



Компьютерные системы и сети

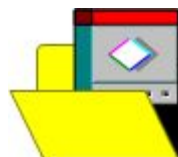
Службы организации корпоративных сетей.
Общий и доступ к ресурсам.
Active Directory.

Олизарович Евгений Владимирович

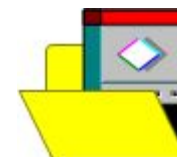
ГрГУ им. Я.Купалы. 2012-2013

Базовые сетевые модели

Программная модель
«клиент - сервер»



Приложение - клиент



Приложение – сервер (URI,
языки запросов, семантика)

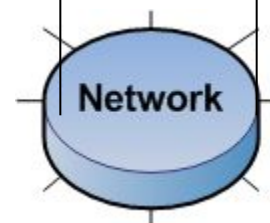
Модель сетевого
взаимодействия
«клиент-сервер» (ВОС,
TCP/IP)



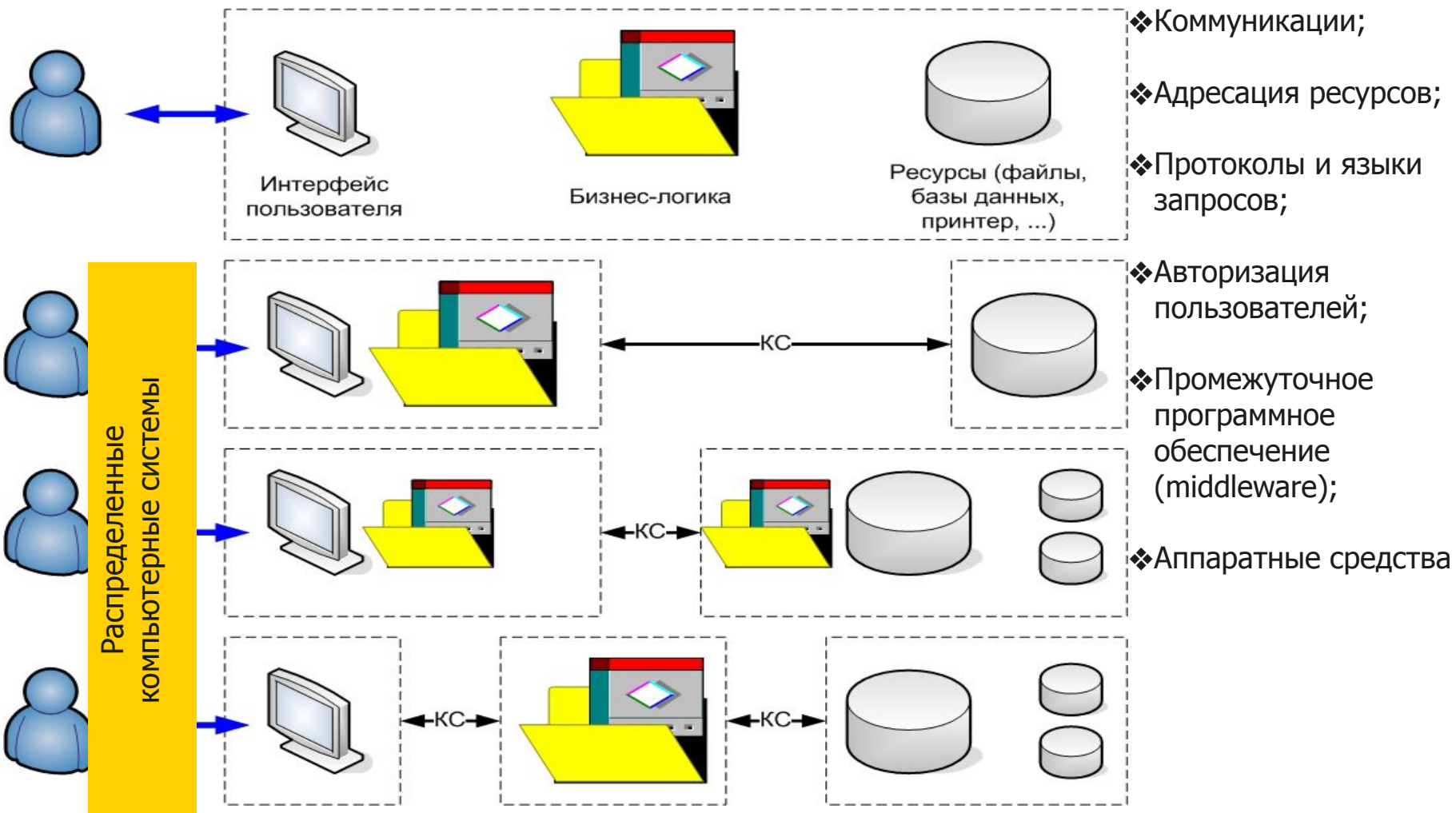
Компьютер 1



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



Обработка данных (модель клиент - сервер)

