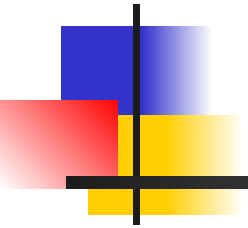


Компьютерные системы и сети

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

Олизарович Евгений Владимирович

ГрГУ им. Я.Купалы. 2011-2012

Компьютерные системы и сети

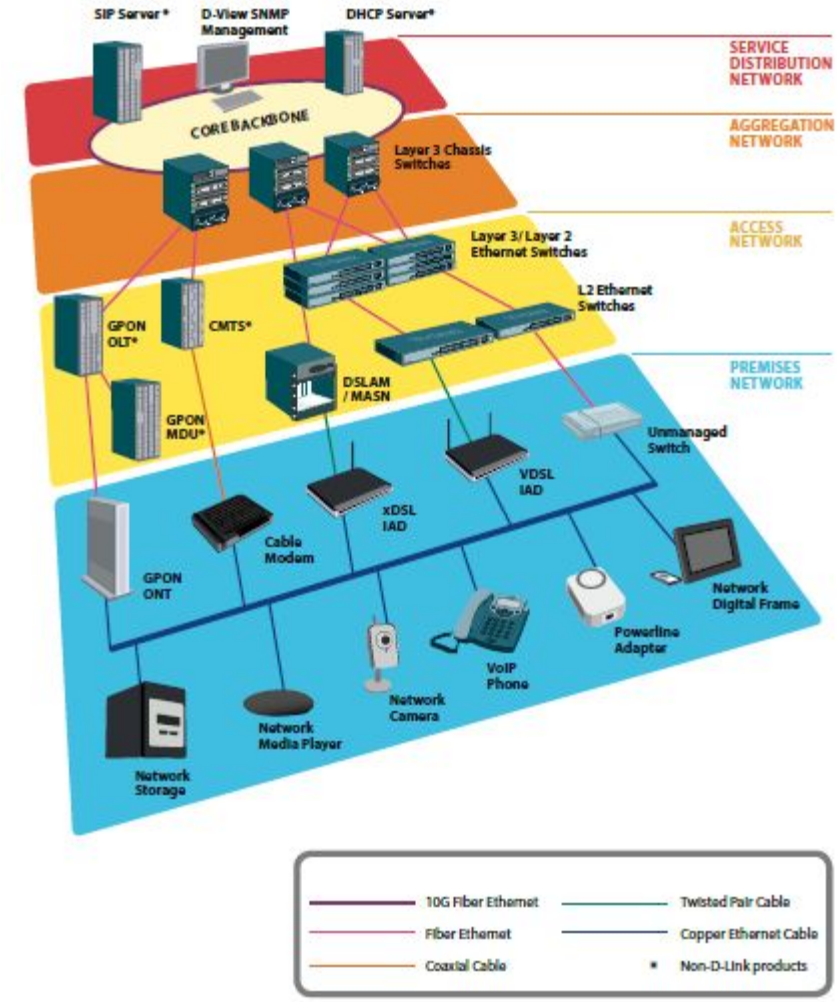
ГрГУ им. Я.Купалы

2011/2012

Основная задача **мультисервисных сетей -** обеспечение единой транспортной среды, в которой для передачи обычного трафика (данных) и трафика реального времени (голоса и видео) используется единая инфраструктура.

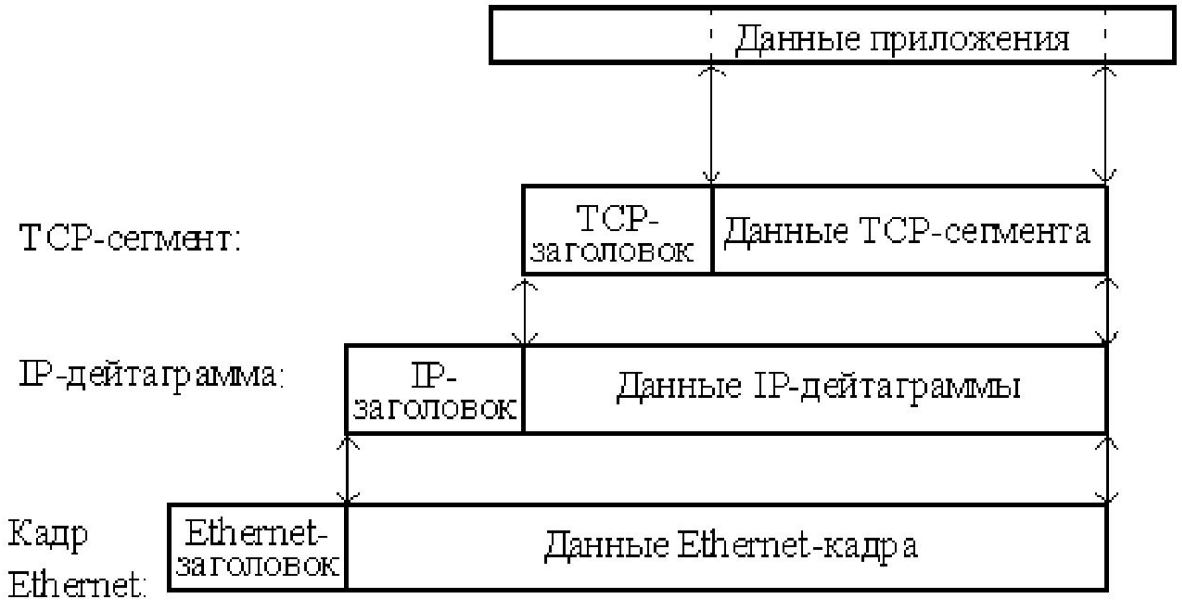
Преимущества **мультисервисной сети**:

- Сокращение расходов на каналы связи и сетевую инфраструктуру;
- Возможность внедрения качественно новых сервисов и приложений.



Компьютерные системы и сети

Пакет –блок данных, передаваемый между абонентскими системами и приложениями.

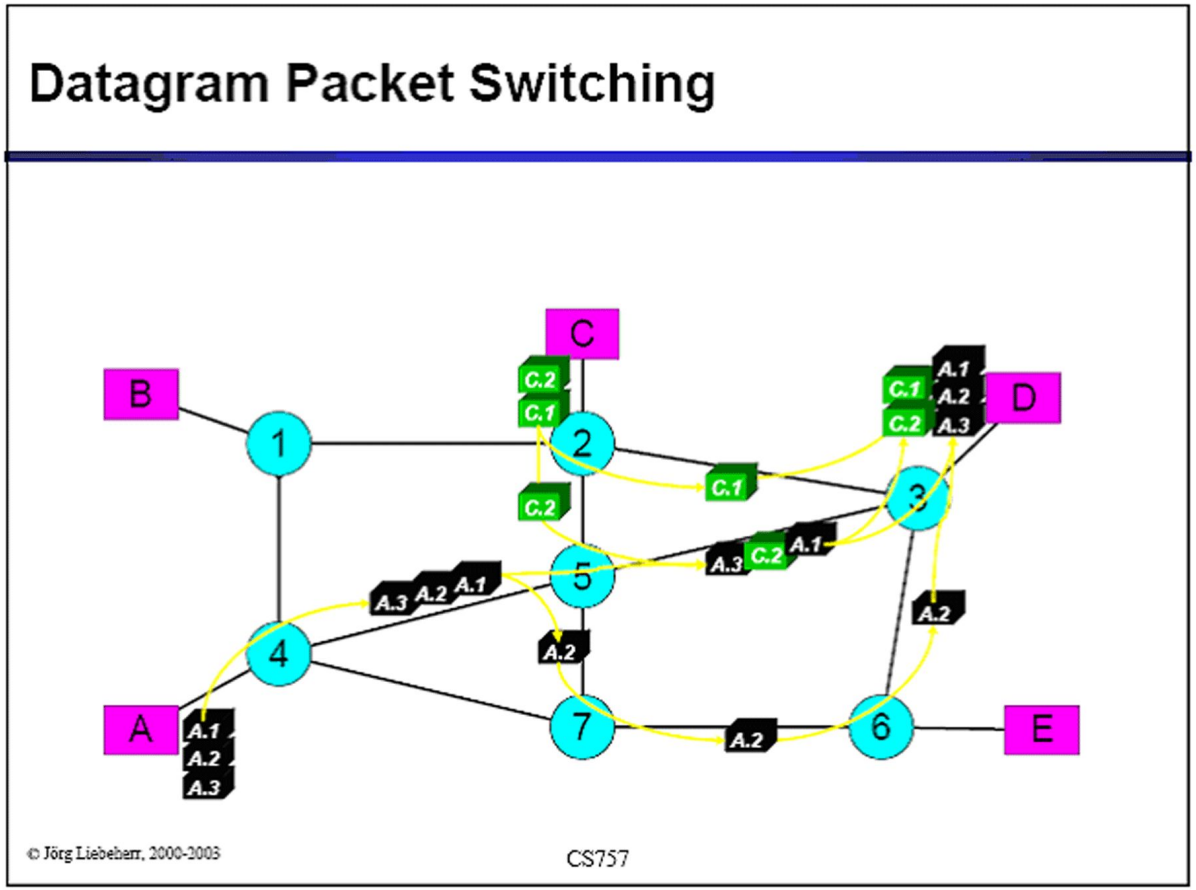


Трафик – поток информации (пакетов), передаваемой по сети за определенный период времени.

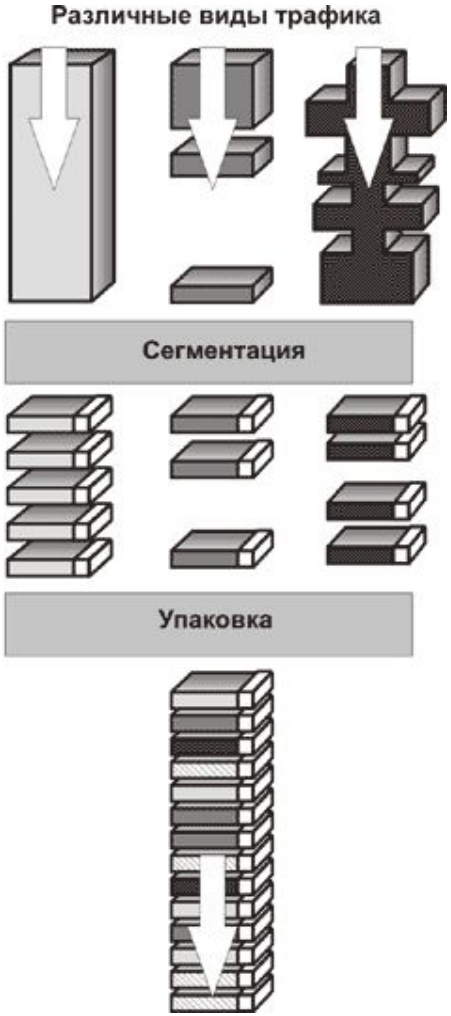
Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012



