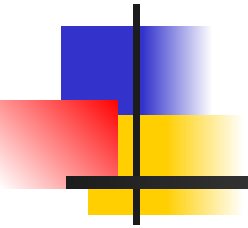


Компьютерные системы и сети

Службы организации корпоративных сетей.
Общий и доступ к ресурсам.
Active Directory.

Олизарович Евгений Владимирович

ГрГУ им. Я.Купалы. 2012-2013

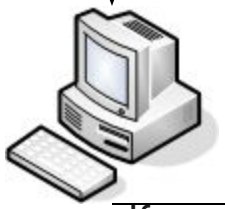
Базовые сетевые модели

Программная модель «клиент - сервер»

Приложение - клиент

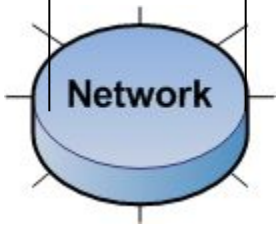
Приложение – сервер (URI, языки запросов, семантика)

Модель сетевого взаимодействия «клиент-сервер» (BOC, TCP/IP)



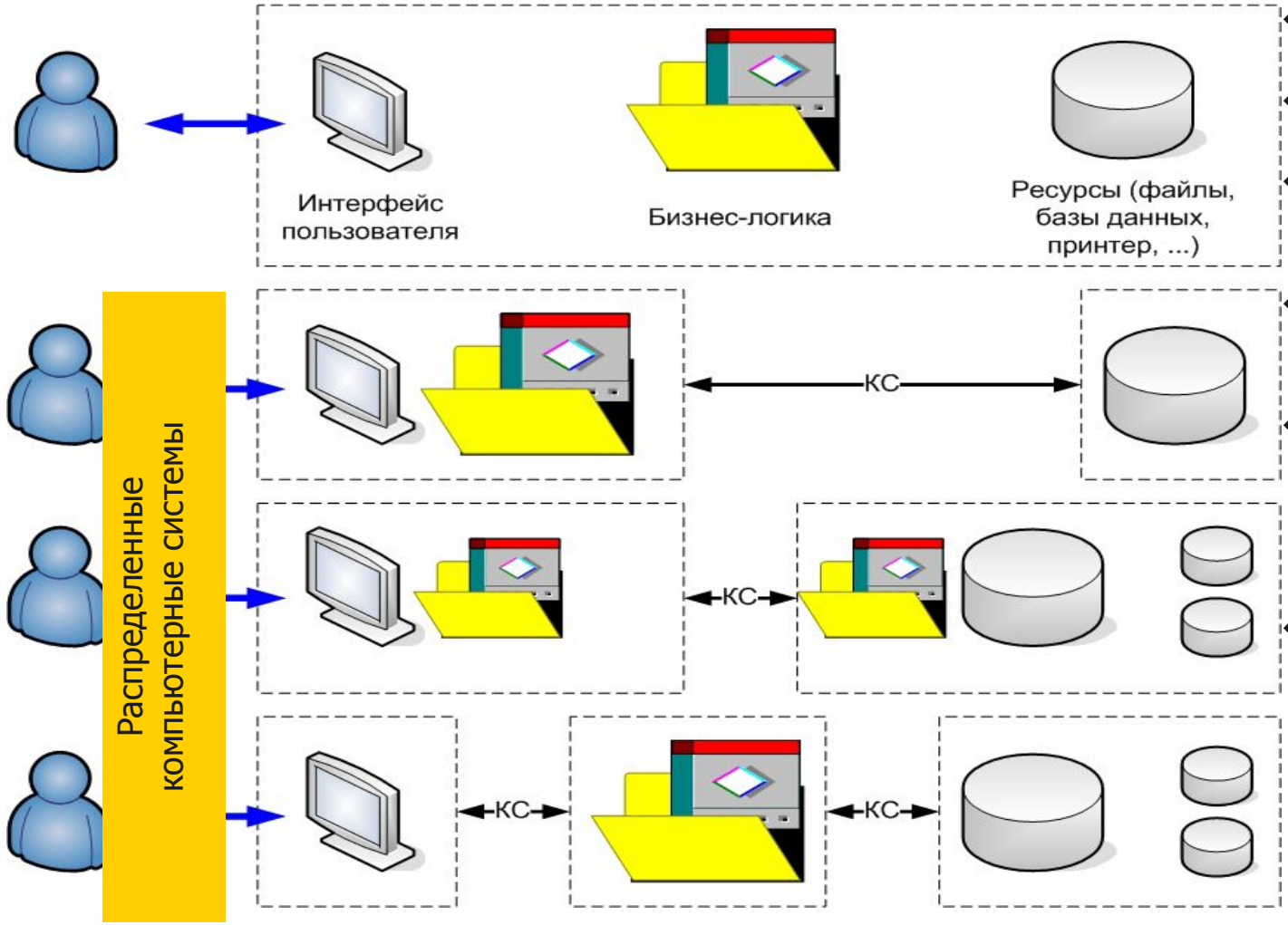
Компьютер 1

Компьютер 2
MAC,
IP, TCP-port
DNS, URI



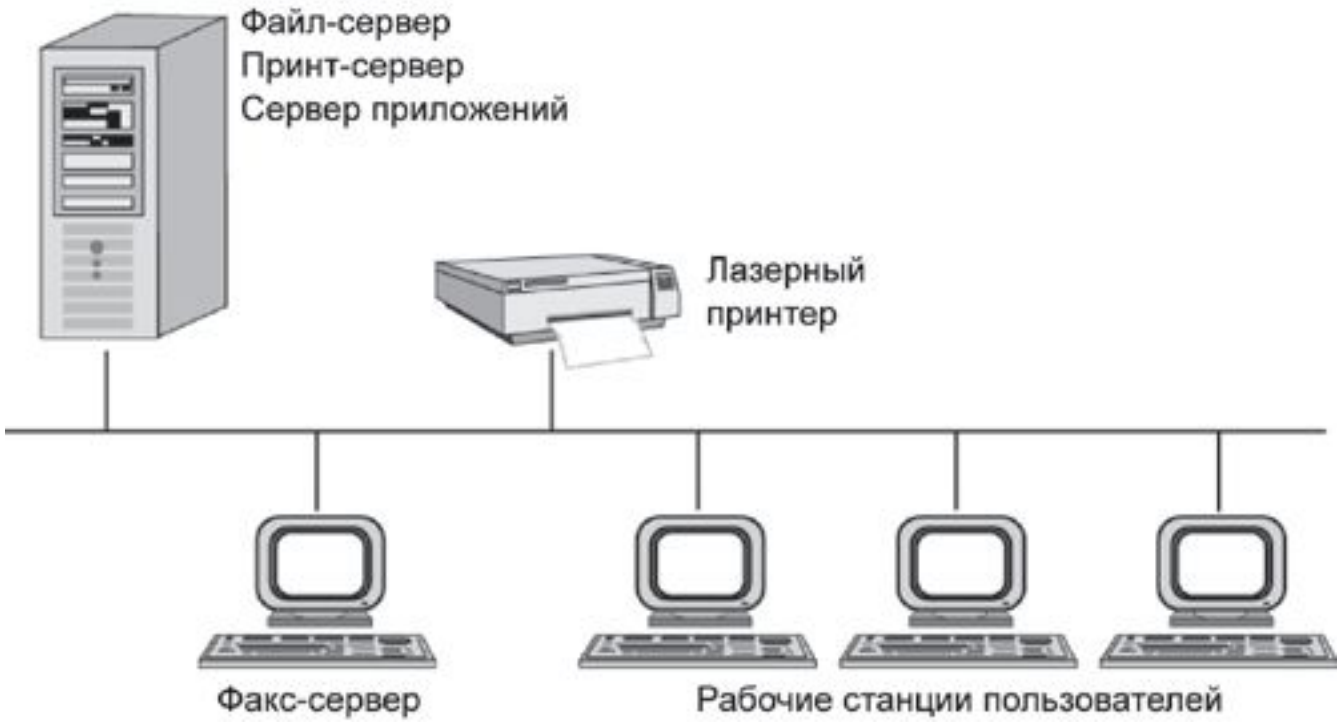
Сетевые модели

Обработка данных (модель клиент - сервер)



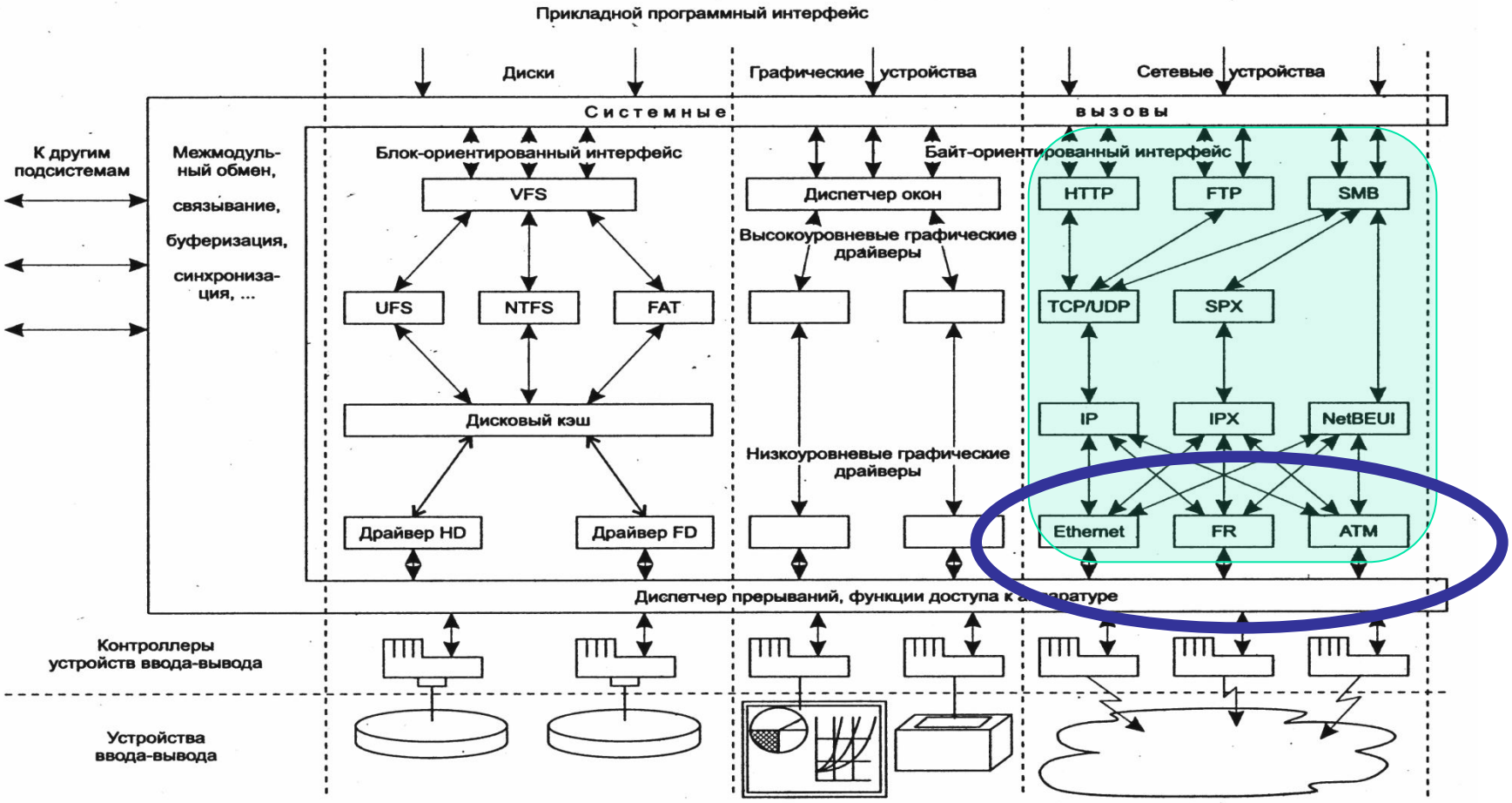
- Коммуникации;
- Адресация ресурсов;
- Протоколы и языки запросов;
- Авторизация пользователей;
- Промежуточное программное обеспечение (middleware);
- Аппаратные средства

