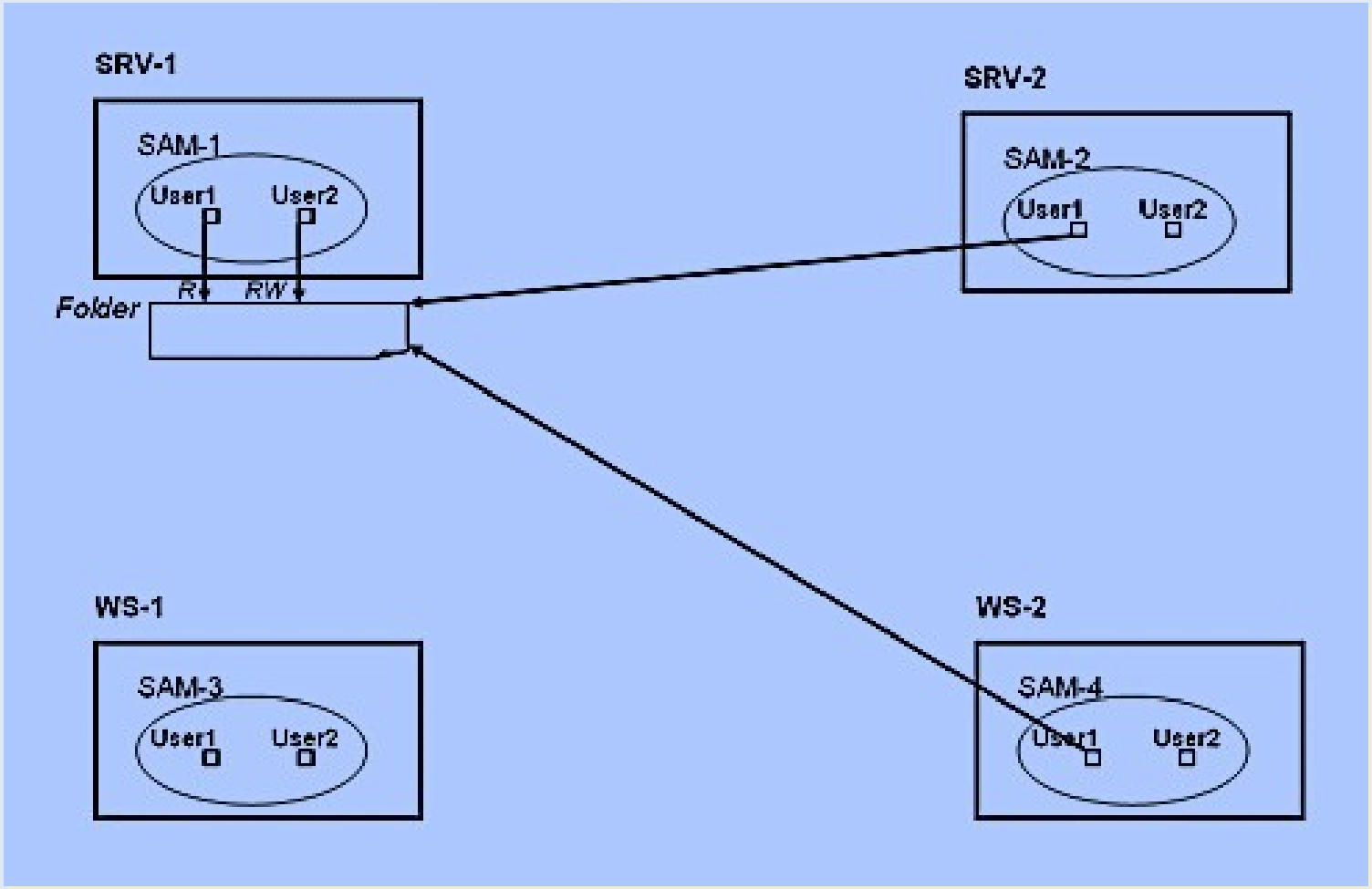
ТЕМА 1

ВВЕДЕНИЕ В СЛУЖБУ КАТАЛОГА ACTIVE DIRECTORY

МОДЕЛЬ БЕЗОПАСНОСТИ «РАБОЧАЯ ГРУППА»