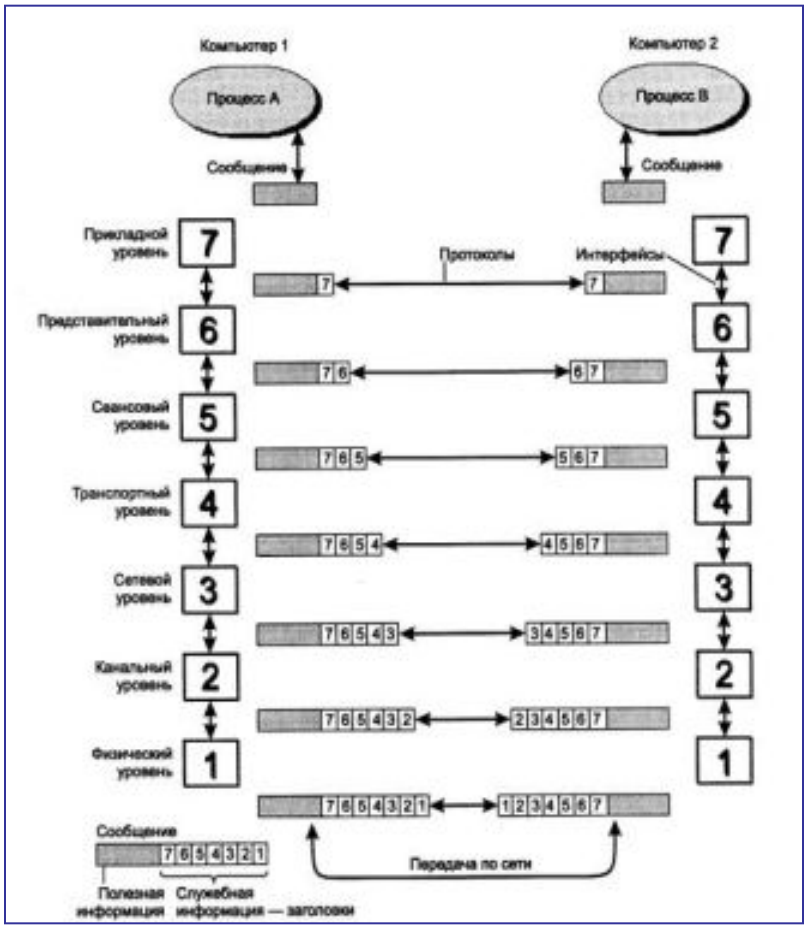
Коммутация пакетов

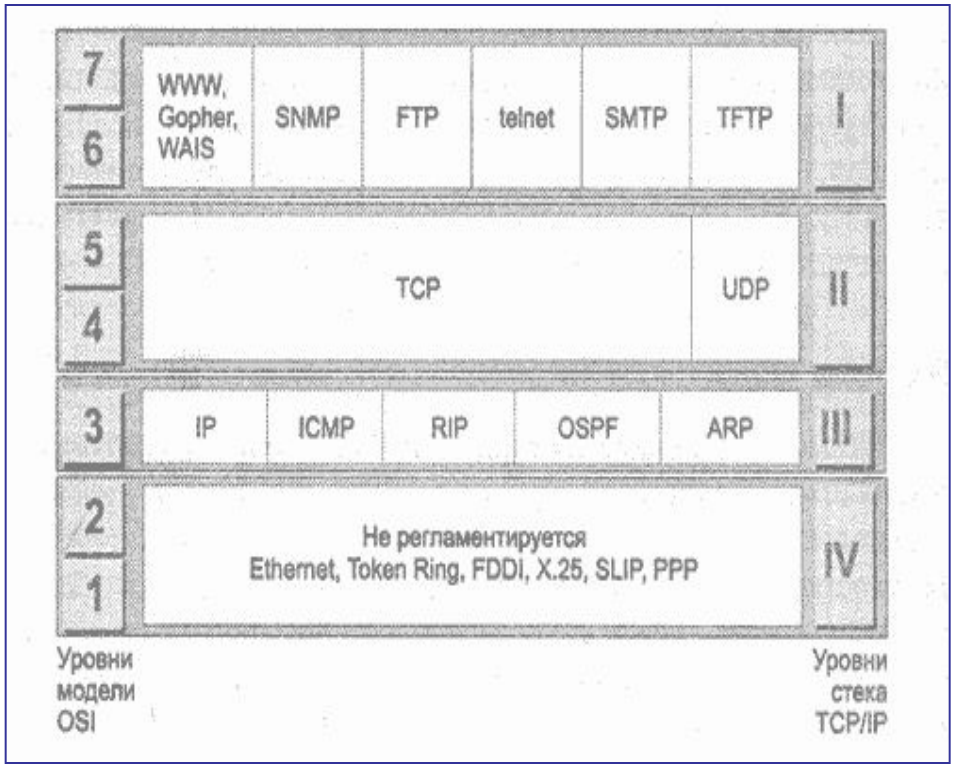


Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

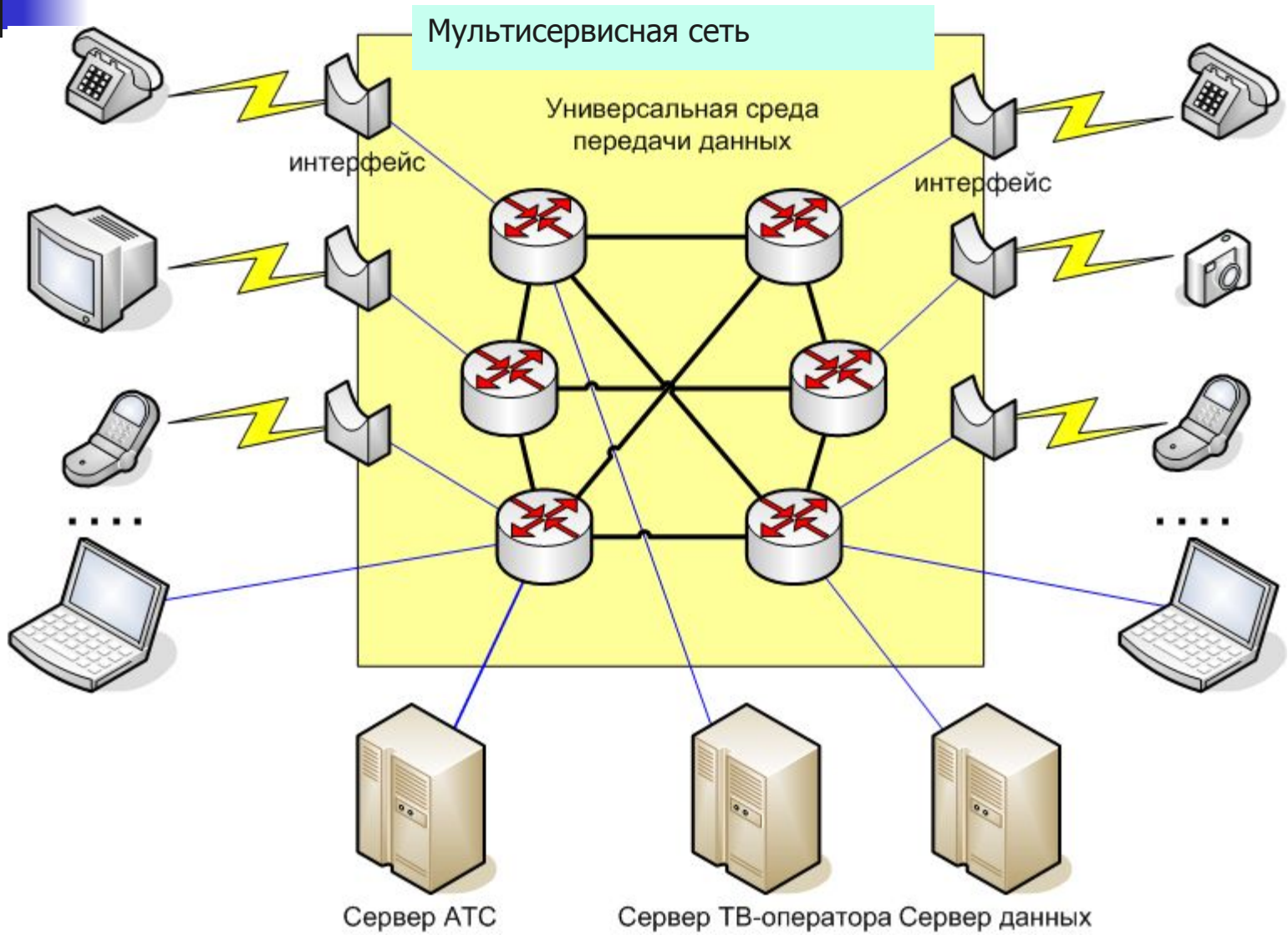




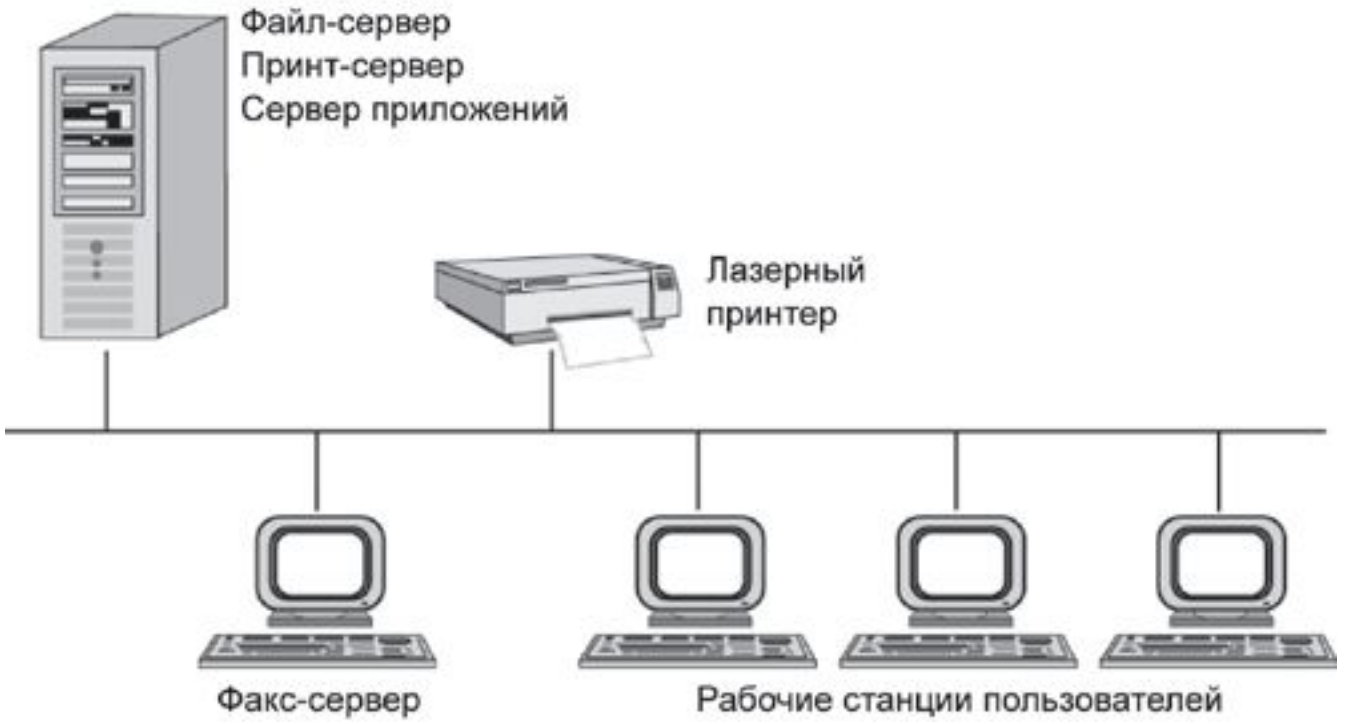
Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012