Клиенты и серверы сети



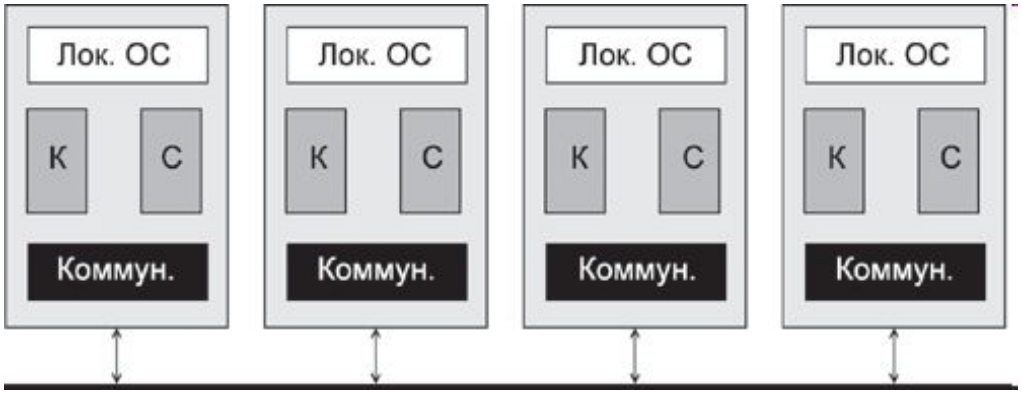
Клиенты и серверы сети

Клиенты и серверы сети



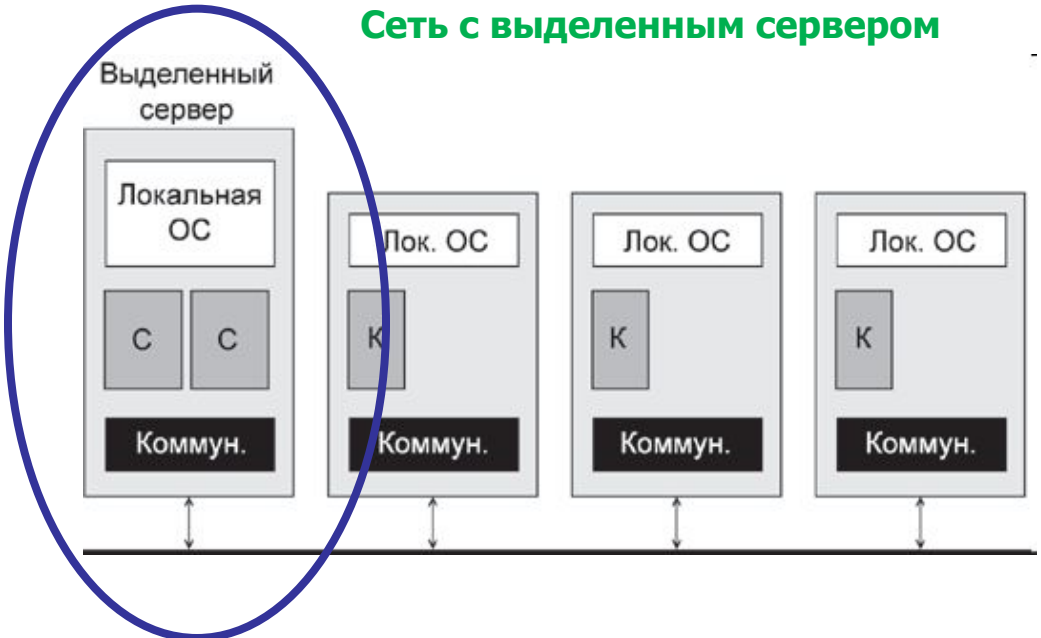
Клиенты и серверы сети

Одноранговая сеть



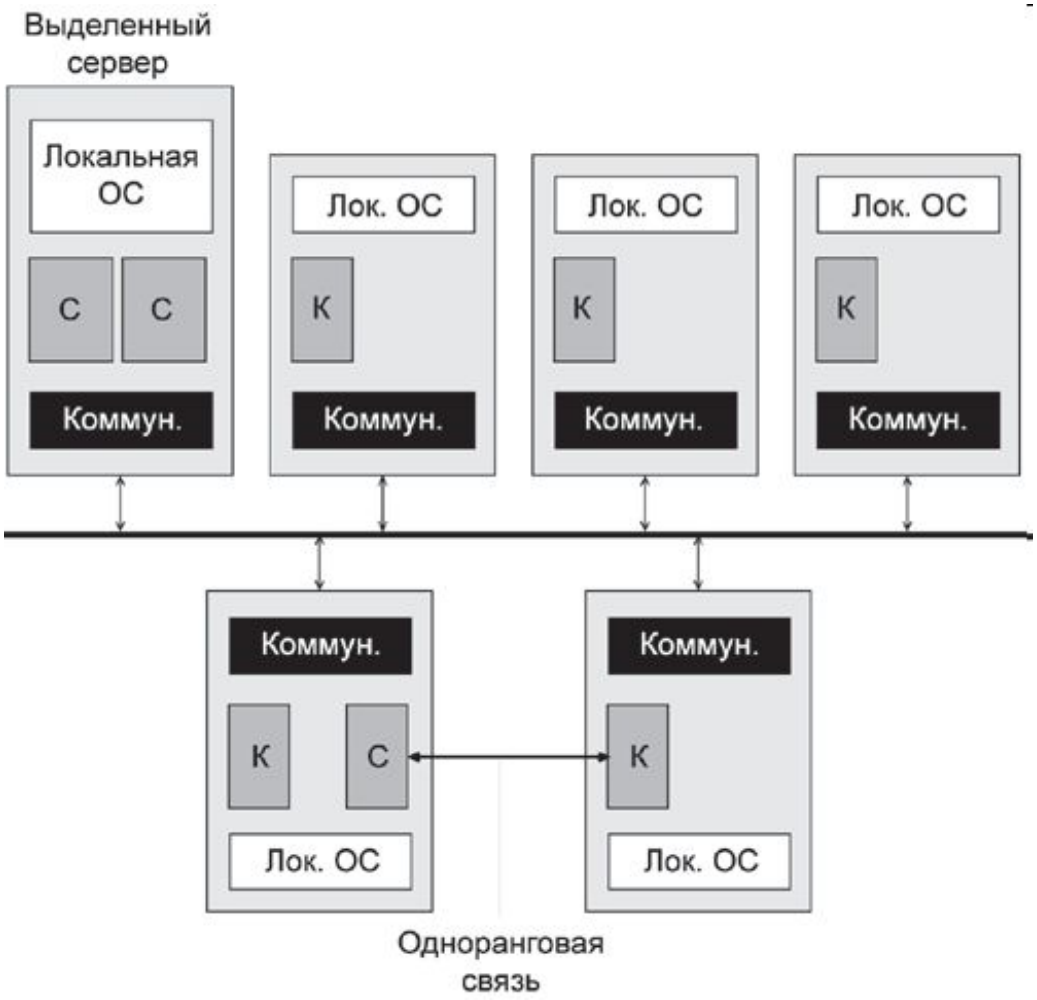
- Специальная ОС;
- Производительное ПО;
- Скоростные коммуникации;
- Общие дорогостоящие ресурсы;
- Повышенная безопасность;
- Резервирование, backup;
- Единое администрирование;
- Удобство обслуживания ….

Сеть с выделенным сервером



Клиенты и серверы сети

Реальная сеть



Компьютерные системы и сети

ГрГУ им. Я.Купалы

Серверы и сервисы

2012/2013

Обеспечение инфраструктуры сети

Обслуживание бизнес-процессов

Обслуживание сети

Права доступа

Виды прав доступа к ресурсам

- **Чтение (R).** Разрешается просматривать вложенные папки и файлы, а также их свойства, такие как имя владельца, разрешения и атрибуты чтения, такие как Только чтение, Скрытый, Архивный и Системный.
- **Запись (W).** Разрешается создавать и размещать внутри папки новые файлы и подпапки, а также изменять параметры папки и просматривать ее свойства, в частности имя владельца и разрешения доступа.
- **Список содержимого папки (L).** Разрешается просматривать имена содержащихся в папке файлов и вложенных папок.
- **Чтение и выполнение (X).** Разрешается получение доступа к файлам во вложенных папках, даже если нет доступа к самой папке. Кроме того, разрешены те же действия, которые предусмотрены для разрешений Чтение и Список содержимого папки.
- **Изменение (M).** Разрешены все действия, предусмотренные для разрешений Чтение и Чтение и выполнение, а также разрешено удаление папки.
- **Полный доступ (A)**. Разрешается полный доступ к папке. Другими словами, допускаются все действия, предусмотренные всеми перечисленными выше разрешениями. Дополнительно разрешено стать владельцем папки и изменять ее разрешения.

Права устанавливаются для ресурса или для пользователя

Права доступа

MS (NW)	
R	Чтение
W	Запись
X	Выполнение
D (E)	Удаление
P (A)	Изменение разрешений
O	Принятие статуса владельца
A (S)	Все права
L (F)	Просмотр каталога
No Access	Нет доступа

Сочетание прав.

- **LR** — пользователь может просматривать каталоги и имена файлов в каталогах.
- **RX** — пользователь может читать файлы из каталога и запускать программы.
- **WX** — пользователь может добавлять файлы в каталог, но не читать или просматривать содержимое каталога.
- **RWX** — пользователь имеет права на чтение и добавление данных.
- **RWXD** — пользователь имеет право читать, добавлять, менять содержимое каталога и удалять файлы.
- **RWXDPO — пользователь обладает всеми правами доступа.**

ACL (Access Control List) – список управления правами доступа.

Список мер по обеспечению безопасности, применяемый к объекту. (Объектом может быть файл, процесс, событие или какой-либо другой объект).

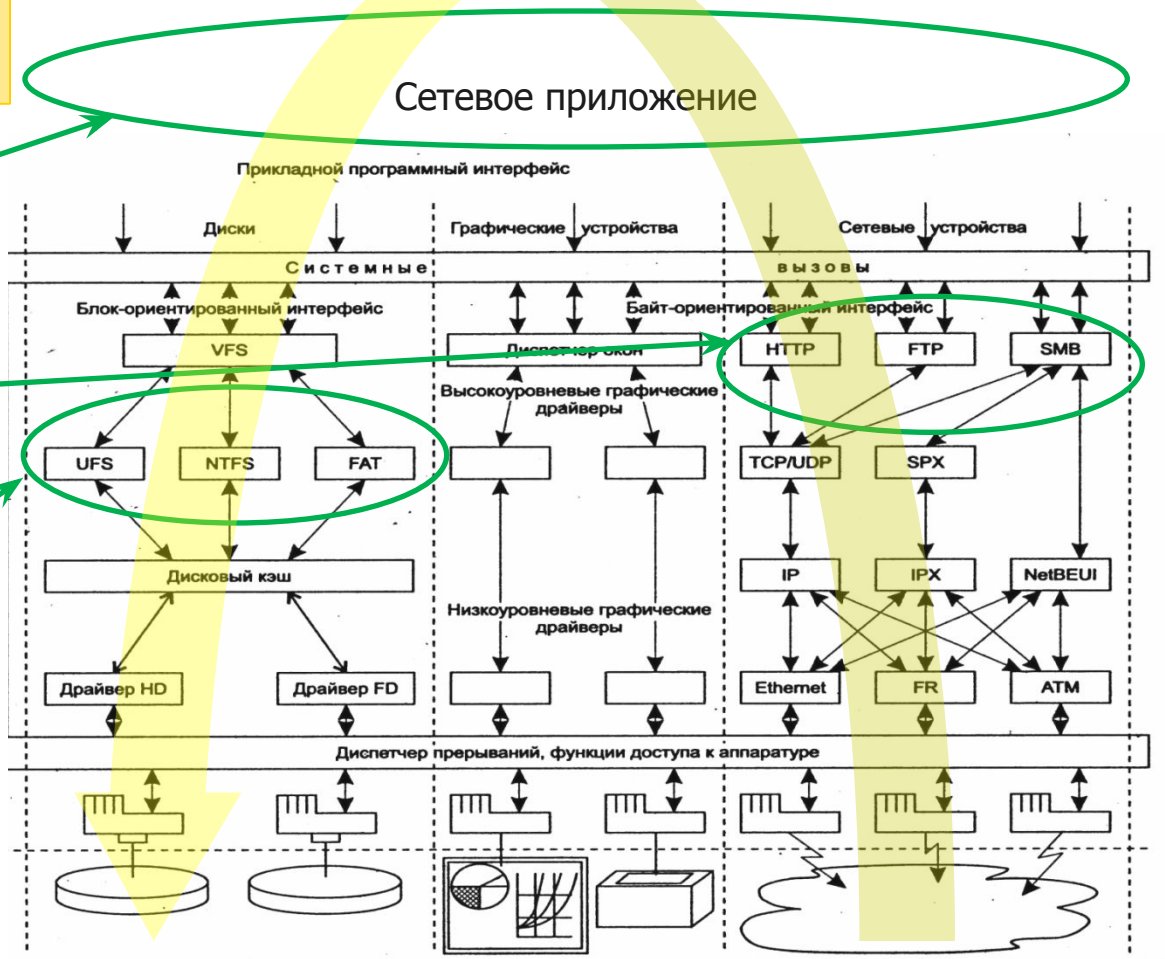
Определяет, кто имеет право доступа к ресурсу и какие именно права (R, W, E, X, …):

Файлы: *ресурс пользователь права,* C:\
USER_2 RW
[user]$ ls -l /bin/ls
-rwxr-xr-x 1 root root 49940 Sep 12 1999 /bin/ls

Трафик:
permit udp host 192.168.1.1 any eq tftp
deny tcp host 172.16.99.1 host 192.168.2.1 gt 100

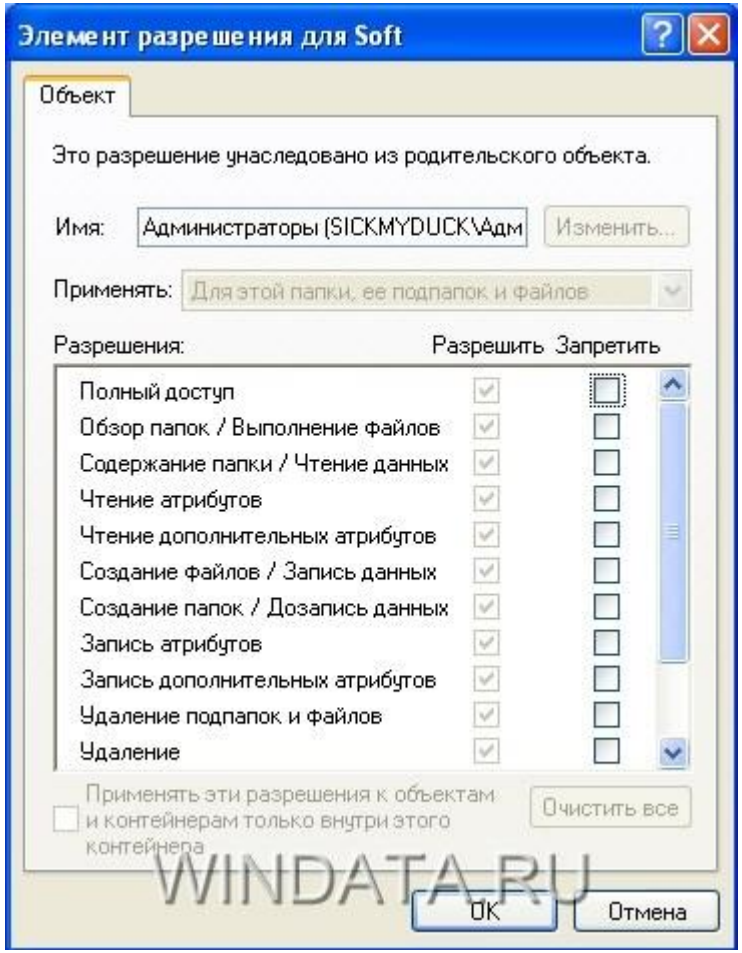
Доступ к файлам и данным. Права доступа.