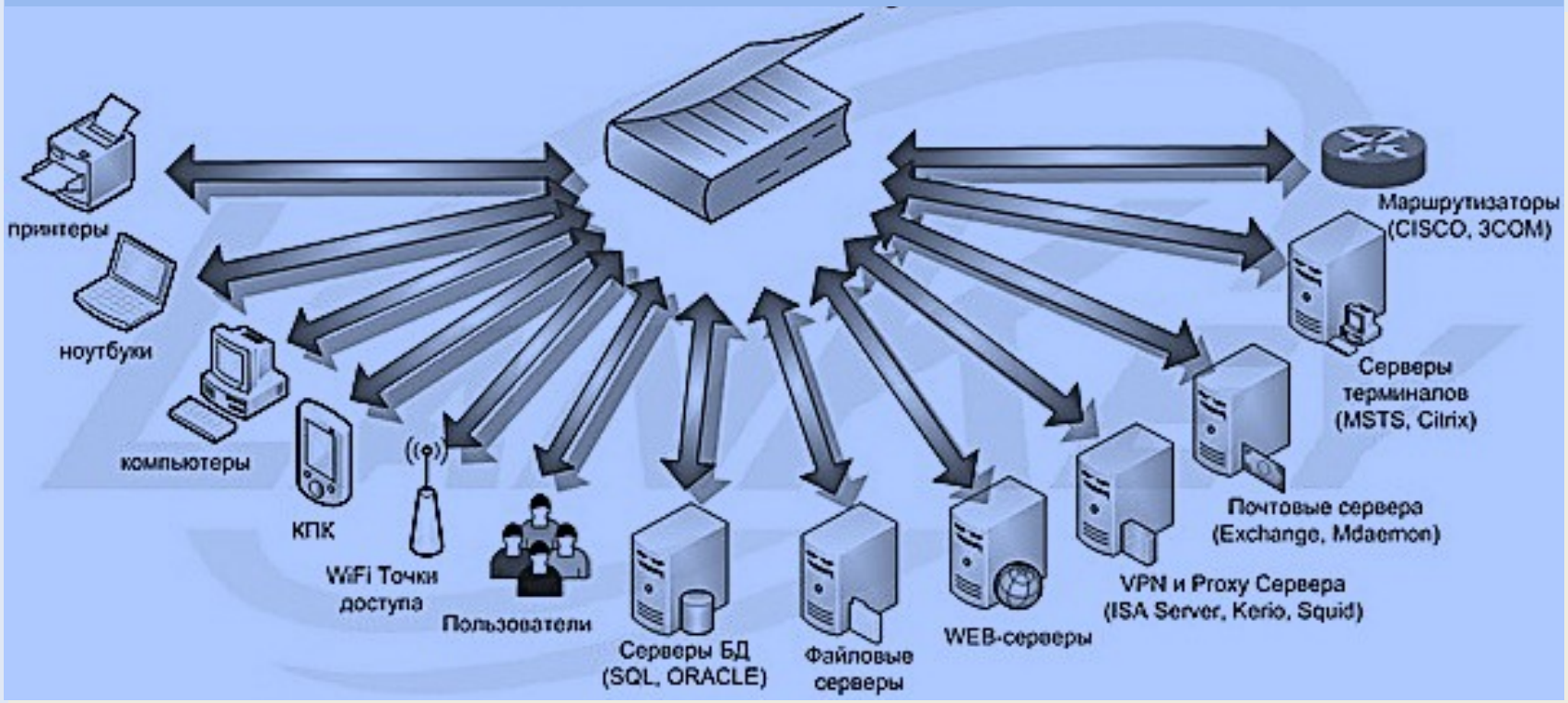
1. Используется в небольших одноранговых сетях (3–10 компьютеров)
2. Каждый компьютер в сети имеет свою собственную локальную базу данных учетных записей
3. Базы данных отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой

МОДЕЛЬ БЕЗОПАСНОСТИ «РАБОЧАЯ ГРУППА»