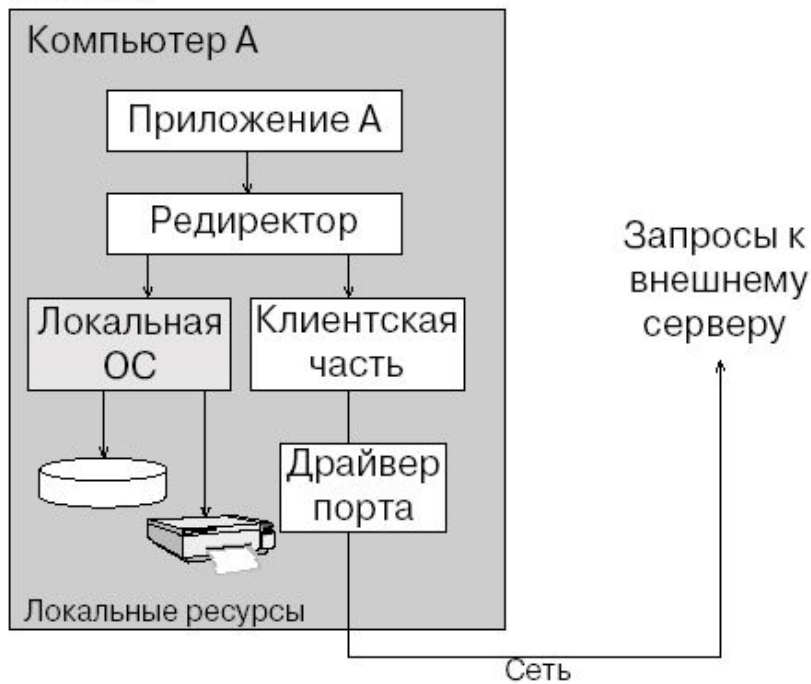


Клиенты и серверы сети

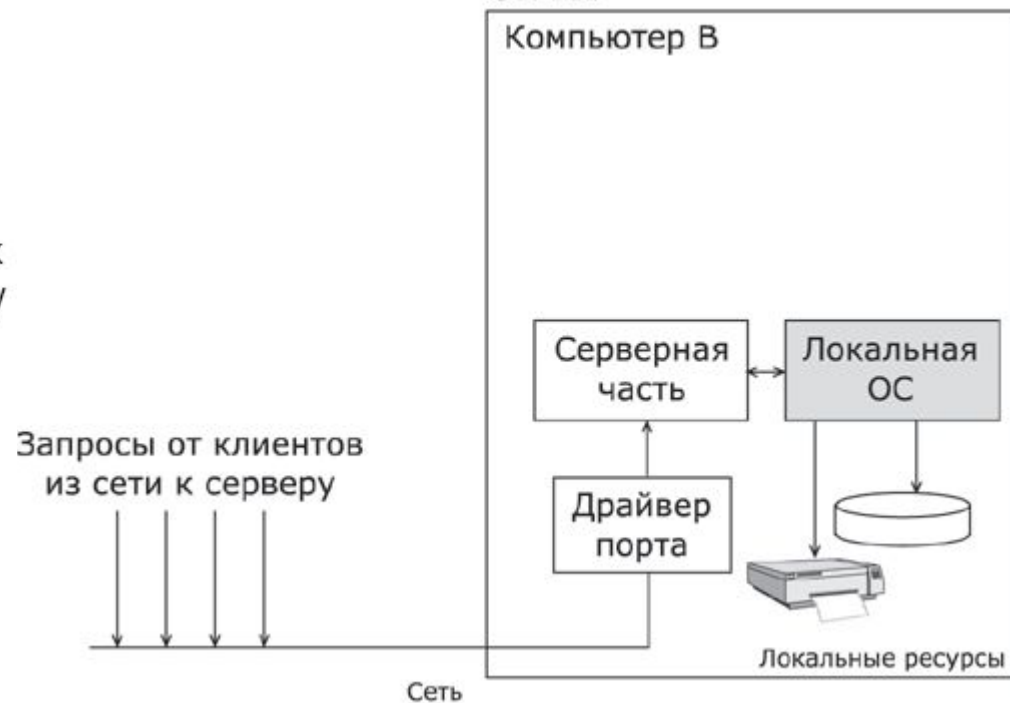
2012/2013



КЛИЕНТ

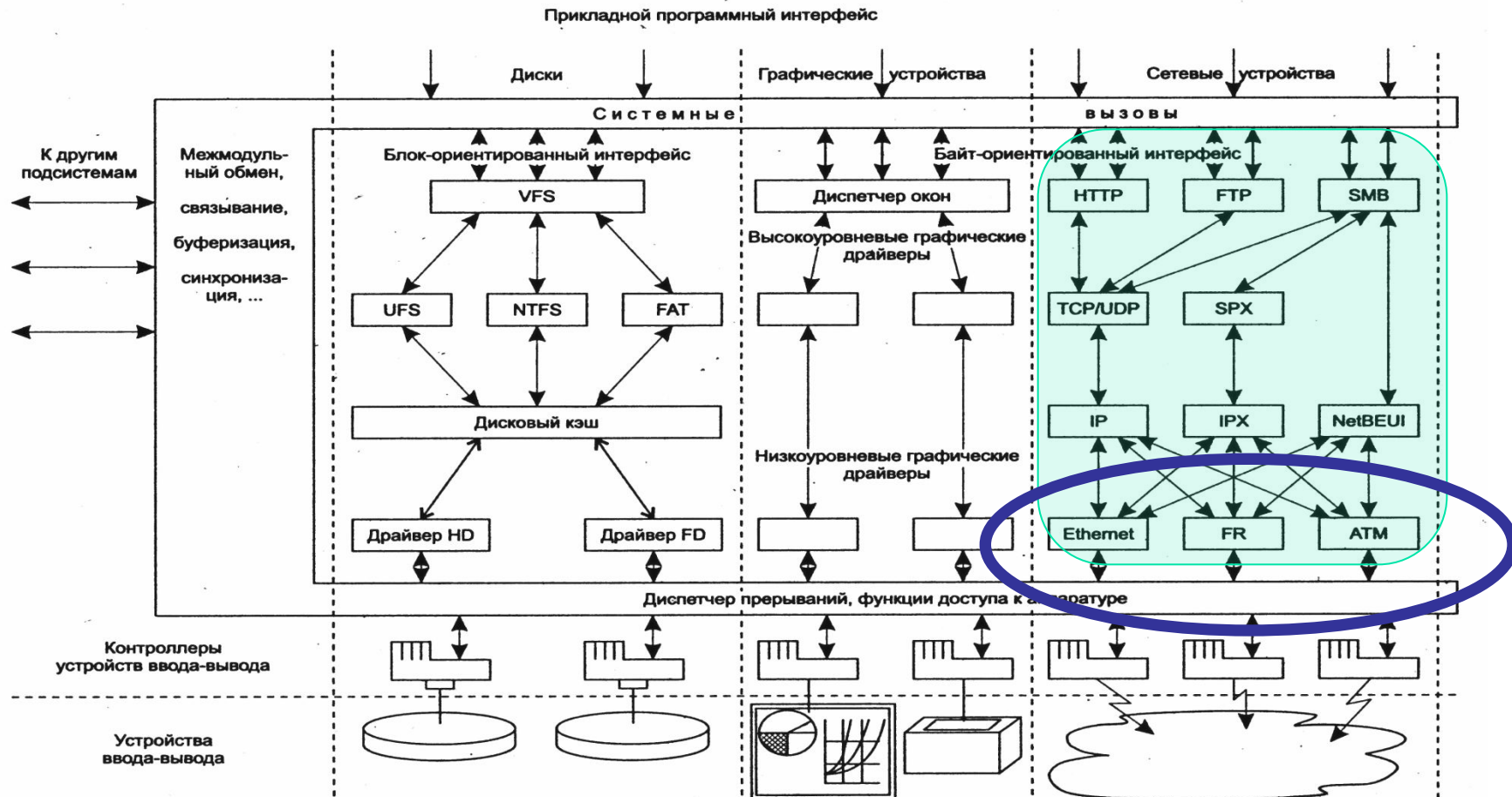


СЕРВЕР



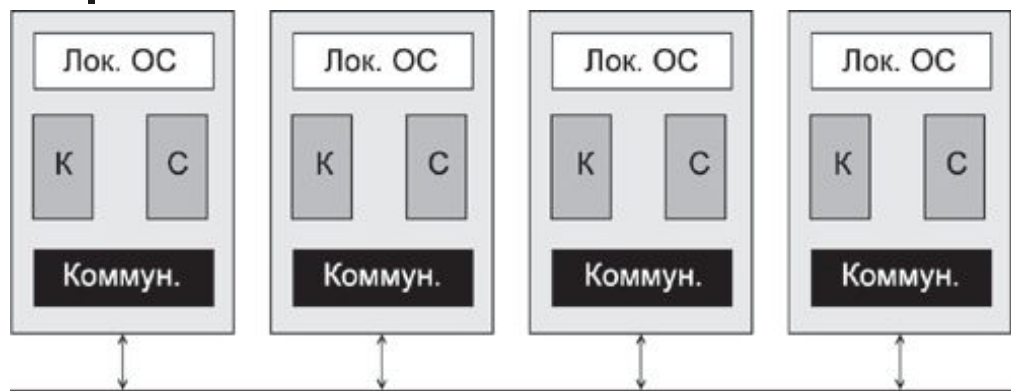
Клиенты и серверы сети

2012/2013



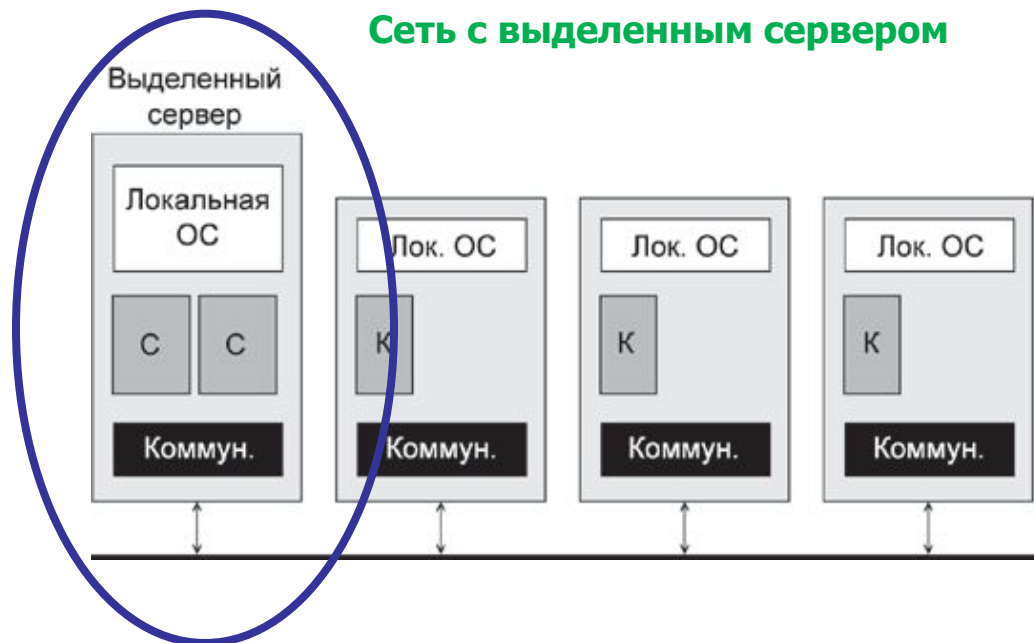
Клиенты и серверы сети

Одноранговая сеть

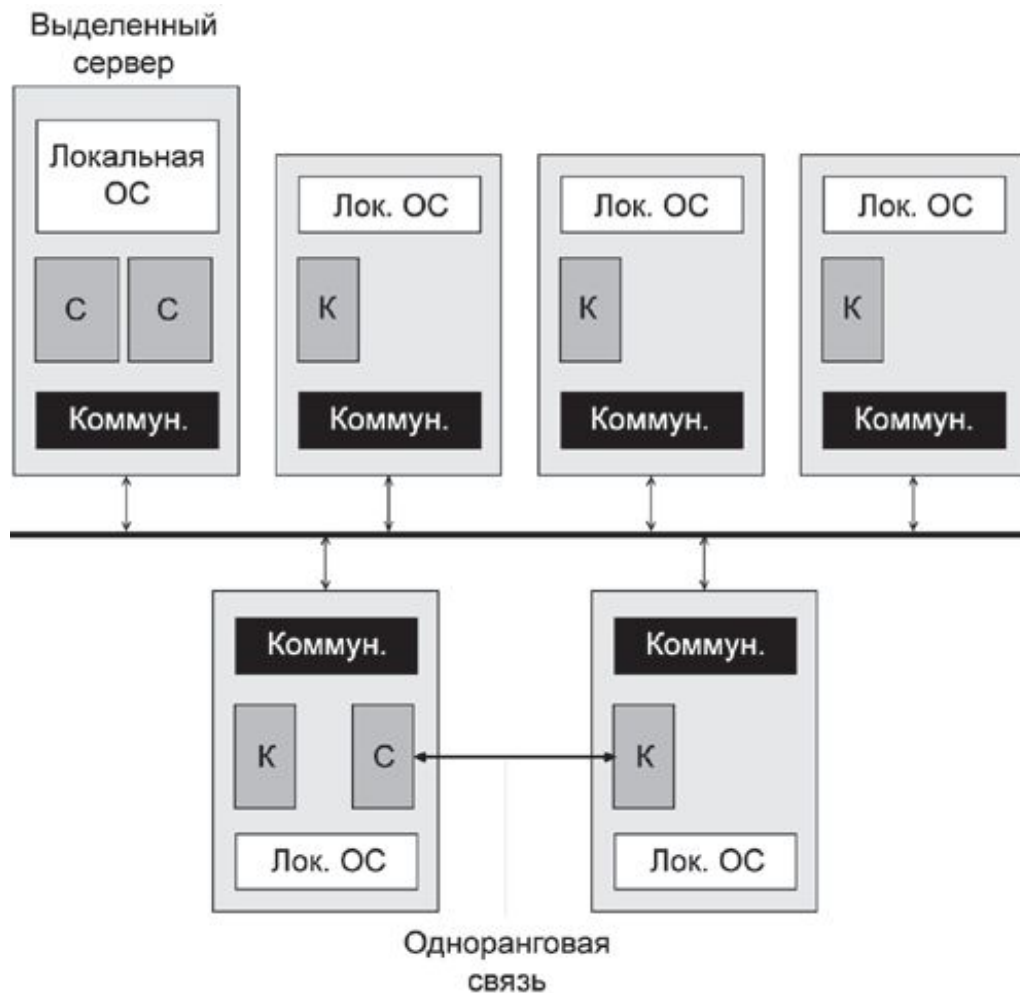


- ❖ Специальная ОС;
- ❖ Производительное ПО;
- ❖ Скоростные коммуникации;
- ❖ Общие дорогостоящие ресурсы;
- ❖ Повышенная безопасность;
- ❖ Резервирование, backup;
- ❖ Единое администрирование;
- ❖ Удобство обслуживания

Сеть с выделенным сервером



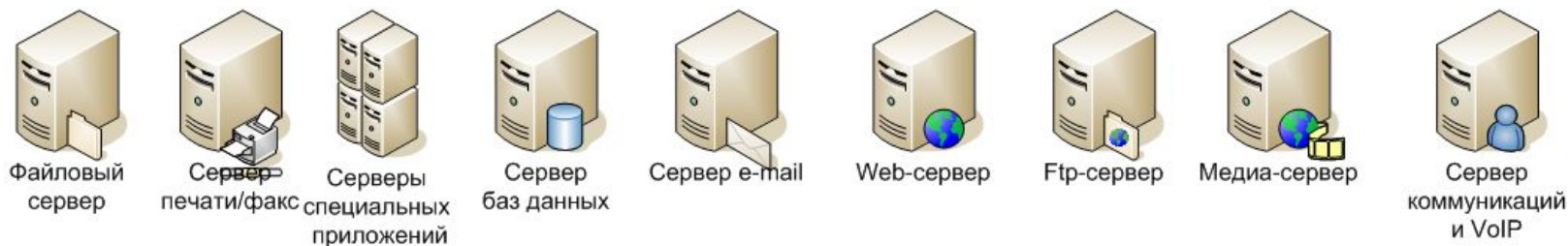
Реальная сеть



Обеспечение инфраструктуры сети



Обслуживание бизнес-процессов



Обслуживание сети



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

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.

Доступ к файлам и данным.
Права доступа.

Сетевое приложение

1. Приложения

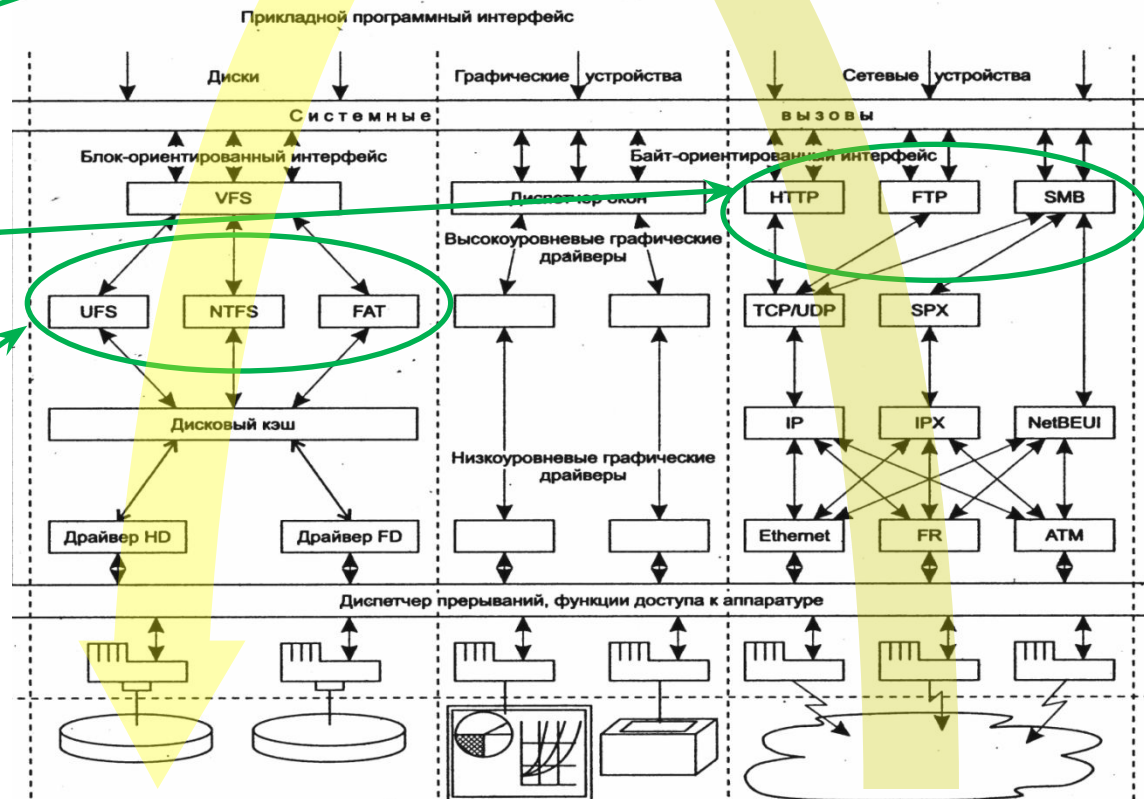
(доступ к данным)