Компьютерные системы и сети



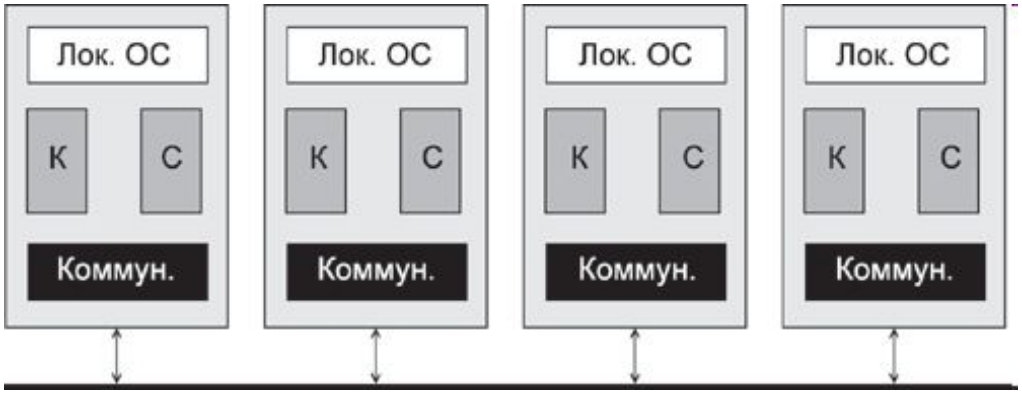
Компьютерные системы и сети

Компьютерные системы и сети

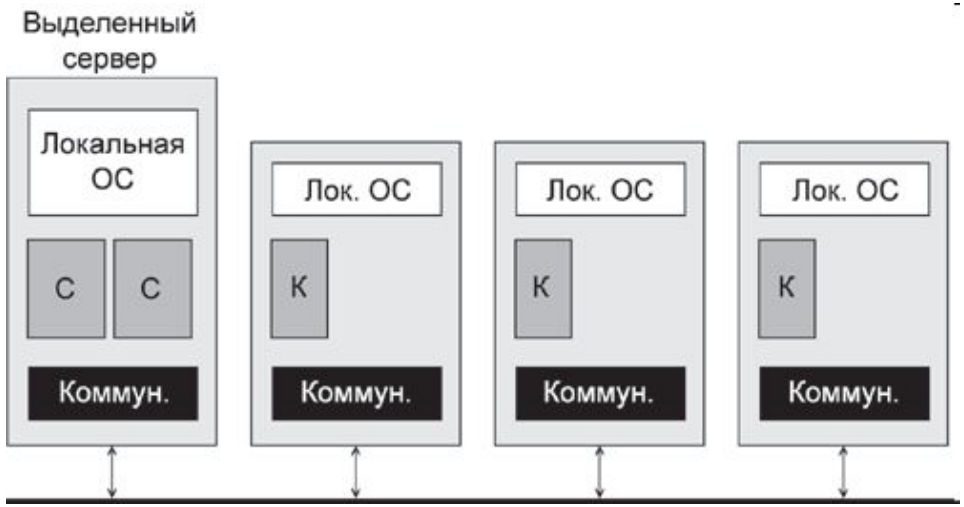
ГрГУ им. Я.Купалы

2011/2012

Одноранговая сеть



Сеть с выделенным сервером



Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

Обеспечение инфраструктуры сети

Обслуживание бизнес-процессов

Обслуживание сети

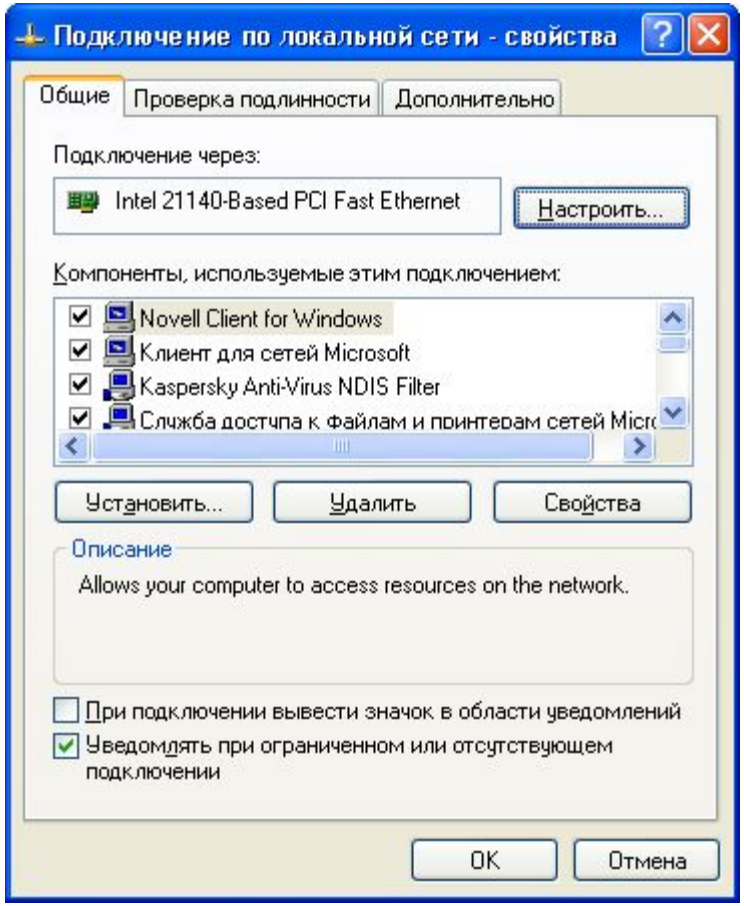
ДОСТУП К РЕСУРСАМ СЕРВЕРА

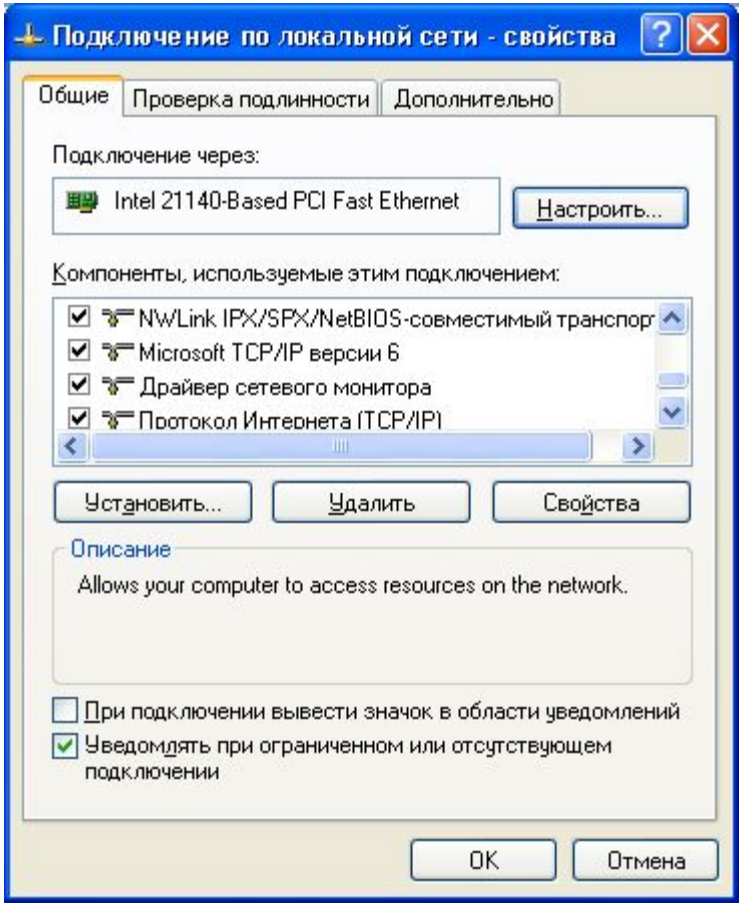
Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

Сетевые клиенты





Компьютерные системы и сети

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**

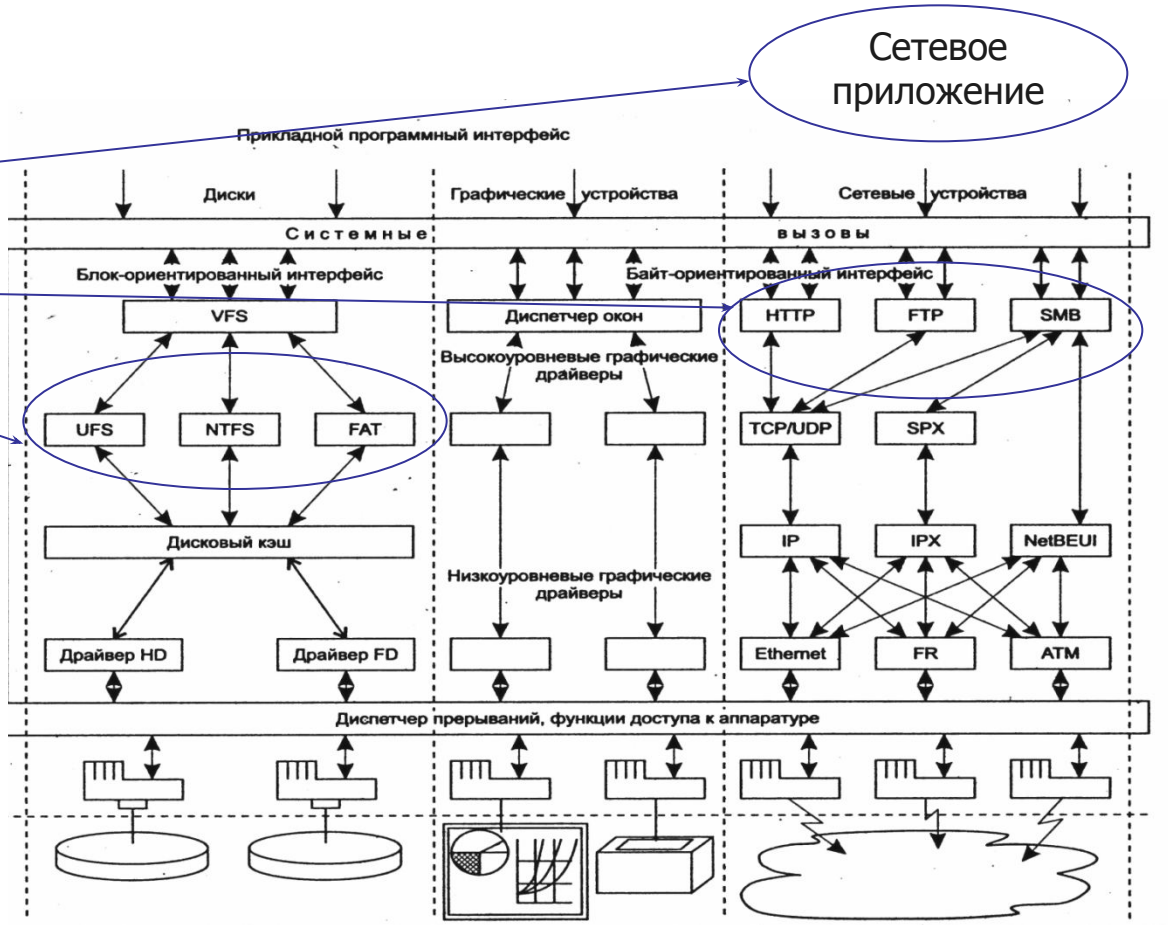
Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

Доступ к файлам и данным. Права доступа.

1. Приложения.
2. Сетевая подсистема.
3. Файловая система.



AAA

Аутентификация

Авторизация

Аудит

Компьютерные системы и сети

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.

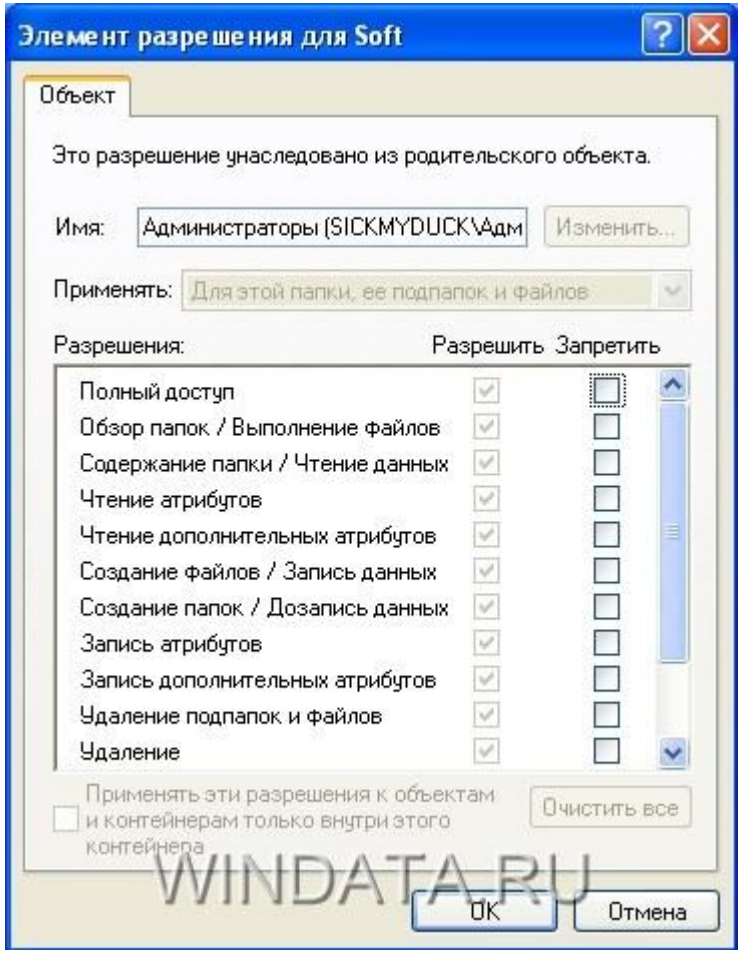
- **LR** — пользователь может просматривать каталоги и имена файлов в каталогах.
- **RX** — пользователь может читать файлы из каталога и запускать программы.
- **WX** — пользователь может добавлять файлы в каталог, но не читать или просматривать содержимое каталога.
- **RWX** — пользователь имеет права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

