пароли необходимо изменить, а это очень трудоемкий процесс. По этим причинам одноранговые сети непригодны для создания крупных сетей или сетей, требующих централизованного управления.

### 1.3.2. Доменная структура

Доменная структура предоставляет большую гибкость и упрощенный способ администрирования, который приемлем даже для самых крупных и сложных систем.

**Домен** – представляет собой группу компьютеров, использующих общую базу данных и общую политику безопасности. Домен включает в себя компьютер, выполняющий роль основного контроллера домена, хотя бы один компьютер, выполняющий роль резервного контроллера домена и, по крайней мере, одну рабочую станцию. В состав домена могут входить дополнительные резервные контроллеры домена, а также дополнительные серверы и рабочие станции.

Основной контроллер домена является самым важным компьютером домена. Он реализует политику безопасности домена и является основным местом хранения базы данных учетных записей.

Также можно сказать, что домен - это такая рабочая группа, в состав которой входит сервер. Она остается логическим объединением пользователей, которых связывают друг с другом не только провода, протянутые между компьютерами; другими словами - пользователей, совместно использующих общую информацию или занимающихся одним видом деятельности. Цель остается все той же: дать возможность членам группы совместно использовать информацию и таким образом облегчить им совместную работу и повысить производительность. Ключевым отличием является наличие в домене сервера,

что позволяет осуществлять администрирование и управление из единого центра.

Информационная система может состоять из одного домена или из нескольких связанных между собой доменов, как, например, корпоративная сеть, в которую входят тысячи отдельных рабочих станций, разбросанных по всему миру. В последнем случае отдельные рабочие станции объединяются в домены исходя из заданных требований доступа. Плюс концепции доменов состоит в том, что сеть легко расширяется или сужается, обеспечивая соответствующие модели доменов и различные их варианты и сочетания. Домены могут быть разделены на поддомены — произвольные имена, вводимые сетевым администратором для дальнейшего подразделения имени домена.

#### **1.4. Преимущества модели доменов**

Модель доменов обеспечивает следующие преимущества:

- 1 - гибкость при разработке конфигурации;
- 2 - централизованное администрирование сети;
- 3 - гибкость при добавлении новых пользователей и смене ограничений доступа;
- 4 - единая база данных учетных записей пользователей;
- 5 - объединенная система безопасности для всего домена;
- 6 - простота предоставления прав доступа к файлам и каталогам.

Последовательное администрирование всех компьютеров, которое необходимо выполнять в одноранговой сети, сильно ограничивает максимальный размер эффективной рабочей группы. В системе с доменами ограничения определяются только логической структурой организации. Вся компания целиком, даже крупная, может представлять собой один домен. В сети, организованной в виде домена, системный администратор может вносить в систему изменения с любого входящего в нее компьютера.

## 2. ИНСТАЛЯЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

**Цель построения всякой системы** — достижение состояния, при котором все имеющиеся объекты управления будут находиться под контролем и готовы адекватно реагировать на управляющие воздействия.

### 2.1. Планирование информационной системы

- Перед установкой системы необходимо знать ответы на следующие вопросы:
- Какие задачи по обработке информации решает информационная система?
- Сколько и какие компьютеры используются в информационной системе?
- Как построена сеть (топология, маршрутизация и т.п.)?
- Какова политика безопасности в информационной системе? и т.д.

Развертывание новой сетевой структуры целесообразно начать с создания единственного домена, который легче всего администрировать, и по мере необходимости добавлять новые домены. При этом один домен может содержать несколько географически разнесенных и администрируемых индивидуально объектов – подразделений или организационных единиц.

Для создания нескольких доменов могут быть следующие причины:

- различные требования к безопасности для отдельных подразделений;
- очень большое количество объектов;
- различные Internet-имена для доменов;
- децентрализованное администрирование сети.

После того как разработана сетевая структура организации ( т.е. создано несколько доменов или один с несколькими подразделениями и по ним распределены пользователи), следующий этап - продумать административную иерархию.

Если внутри домена создано дерево организационных единиц или подразделений, то обязанности администраторов отдельных подразделений можно распределить между определенными пользователями и группами. В этом случае уменьшается число сотрудников, которые получают полный контроль над всем доменом.

Этот процесс называется **делегированием прав администрирования**.