2. Сетевая подсистема

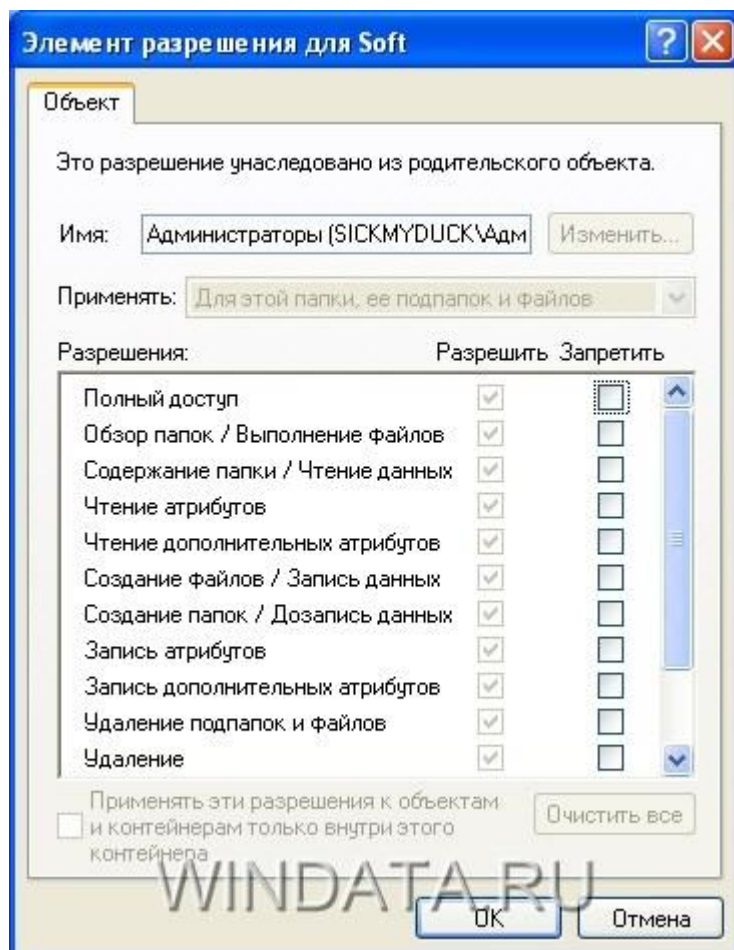
(доступ к приложениям)

3. Файловая система

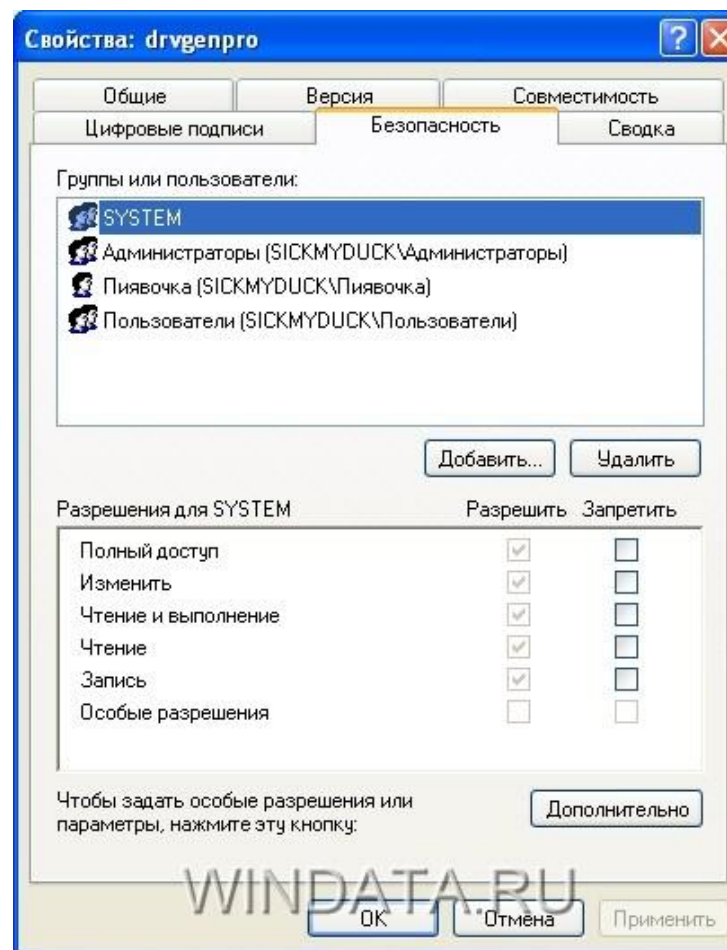
(доступ к файлам)



Установка прав сетевого доступа



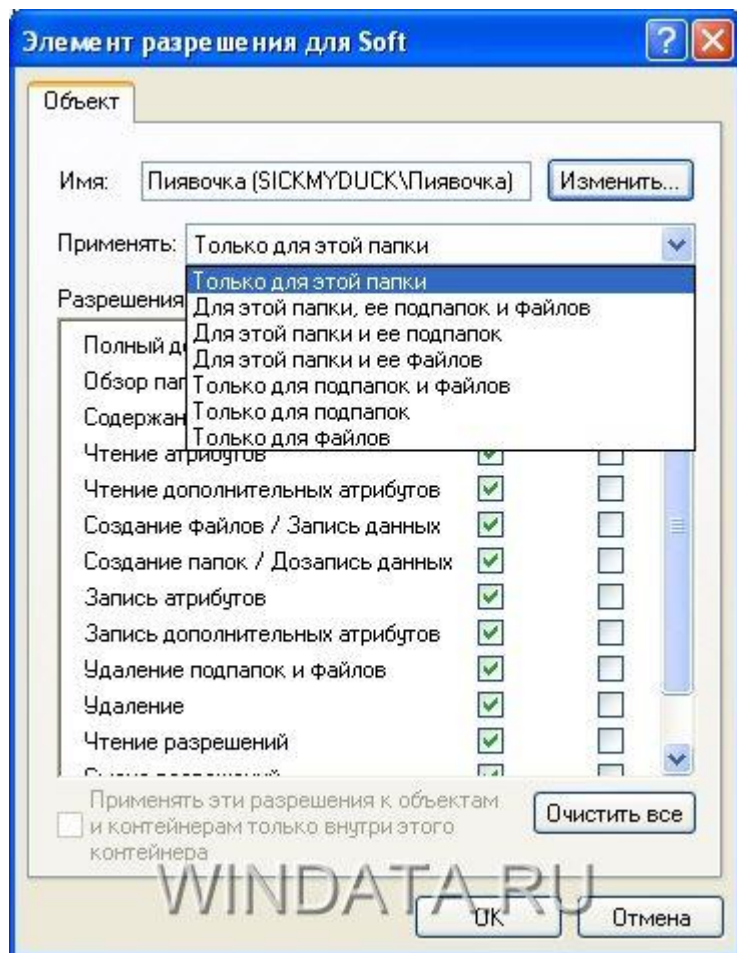
Установка прав файлового доступа



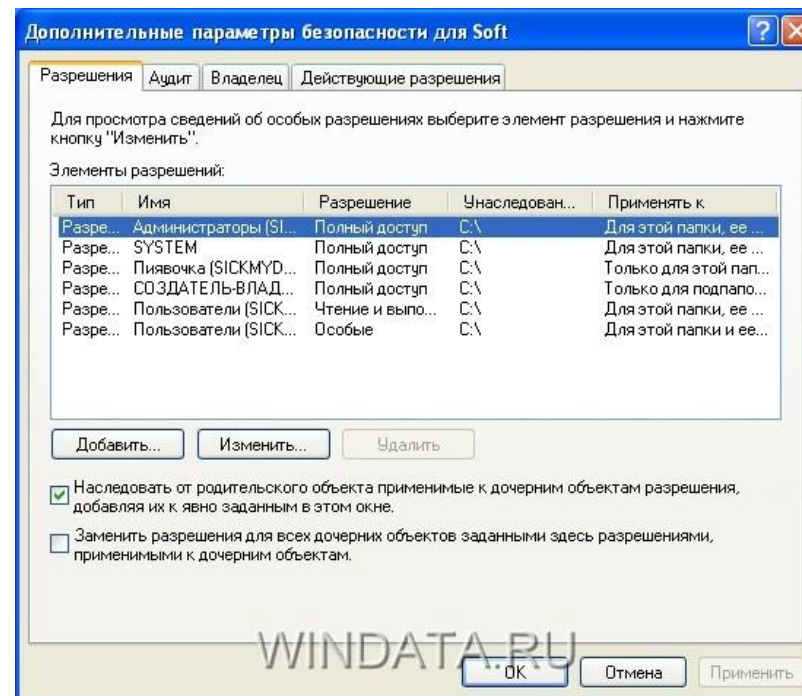
Права доступа

2012/2013

Наследование прав

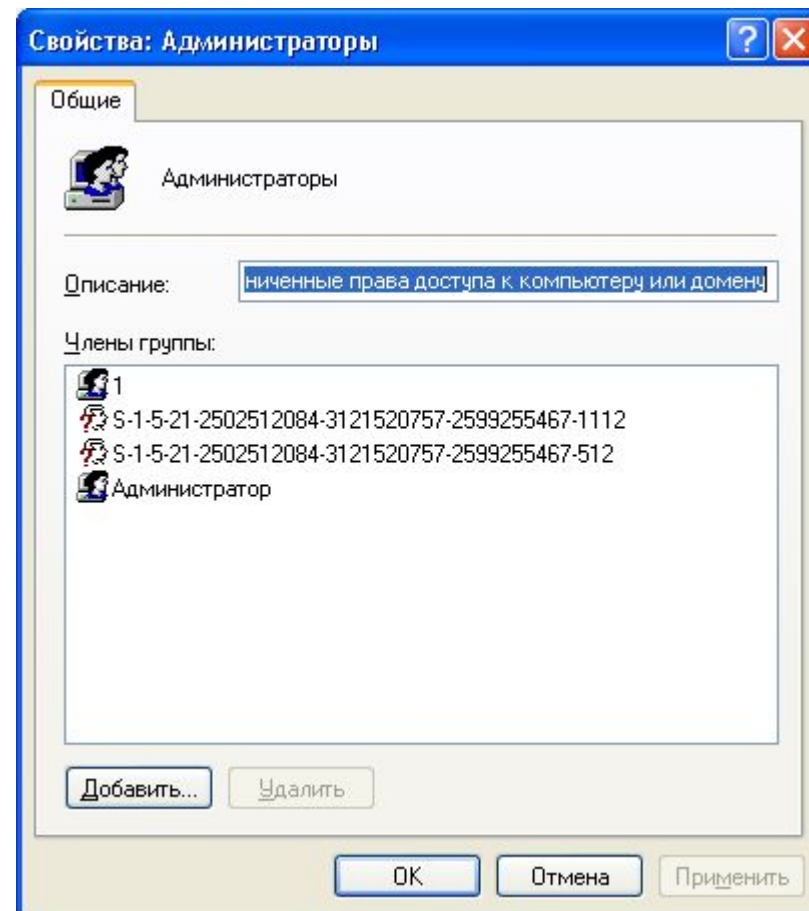
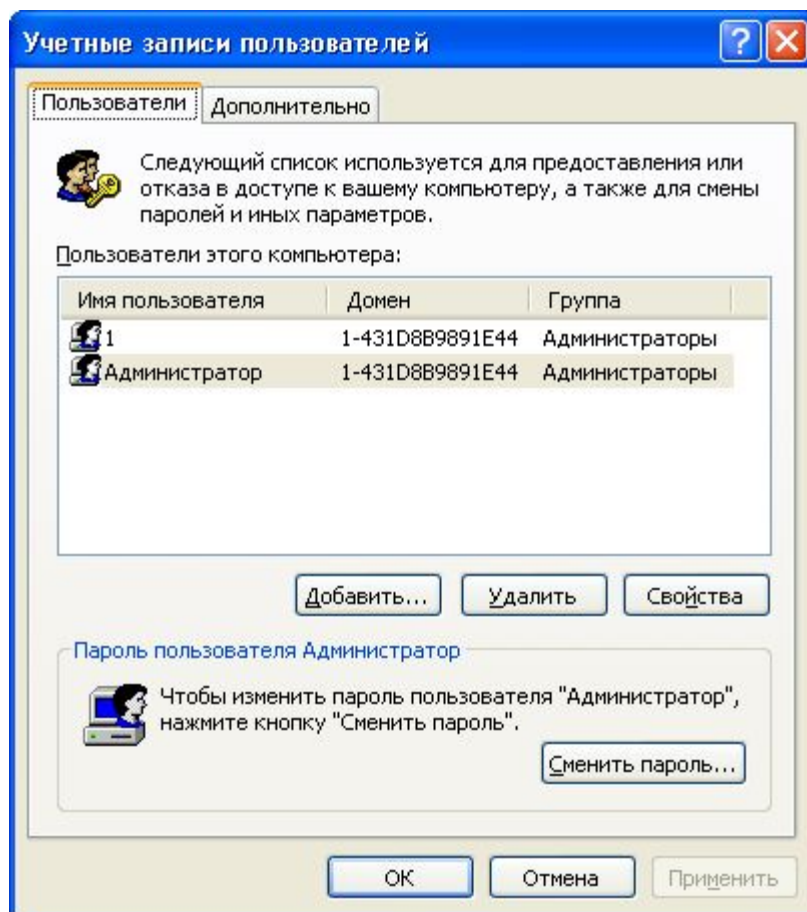