1. Приложения
   (доступ к данным)
2. Сетевая подсистема
   (доступ к приложениям)
3. Файловая система
   (доступ к файлам)

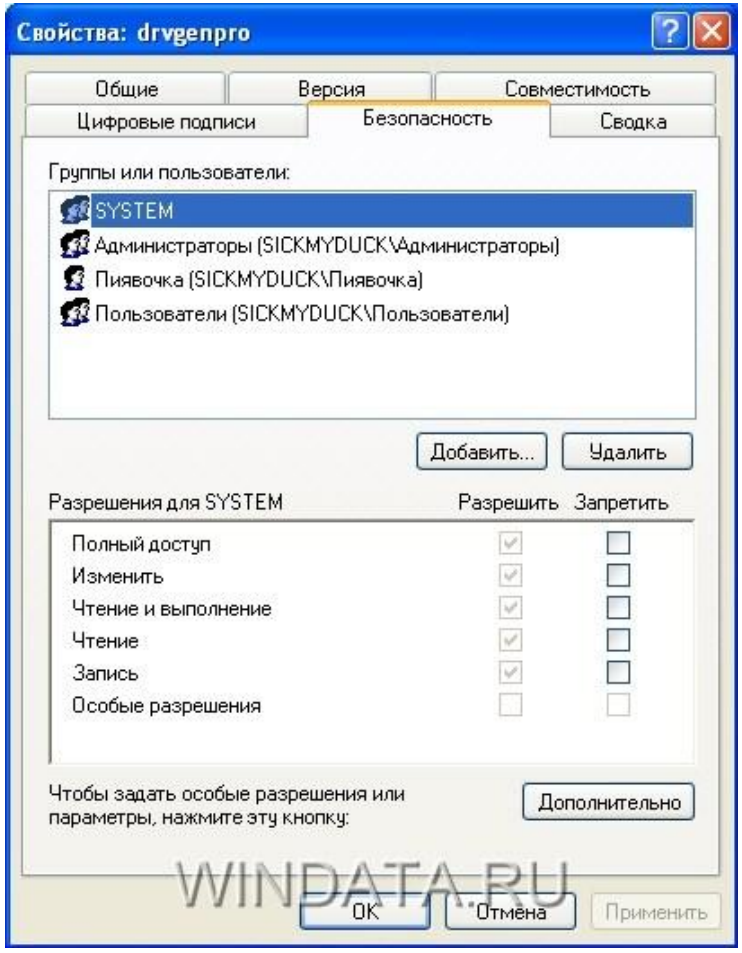


Права доступа

Установка прав сетевого доступа

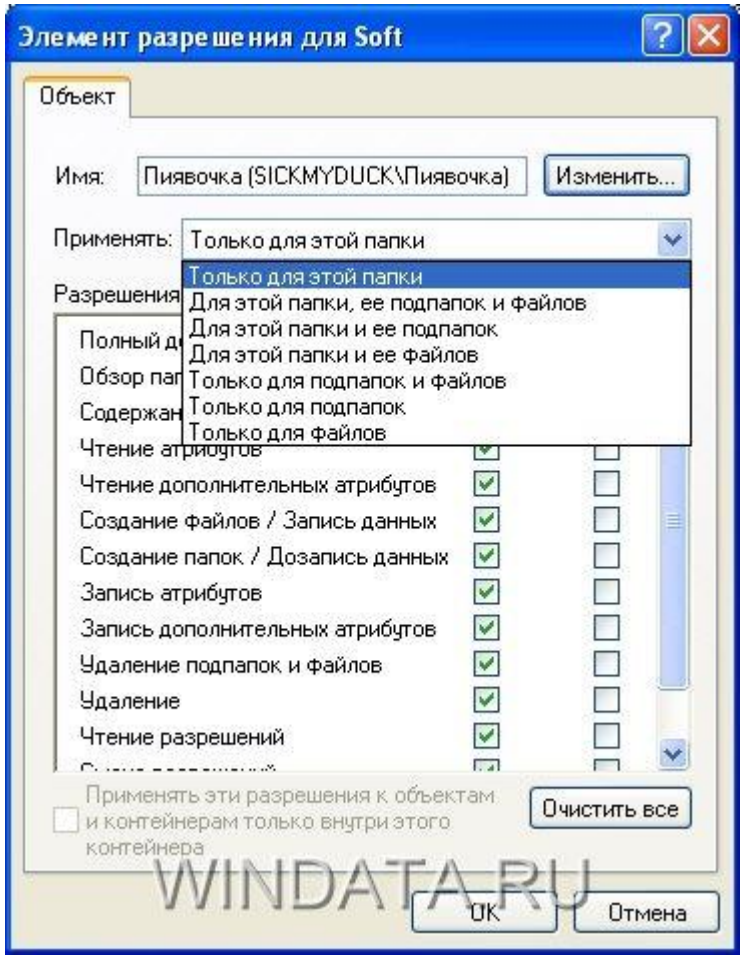


Установка прав файлового доступа

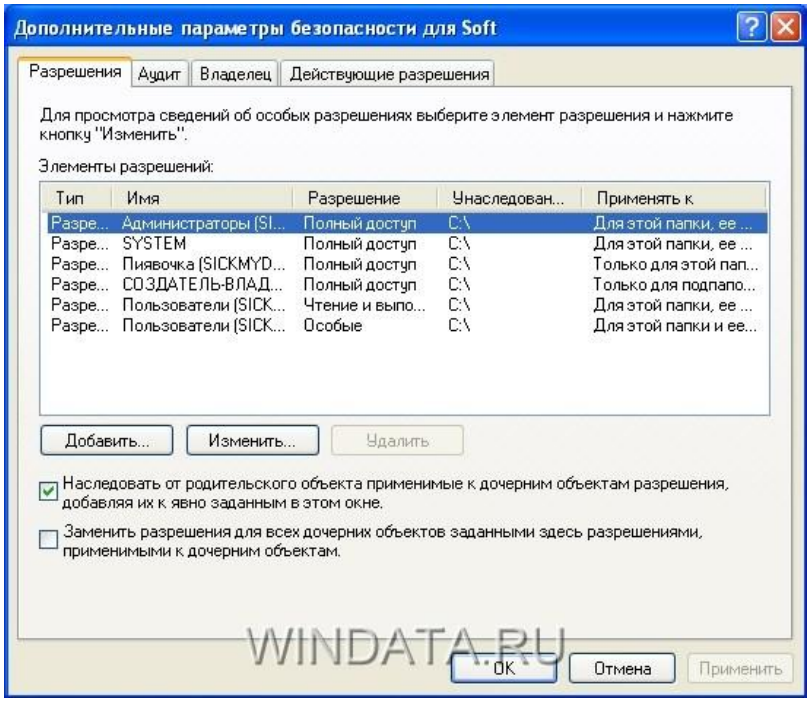


Права доступа

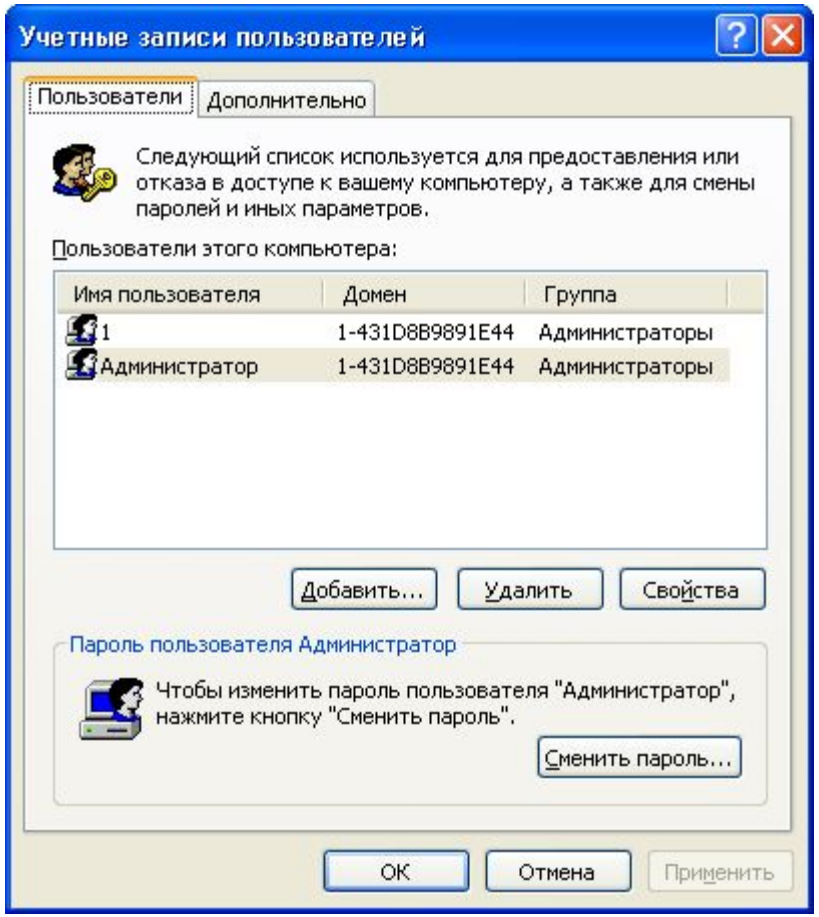
Наследование прав

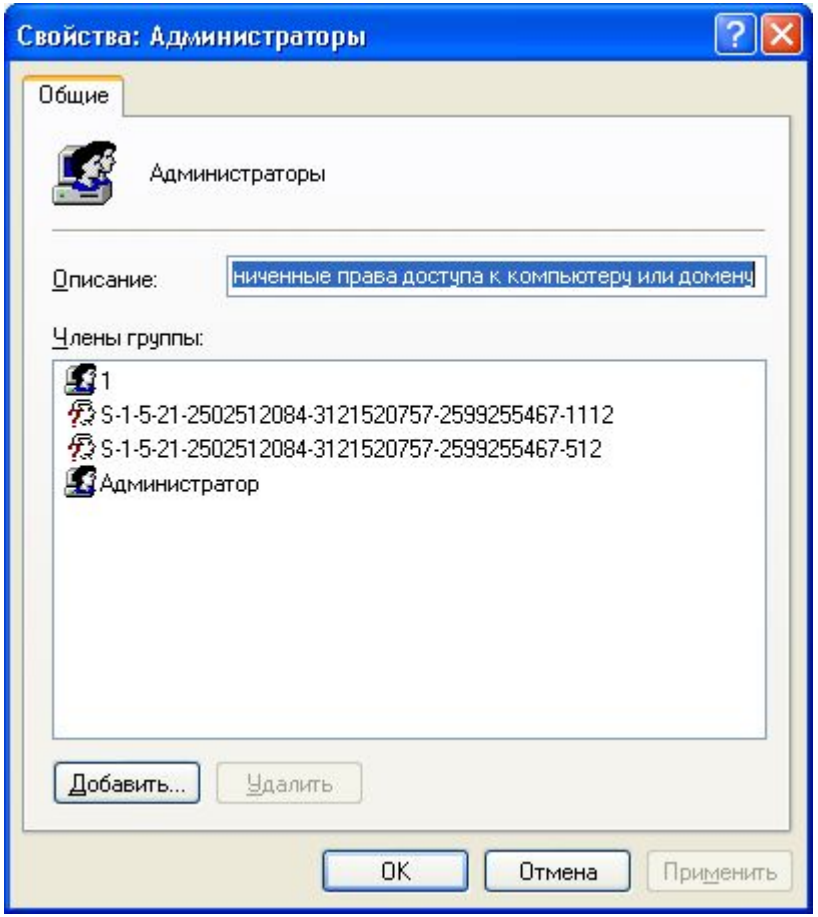


Результирующие права

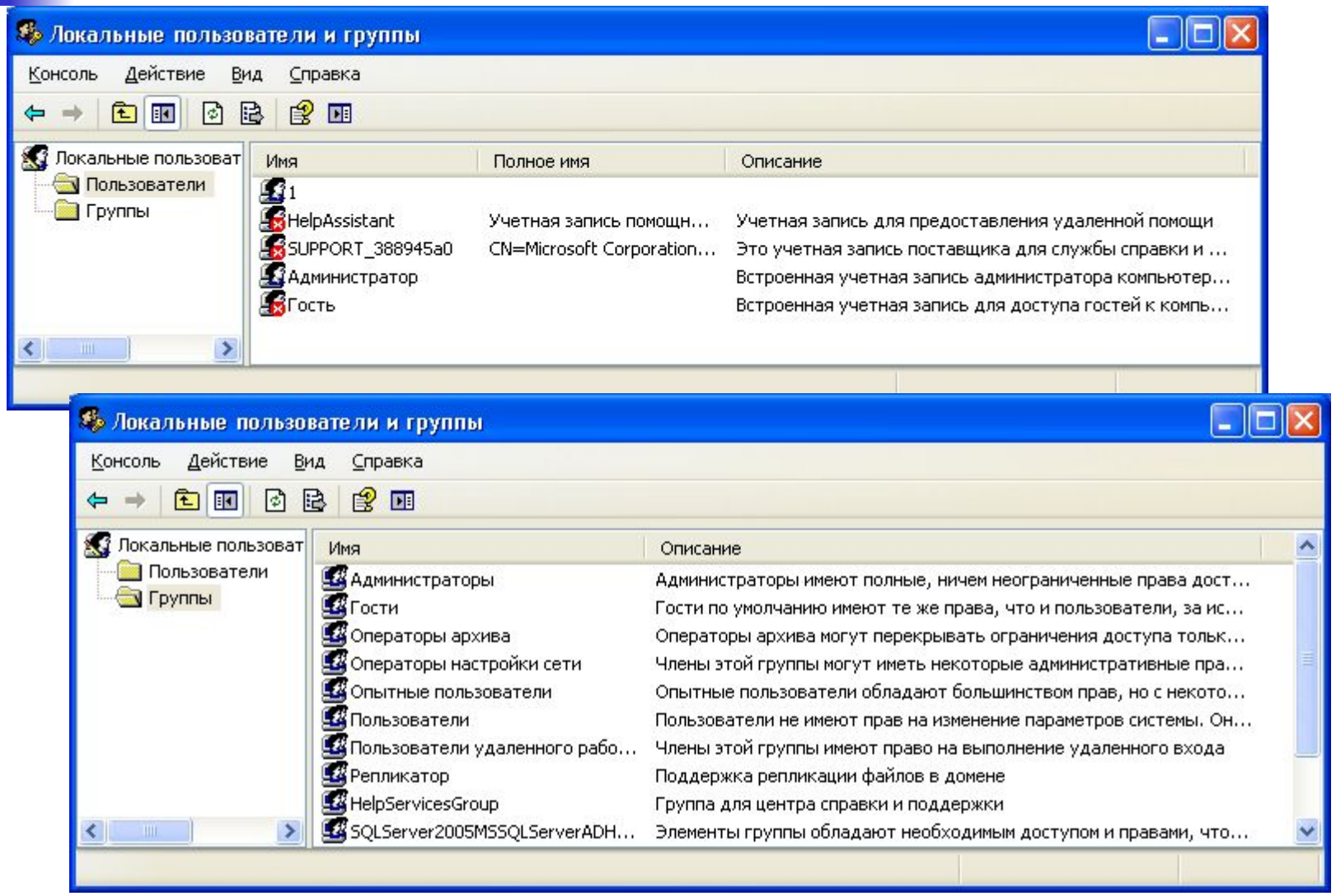


Учётные записи





Учётные записи



Обращение к хосту

NetBIOS – имя **PC1**
DNS – имя **pc1.grsu.by**
IP-адрес **10.31.17.203**

Обращение к файлу

UNC *Server*\disk_d\folder\file.txt **\\PC1\disk_d\folder\file.txt**
\\pc1.grsu.by\disk_d\folder\file.txt
\\10.31.17.203\disk_d\folder\file.txt

URI **smb://10.31.17.203/disk_d/folder/file.txt**
ftp://10.31.17.203/disk_d/folder/file.txt
http://10.31.17.203/disk_d/folder/file.txt

UNCW **\\serverNW\disk_d:folder\file.txt**

УПРАВЛЕНИЕ РЕСУРСАМИ СЕТИ

Большая компьютерная сеть нуждается в централизованном хранении как можно более полной справочной (технической) информации:

- **о пользователях сети** (именах для входа в систему, паролях, правах доступа к ресурсам и т.д.);
- **о компонентах сети** (серверах, клиентских компьютерах, маршрутизаторах, шлюзах и т.д.);
- **о ресурсах сети** (томах файловых систем, принтерах и др.)

Одноранговая сеть

