Инсталляция информационной системы

Администрирование ИС

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

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?*

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. 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.*

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.

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**.

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.**

Модели доменов

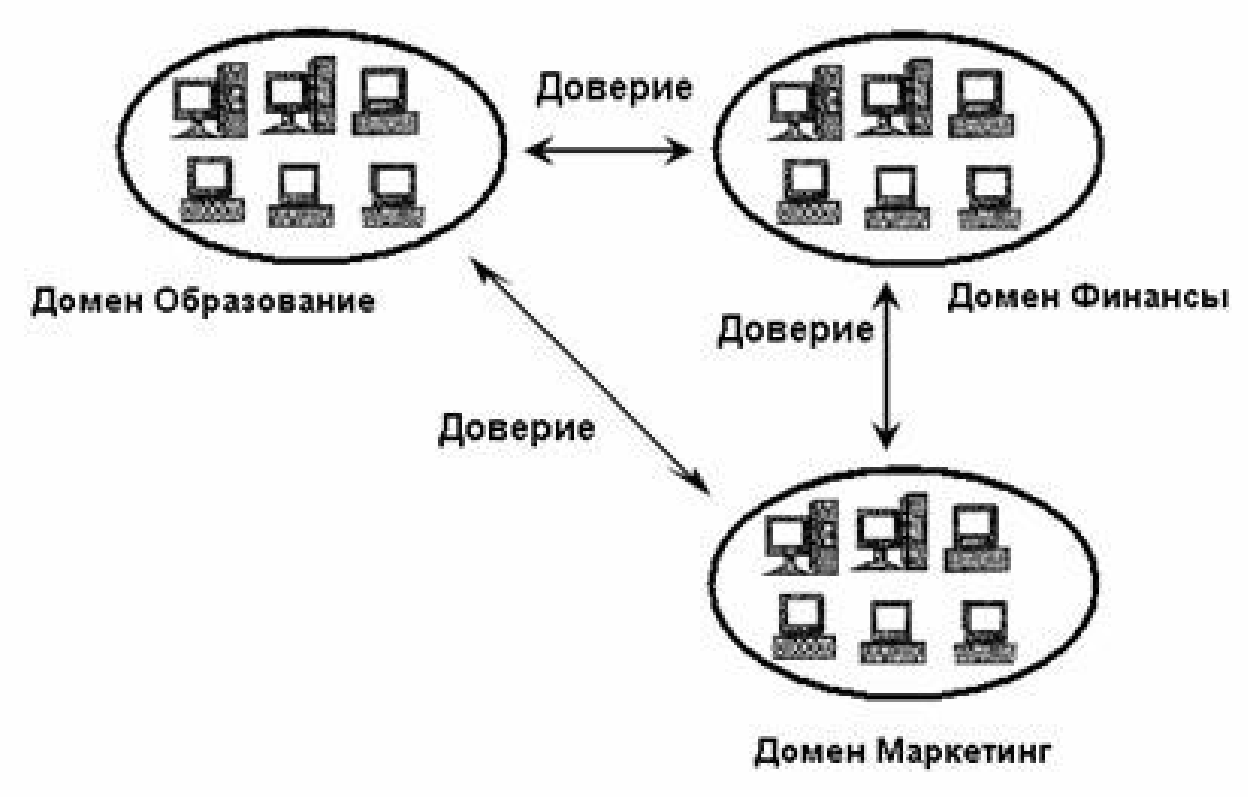
Существуют четыре модели структуры доверительных отношений между доменами.

Это модели:

- *с одним доменом;*
- *одним главным доменом;*
- *несколькими главными доменами;*
- *полностью доверительными отношениями.*

Сеть может использовать *одну из этих моделей, некую вариацию модели или сочетание двух и более моделей, используемых в различных частях сети.*

Но базовые кирпичики остаются теми же.



Несколько доменов с полным набором доверительных отношений

Модель с одним доменом

Это самая простая модель; все серверы и клиенты входят в один домен. Локальные и глобальные группы совпадают, а все администраторы могут администрировать все серверы. Поскольку домен один, нет нужды в доверительных отношениях.

Сеть с одним доменом является эффективной и полезной моделью для небольшого предприятия, где не так уж много серверов и пользователей.

Модель с одним доменом не подходит, если:

- пользователи используют различные наборы ресурсов и имеют различные потребности;
- предприятие разрастается и отделы располагаются в нескольких зданиях, на разных этажах или вообще далеко друг от друга;
- время, затрачиваемое на просмотр ресурсов сети, огромно.