Компьютерные системы и сети

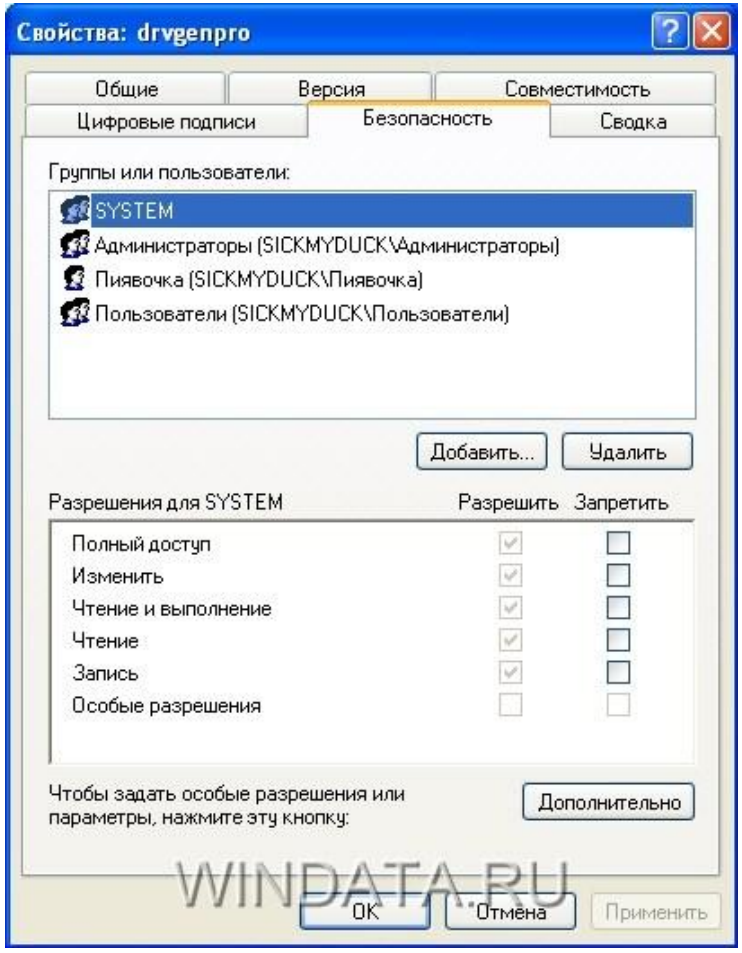
ГрГУ им. Я.Купалы

2011/2012

Установка прав сетевого доступа



Установка прав доступа к файлам

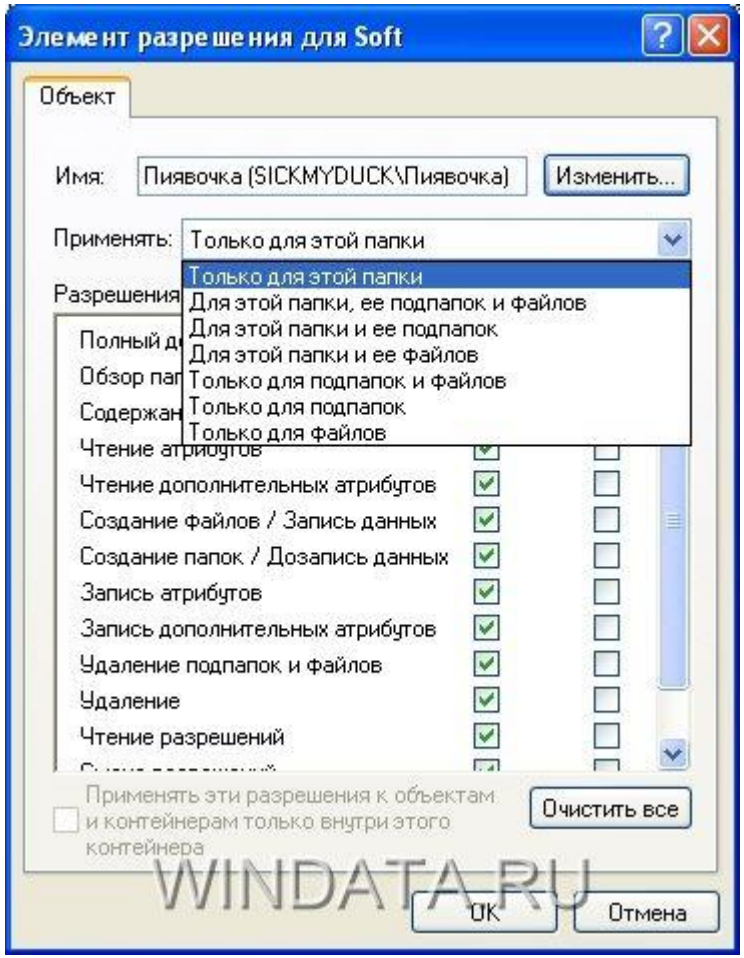


Компьютерные системы и сети

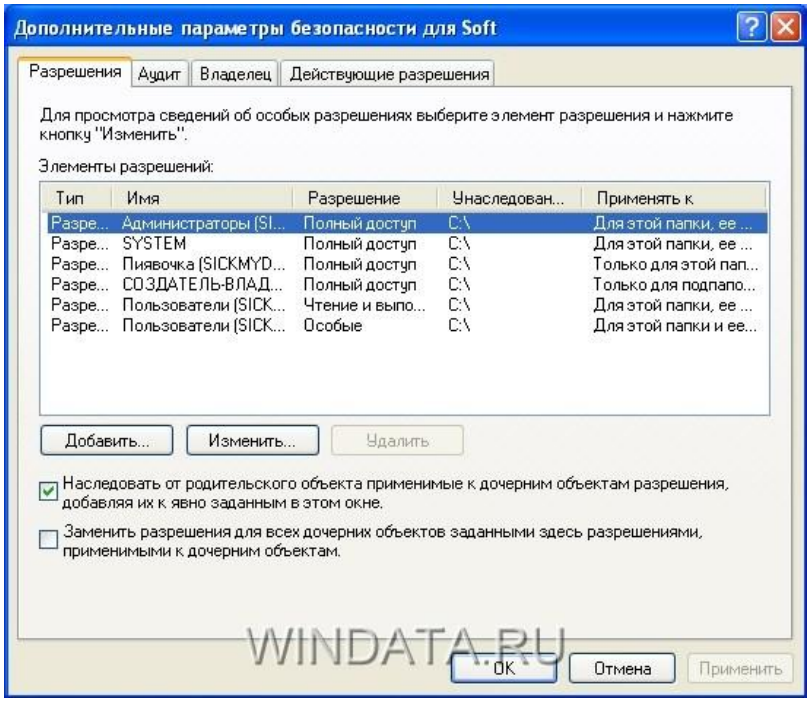
ГрГУ им. Я.Купалы

2011/2012

Наследование прав



Результирующие права

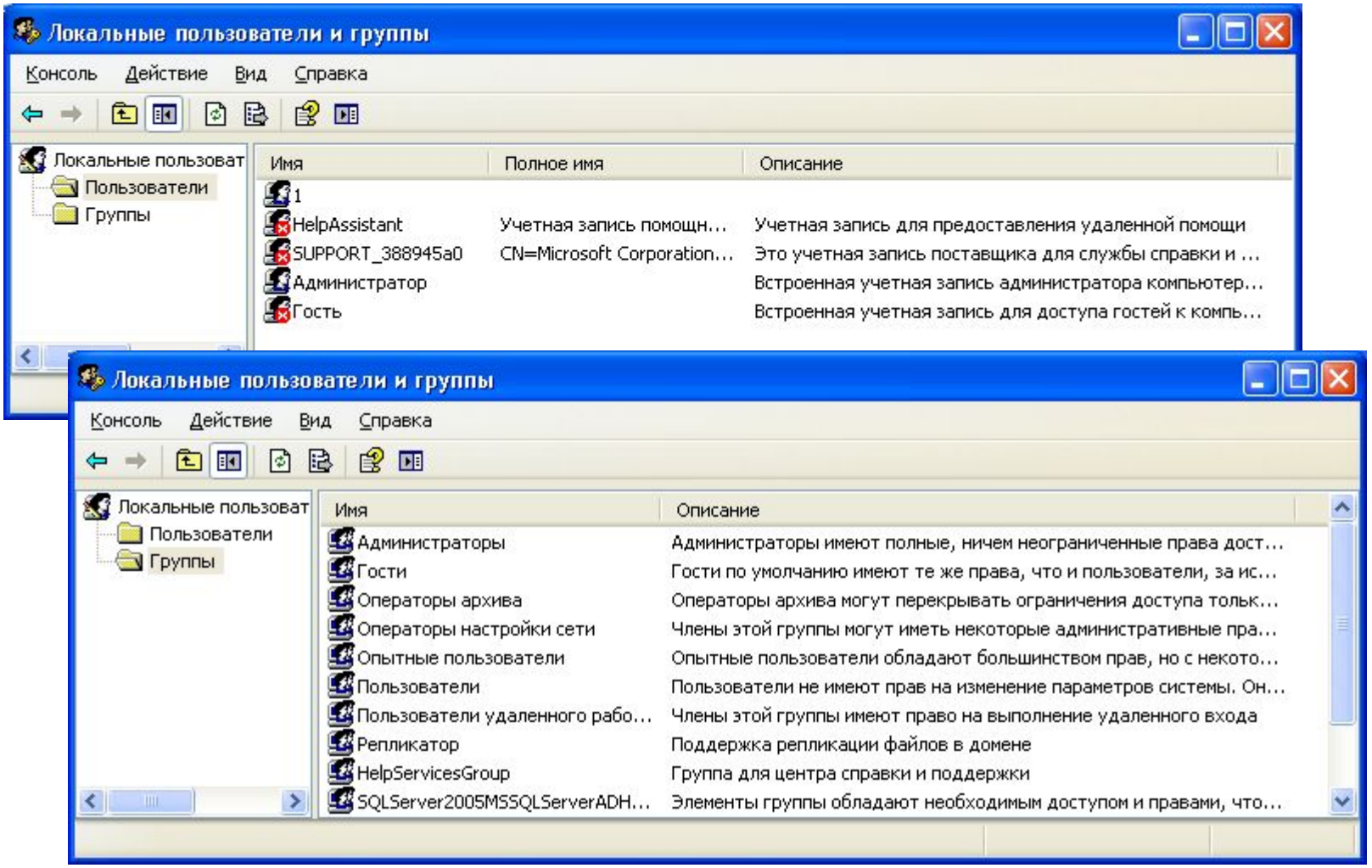


Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

Учетные записи

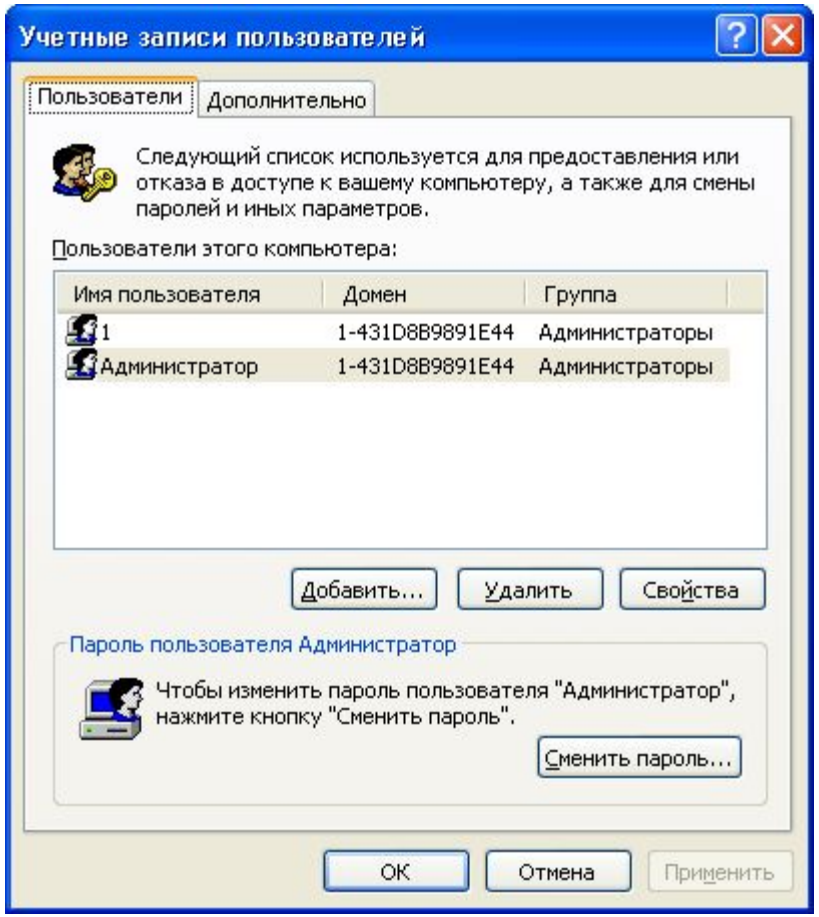


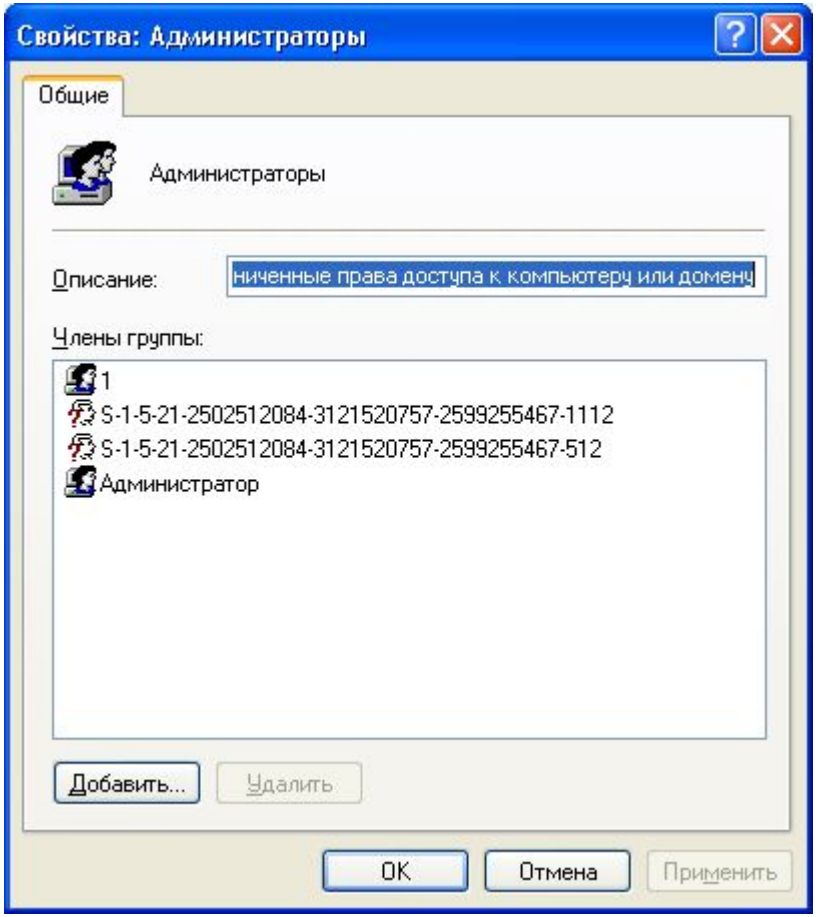
Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

Учетные записи





УПРАВЛЕНИЕ РЕСУРСАМИ СЕТИ

Компьютерные системы и 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.)

