

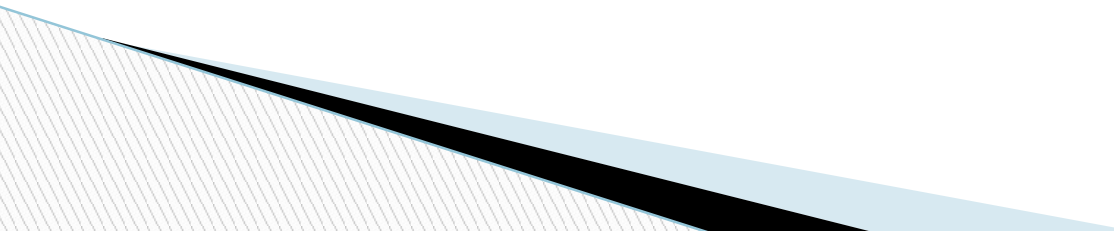
# Все по реестр

Презентацию подготовили  
Старикова Анастасия Самойлова Светлана  
Москвичев Яков Тимиркеев Алексей

- В систему Windows, начиная с Windows 95, включается единое хранилище, которое называется реестром (registry) и используется для хранения информации об этой операционной системе и установленных приложениях. Реестр является базой данных, и он используется почти во всем, что вы делаете. Он содержит информацию о самом компьютере, его оборудовании, периферийных устройствах, подсоединенных к компьютеру, об установленном ПО, а также о пользователях, выполняющих вход на этот компьютер. Реально реестр принадлежит программному обеспечению (включая операционную систему) и предназначен для того, чтобы предоставлять информацию для ПО, а не для пользователей.

# Обзор реестра

- В системе Microsoft Windows 3.1, которая была первой широко используемой версией Windows (особенно в бизнесе) использовались три типа файлов, определяющих оборудование компьютера и приложения для этой операционной системы. Два типа файлов использовались для инициализации и имели расширение имени .ini, и третий тип файлов использовался как база данных для регистрации. Среди файлов инициализации (.ini-файлов) имелись файлы, включенные в Windows, а также множество частных .ini-файлов из приложений (прикладного ПО).
- В Windows 3.1 использовались шесть .ini-файлов для загрузки и управления средой Windows (control.ini, progman.ini, protocol.ini, system.ini, win.ini и winfile.ini).

- Файл win.ini был
  - Файл system.ini
  - Файл progman.ini
  - файл winfile.ini
  - Файл protocol.ini
- 
- Эти файлы содержали конкретную информацию о состоянии приложения, включая такие элементы, как положение на экране, список недавно использовавшихся файлов и т.д.
- 

# Структура реестра

Реестр – это иерархическая база данных, содержащая вложенные контейнеры и данные следующего типа.

- ✓ *Поддеревья (Subtree)*. Корни, или основные группы этой иерархии.
- ✓ *Разделы (Key)*. Основные контейнеры, находящиеся непосредственно в поддеревьях.
- ✓ *Подразделы (Subkey)*. Дочерние подразделы. Подразделы могут содержать вложенные подразделы или записи.
- ✓ *Записи (Entry)*. Реальные данные (значения), которые влияют на систему. Записи представлены в правой панели редактора реестра.

# Ульи и файлы ульев

- Физически реестр – это набор файлов, которые называются ульями. Улей (hive) – это определенная часть реестра (определенный набор разделов, подразделов и параметров), которая представлена файлом на вашем компьютере. Файлы ульев можно просматривать или редактировать только с помощью редактора реестра. Однако их можно копировать, что является способом их резервного копирования вручную.

# Элементы данных реестра

Элементы данных реестра находятся на нижнем уровне иерархии реестра. Они содержат данные, которые определяют поведение разделов и подразделов (хотя не все разделы и подразделы содержат записи данных). Записи представлены в правой панели редактора реестра.

Любая запись содержит три элемента.

- Имя (параметр).
- Тип данных.
- Значение данных.

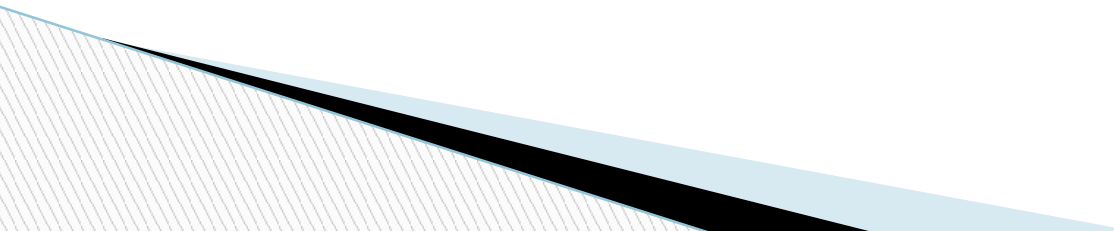
# Типы данных записи

Каждая запись имеет тип данных, которые может хранить эта запись. Существуют десять типов данных, но некоторые из них не используются системой Windows Server 2003.