Модель с одним доменом

Преимущества модели с одним доменом	Недостатки модели с одним доменом
-Простота администрирования -Централизованное управление учетными записями пользователей -Отсутствие доверительных отношений и необходимости управлять ими -Локальные группы задаются только один раз	-Отсутствие группирования пользователей по подразделениям или другим признакам -Снижение производительности при увеличении числа ресурсов -Отсутствие логического группирования ресурсов -Время на просмотр ресурсов растет с увеличением числа серверов

Модель с одним главным доменом

Модель с одним главным доменом подходит для организации, в которой сравнительно мало пользователей и возможно логичное объединение ресурсов в группы, когда число ресурсов возрастает.

Все учетные записи пользователей, а также глобальные группы создаются в главном домене. Но каждый домен подразделения может завести свои локальные группы.

Первейшей функцией главного домена является **централизованное ведение учетных записей**.

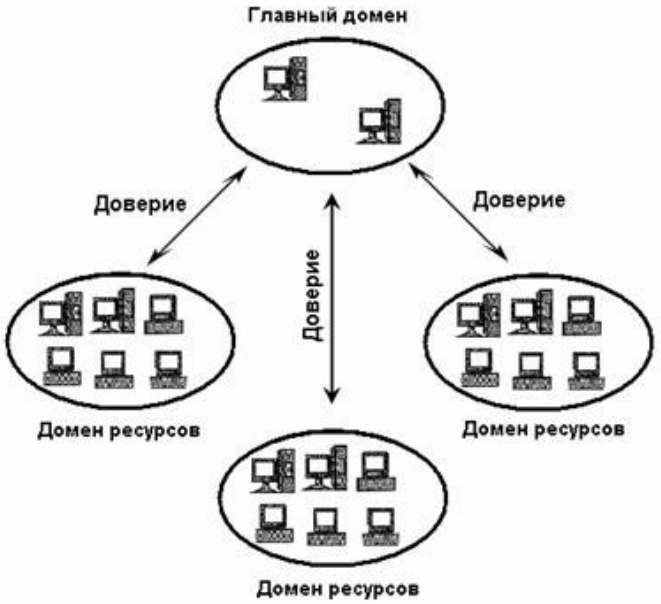
Обязательно также **наличие хотя бы одного резервного контроллера домена**, так как база данных всех учетных записей пользователей хранится только на основном и резервных контроллерах главного домена.

Все остальные домены (домены ресурсов) действуют в основном как распорядители ресурсов. У каждого из них имеется свой набор ресурсов, которые доступны во всей сети, но могут администрироваться на месте.

Модель с одним главным доменом это естественное развитие модели с одним доменом. Однако эта модель перестает быть пригодной, если число пользователей становится слишком большим. Производительность значительно снижается, так как подлинность каждой учетной записи проверяет один главный домен.

Модель с одним главным доменом

Преимущества модели с одним главным доменом	**Недостатки модели с одним главным доменом**
-Централизованное управление учетными записями пользователей -Глобальные группы задаются только один раз -Управление ресурсами на уровне подразделений -Для каждого домена ресурса требуется установить только одностороннее доверительное отношение	-Снижение производительности при увеличении числа пользователей - Зависимость от надежности контроллеров главного домена - В каждом домене ресурсов требуется определять локальные группы



Модель с одним главным доменом

Модель с несколькими главными доменами

Такая модель подходит *для организаций с большим числом пользователей и централизованной структурой управления*.

В ней *обеспечивается централизованное администрирование двух и более главных доменов*, а *ресурсы распределены между доменами ресурсов*.

В этой модели имеется *небольшое число главных доменов, между которыми установлены двусторонние доверительные отношения*.

Учетные записи пользователей хранятся в главных доменах и распределены между ними сравнительно равномерно.

Делить учетные записи пользователей между главными доменами можно исходя из логического объединения пользователей в группы или чисто формально, например, по именам в алфавитном порядке.

Для каждого пользователя имеется только одна учетная запись в одном из главных доменов.

Все домены ресурсов доверяют каждому главному домену, но наличие доверительных отношений между доменами ресурсов совсем не обязательно.

Управление ресурсами, такими как принтеры и файлы, осуществляется на уровне доменов ресурсов.