Компьютерные системы и сети

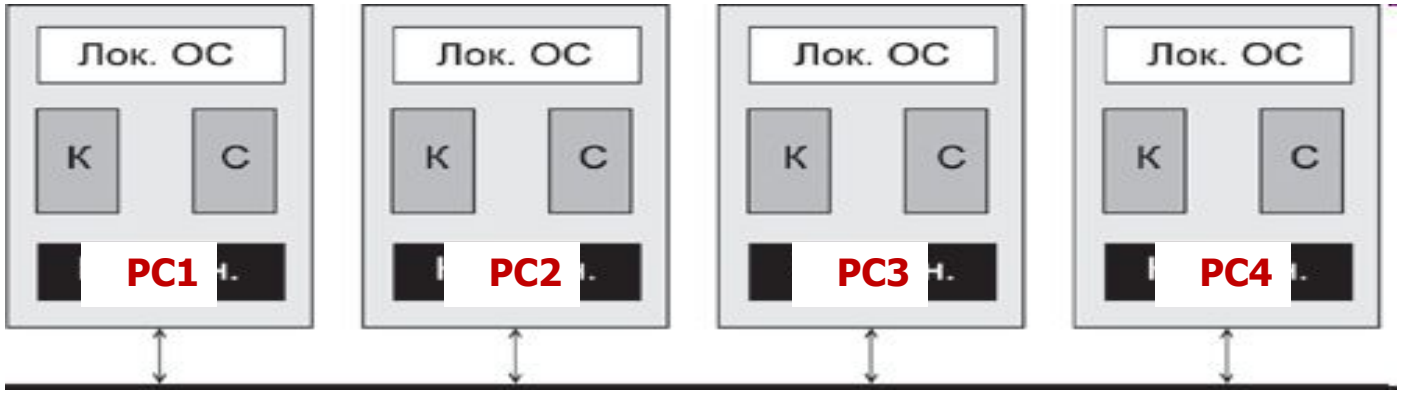
Списки прав доступа

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

Компьютерные системы и сети

ГрГУ им. Я.Купалы

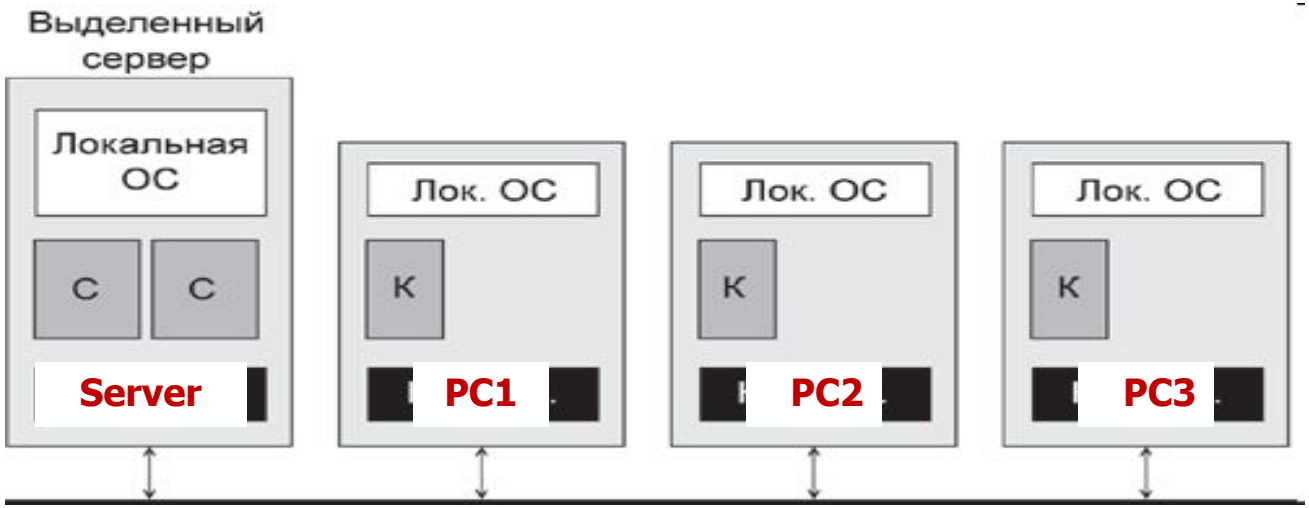
2011/2012

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

Компьютерные системы и сети

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.*

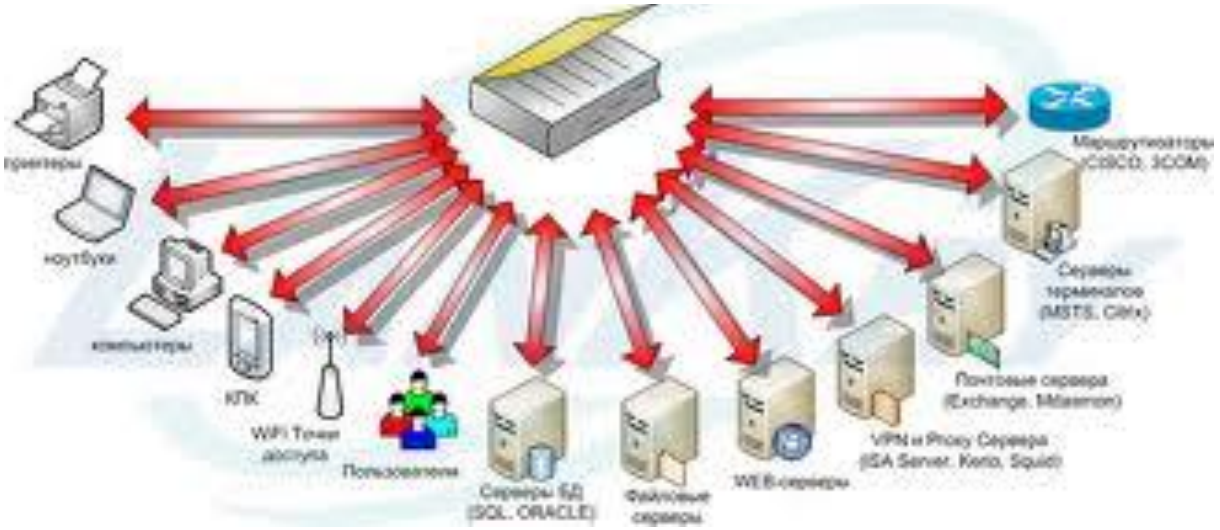
Компьютерные системы и сети

Наибольшее распространение получили каталоги:

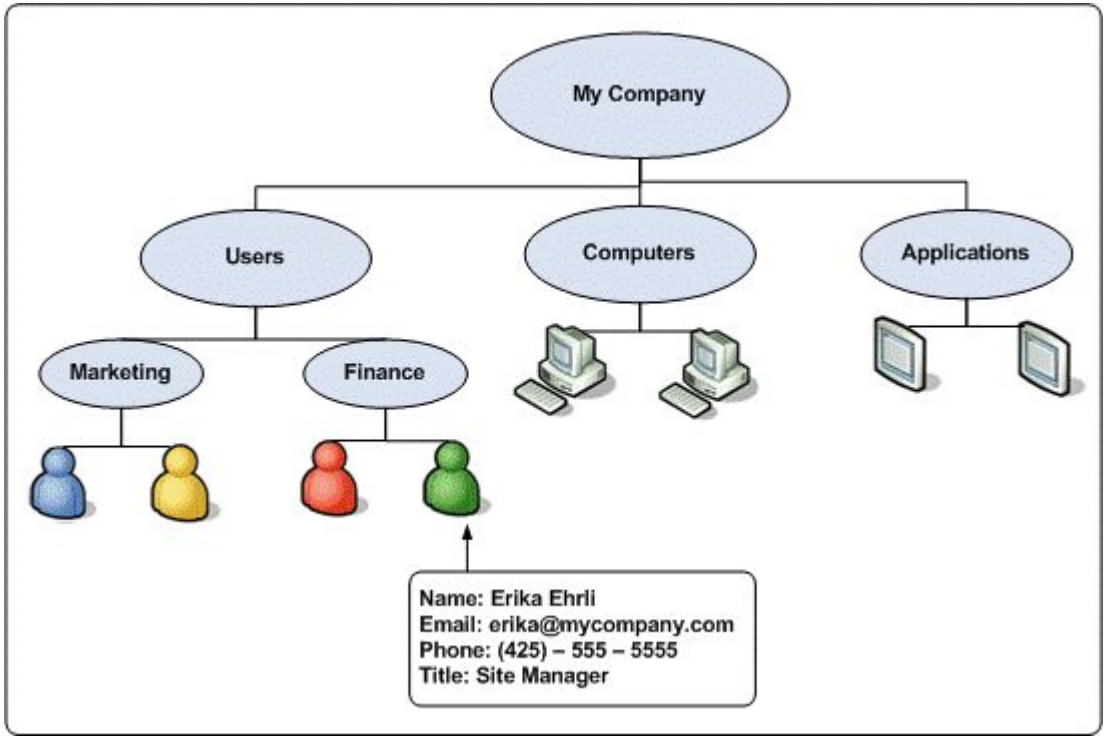
- служба **Active Directory** для Windows;
- служба **NDS** компании Novell.

Компьютерные системы и сети

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



Компьютерные системы и сети



Active Directory (AD)

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

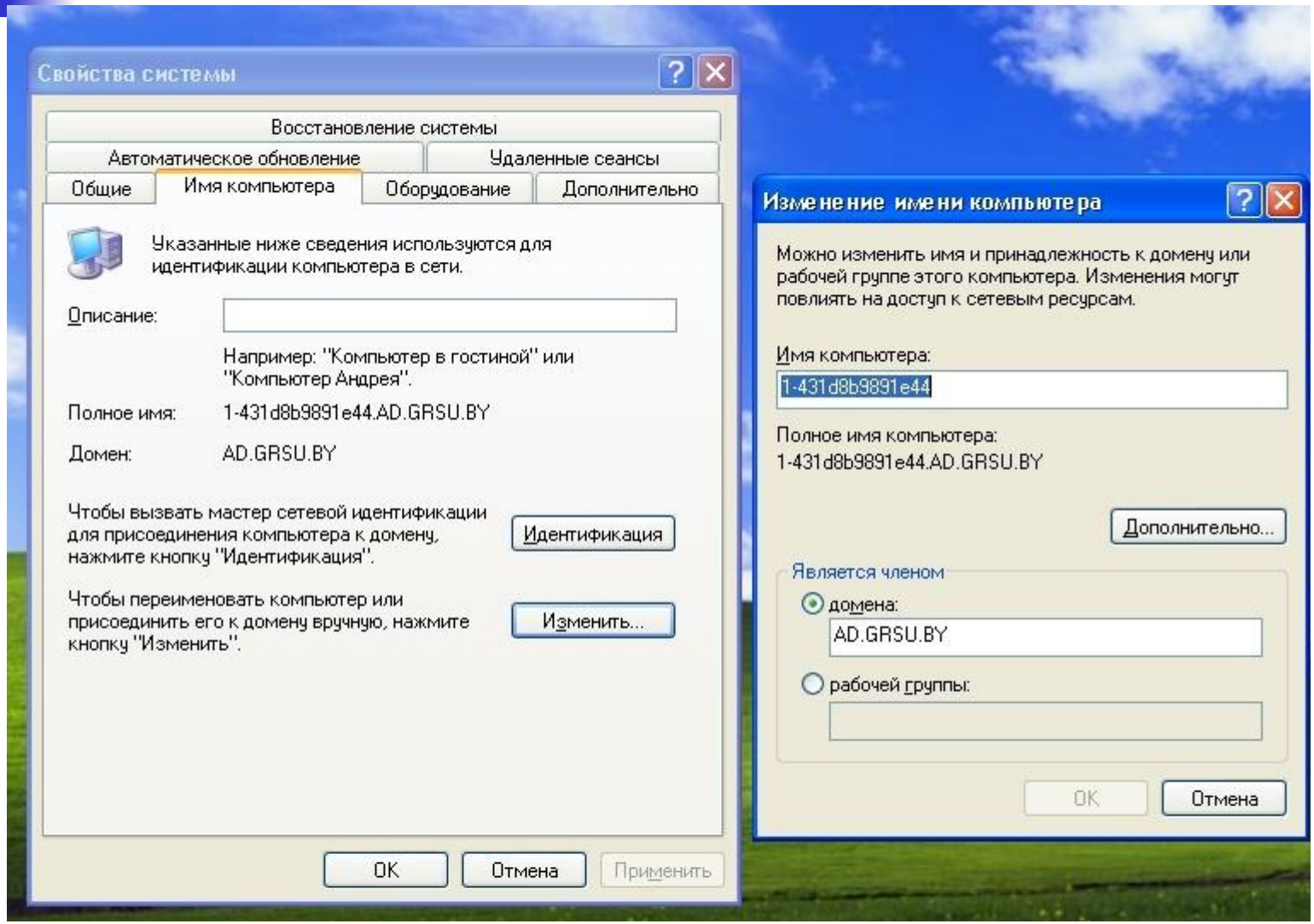
Active Directory поддерживается в Windows Server 2003, Windows Server 2003.