СЛУЖБА КАТАЛОГА

КАТАЛОГ

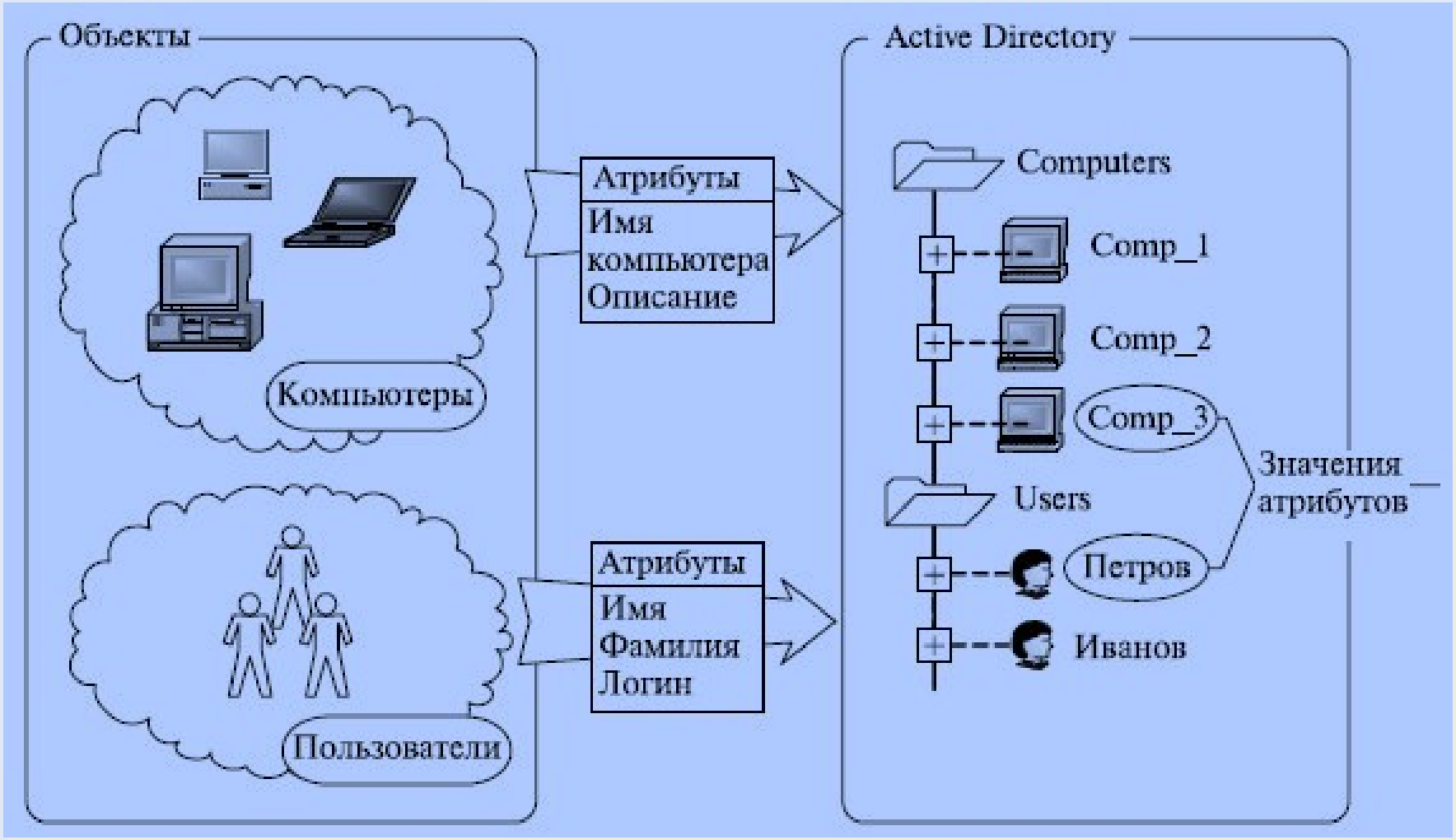


УПРАВЛЕНИЕ С ПОМОЩЬЮ ГРУППОВЫХ ПОЛИТИК

ПРЕИМУЩЕСТВА ACTIVE DIRECTORY

- Единая регистрация в сети
- Централизованное управление
- Масштабируемость
- Репликация информации
- Гибкость запросов к каталогу
- Стандартные интерфейсы программирования
- Безопасность информации

ОБЪЕКТЫ ACTIVE DIRECTORY



ОСНОВНЫЕ ПОНЯТИЯ

ДОМЕН – основная единица системы безопасности Active Directory

КОНТРОЛЛЕРЫ ДОМЕНА — специальные серверы, которые хранят соответствующую данному домену часть базы данных Active Directory.