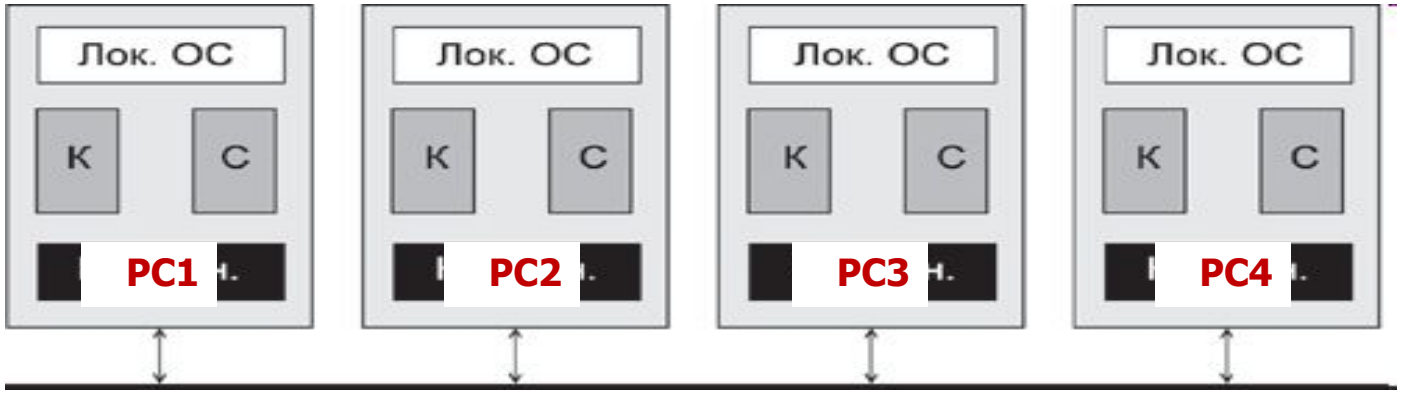
Списки прав доступа

ACL PC1:
D:\ USER_1 R
C:\ USER_2 RW

ACL PC2:
D:\ USER_1 R
C:\ USER_2 RW

ACL PC3:
D:\ USER_1 R
C:\ USER_2 RW

ACL PC4:
D:\ USER_1 R
C:\ USER_2 RW



Локальные учетные записи

SAM PC1:
USER_1
USER_2
…
USER_N

SAM PC2:
USER_1
USER_2
…
USER_N

SAM PC3:
USER_1
USER_2
…
USER_N

SAM PC4:
USER_1
USER_2
…
USER_N

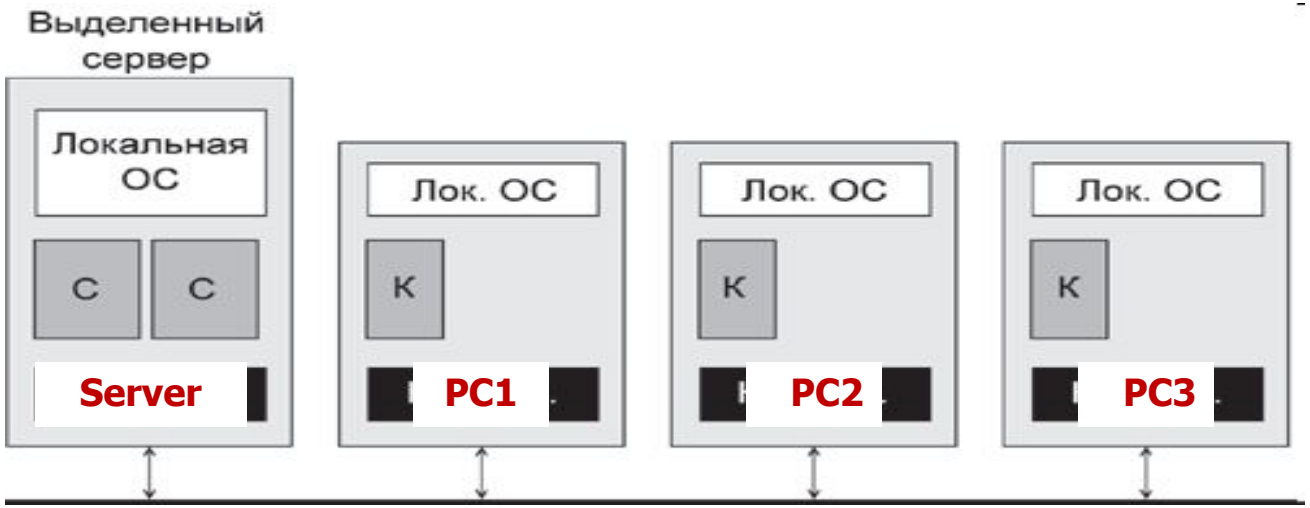
Сеть с сервером учётных записей

Списки прав доступа

ACL PC1:
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW

ACL PC2:
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW

ACL PC3:
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW



Локальные учетные записи

SAM SERVER:
USER_1
USER_2
...
USER_N

SAM PC1:
Administrator

SAM PC1:
Administrator

SAM PC1:
Administrator

Служба каталогов

В сетевых операционных системах для хранения упорядоченной справочной информации используется централизованная база справочной информации –

служба каталогов (Directory Services).

Стандарты служб каталогов:

OSI X.500, DAP (Directory Access Protocol), **LDAP**

Служба каталогов *обычно строится на основе модели клиент-сервер:*

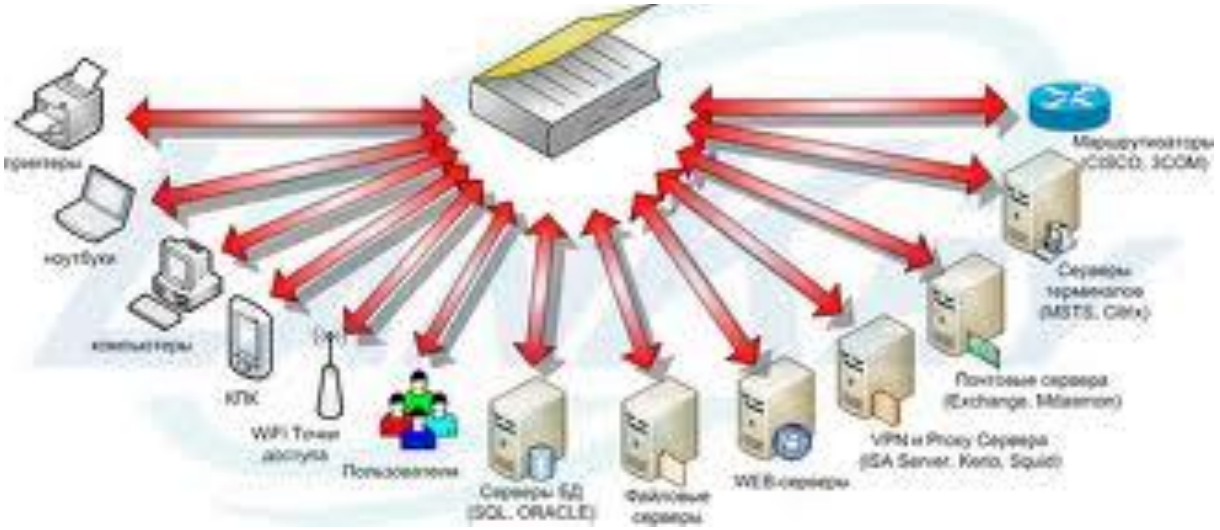
- *серверы хранят базу справочной информации.*
- *клиенты используют эту информацию.*

Наибольшее распространение получили каталоги:

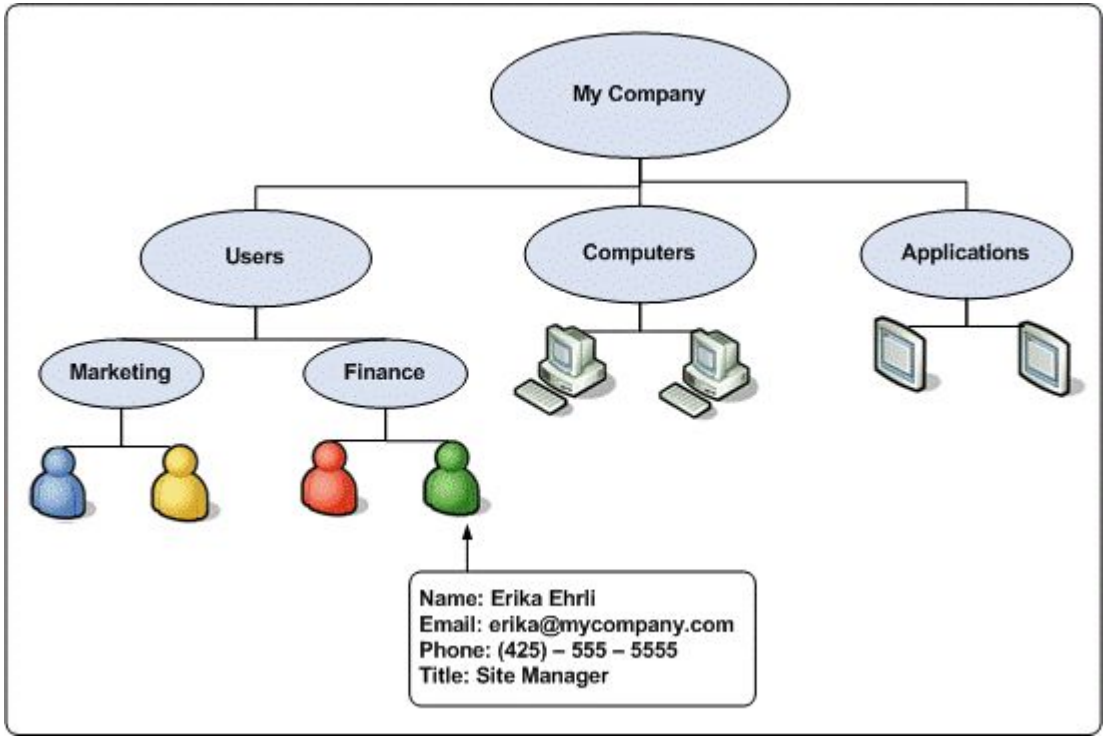
- служба **Active Directory** для Windows;
- служба **NDS** компании Novell.