AD - база данных LDAP

Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012



Компьютерные системы и сети

функции *контроллеров доменов:*

- 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.

Компьютерные системы и сети

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* (оптимально иметь два или более). Домены Active Directory организованы в иерархическом порядке. Первый домен на предприятии становится корневым доменом леса, обычно он называется корневым доменом или доменом леса.
- ***Деревья доменов*.** Домены, которые создаются в инфраструктуре Active Directory после создания корневого домена, могут использовать существующее пространство имен Active Directory совместно или иметь отдельное пространство имен. Чтобы выделить отдельное пространство имен для нового домена, нужно создать новое дерево домена.
- **Леса**. *Лес* определяет границу безопасности для предприятия, являясь общим для всех *контроллеров домена* в лесу. Все домены и доменные деревья существуют в пределах одного или несколько лесов Active Directory.
- **Сайты**. *Сайт* представляет область сети, где все *контроллеры домена* связаны быстрым, недорогим и надежным сетевым подключением. Независимость логических компонентов от сетевой инфраструктуры возникает вследствие использования сайтов в Active Directory: они обеспечивают соединение между логическими компонентами Active Directory и физической сетевой инфраструктурой.
- **Организационные единицы**. *Организационные единицы* предназначены для того, чтобы облегчить управление службой Active Directory. Они служат для создания иерархической структуры в пределах домена и используются, чтобы сделать более эффективным управление единственным доменом (вместо управления несколькими доменами Active Directory).

Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

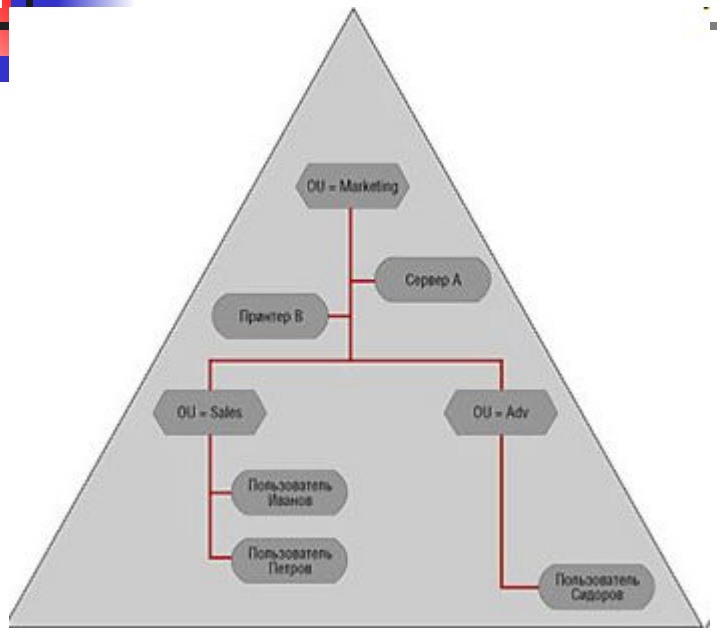


Рисунок 1. Типичная структура домена AD.

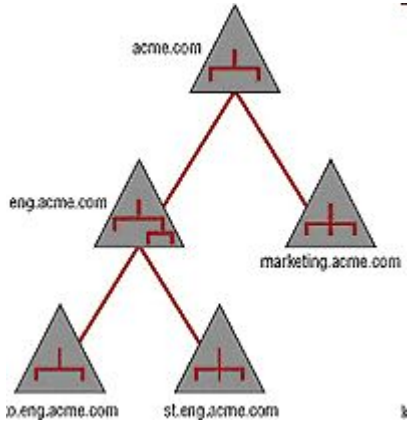


Рисунок 2. Дерево доменов AD.

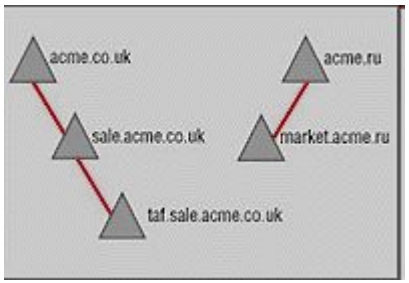


Рисунок 3. Лес доменов AD.

Active Directory

Компьютерные системы и сети

- **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.

Компьютерные системы и сети

Имена объектов каталогов:

DN (Distinguished Name, уникальное имя):

=

DC (компонент домена)

+

OU (организационный модуль)

+

CN (общее имя)

Примеры:

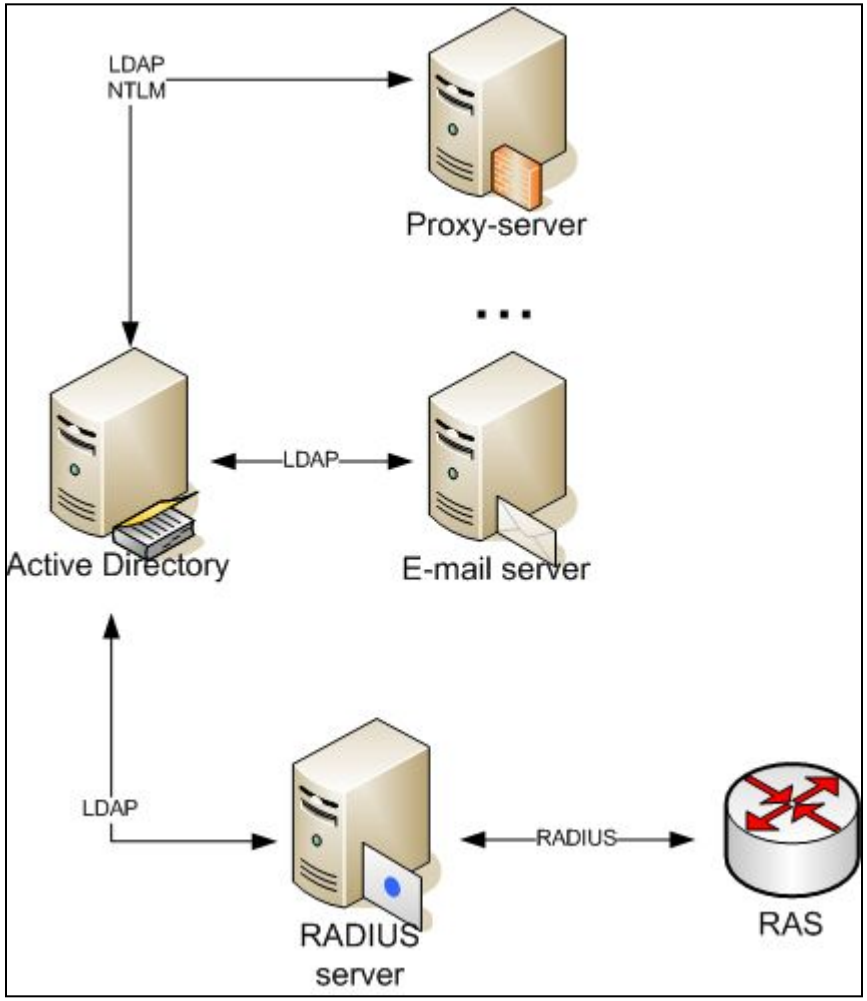
DC=grsu OU=main CN=users CN=Sidorov

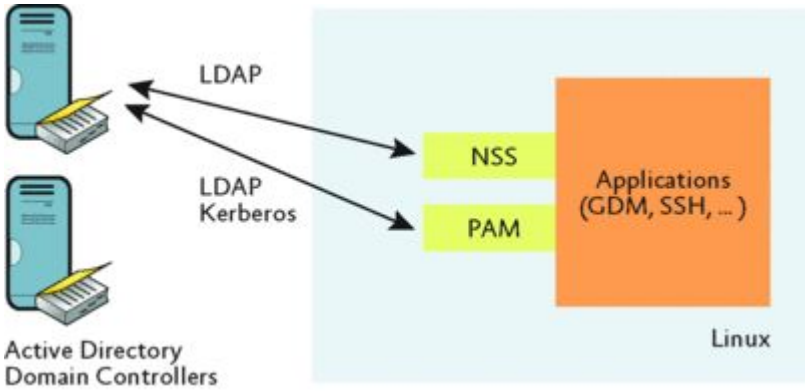
LDAP://cn=Sidorov, cn=users, ou=main, dc=grsu

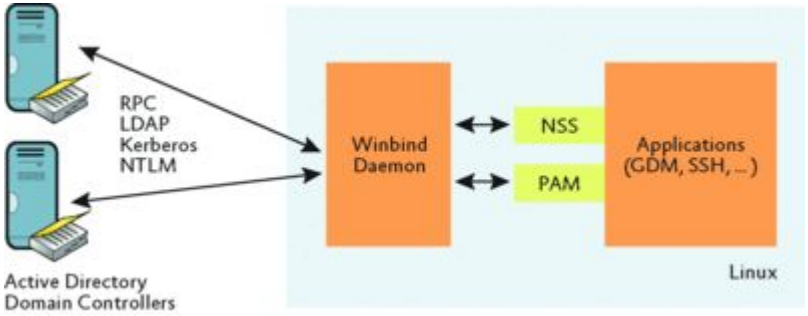
Компьютерные системы и сети

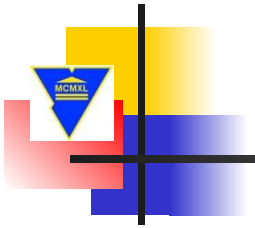
ГрГУ им. Я.Купалы

2011/2012









Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

Протоколы аутентификации в AD

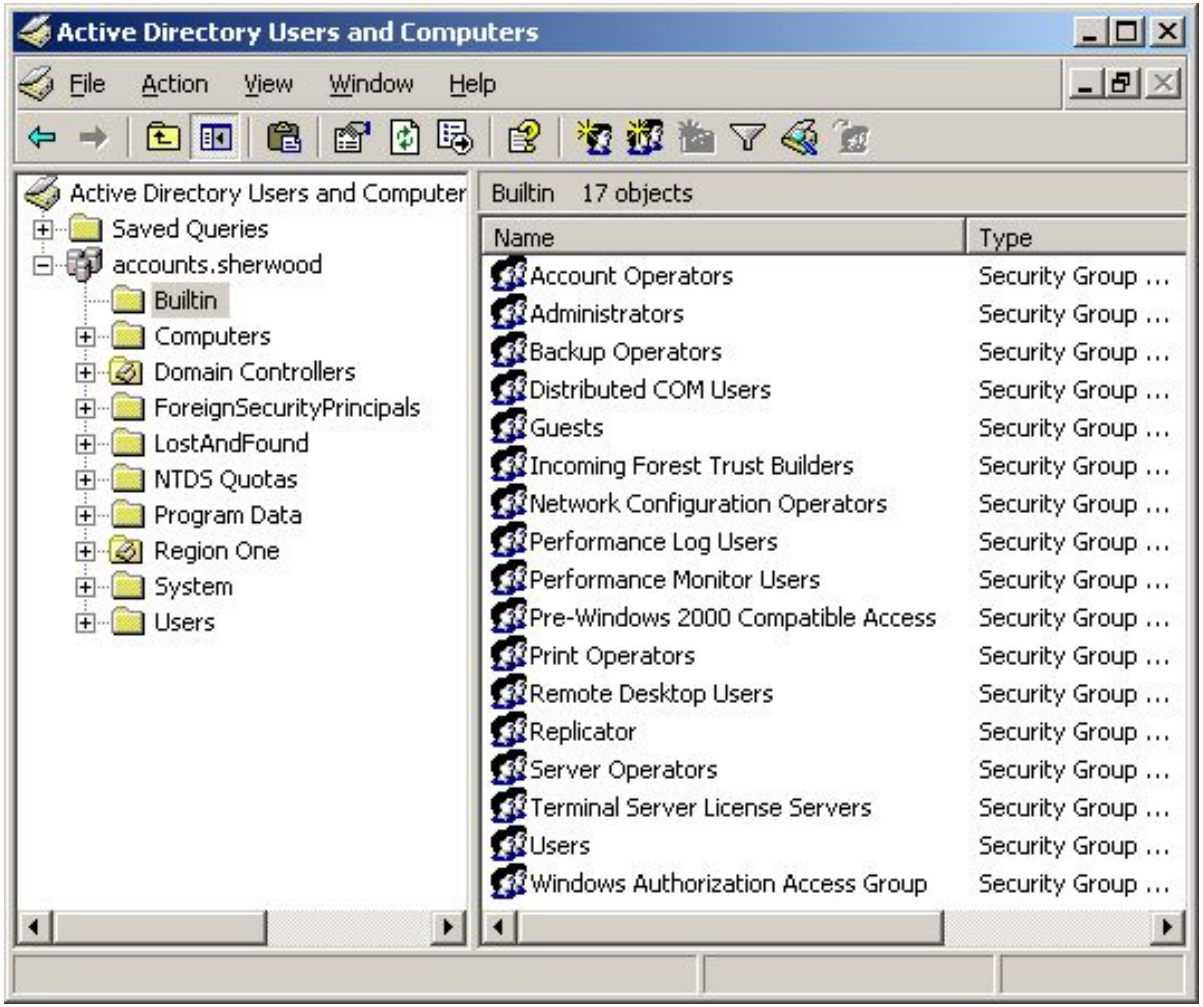
NT LAN Manager (NTLM)