Результирующие права



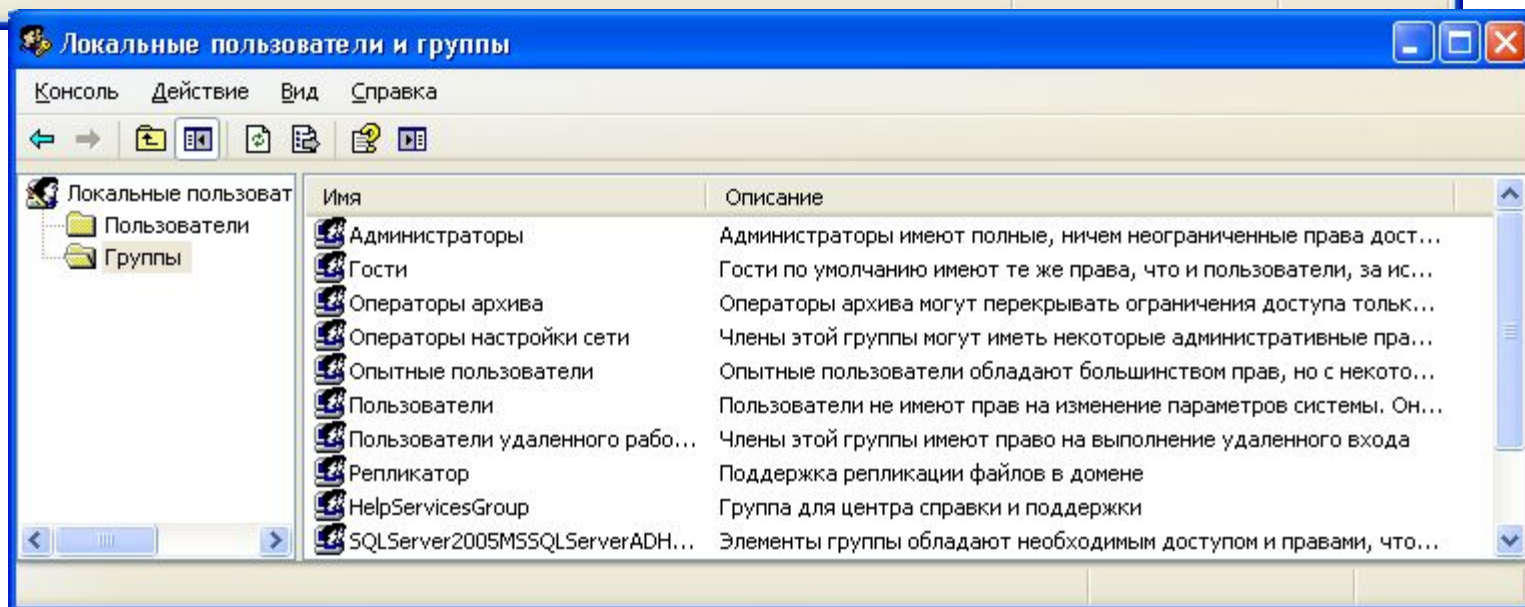
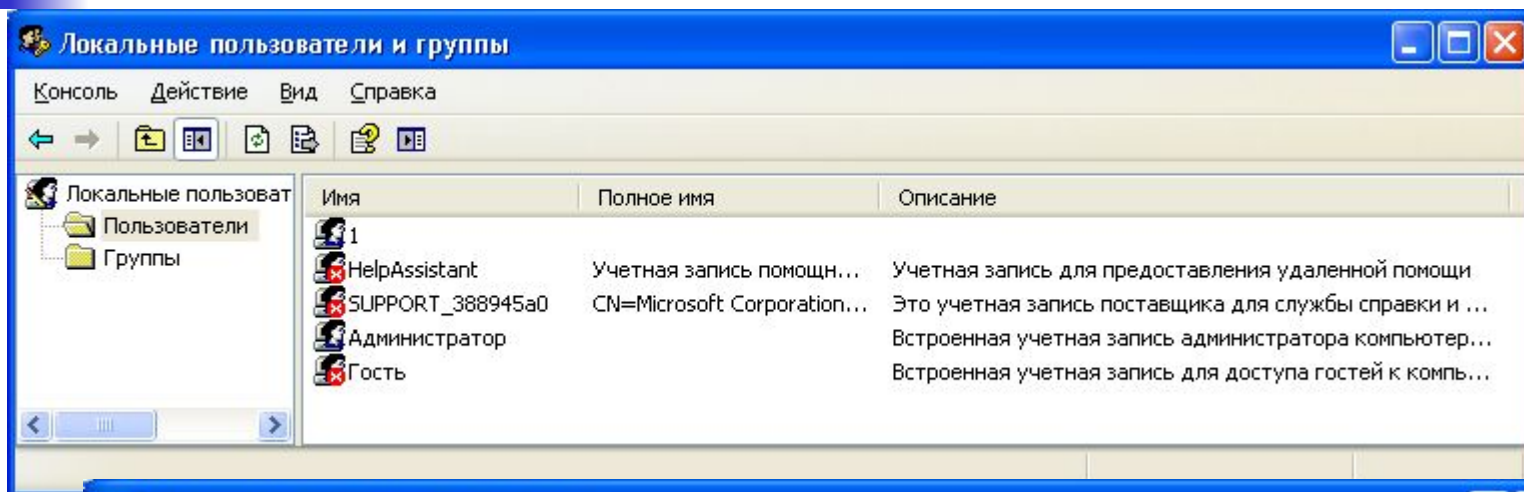
Учётные записи

2012/2013



Учётные записи

2012/2013



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

2012/2013

Списки
прав доступа

ACL PC1:

D:\ USER_1 R
C:\ USER_2 RW

ACL PC2:

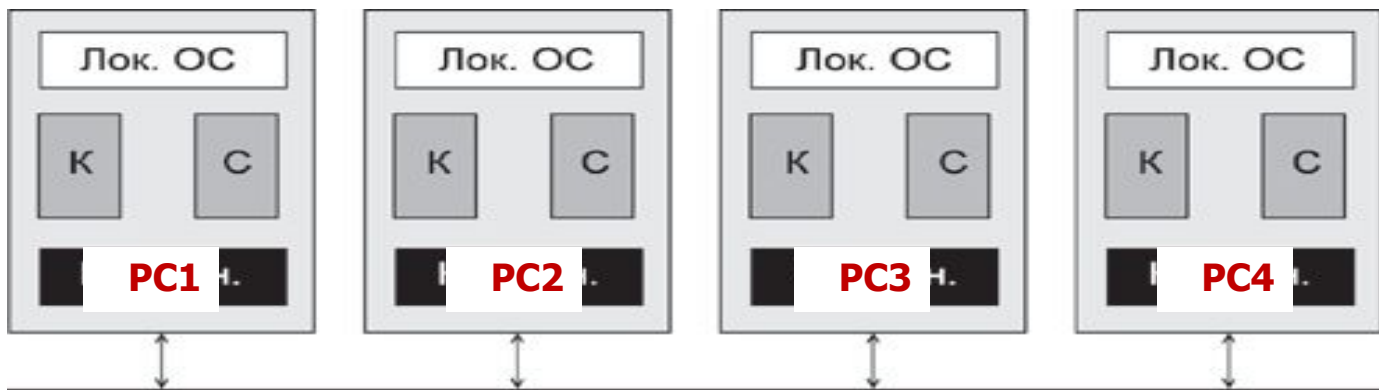
D:\ USER_1 R
C:\ USER_2 RW

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

2012/2013

Списки
прав доступа

ACL PC1:

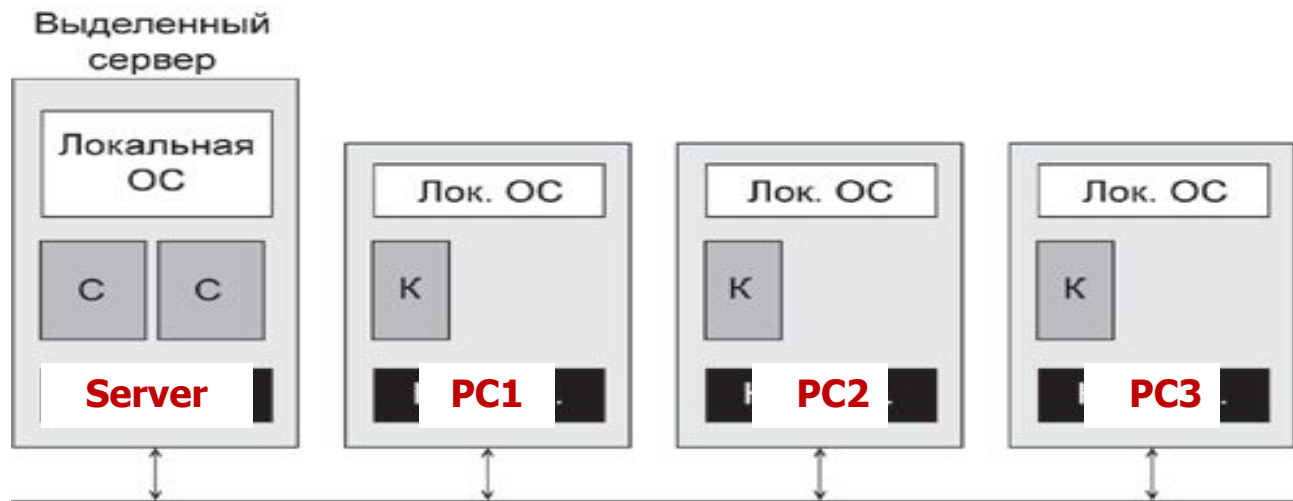
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW

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

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**

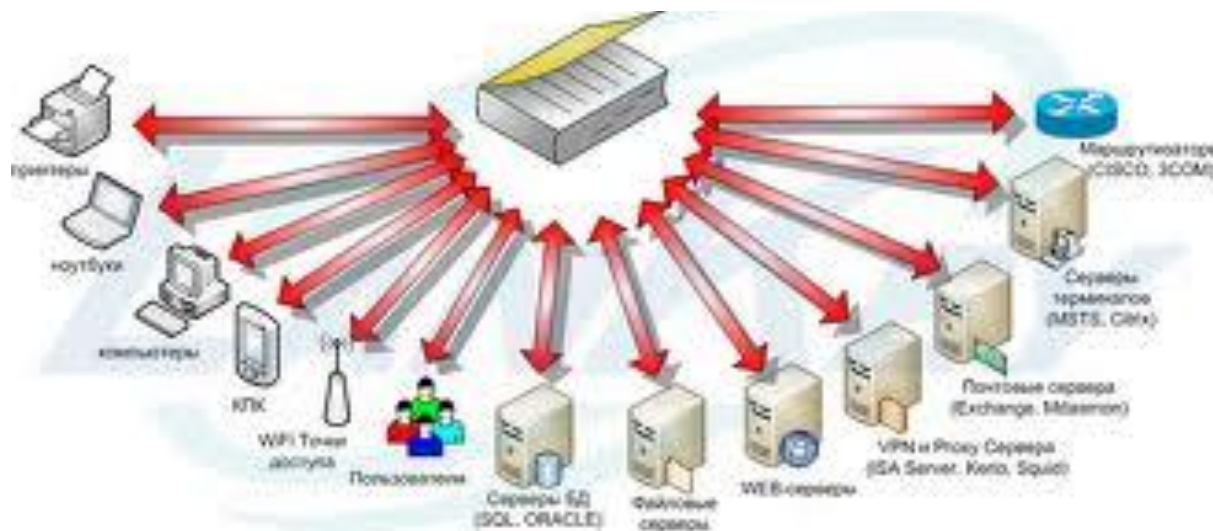
Служба каталогов обычно строится на основе модели клиент-сервер:

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

Наибольшее распространение получили каталоги:

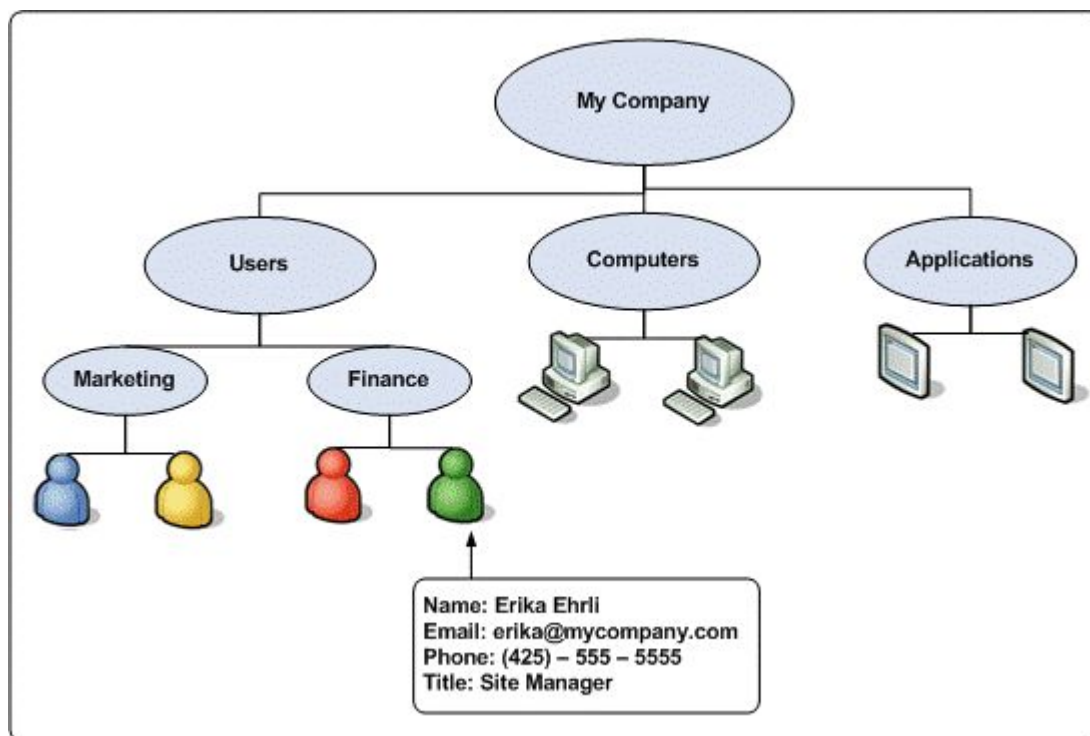
- служба **Active Directory** для Windows;
- служба **NDS** компании Novell.

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



Домен Windows

2012/2013



Active Directory (AD)

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

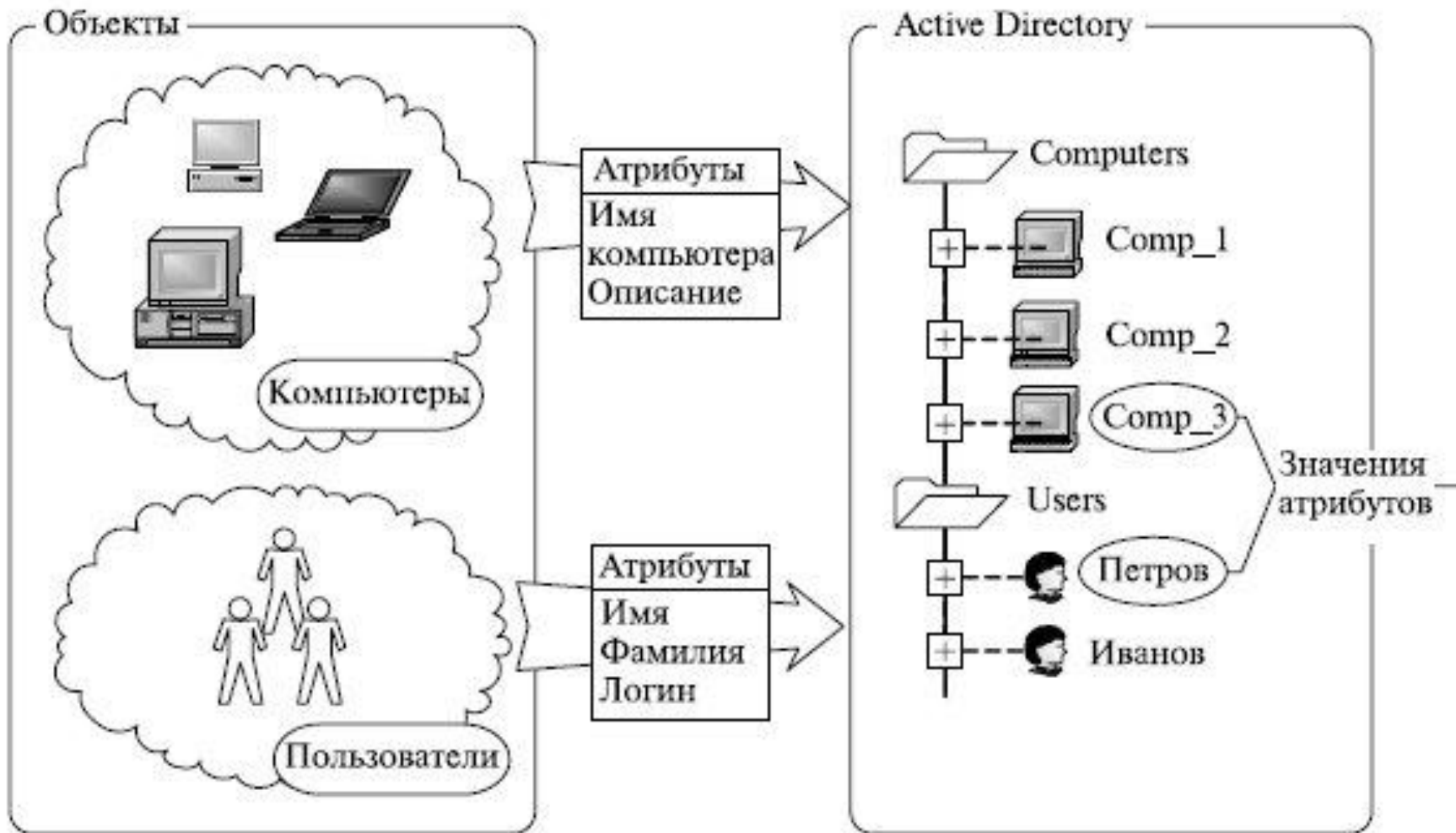
Active Directory поддерживается в Windows Server 2003, Windows Server 2008.

AD - база данных LDAP



Служба каталогов Active Directory

2012/2013



Служба каталогов Active Directory

2012/2013



The image shows two overlapping Windows XP dialog boxes. The background window is titled "Свойства системы" (System Properties) and is on the "Имя компьютера" (Computer Name) tab. It displays the current computer name "1-431d8b9891e44" and domain "AD.GRSU.BY". It includes instructions on how to identify the computer and how to rename it, with buttons for "Идентификация" (Identify) and "Изменить..." (Change...). The foreground window is titled "Изменение имени компьютера" (Change Computer Name) and provides a detailed explanation of the process. It shows the current name and domain, and offers options to change the domain or workgroup. Buttons for "Дополнительно..." (Advanced...), "OK", and "Отмена" (Cancel) are visible.

Свойства системы

Восстановление системы

Автоматическое обновление | Удаленные сеансы

Общие | **Имя компьютера** | Оборудование | Дополнительно

Указанные ниже сведения используются для идентификации компьютера в сети.

Описание:

Например: "Компьютер в гостиной" или "Компьютер Андрея".

Полное имя: 1-431d8b9891e44.AD.GRSU.BY

Домен: AD.GRSU.BY

Чтобы вызвать мастер сетевой идентификации для присоединения компьютера к домену, нажмите кнопку "Идентификация".

Чтобы переименовать компьютер или присоединить его к домену вручную, нажмите кнопку "Изменить".

Идентификация

Изменить...

OK | Отмена | Применить

Изменение имени компьютера

Можно изменить имя и принадлежность к домену или рабочей группе этого компьютера. Изменения могут повлиять на доступ к сетевым ресурсам.

Имя компьютера:

Полное имя компьютера: 1-431d8b9891e44.AD.GRSU.BY

Дополнительно...

Является членом

домена:

рабочей группы:

OK | Отмена



Вход в Windows



© 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

2012/2013

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

2012/2013

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.

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

2012/2013

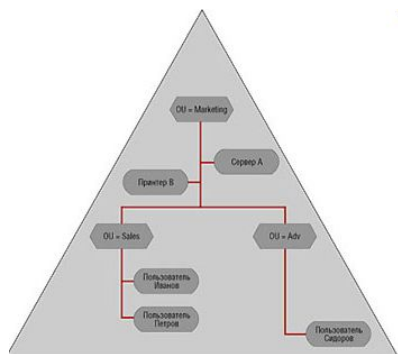


Рисунок 1. Типичная структура домена AD.

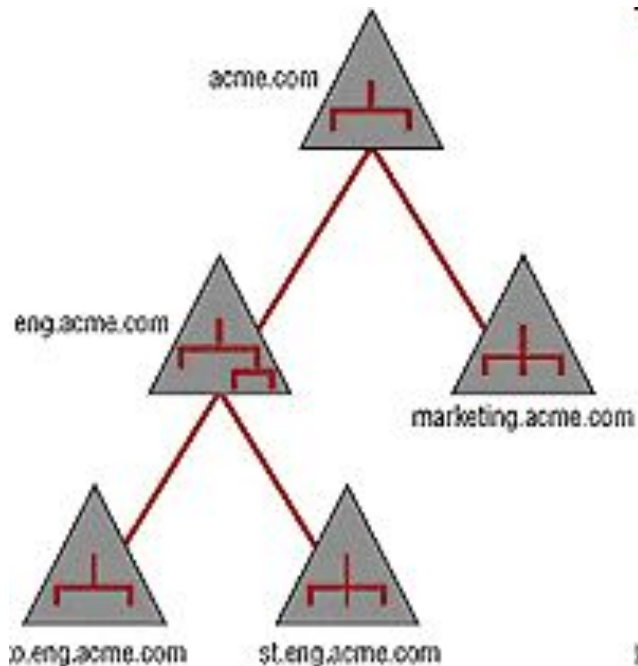


Рисунок 2. Дерево доменов AD.