Домен Windows

Домен Windows - группа компьютеров, пользователей и ресурсов, образующих общую область администрирования и управляемых, как одно целое



Домен Windows



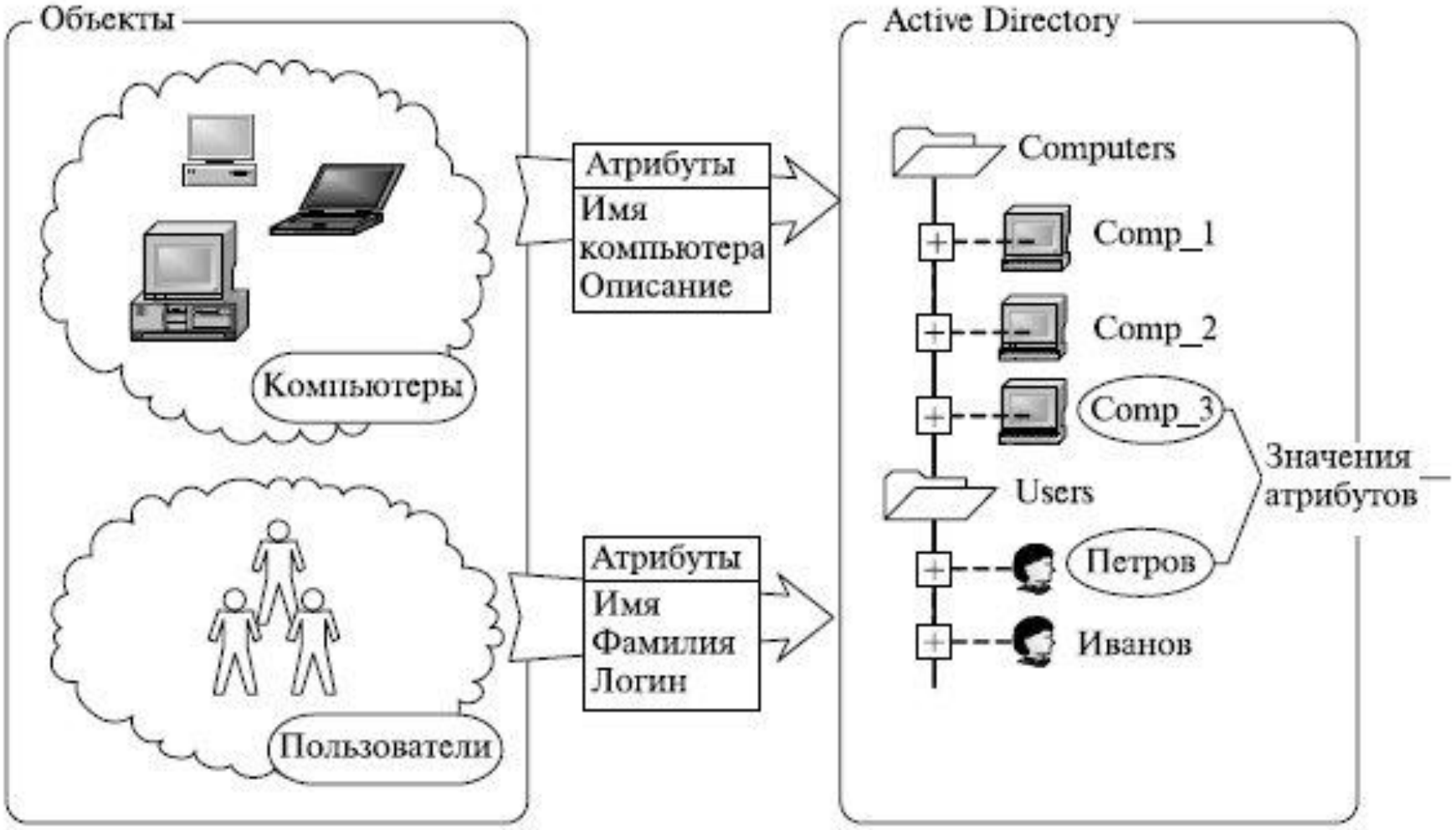
Active Directory (AD)

Active Directory содержит информацию о таких объектах, как сетевые учетные записи, группы, серверы и принтеры, а также другую информацию о домене.

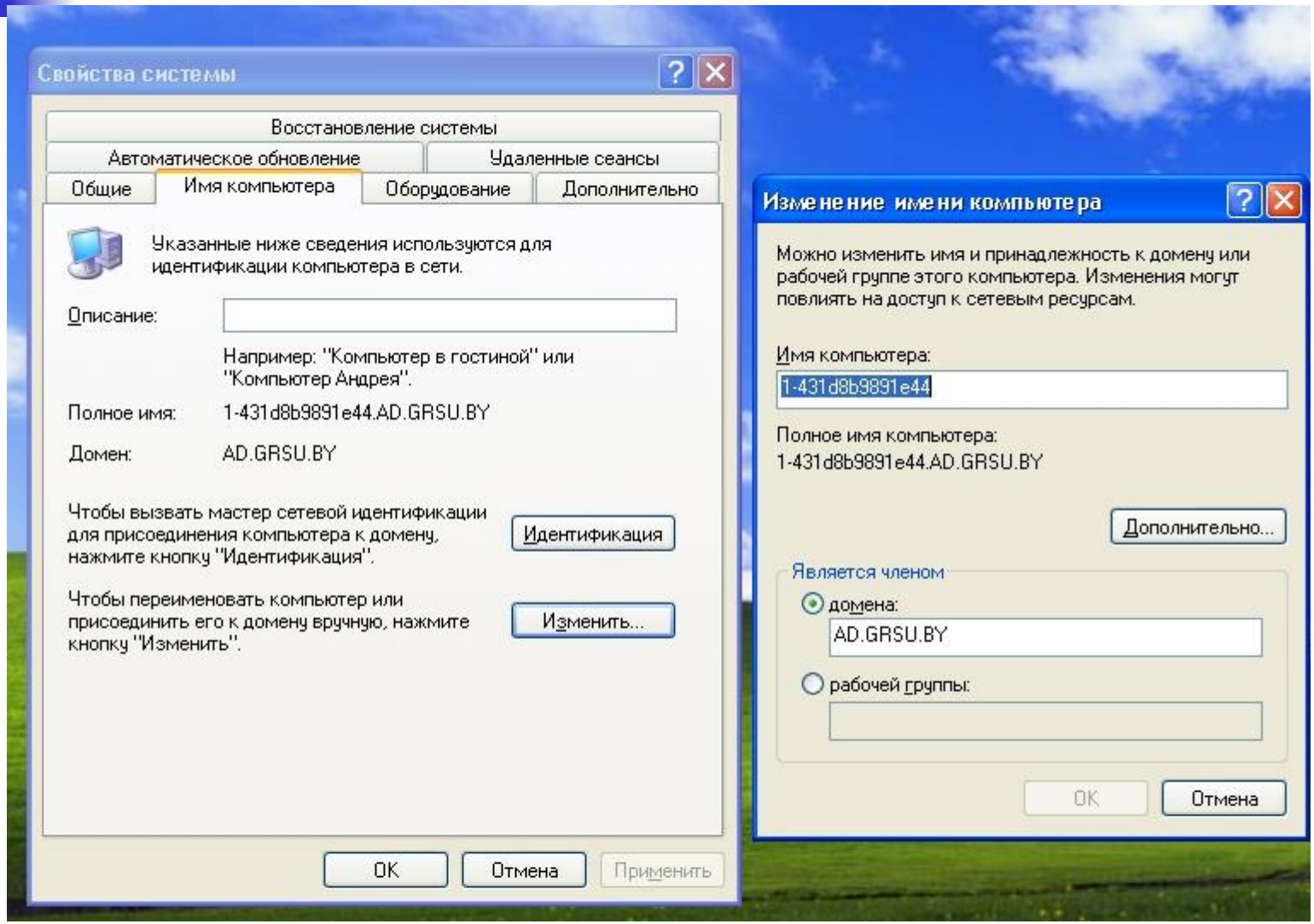
Active Directory поддерживается в Windows Server 2003, Windows Server 2008.

AD - база данных LDAP

Служба каталогов Active Directory



Служба каталогов Active Directory




Вход в Windows
Microsoft
Windows xp
Professional
© 1985-2001
Корпорация Майкрософт
Microsoft
Пользователь:
netuser
Пароль:
Вход в:
TEST1 (этот компьютер)
AD-GRSU
MF
TEST1 (этот компьютер)
EN
OK
Отмена
Завершение работы...
Параметры <<

- **Доменный компонент (DC - Domain Component).** Используется для определения компонента DNS-имени объекта Active Directory.
- **Организационная единица (OU).** Организационная единица.
- **Общее имя (CN - Common Name).** Объект, отличный от DC или OU; например, CN можно использовать для определения компьютерной или пользовательской учетной записи.

Служба каталогов Active Directory

Имена объектов каталогов:

DN (Distinguished Name, уникальное имя):

=

DC (компонент домена)

+

OU (организационный модуль)

+

CN (общее имя)

Примеры:

DC=grsu OU=main CN=users CN=Sidorov

LDAP://cn=Sidorov, cn=users, ou=main, dc=grsu

Служба каталогов Active Directory

База данных Active Directory содержит следующие структурные объекты:

- **Домены**. *Домен* служит в качестве административной границы, он определяет и границу политик безопасности. Каждый домен имеет, по крайней мере, один *контроллер домена* .
  ad.grsu.by
  AD-GRSU

- ***Деревья доменов*.** **ad.grsu.by**

  mf.ad.grsu.by **ftf.ad.grsu.by**

- **Леса**. *Лес* определяет границу безопасности для предприятия.

  ad.grsu.by **grsu.com**

- **Сайты**. *Сайт* представляет область сети, где все *контроллеры домена* связаны быстрым, недорогим и надежным сетевым подключением.

- **Организационные единицы**. *Организационные единицы* предназначены для того, чтобы облегчить управление службой Active Directory.

Служба каталогов Active Directory

функции *контроллеров доменов AD:*

- Каждый *контроллер домена* хранит полную копию всей информации Active Directory, относящейся к его домену.

- Все контроллеры в домене автоматически реплицируют между собой все объекты в домене.

***

Все контроллеры равноправны, и каждый из них содержит копию базы данных каталога, в которую разрешается вносить изменения.

***

Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость.

Служба каталогов Active Directory

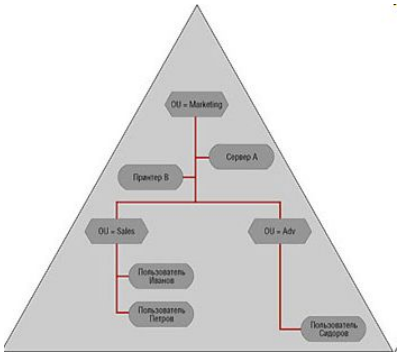


Рисунок 1. Типичная структура домена AD.

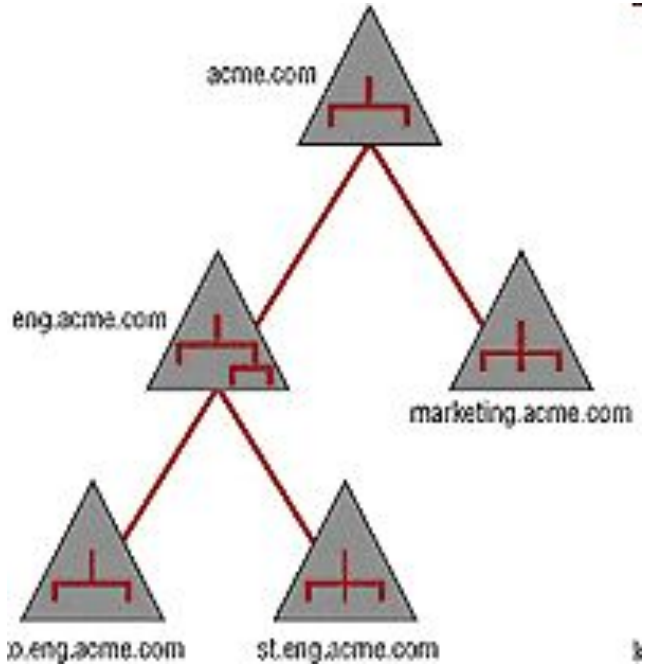


Рисунок 2. Дерево доменов AD.