При модернизации устаревших систем, а также при добавлении к действующим вновь созданных объектов возникает проблема интеграции. Это означает соединение различных информационных систем в пределах одной организации или же различных организаций в одно целое. Различия в технологии и операционных системах могут сделать интеграцию очень

сложной. Стратегией для преодоления этих трудностей является одновременная разработка всей системы.

Для того чтобы в дальнейшем избежать отказов систем вследствие их недостаточной нагрузочной способности, а также для обеспечения надлежащей производительности компьютеров и емкости запоминающих устройств, следует оценить будущие потребности в их нагрузочной способности на основе прогноза. Этот прогноз должен учитывать требования к новым системам, а также текущие и прогнозируемые тенденции использования компьютеров и сетей.

## 2.2. Приемка систем

Необходимо задать критерии приемки новых систем и провести соответствующие испытания до их приемки. Для этого рассматриваются следующие пункты:

- требования к производительности и нагрузочной способности компьютеров;
- подготовка процедур восстановления и перезапуска систем после сбоев, а также планов действий в экстремальных ситуациях;
- подготовка и тестирование повседневных операционных процедур в соответствии с заданными стандартами;
- указание на то, что установка новой системы не будет иметь пагубных последствий для функционирующих систем, особенно в моменты пиковой нагрузки на процессоры (например, в конце месяца);
- подготовка персонала к использованию новых систем.

## 2.3. Учетные записи пользователей и группы

Создание учетных записей и групп занимает важное место в обеспечении безопасности информационной системы, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации компьютерной сети, разрешить или запретить им выполнение в сети определенного действия, например, архивацию данных или завершение работы компьютера. Каждый пользователь сети должен иметь в одном из доменов свою учетную запись. В учетную запись заносятся имя пользователя, пароль, различные ограничения на работу в сети.

Пользователей можно объединять в **локальные и глобальные группы**, имеющие единый набор разрешений и прав доступа. Объединение пользователей в группы позволяет изменять права доступа и разрешения для всей группы одновременно.

Например, в операционной системе Windows 2000 имеется ряд встроенных глобальных и локальных групп, на основе которых можно начинать работу по управлению правами пользователей сети. Локальная группа существует и сохраняет свои разрешения только в том домене, в котором она создана, в то

время как глобальная группа находится в одном из доменов, но сохраняет разрешения во всех доменах-доверителях.

Хорошо продуманная структура групп может сэкономить время на администрирование, а также предотвратить нежелательный доступ.

## **2.4. Имена доменов**

У каждого компьютера в сети должно быть уникальное имя. Например – КОМ-1. Рекомендуется использовать не более 15 символов для имени компьютера. Если на компьютере планируется использовать выход в глобальную сеть Интернет и установлен сетевой протокол TCP/IP, то имя компьютера может содержать до 63 символов, включающих только числа 0-9, буквы A-Z, a-z и дефисы. Можно использовать и другие символы, но только если это не будет мешать другим пользователям найти компьютер в сети.

Компьютеры, имеющие непосредственный доступ в глобальную сеть, часто называют хост-компьютерами. Имя хост-узла - это имя, которое можно присвоить компьютеру для облегчения к нему доступа в сети IP.

Формат имени хост-узла с именами поддомена и домена:

**[HostName].[SubdomainName].[DomainName]**

Например, **КОМ-1.инф.com**

Имена домена и поддомена являются дополнительными дескрипторами компьютера.

## **2.5. Отношения доменов**

В сети, состоящей из двух и более доменов, каждый домен действует как отдельная сеть со своей базой данных учетных записей. Однако даже в наиболее жестко структурированной организации некоторым пользователям из одного домена могут понадобиться какие-нибудь ресурсы из другого домена. Обычное решение этой проблемы, связанной с настройкой уровней доступа пользователей между различными доменами, называется установлением доверительных отношений.

### **2.5.1. Недоверительные отношения между доменами**

Может существовать несколько доменов, между которыми не установлены доверительные отношения. Например, у пользователя могут быть учетные записи в каждом домене многодоменной сети. На рис.1 показана сеть с двумя доменами; один домен называется Финансы (Ф), а другой Маркетинг (М).

Когда пользователь регистрируется в домене М, он получает доступ к его ресурсам, как установлено администратором, но у него нет при этом доступа к домену Ф. Аналогично при входе в домен Ф у пользователя нет доступа к домену М. Чтобы снова добраться до ресурсов домена М, пользователь должен выйти из домена Ф и войти в домен М.