Active Directory

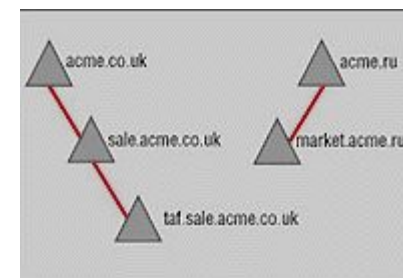
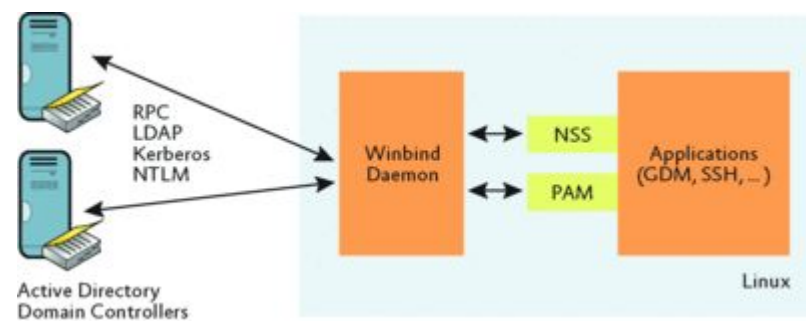
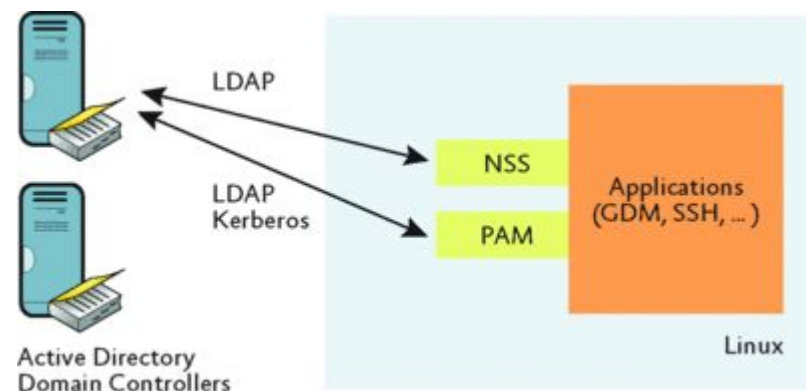
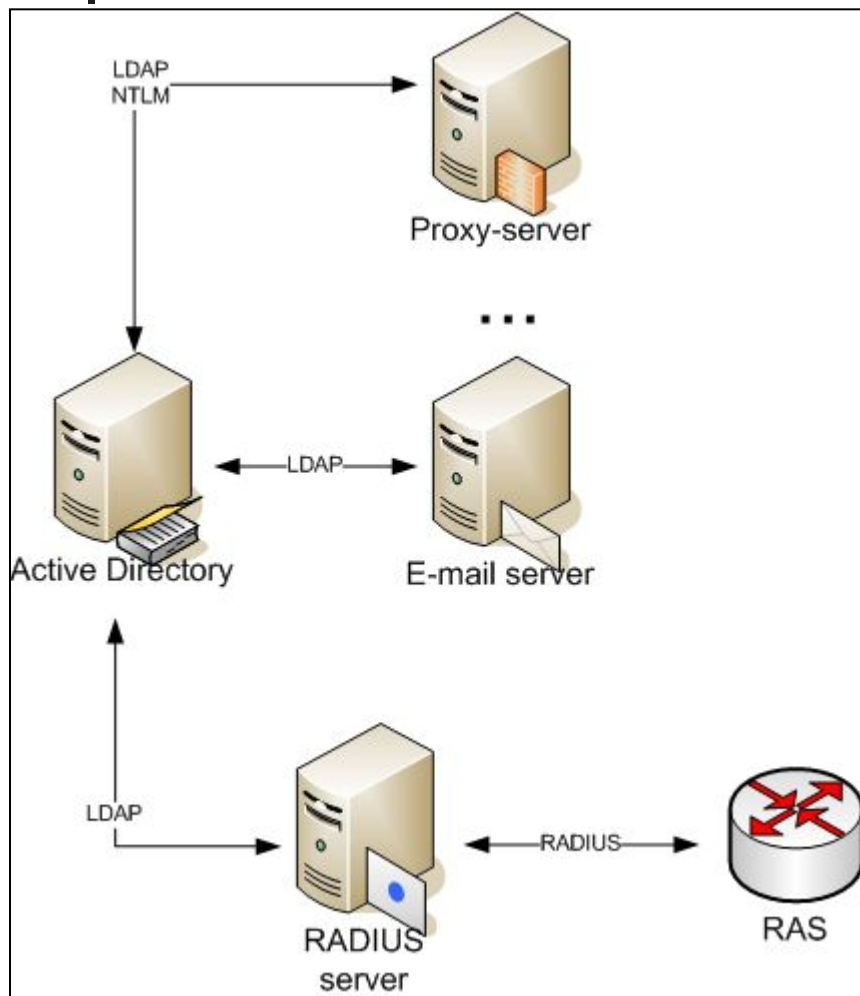


Рисунок 3. Лес доменов AD.

Служба каталогов Active Directory

2012/2013



Протоколы аутентификации в AD

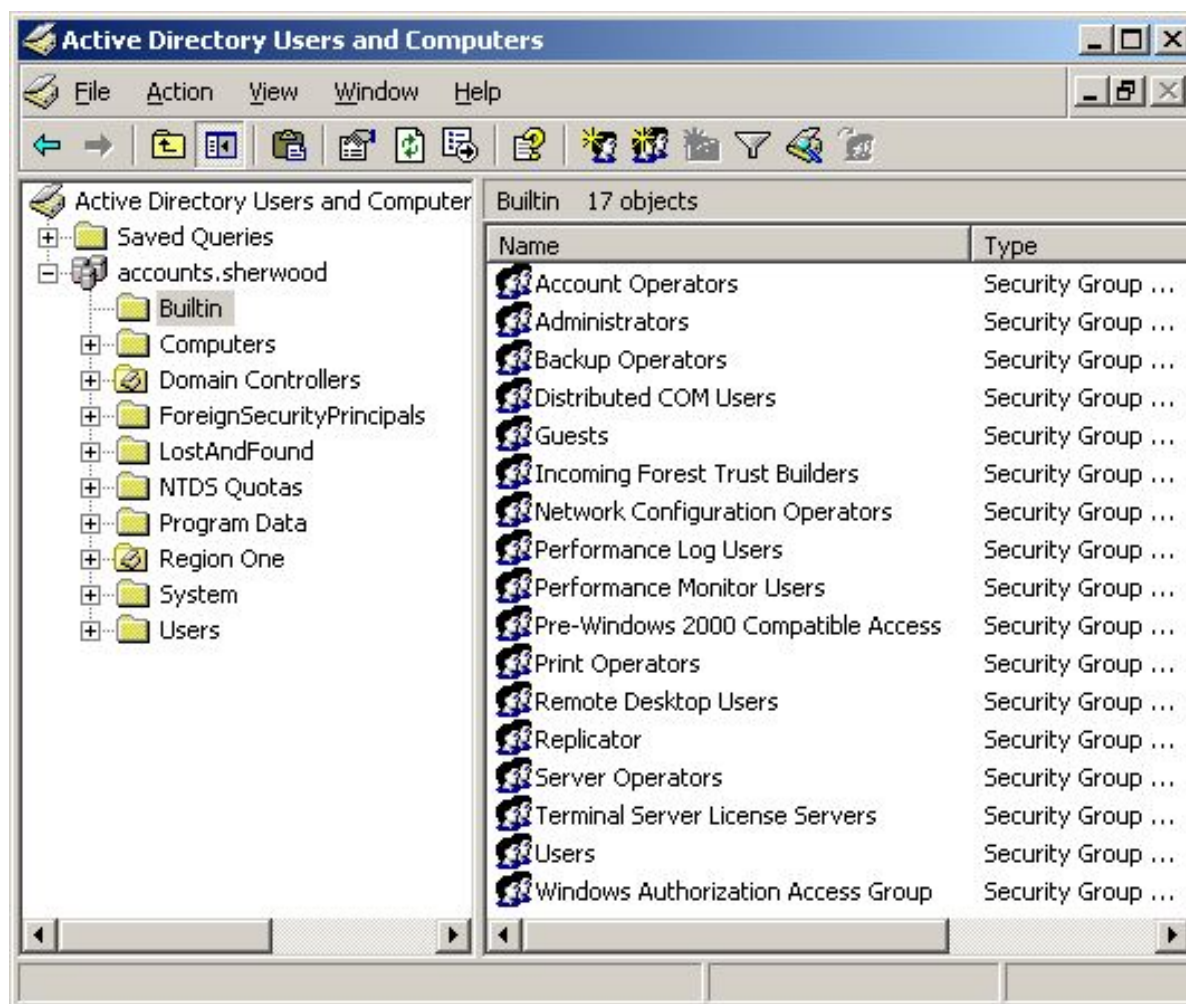
NT LAN Manager (NTLM)

Kerberos v.5

LDAP

Служба каталогов Active Directory

2012/2013



%systemroot%\NTDS\NTDS.DIT

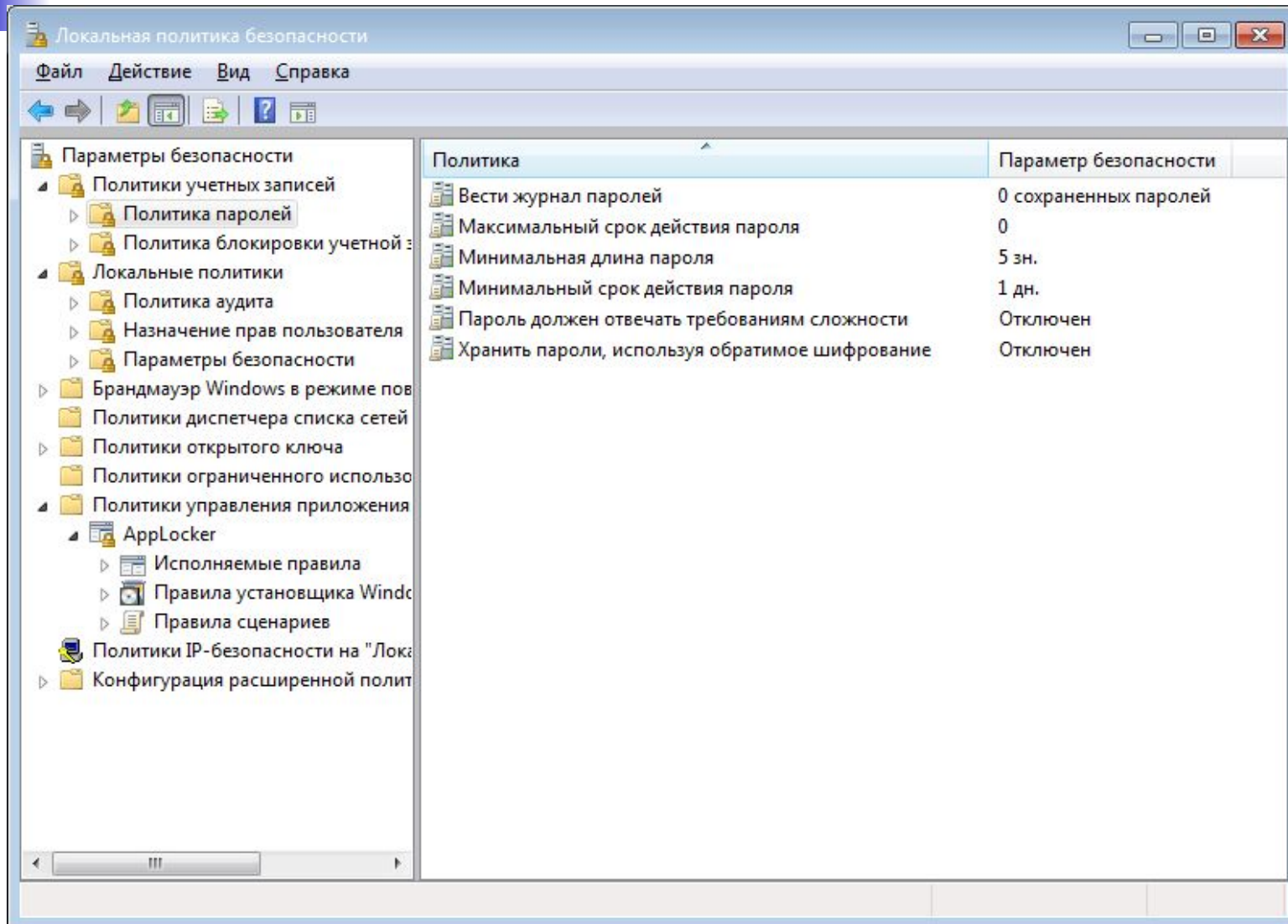
- **Локальные политики**
(secpol.msc)
- **Групповые политики**
(gpedit.msc)