Active Directory

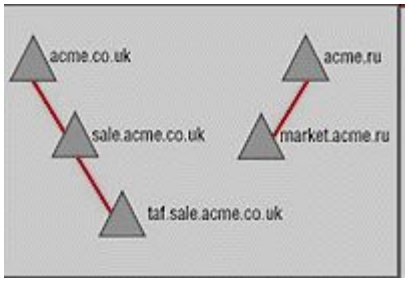
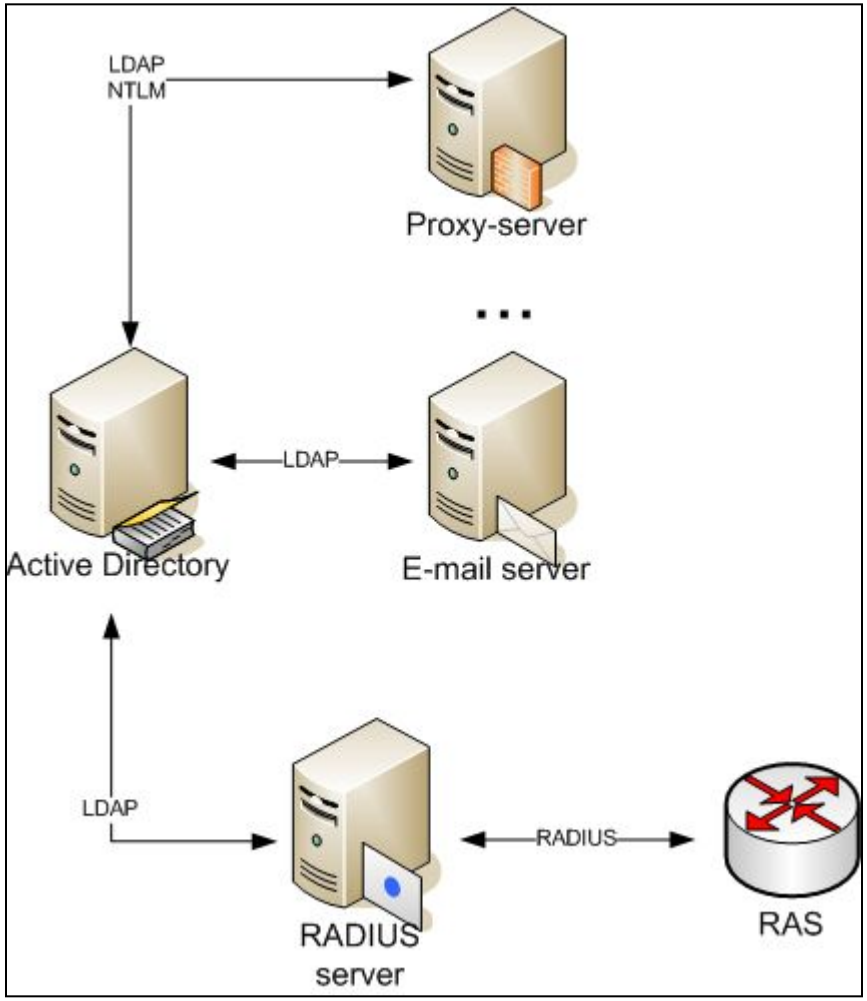
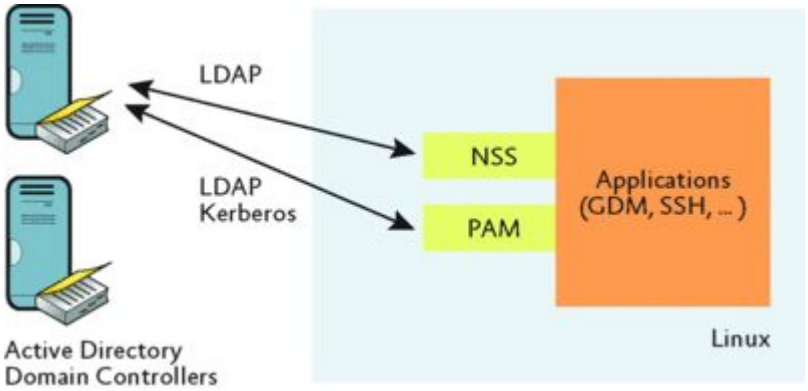
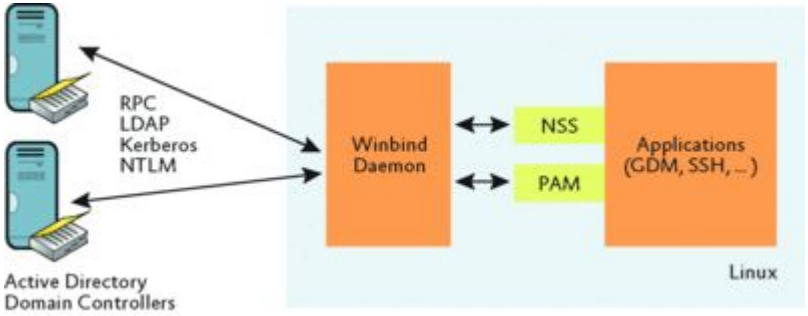


Рисунок 3. Лес доменов AD.

Служба каталогов Active Directory







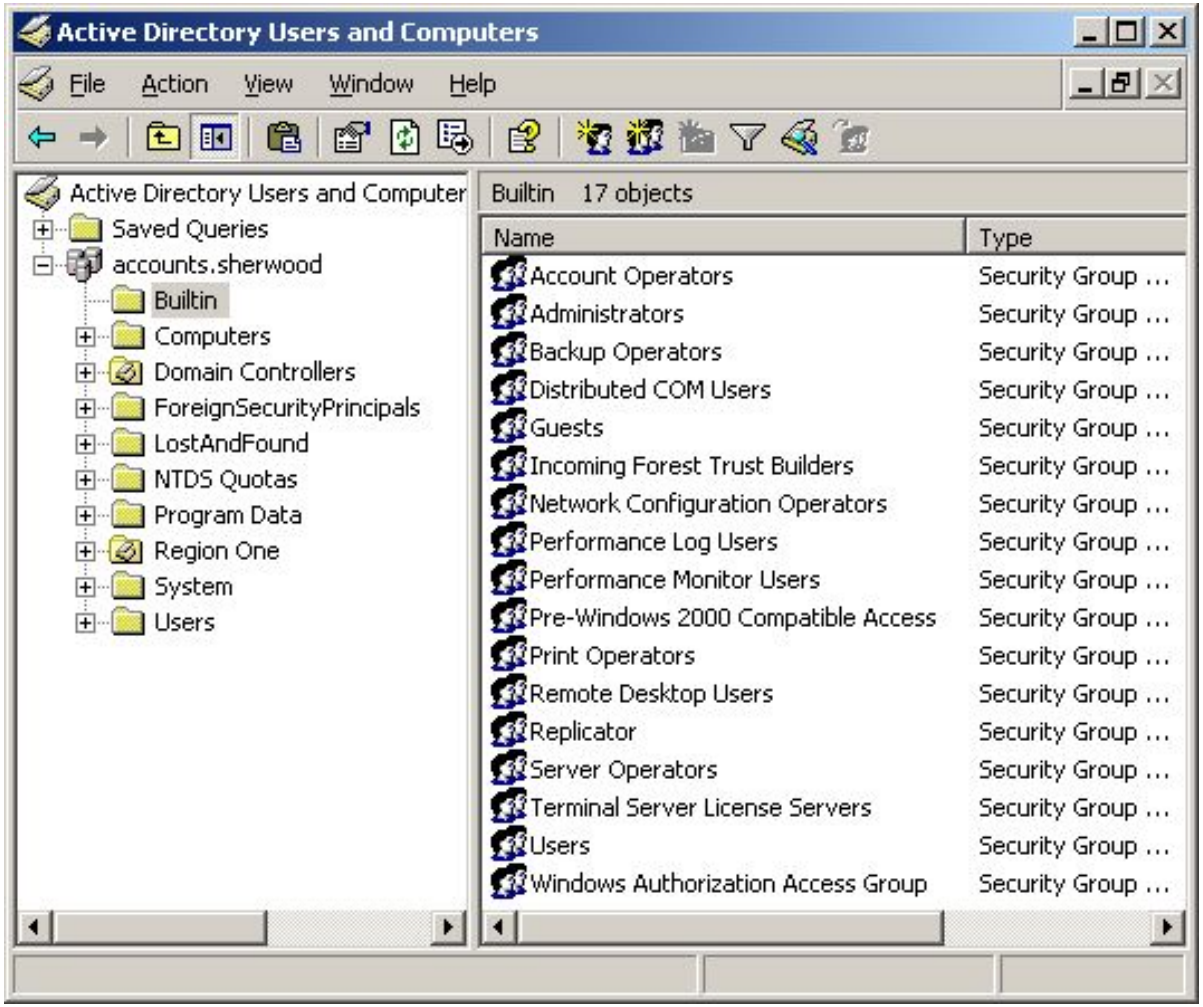
Протоколы аутентификации в AD

NT LAN Manager (NTLM)

Kerberos v.5

LDAP

Служба каталогов Active Directory



%systemroot%\NTDS\NTDS.DIT

Политики Active Directory

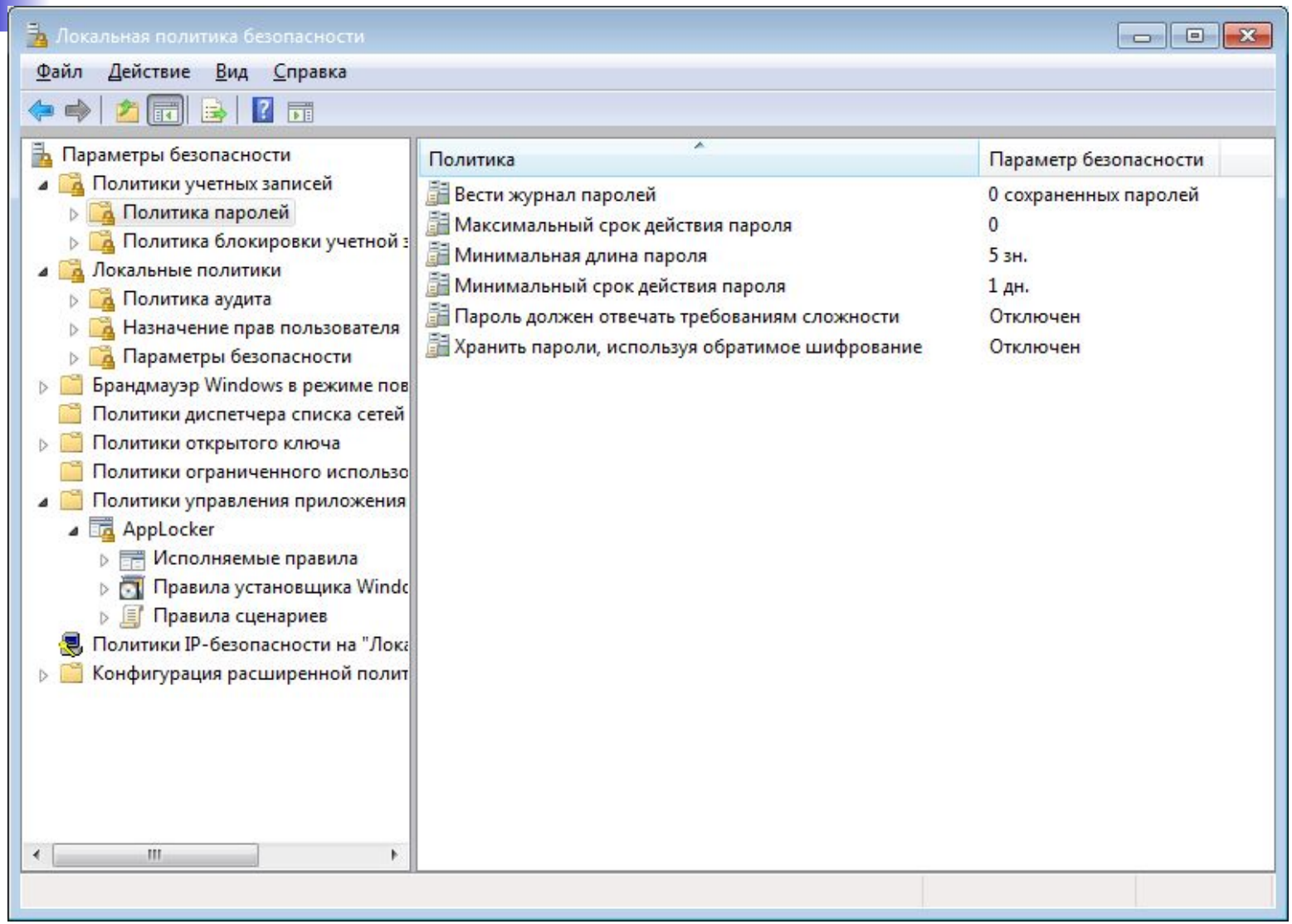
- Локальные политики (secpol.msc)
- Групповые политики (gpedit.msc)

Политики Active Directory

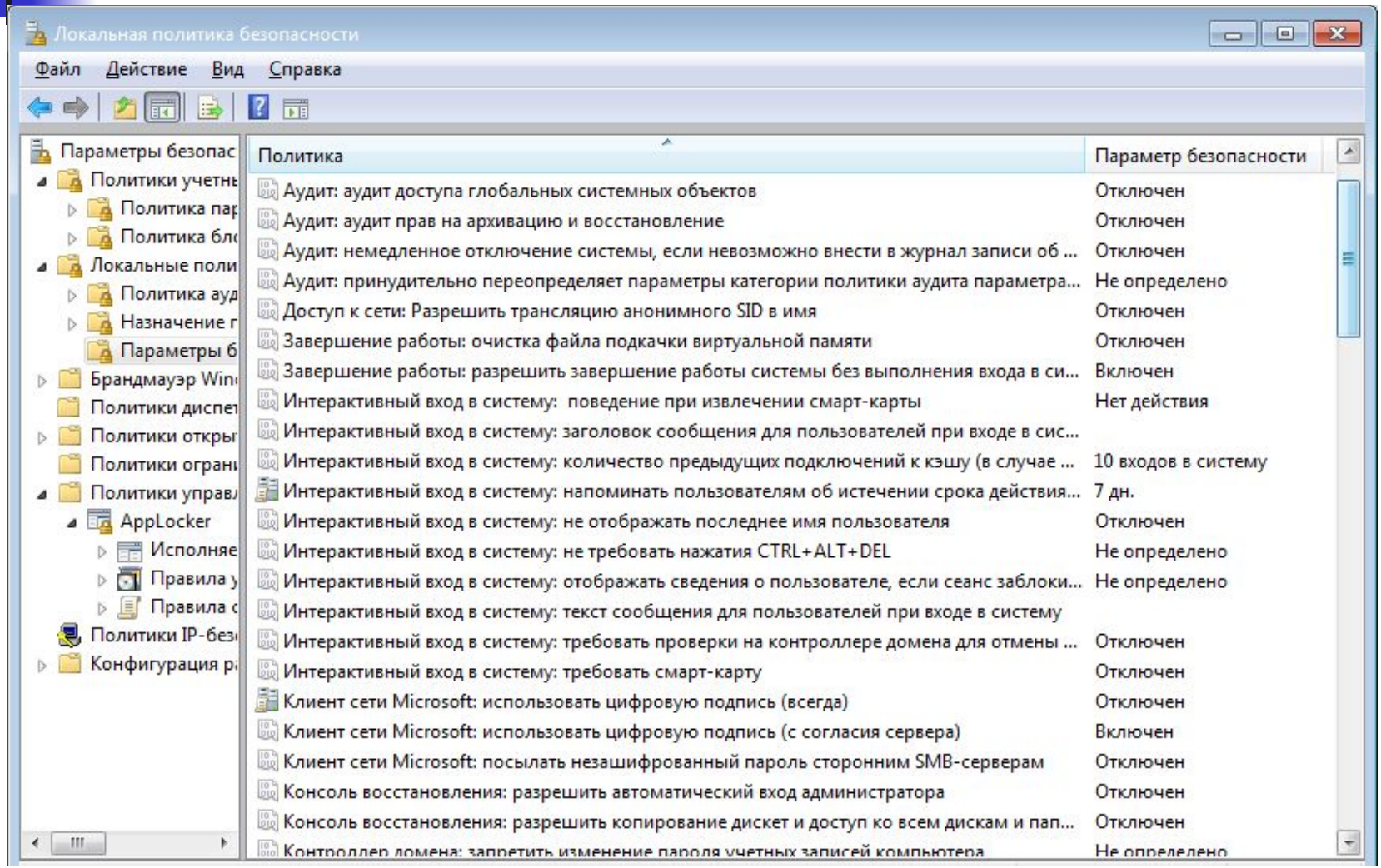
Управление на основе групповых политик (GPO)