Kerberos v.5

Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012



%systemroot%\NTDS\NTDS.DIT

Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

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

Компьютерные системы и сети

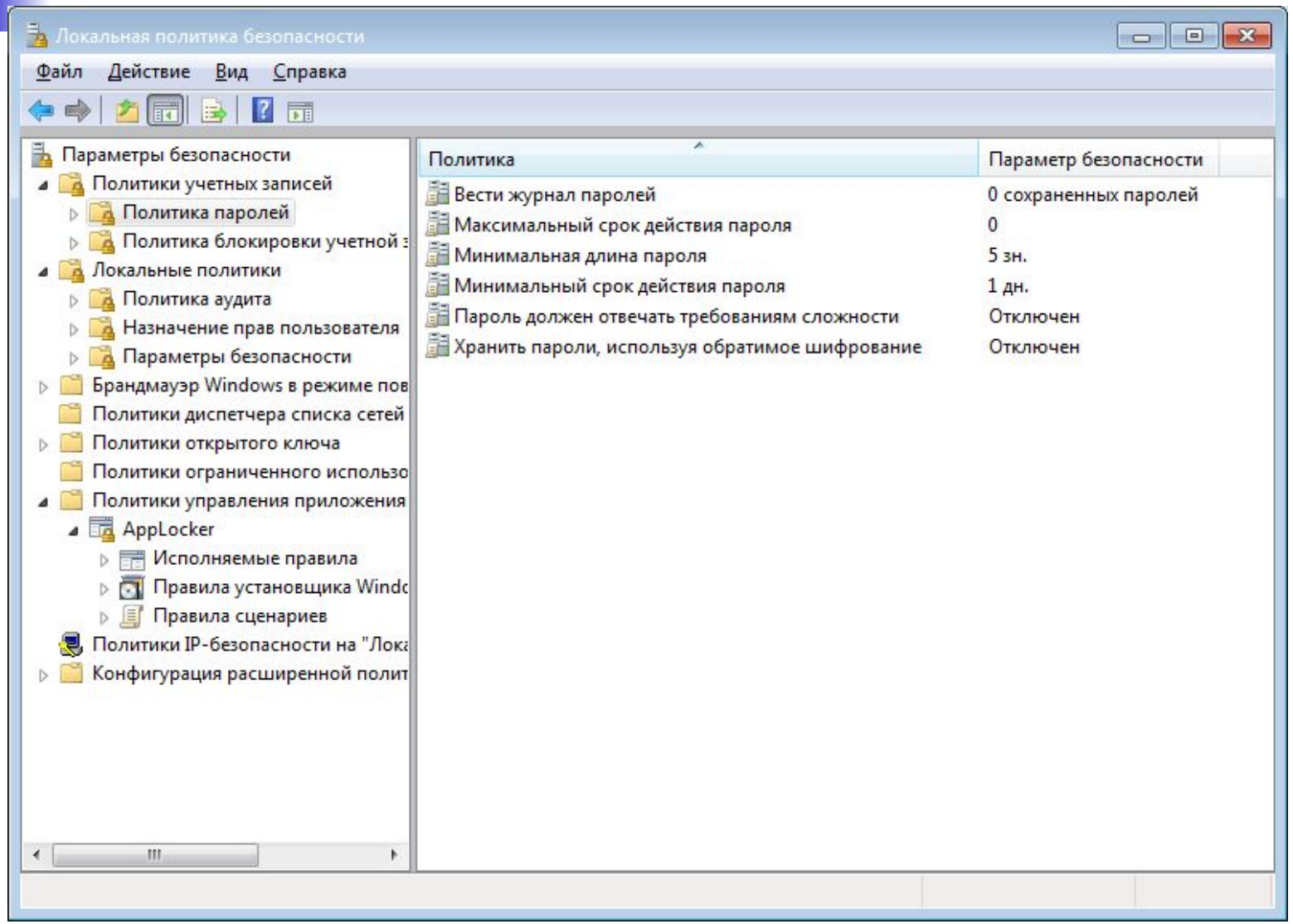
Управление на основе групповых политик (GPO)

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.**

Компьютерные системы и сети

ГрГУ им. Я.Купалы

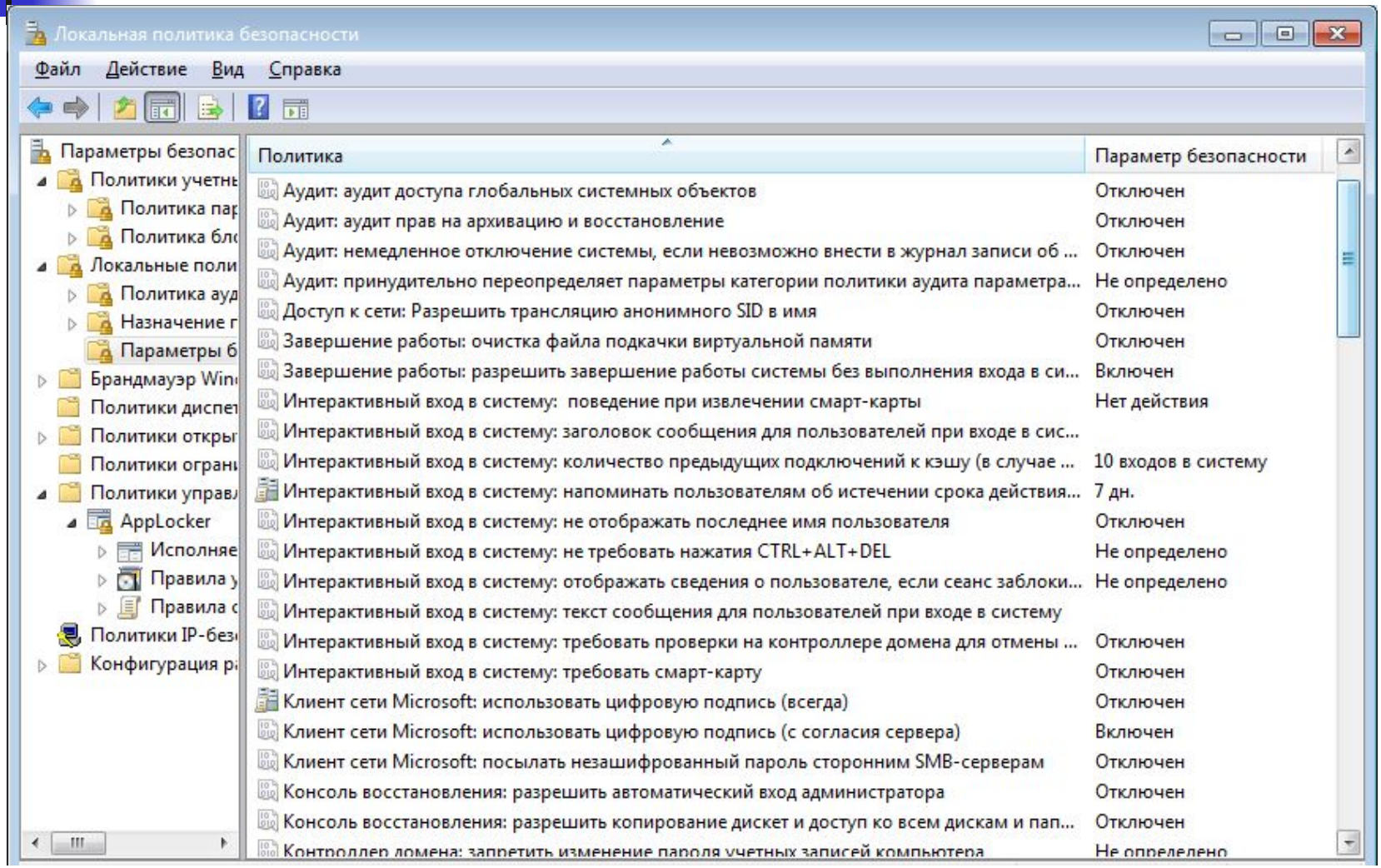
2011/2012



Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012



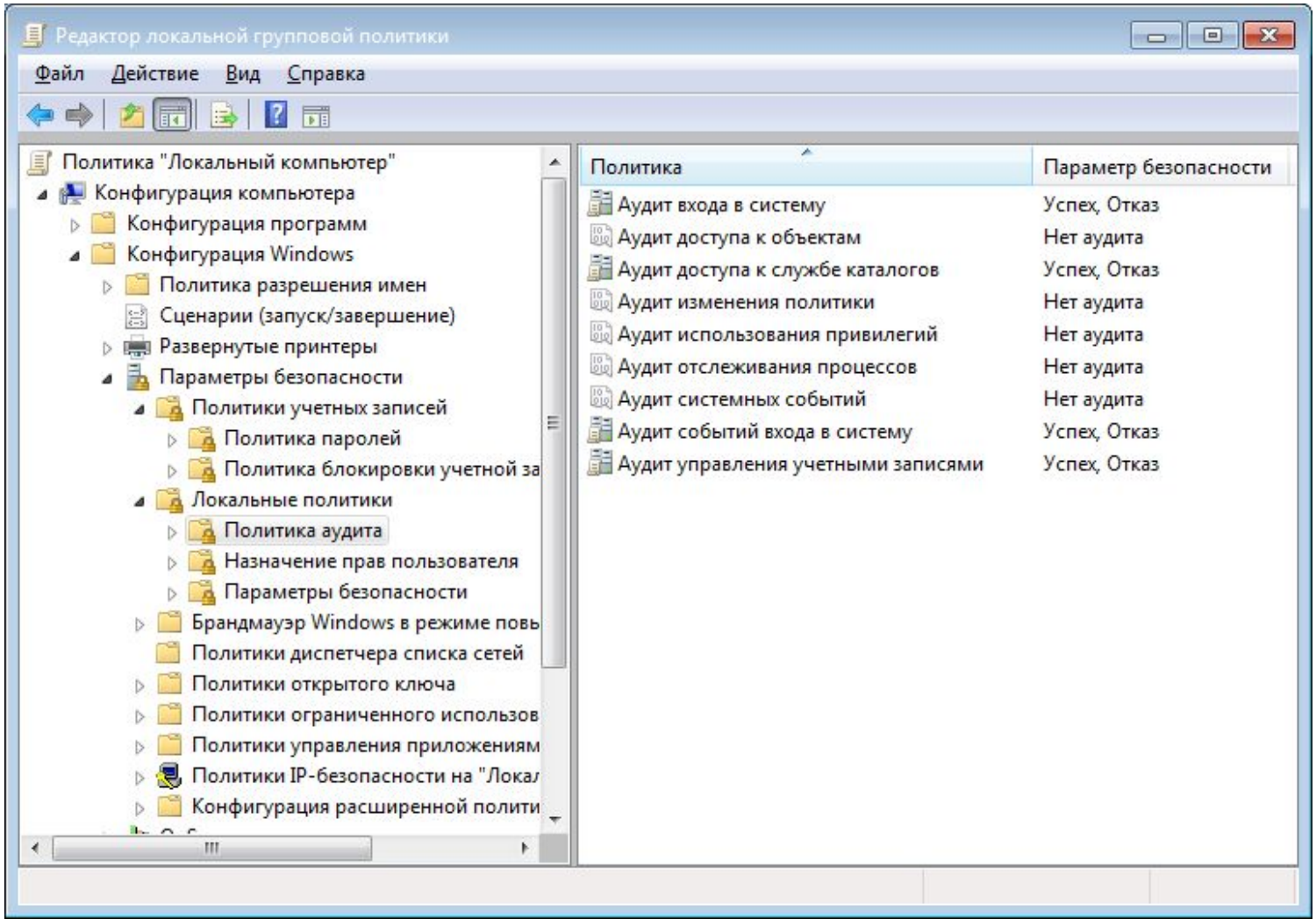
Enabled (Включен), Disabled (Отключен) и Not Configured (Не определено)

Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012

gpedit.msc



Компьютерные системы и сети

- 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

Компьютерные системы и сети

Инструменты управления групповой политикой

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

Компьютерные системы и сети

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.