Модель с несколькими главными доменами

Модель с несколькими главными доменами

Преимущества модели с несколькими главными доменами	Недостатки модели с несколькими главными доменами
- Централизованное управление учетными записями пользователей - Наращиваемость в соответствии с текущими требованиями -Управление ресурсами на уровне подразделений - Логическое объединение ресурсов	- Отсутствие единого места управления учетными записями пользователей и группами - Необходимость определять глобальные и локальные группы несколько раз и вносить в них изменения в нескольких местах - Возрастающая сложность доверительных отношений

Модель с несколькими главными доменами и полностью доверительными отношениями

Модель с несколькими главными доменами и полностью доверительными отношениями имеет смысл в *относительно небольших организациях, которые переросли модель с одним доменом, но она не подходит для случая, когда доменов становится слишком много.*

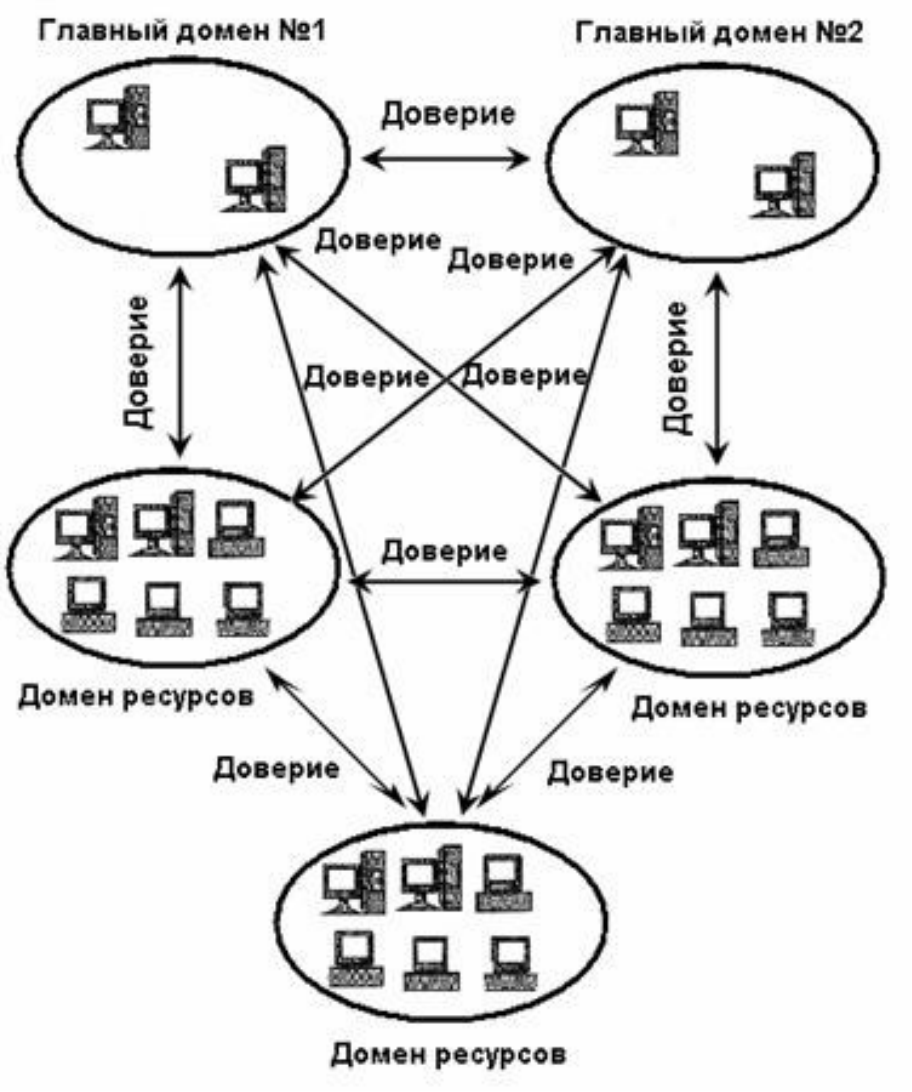
У каждого домена должны быть установлены двусторонние доверительные отношения со всеми остальными доменами.

Таким образом, число доверительных отношений растет экспоненциально с увеличением числа доменов.

Число доверительных отношений, которые требуется установить в сети с п доменами, равно п*(п-1).

Если у вас пять доменов, то понадобится двадцать доверительных отношений, добавление еще одного домена приведет к необходимости установить дополнительно десять доверительных отношений.

Модель с несколькими главными доменами и полностью доверительными отношениями



Модель с несколькими главными доменами и полностью доверительными отношениями

Преимущества модели с несколькими главными доменами и полностью доверительными отношениями	Недостатки модели с несколькими главными доменами и полностью доверительными отношениями
-Логическое объединение в группы пользователей и ресурсов -Управление ресурсами на уровне подразделений - Наращиваемость в соответствии с текущими требованиями -Требуется полное взаимное доверие между администраторами всех доменов	- Отсутствие единого места управления учетными записями пользователей и группами - Необходимость определять глобальные и локальные группы несколько раз и вносить в них изменения в нескольких местах - Очень сложные доверительные отношения