Administrative templates (Административные шаблоны)	**Используется для управления параметрами, связанными с системным реестром, для конфигурирования параметров настройки приложений и пользовательского рабочего стола, включая доступ к компонентам операционной системы, к панели управления и конфигурацию автономных файлов.**
Security (Безопасность)	**Используется для управления локальным компьютером, доменом и параметрами настройки сетевой защиты, включая управление пользовательским доступом к сети, конфигурирование политик учетных записей и управление правами пользователей.**
Software installation (Установка программного обеспечения)	**Используется для централизованного управления установкой программного обеспечения.**
Scripts (Сценарии)	**Используется для определения сценариев, которые могут выполняться при запуске или выключении компьютера, при входе пользователя в систему и выходе из нее.**
Folder redirection (Перенаправление папки)	**Используется для хранения некоторых папок пользовательского профиля на сетевом сервере. Папки My Documents (Мои документы) выглядят так, будто они хранятся локально, но фактически они хранятся на сервере, где к ним можно обращаться с любого компьютера в сети.**

Политики Active Directory



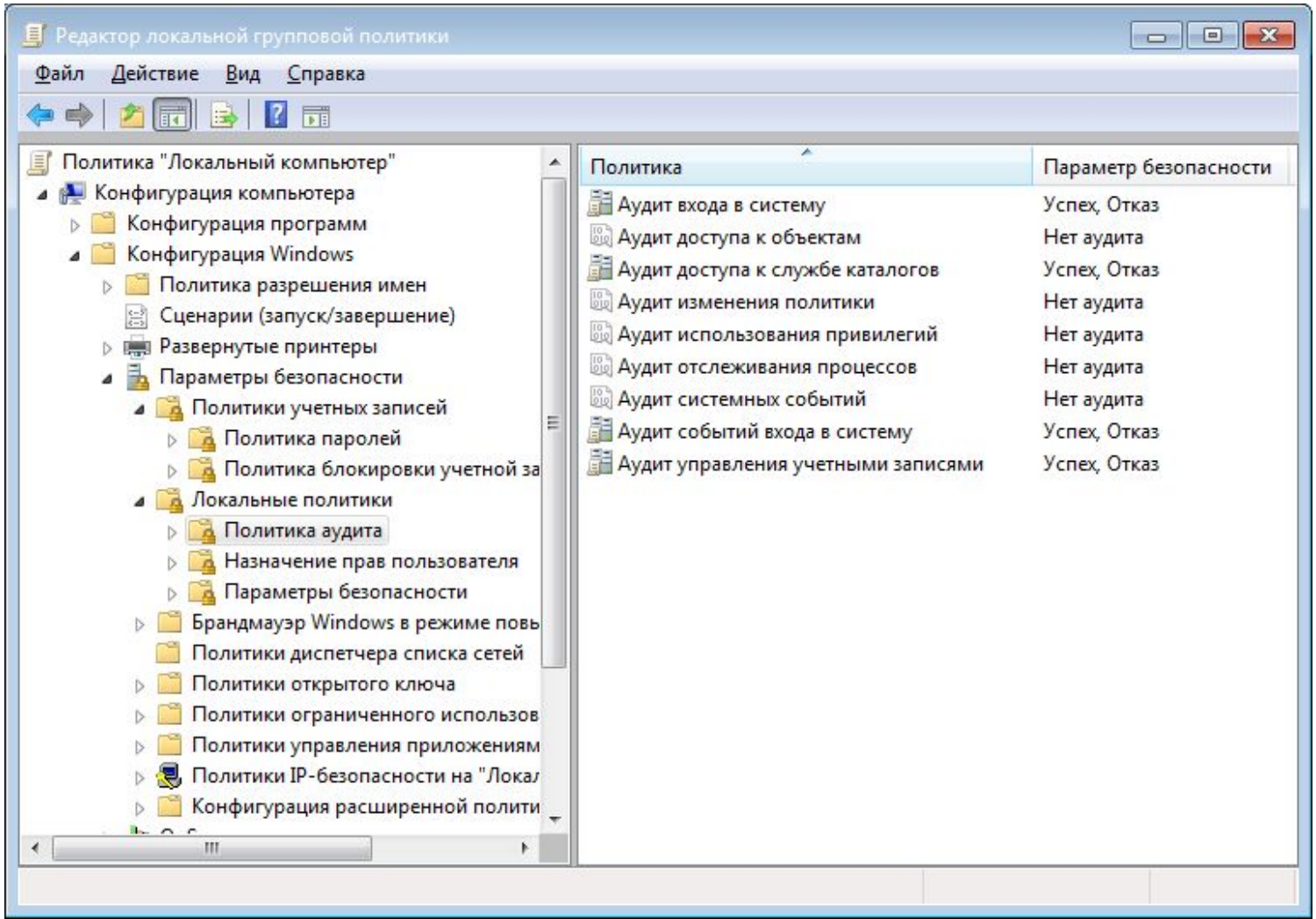
Политики Active Directory



Enabled (Включен), Disabled (Отключен) и Not Configured (Не определено)

Политики Active Directory

gpedit.msc



Политики Active Directory

- Default Domain Policy (Заданная по умолчанию политика домена)
- Default Domain Controllers Policy (Заданная по умолчанию политика контроллеров домена)

Виды групповых политик и порядок их применения

- 1**. Local group policy (Локальная групповая политика).**
- 2. **Site-level group policies (Групповые политики уровня сайта).** Групповые политики, связанные с объектом сайта в Active Directory.
- 3. **Domain-level group policies (Групповые политики уровня домена).** Групповые политики, связанные с объектом домена в Active Directory.
- 4**. OU-level group policies (Групповые политики уровня OU).** Если домен содержит несколько уровней OU, вначале применяются групповые политики более высоких уровней OU, а затем — OU низшего уровня.

GPResult.msc

Политики Active Directory

Инструменты управления групповой политикой

- GPEdit.msc
- GPUpdate.msc
- GPResult.msc

Сетевое управление программным обеспечением рабочих станций
IntelliMirror

- User Data Management (**управление данными пользователя**). Обеспечивает пользователям доступ к рабочим файлам с любого компьютера сети, или даже после отключения от нее, с помощью Windows Synchronization Manager, который позволяет дублировать каталоги на локальном диске.

- Software Installation and Maintenance (**установка и поддержка программного обеспечения**). Устанавливает приложения и программы на любую рабочую станцию, на которых имеется соответствующая потребность.

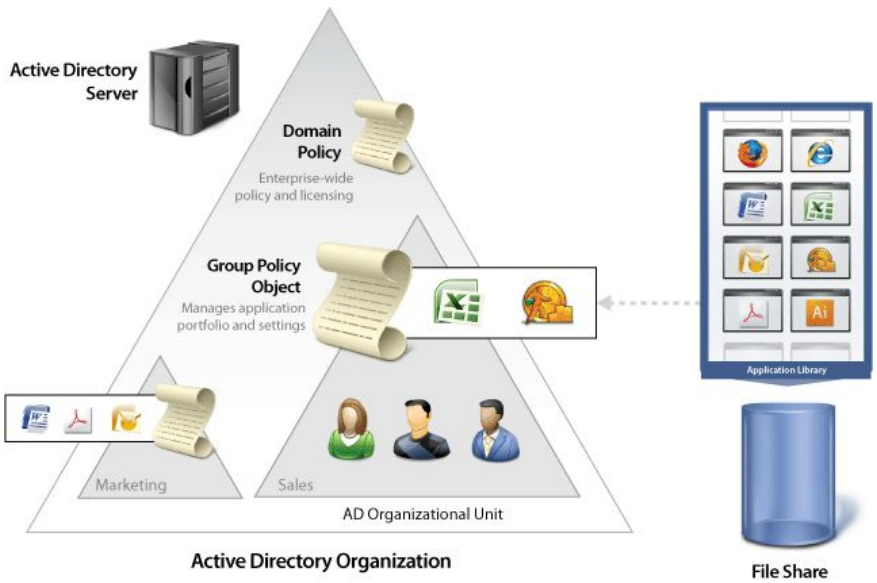
- User Settings Management (**управление пользовательскими установками**). Предоставляет пользователям их собственные настройки конфигурации рабочего стола, прикладных программ и другие персональные предпочтения при работе с любого компьютера сети.

Active Directory

Сетевое управление программным обеспечением рабочих станций

- Групповые политики
- Microsoft Systems Management Server (SMS)
- Software Update Service (SUS)
- LANDesk Intel и др.

wake-on-LAN



Программирование Active Ditectory

VB/VBScript, JScript, C/C++

- интерфейсы службы Active Directory (ADSI);
- интерфейсы MAPI;
- интерфейс программирования LDAP API.

класс DirectoryEntry

Инструменты управления каталогом

- Adsiedit.msc
- Ldp.exe
- Domain.msc
- Dsa.msc
- Active Directory Web Services (ADWS)

Инструменты управления каталогом (командная строка)

Команда	Функции
DSAdd	Добавление объектов (пользователи, группы, ОП и др.)
DSGet	Отображение атрибутов объекта
DSMod	Модификация объекта
DSMove	Перемещение и переименование объекта
DSQuery	Отработка запросов
DSRM	Удаление объектов

Восстановление контроллера домена:

- Репликация с действующим контроллером;
- Использование резервной копии сервера;
- Использование резервной копии базы данных домена.