Компьютерные системы и сети

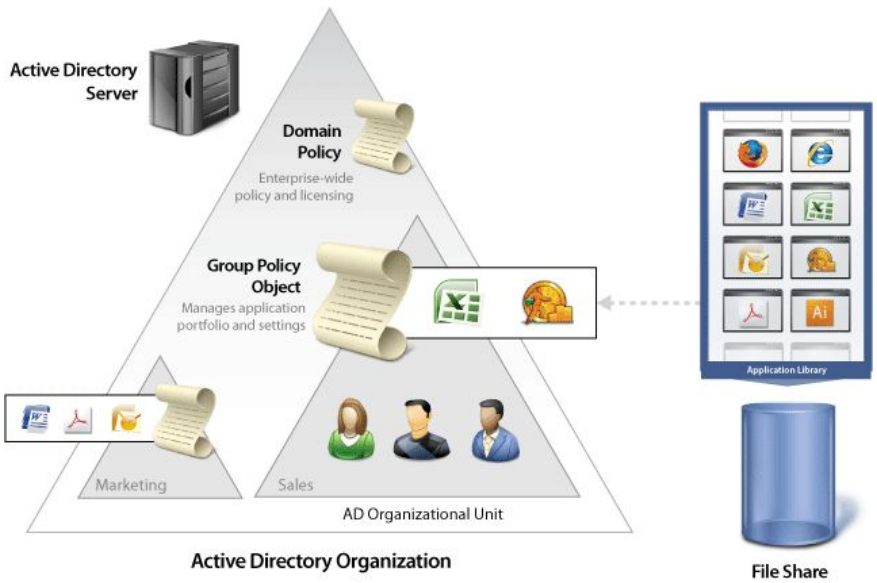
ГрГУ им. Я.Купалы

2011/2012

Сетевое управление программным обеспечением рабочих станций

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

wake-on-LAN



Компьютерные системы и сети

Программирование Active Directory

VB/VBScript, JScript, C/C++

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

класс DirectoryEntry

Компьютерные системы и сети

Инструменты управления каталогом

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

Компьютерные системы и сети

Восстановление контроллера домена:

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

Backup

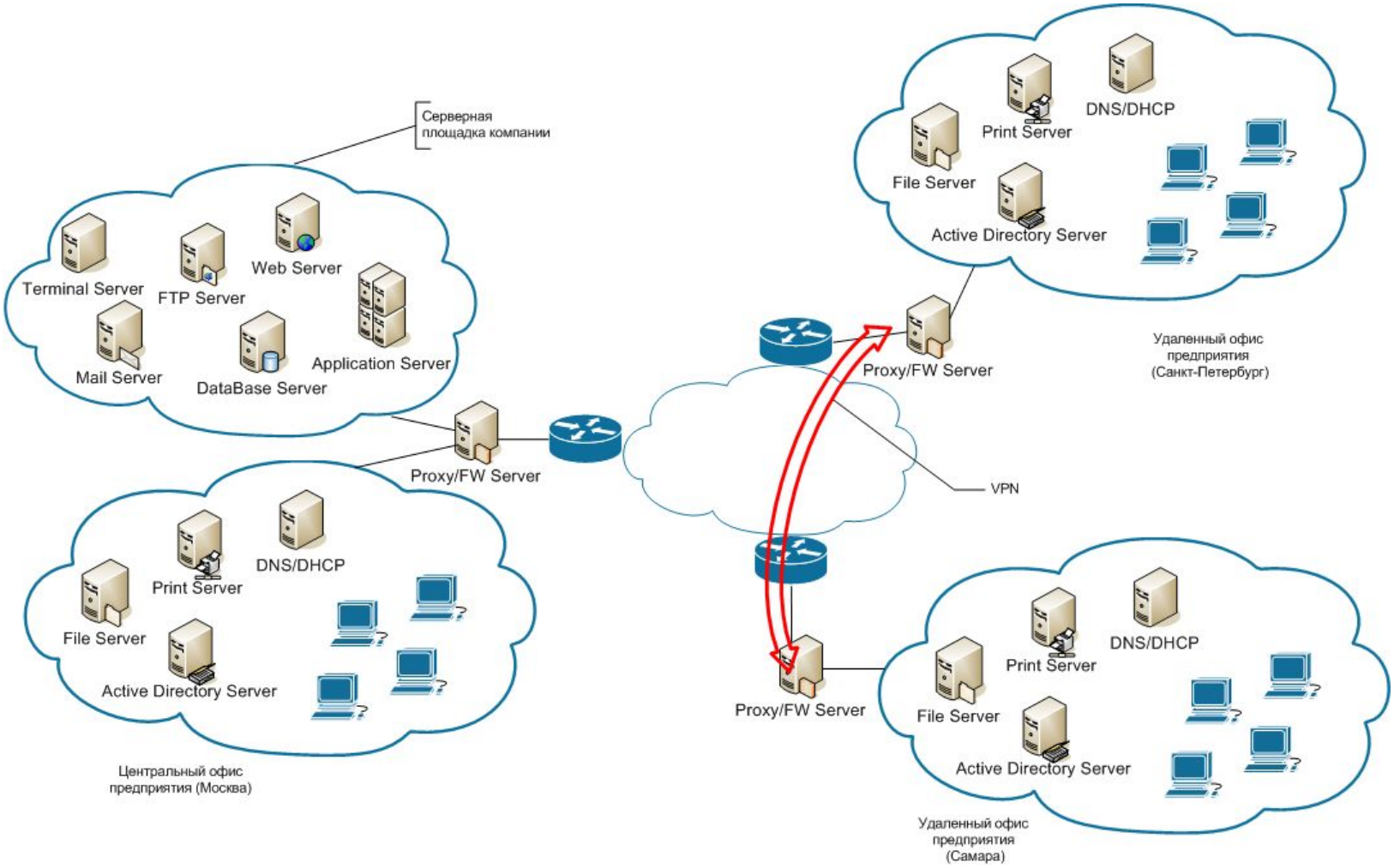
Ntdsutil.exe

Automated System Recovery - ASR

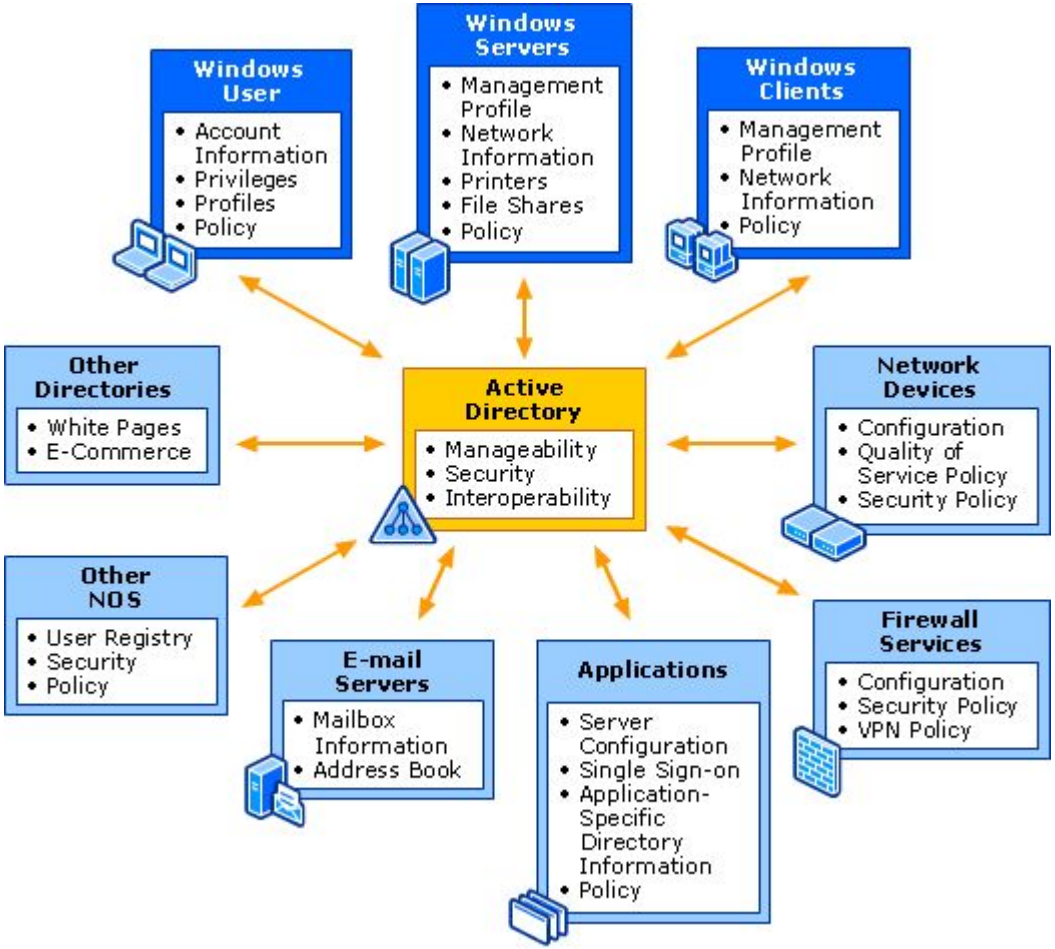
Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012



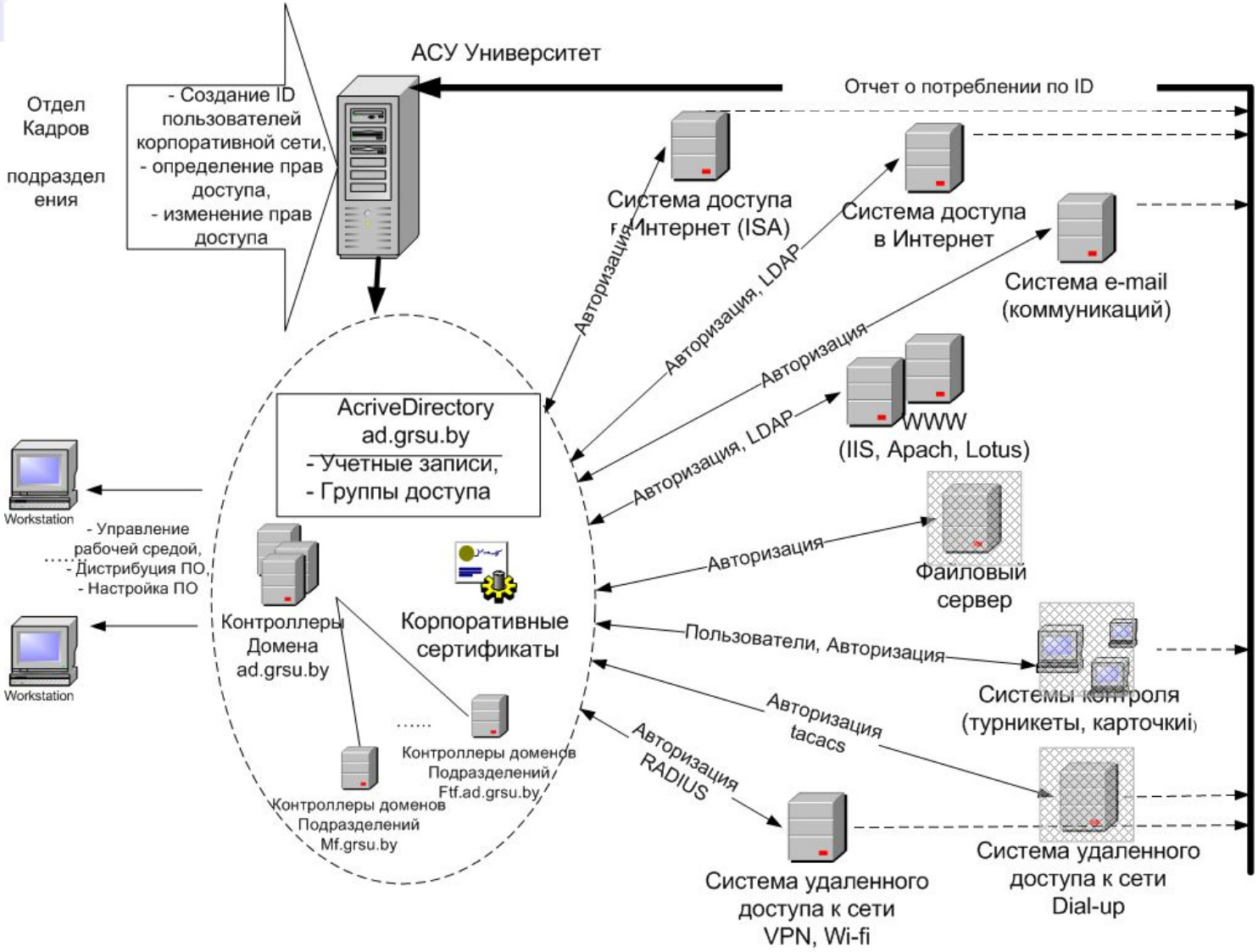
Компьютерные системы и сети

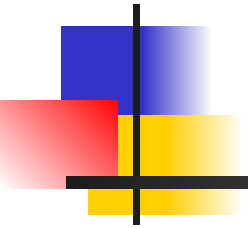


Компьютерные системы и сети

ГрГУ им. Я.Купалы

2011/2012





Компьютерные системы и сети

Олизарович Евгений Владимирович

ГрГУ им. Я.Купалы. 2011-2012