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

2012/2013



Локальная политика безопасности

Файл Действие Вид Справка

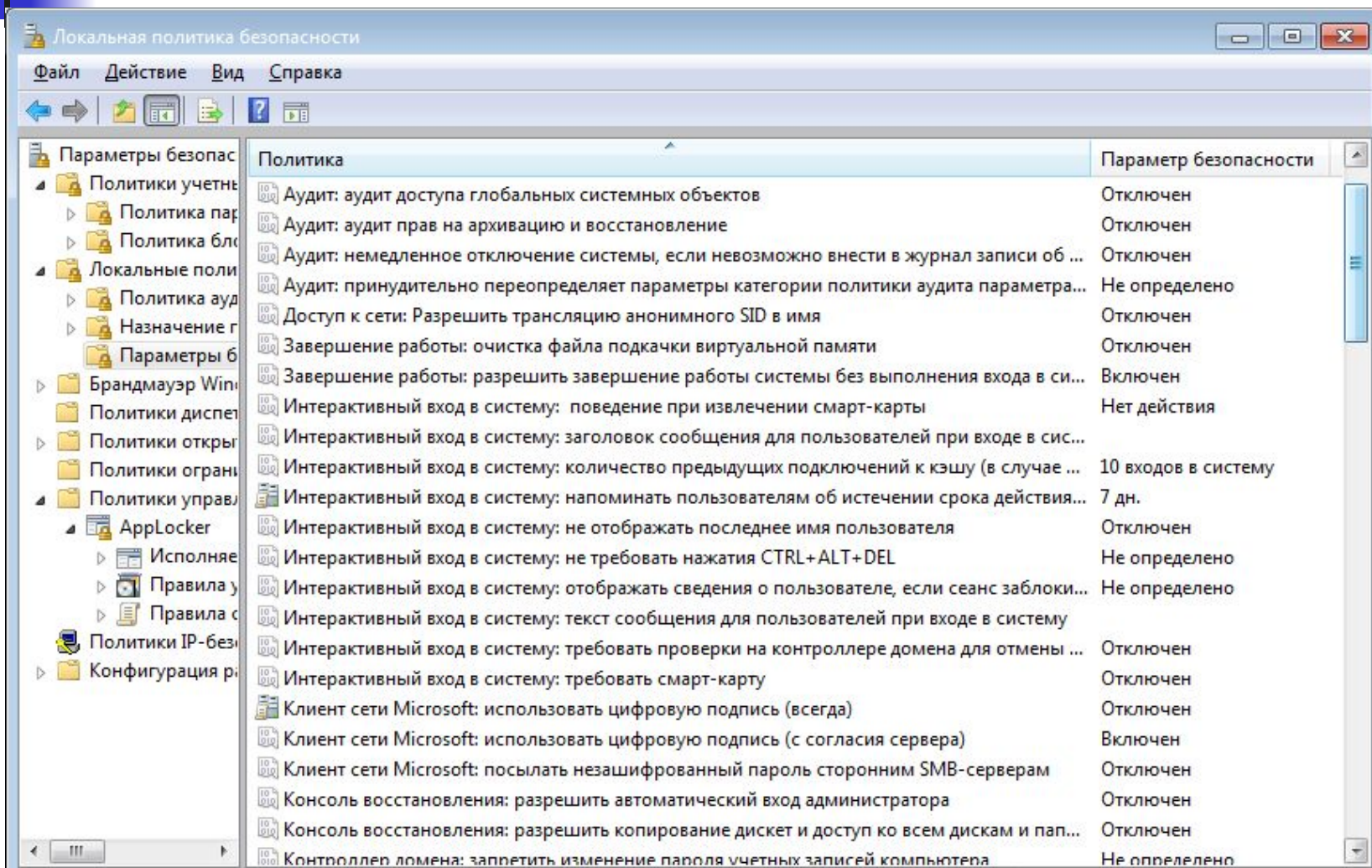
Параметры безопасности

- Политики учетных записей
 - Политика паролей
 - Политика блокировки учетной записи
- Локальные политики
 - Политика аудита
 - Назначение прав пользователя
 - Параметры безопасности
- Брандмауэр Windows в режиме повышенной безопасности
- Политики диспетчера списка сетей
- Политики открытого ключа
- Политики ограниченного использования
- Политики управления приложениями
 - AppLocker
 - Исполняемые правила
 - Правила установщика Windows
 - Правила сценариев
- Политики IP-безопасности на "Локальная политика безопасности"
- Конфигурация расширенной политики

Политика	Параметр безопасности
Вести журнал паролей	0 сохраненных паролей
Максимальный срок действия пароля	0
Минимальная длина пароля	5 зн.
Минимальный срок действия пароля	1 дн.
Пароль должен отвечать требованиям сложности	Отключен
Хранить пароли, используя обратимое шифрование	Отключен

Политики Active Directory

2012/2013



Локальная политика безопасности

Файл Действие Вид Справка

Политика	Параметр безопасности
Аудит: аудит доступа глобальных системных объектов	Отключен
Аудит: аудит прав на архивацию и восстановление	Отключен
Аудит: немедленное отключение системы, если невозможно внести в журнал записи об ...	Отключен
Аудит: принудительно переопределяет параметры категории политики аудита параметра...	Не определено
Доступ к сети: Разрешить трансляцию анонимного SID в имя	Отключен
Завершение работы: очистка файла подкачки виртуальной памяти	Отключен
Завершение работы: разрешить завершение работы системы без выполнения входа в си...	Включен
Интерактивный вход в систему: поведение при извлечении смарт-карты	Нет действия
Интерактивный вход в систему: заголовок сообщения для пользователей при входе в сис...	Нет действия
Интерактивный вход в систему: количество предыдущих подключений к кэш (в случае ...	10 входов в систему
Интерактивный вход в систему: напоминать пользователям об истечении срока действия...	7 дн.
Интерактивный вход в систему: не отображать последнее имя пользователя	Отключен
Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Не определено
Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблоки...	Не определено
Интерактивный вход в систему: текст сообщения для пользователей при входе в систему	Нет действия
Интерактивный вход в систему: требовать проверки на контроллере домена для отмены ...	Отключен
Интерактивный вход в систему: требовать смарт-карту	Отключен
Клиент сети Microsoft: использовать цифровую подпись (всегда)	Отключен
Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Включен
Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам	Отключен
Консоль восстановления: разрешить автоматический вход администратора	Отключен
Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и пап...	Отключен
Контроллер домена: запретить изменение пароля учетных записей компьютера	Не определено

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

Политики Active Directory

2012/2013

gpedit.msc

Политика	Параметр безопасности
Аудит входа в систему	Успех, Отказ
Аудит доступа к объектам	Нет аудита
Аудит доступа к службе каталогов	Успех, Отказ
Аудит изменения политики	Нет аудита
Аудит использования привилегий	Нет аудита
Аудит отслеживания процессов	Нет аудита
Аудит системных событий	Нет аудита
Аудит событий входа в систему	Успех, Отказ
Аудит управления учетными записями	Успех, Отказ

- 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.

Инструменты управления групповой политикой

- GPEdit.msc
- GPUUpdate.msc
- GPRResult.msc

□ Active Directory

2012/2013

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.

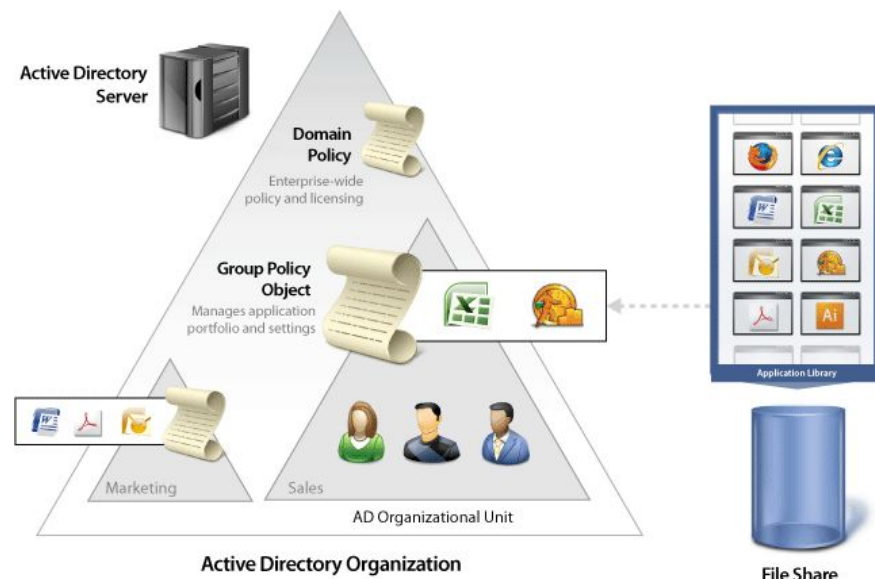
Active Directory

2012/2013

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 Directory 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)

□ Active Directory

2012/2013

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

2012/2013

Списки
прав доступа

ACL PC1:

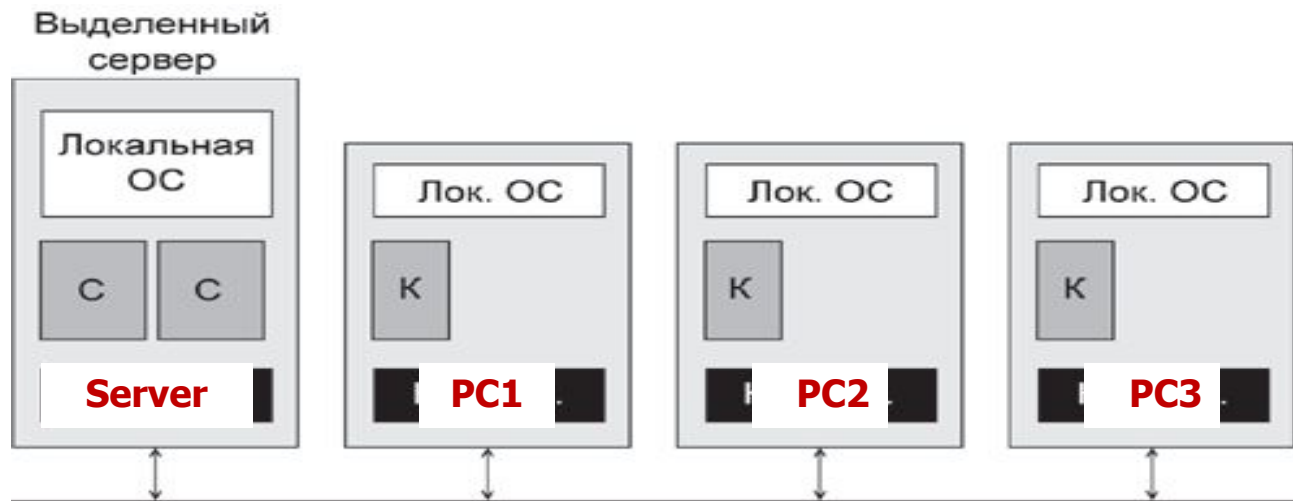
D:\ SERVER/USER_1 R
C:\ SERVER/USER_2 RW

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:

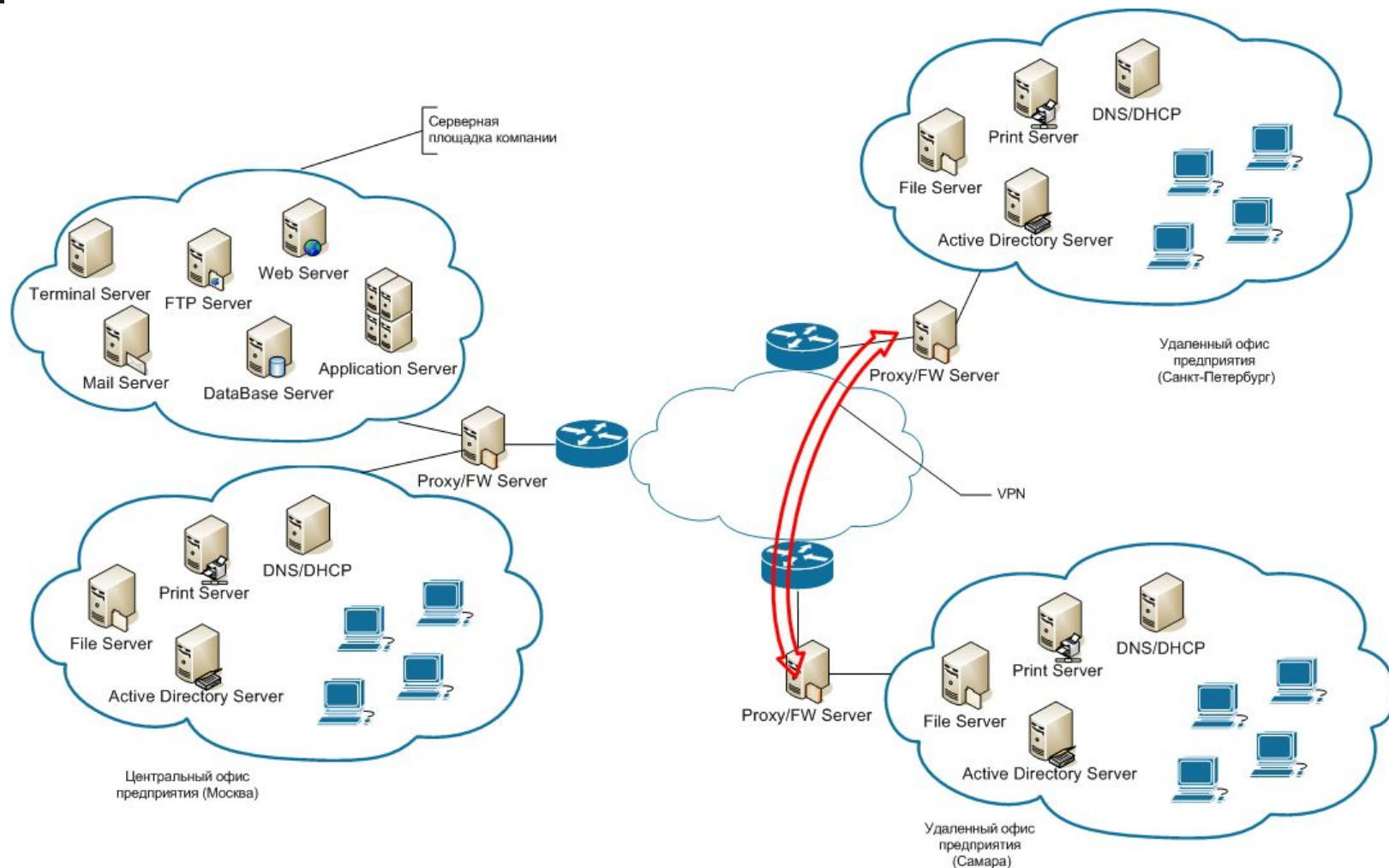
Administrator

SAM PC1:

Administrator

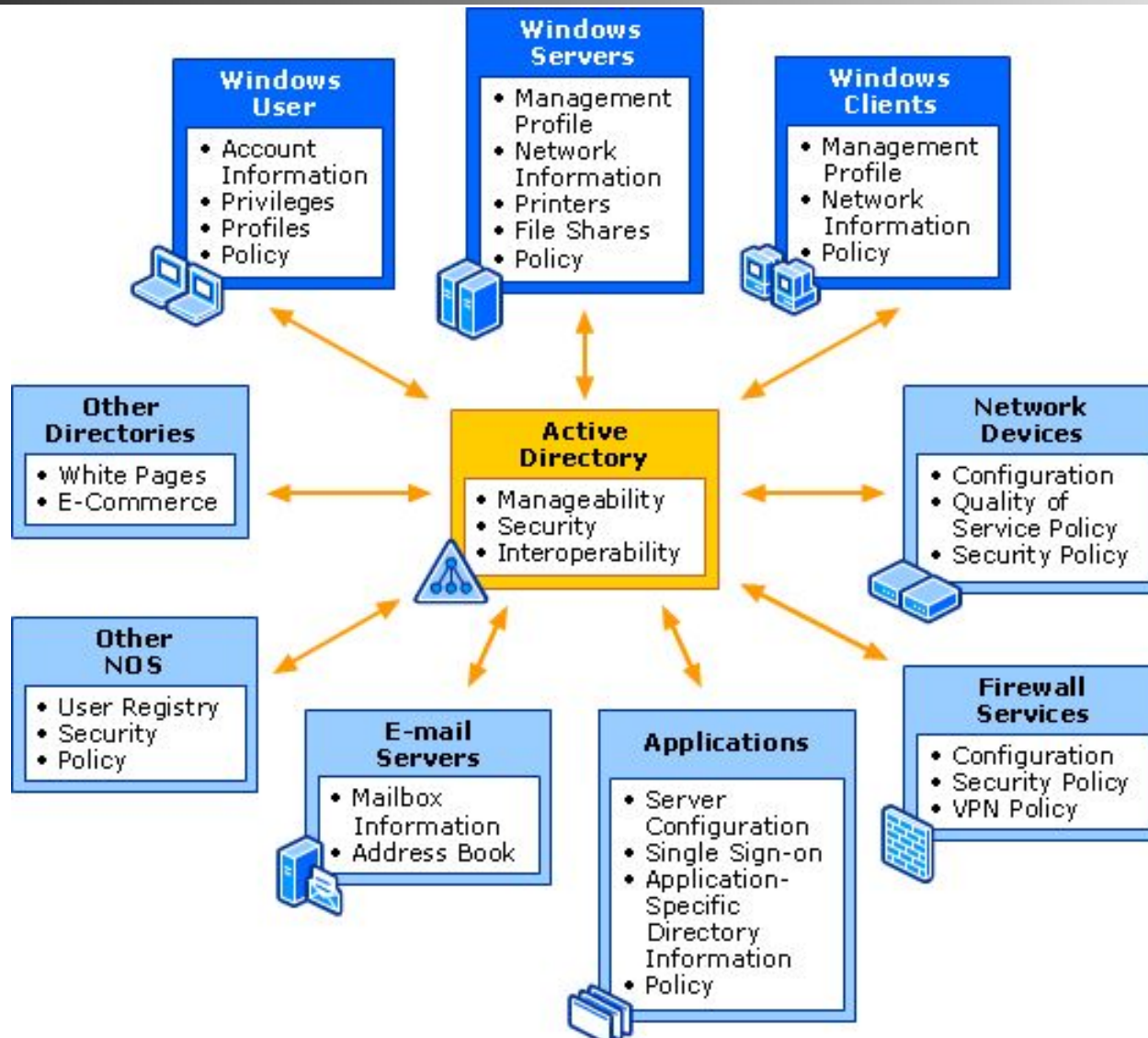
Active Directory

2012/2013



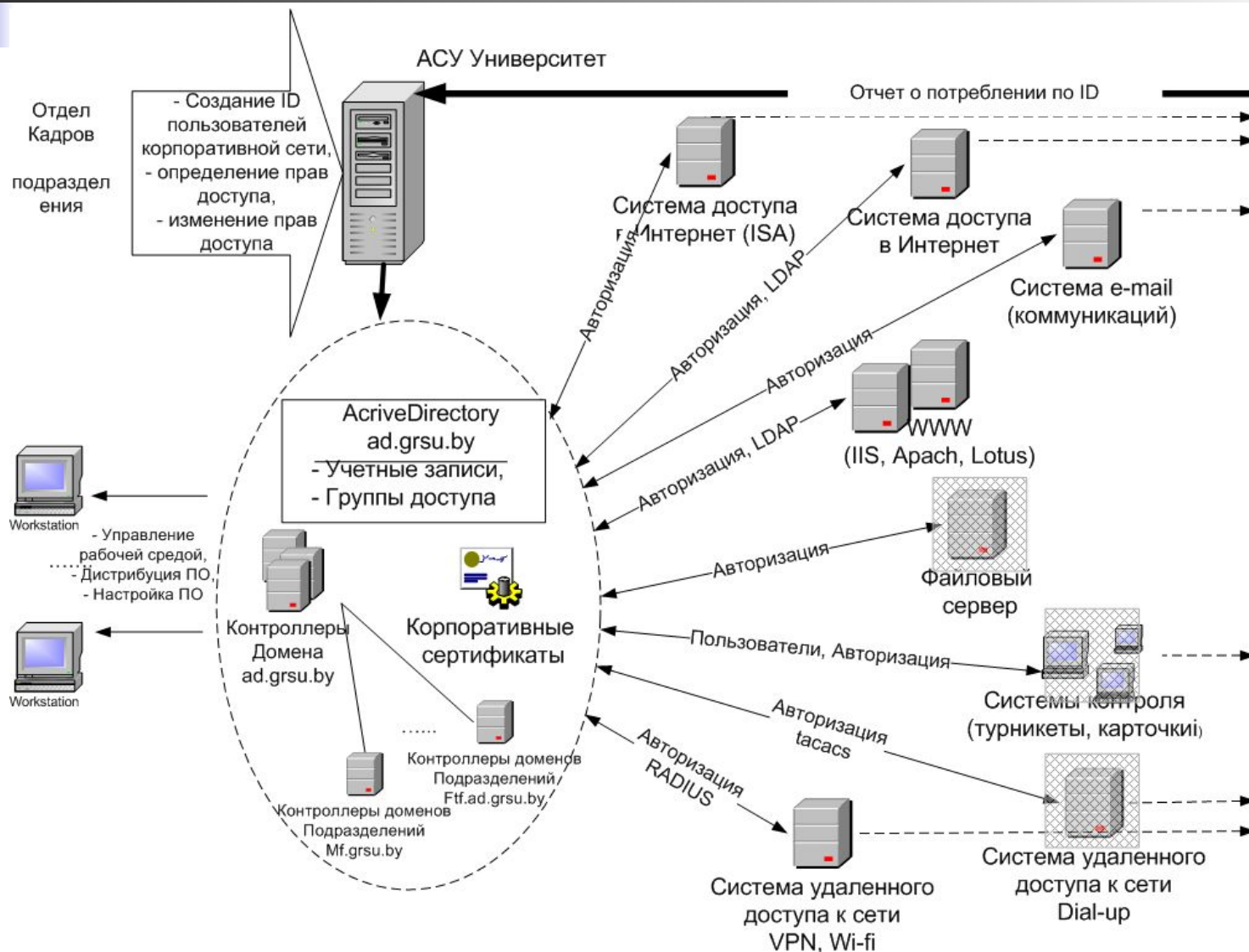
Active Directory

2012/2013



Active Directory

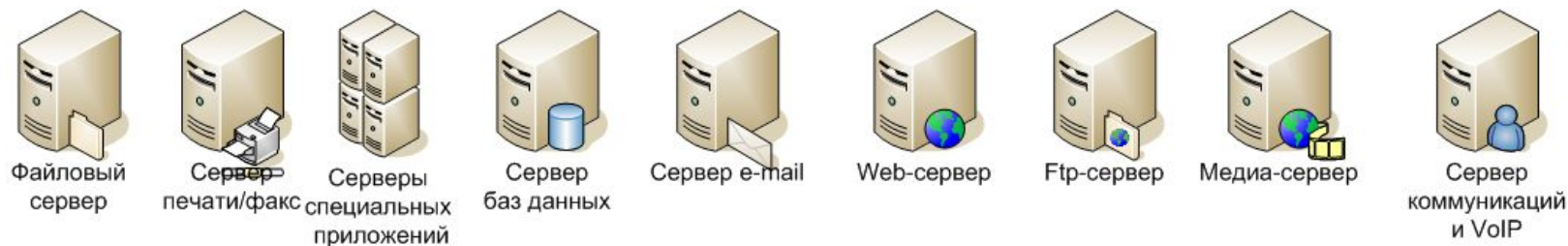
2012/2013



Обеспечение инфраструктуры сети



Обслуживание бизнес-процессов



Обслуживание сети



Цифровой сертификат

2012/2013

Сертификат

Общие Состав Путь сертификации

Сведения о сертификате

Недостаточно информации для проверки сертификата.

Кому выдан: mail.in.grsu.by

Кем выдан: mail.in.grsu.by

Действителен с 17. 09. 2010 по 16. 09. 2015

Заявление поставщика

Подробнее о [сертификатах](#)

OK

Предупреждение безопасности Интернета

Сервер, с которым установлено соединение, использует сертификат безопасности, который не может быть проверен.

Главное конечное имя неверно.

Показать сертификат...

Продолжать использовать этот сервер?

Да Нет

Сертификат

Общие Состав Путь сертификации

Показать: <Все>

Значение
mail.in.grsu.by, Zimbra Collab...
17 сентября 2010 г. 12:21:10
16 сентября 2015 г. 12:21:10
mail.in.grsu.by, Zimbra Collab...
RSA (1024 Bits)
Тип субъекта=Конечный су...
Цифровая подпись, Неотрек...
sha1

В a3 3e f0 1e 7d 46 d9 d0

7f 03 f8 88 71 28

Свойства... Копировать в файл...

Подробнее о [составе сертификата](#)

OK



Компьютерные системы и сети

Олизарович Евгений Владимирович

ГрГУ им. Я.Купалы. 2012-2013