Backup

Ntdsutil.exe

Automated System Recovery - ASR

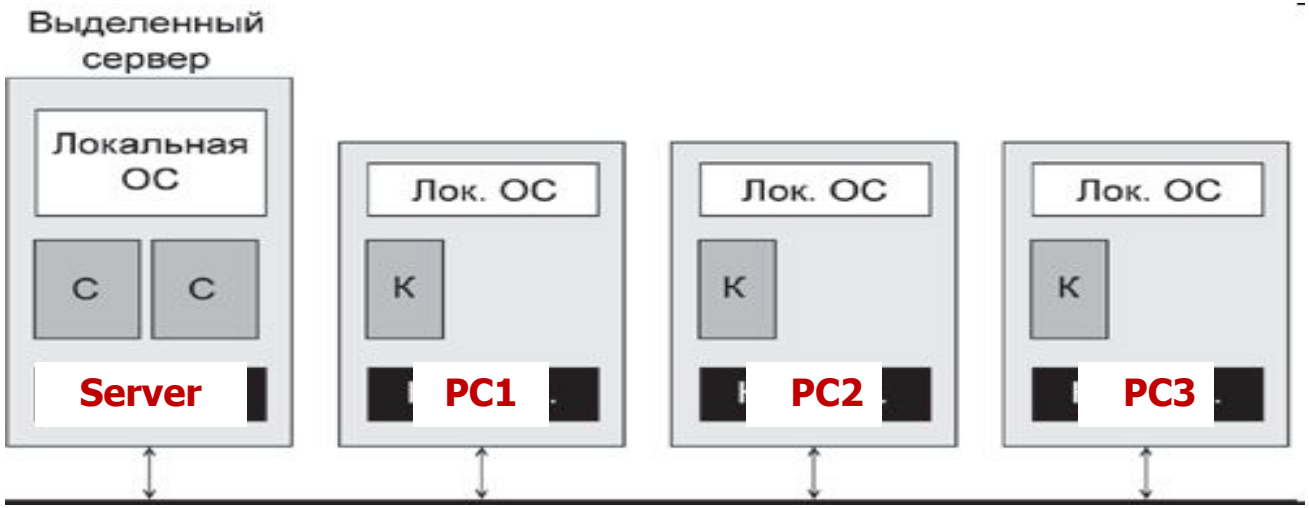
Active Directory

Списки прав доступа

ACL PC1:
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW

ACL PC2:
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW

ACL PC3:
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW



Локальные учетные записи

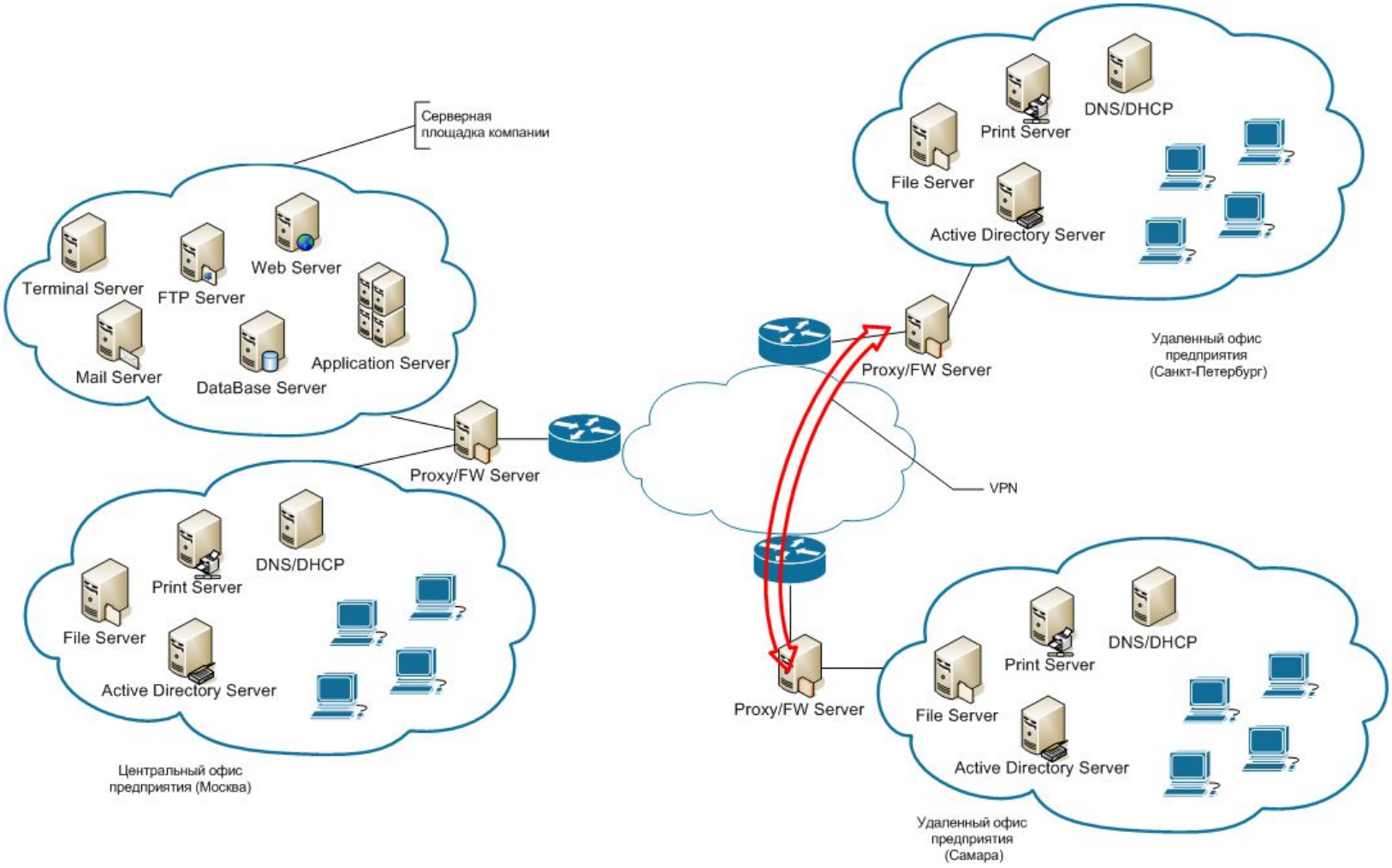
SAM SERVER:
USER_1
USER_2
...
USER_N

SAM PC1:
Administrator

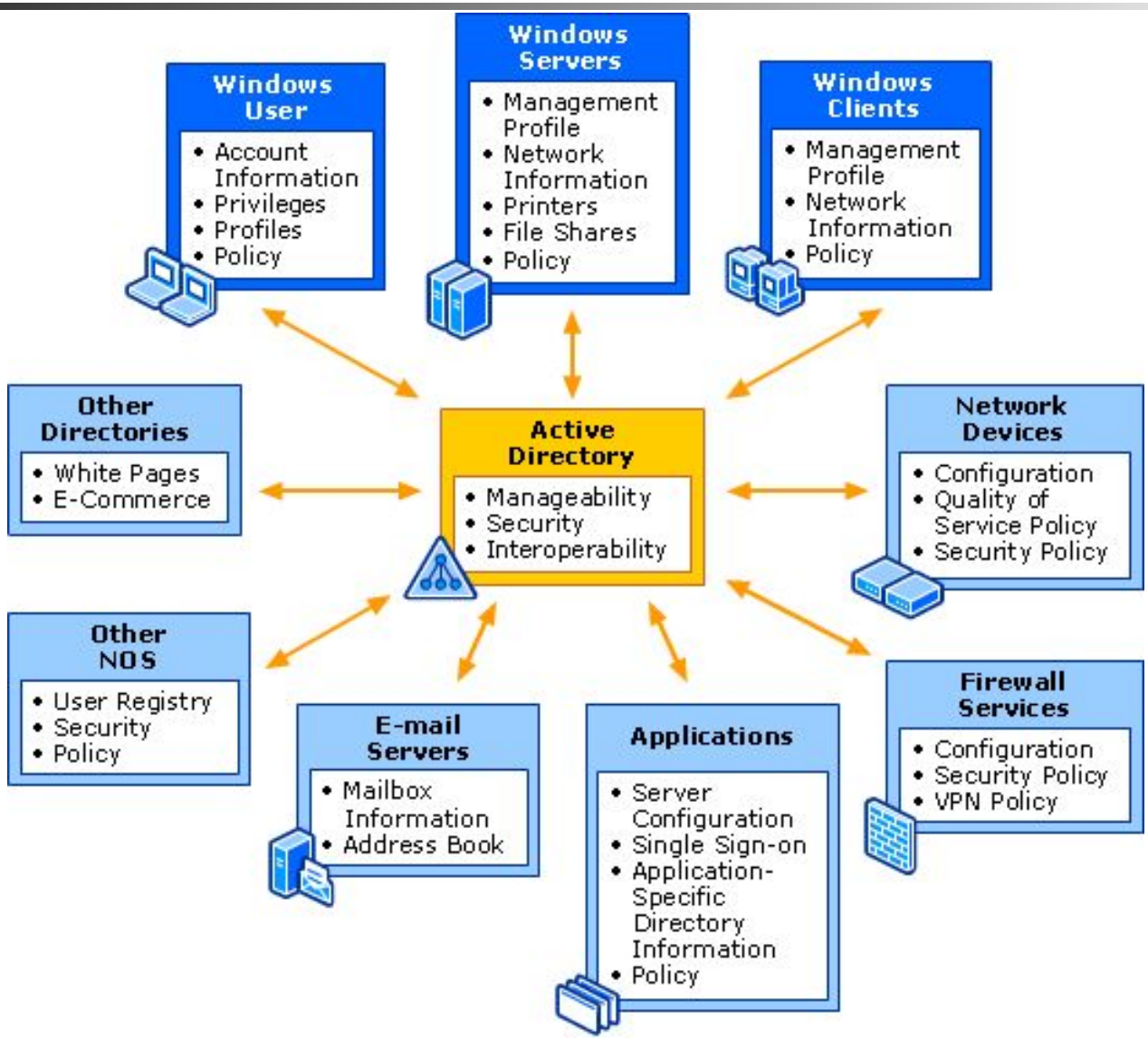
SAM PC1:
Administrator

SAM PC1:
Administrator

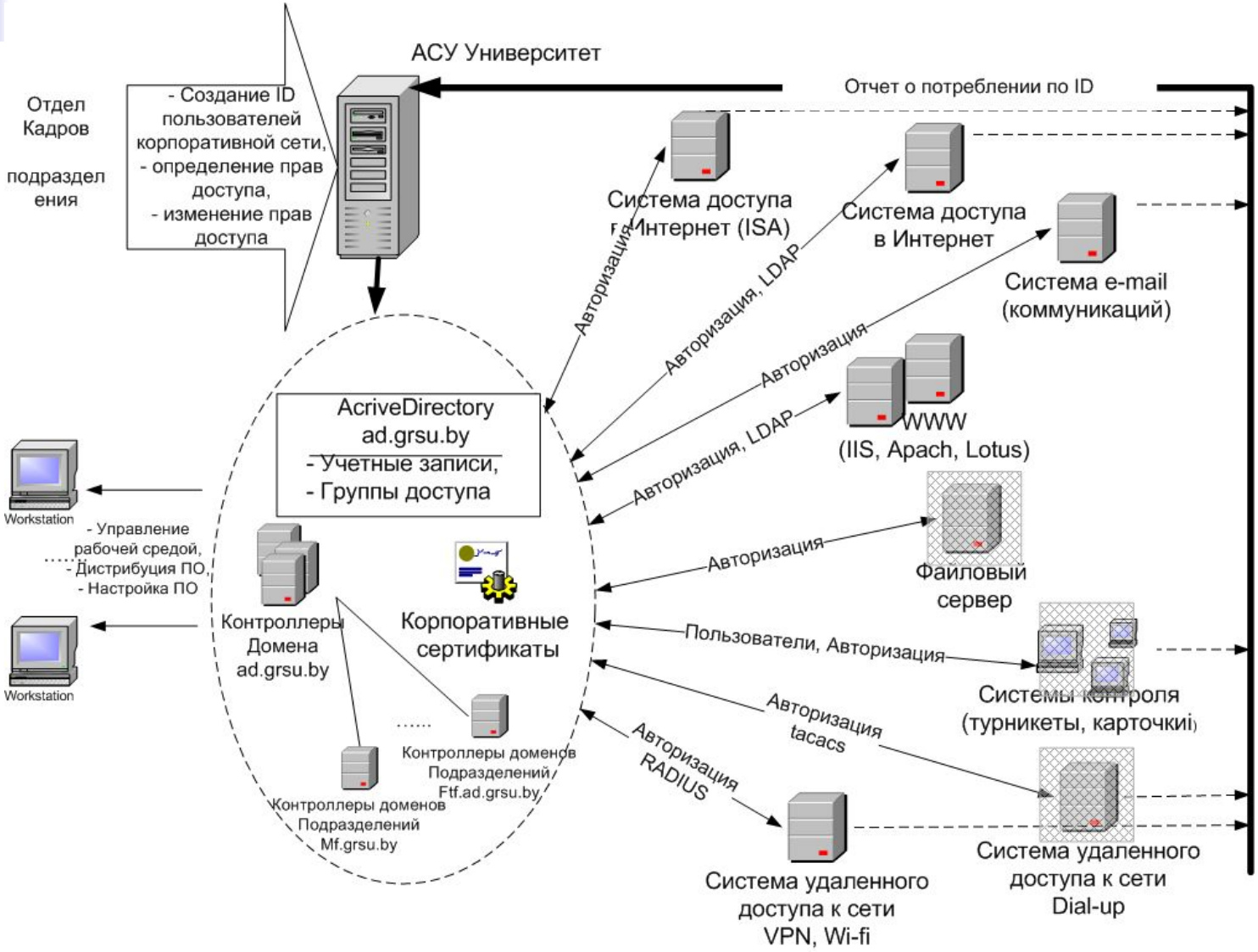
Active Directory



Active Directory



Active Directory

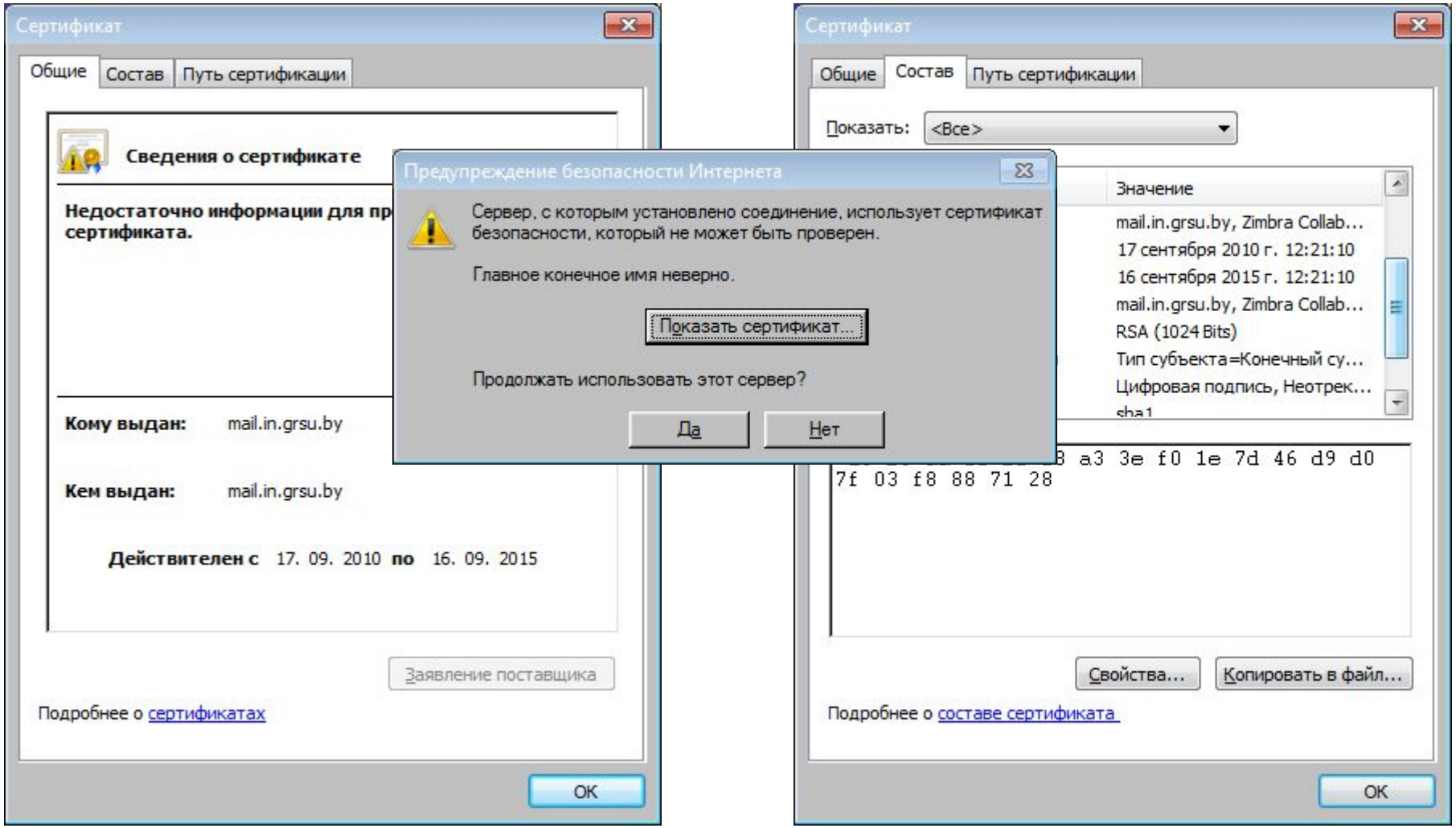


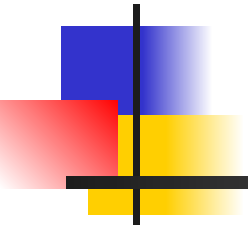
Обеспечение инфраструктуры сети

Обслуживание бизнес-процессов

Обслуживание сети

Цифровой сертификат





Компьютерные системы и сети

Олизарович Евгений Владимирович

ГрГУ им. Я.Купалы. 2012-2013