ОСНОВНЫЕ ФУНКЦИИ КОНТРОЛЛЕРОВ ДОМЕНА:

- **хранение БД Active Directory**
- **синхронизация изменений в AD**
- **аутентификация пользователей**

ОСНОВНЫЕ ПОНЯТИЯ

Глобальный каталог

Глобальный каталог является перечнем всех объектов, которые существуют в лесу Active Directory. По умолчанию, контроллеры домена содержат только информацию об объектах своего домена. Сервер Глобального каталога является контроллером домена, в котором содержится информация о каждом объекте (хотя и не обо всех атрибутах этих объектов), находящемся в данном лесу.

Схема Active Directory — набор определений типов, или классов, объектов в БД Active Directory

ИМЕНОВАНИЕ ОБЪЕКТОВ

для идентификации объекта в масштабе всего леса используется механизм **ОТЛИЧИТЕЛЬНЫХ ИМЕН** (Distinguished Name, DN).
В Active Directory учетная запись пользователя с именем User домена company.ru, размещенная в стандартном контейнере Users, будет иметь следующее отличительное имя:
"DC=ru, DC=company, CN=Users, CN=User".

DC (Domain Component) — указатель на составную часть доменного имени;
OU (Organizational Unit) — указатель на организационное подразделение (ОП);
CN (Common Name) — указатель на общее имя.

ОТНОСИТЕЛЬНОЕ ОТЛИЧИТЕЛЬНОЕ ИМЯ (Relative Distinguished Name, RDN). Для пользователя User из предыдущего примера RDN-имя будет иметь вид " CN=User ".

ОСНОВНОЕ ИМЯ ОБЪЕКТА (User Principal Name, UPN). Оно имеет формат <имя субъекта>@<суффикс домена>. Для того же пользователя из примера основное имя будет выглядеть как User@company.ru.

ГЛОБАЛЬНО УНИКАЛЬНЫЙ ИДЕНТИФИКАТОР (Globally Unique Identifier, GUID), представляющий собой 128-битное число.

ЛОГИЧЕСКАЯ СТРУКТУРА AD

ДОМЕН — логическая группа пользователей и компьютеров, которая поддерживает централизованное администрирование и управление безопасностью.

ДЕРЕВО является набором доменов, которые связаны отношениями "дочерний"/"родительский", а также используют связанные (смежные, или прилегающие) пространства имен.

ЛЕС — это одно или несколько деревьев, которые разделяют общую схему, серверы Глобального каталога и конфигурационную информацию. В лесу все домены объединены транзитивными двухсторонними доверительными отношениями.

ДОМЕНЫ, ДЕРЕВЬЯ И ЛЕСА

ДОМЕН

основная единица системы безопасности Active Directory

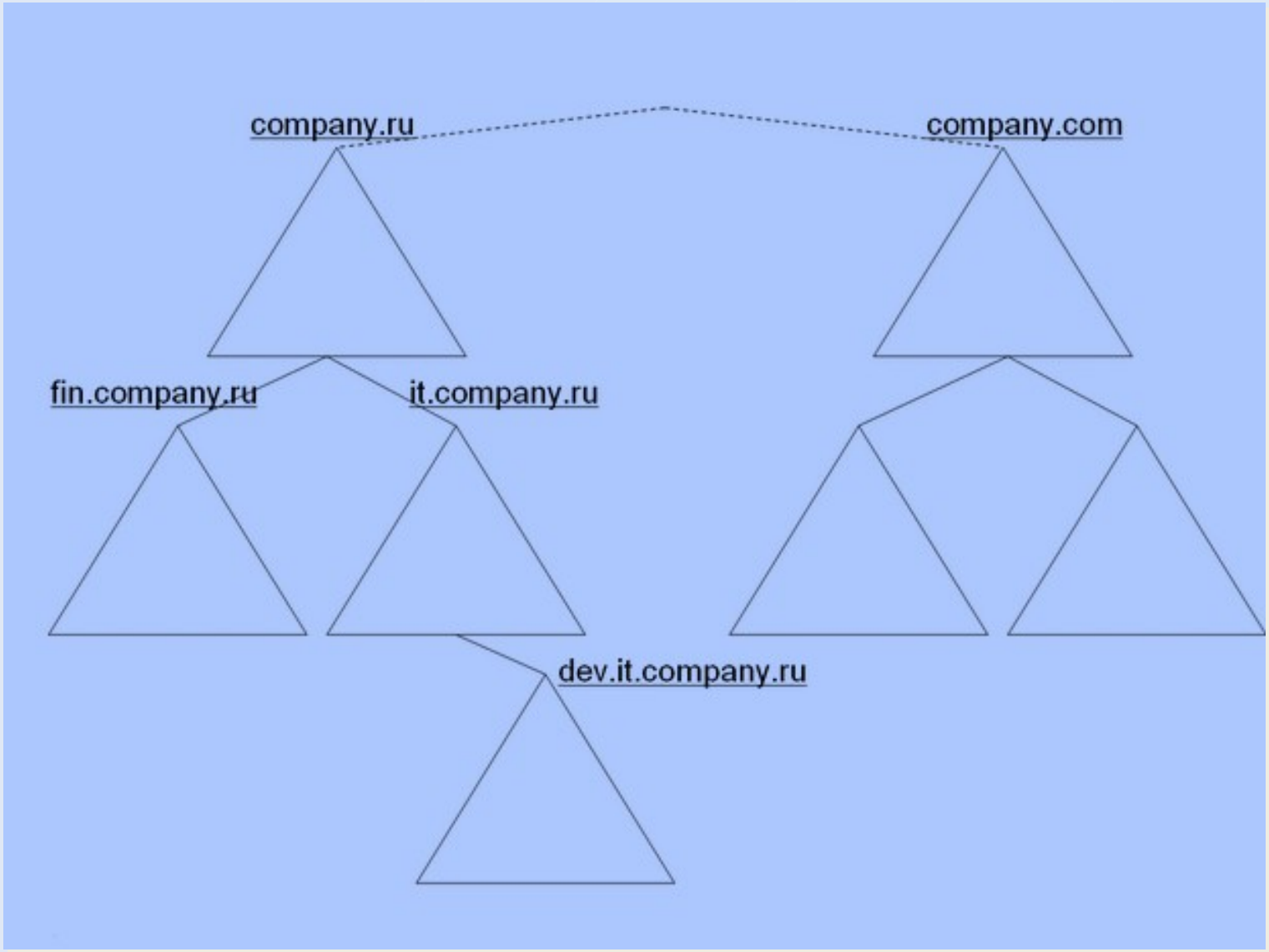
ДЕРЕВО

набор доменов, которые используют единое пространство имен

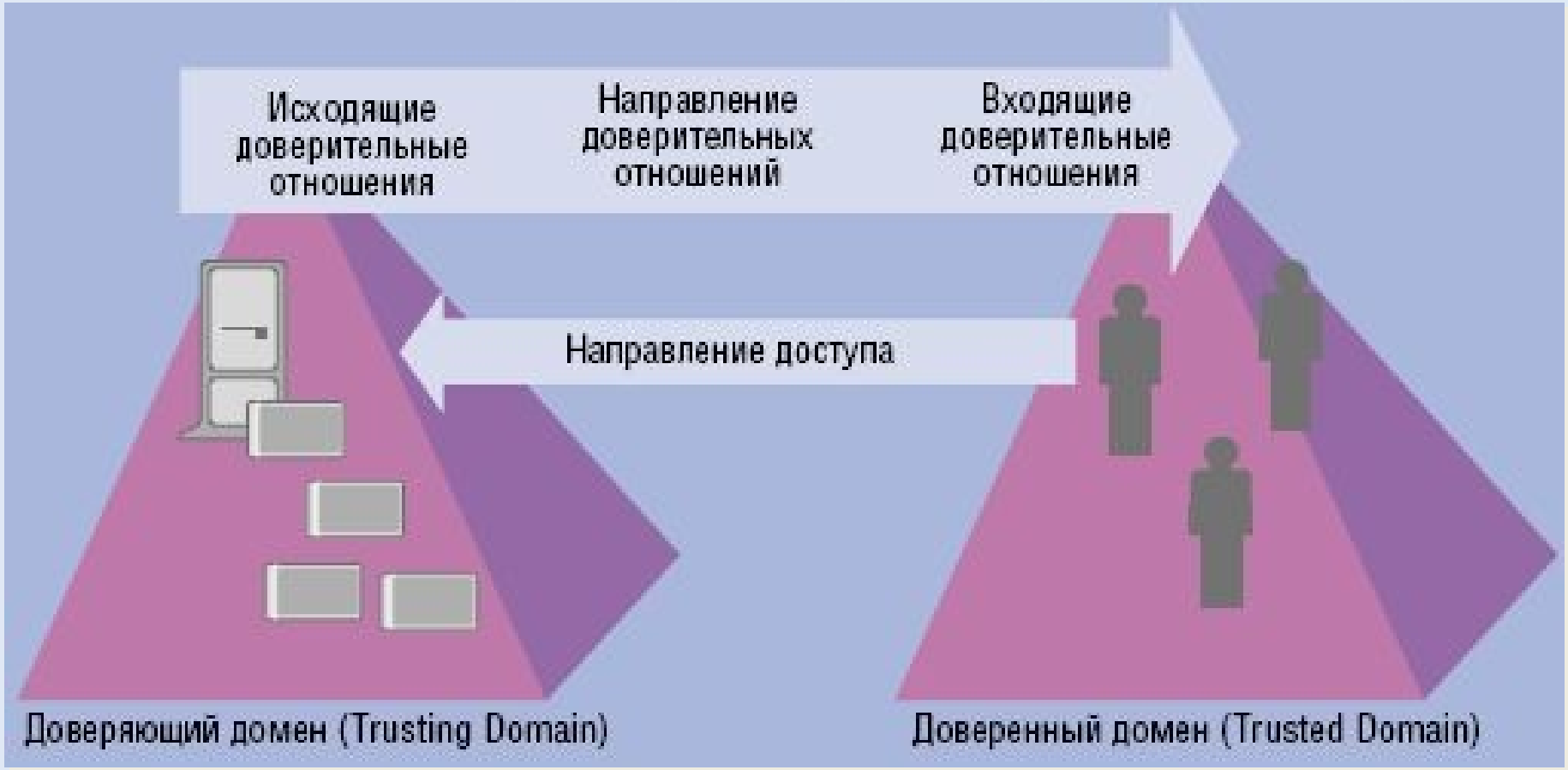
ЛЕС

объединяет деревья, которые поддерживают единую схему

ДОМЕНЫ, ДЕРЕВЬЯ И ЛЕСА

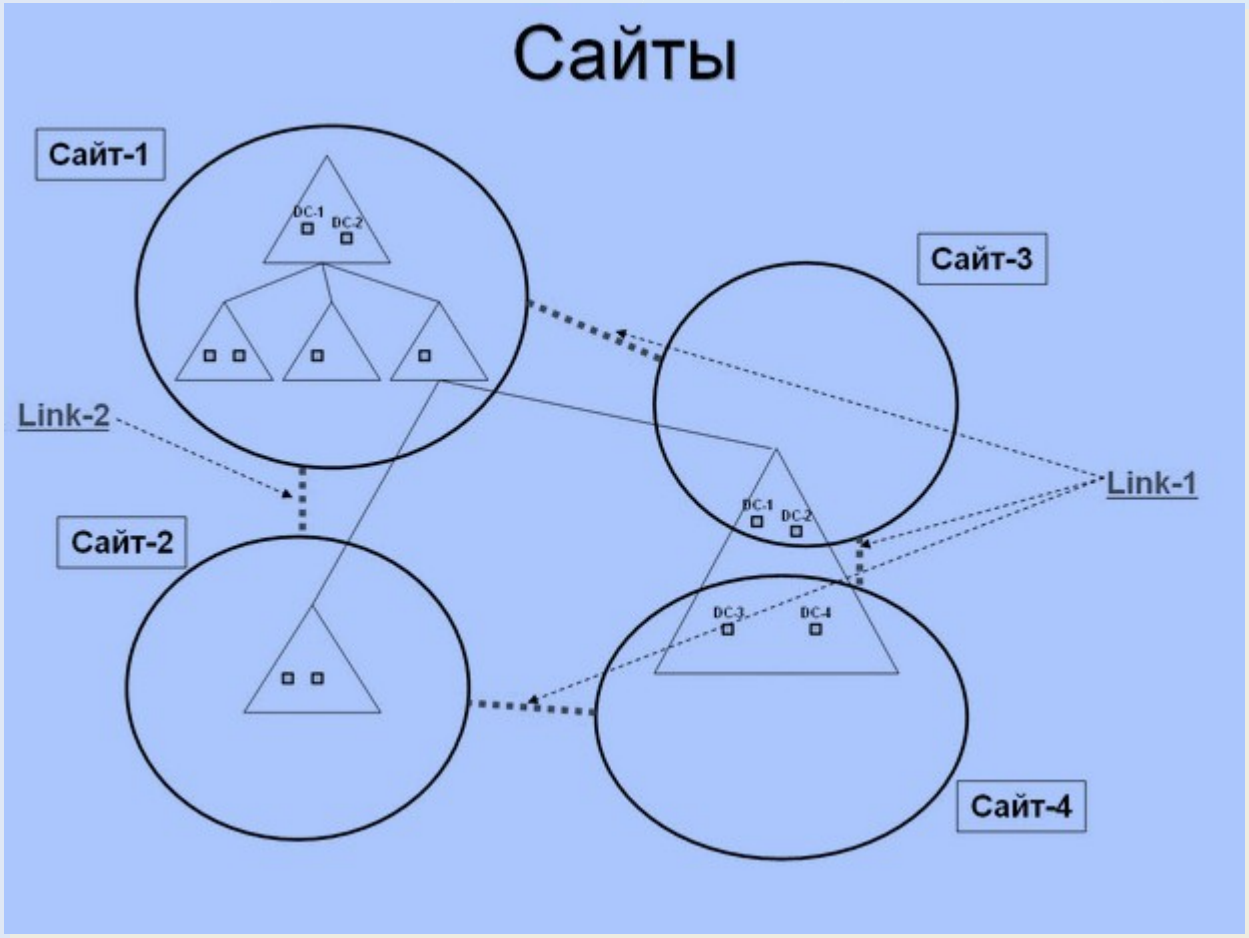


ДОВЕРИТЕЛЬНЫЕ ОТНОШЕНИЯ



ФИЗИЧЕСКАЯ СТРУКТУРА AD

САЙТ — группа IP-сетей, соединенных быстрыми и надежными коммуникациями.



ACTIVE DIRECTORY И DNS

СЛУЖБА DNS LOCATOR

Чтобы облегчить нахождение контроллеров домена, Active Directory использует указатель служб (service locator) или записи SRV. Первая часть SRV-записи идентифицирует службу, на которую указывает запись SRV :

_ldap Active Directory является службой каталога, совместимой с LDAP-протоколом, с контроллерами домена, функционирующими как LDAP-серверы. Записи _ldap SRV идентифицируют LDAP-серверы, имеющиеся в сети. Эти серверы могут быть контроллерами домена Windows Server 2003 или другими LDAP-серверами;

_kerberos - основной опознавательный протокол. SRV-записи _kerberos идентифицируют все ключевые центры распределения (Key Distribution Centers, KDC) в сети. Они могут быть контроллерами домена с Windows Server 2003 или другими KDC-серверами;

_kpassword идентифицирует серверы изменения паролей Kerberos в сети (это контроллеры домена или с Windows Server 2003, или с другими системами изменения пароля Kerberos);