- REG\_DWORD
- REG\_BINARY
- REG\_SZ
- REG\_MULTI\_SZ.
- REG\_EXPAND\_SZ
- REG\_FULL\_RESOURCE\_DESCRIPTOR.
- REG\_LINK.
- REG\_DWORD\_LITTLE\_ENDIAN.
- REG\_DWORD\_BIG\_ENDIAN



# HKKEY\_CLASSES\_ROOT

- HKKEY\_CLASSES\_ROOT заполняется всеми видами базовой информации. У вас редко будет повод работать интерактивно в этом поддереве; это набор "строительных блоков", с помощью которых могут работать операционная система и приложения. В этом поддереве существуют два типа данных.
  - Информация, ассоциируемая с типами файлов.
  - Данные конфигурации для объектов COM.
- 

# HKKEY\_CURRENT\_USER

- HKKEY\_CURRENT\_USER содержит профиль для текущего выполнившего вход пользователя. Это алиас для HKKEY\_USERS\<<идентификатор безопасности выполнившего вход пользователя>. Это поддерево на самом деле не содержит никаких данных; в нем хранится только указатель на содержимое реального поддерева и выводится эта информация. Однако важно знать, что изменения, внесенные в содержимое одного из поддереьев, приводят к изменению обоих поддереьев.
- Это средство экономии времени для операционной системы и приложений, поскольку они выполняют поиск настроек пользователя, прежде чем выполнять задачи.

- При входе пользователя `HKEY_CURRENT_USER` создается заново с использованием данных, которые составляют профиль выполняющего вход пользователя. Если это первый вход данного пользователя, то никакого профиля еще нет, и операционная система загружает настройки профиля `Default User`. При завершении сеанса этого нового пользователя его профиль сохраняется под именем этого пользователя. Сохраняются любые изменения, внесенные в конфигурацию этим пользователем.

# HKKEY\_LOCAL\_MACHINE

- Это поддерево содержит информацию о компьютере, его оборудовании, установленных драйверах устройств и опциях конфигурации (для настроек безопасности и настроек ПО), которые влияют на всех пользователей данного компьютера. Оно содержит пять разделов: Hardware, SAM, Security, Software и System. Все эти разделы, кроме Hardware, присутствуют на диске в виде файлов ульев.
- HKLM\Hardware (Распознаватель оборудования)
- HKLM\SAM (Это данные, используемые для диспетчера учетных записей )
- HKLM\Security (Аналогично подразделу SAM )
- HKLM\Software (Это поддерево для внешних программ)
- HKLM\System (для настроек конфигурации компьютера)

## HKKEY\_USERS

- Это поддерево содержит подразделы для профиля Default User и всех известных профилей пользователей для данного компьютера. Каждый подраздел с профилем отдельного пользователя идентифицируется идентификатором безопасности (Security ID, SID) и раскрывается в виде полного набора подразделов с настройками (для раздела HKKEY\_CURRENT\_USER, когда данный пользователь выполняет вход).

## HKKEY\_CURRENT\_CONFIG

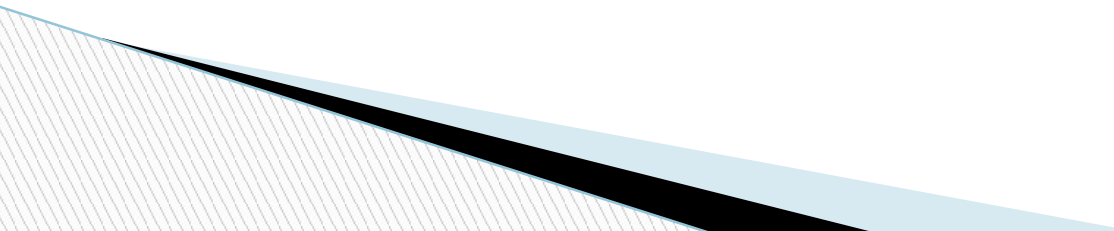
- Это поддерево содержит информацию о профиле оборудования, который используется данным компьютером при загрузке

# Regedit.exe

Regedit.exe – это редактор реестра.

- Дистанционный доступ к реестрам
- Поиск в реестре
- Создание списка Favorites

# Работа с реестром

- Экспорт разделов
  - Добавление элементов в реестр
  - Удаление элементов реестра
  - Изменение значений элементов реестра
  - Использование файлов регистрации
- 

# Использование файлов регистрации

Файлы регистрации – это текстовые файлы с расширением .reg, использующие следующий формат.

- Имя инструментального средства
- пустая строка
- [Путь в реестре]
- "Имя элемента данных"=Тип данных:значение
- "Имя элемента данных"=Тип данных:значение
- "Имя элемента данных"=Тип данных:значение



# Средства безопасности для реестра

- Работа со средствами безопасности для реестра очень похожа на работу со средствами безопасности, которые вы получаете с помощью файловой системы NTFS.
- По умолчанию заданы довольно жесткие уровни безопасности реестра. Администраторы имеют полный доступ ко всему реестру, но другие пользователи имеют полный доступ только к разделам, которые относятся к их собственным пользовательским учетным записям (сюда включается `HKEY_CURRENT_USER`), а также доступ только по чтению к разделам, которые относятся к данному компьютеру и установленному ПО. Тем не менее, вам может потребоваться изменение настроек безопасности реестра, чтобы предоставлять или отменять полномочия на уровне группы или пользователя. В этом разделе дается описание задач, связанных с заданием полномочий.

# Аудит реестра

У вас имеются достаточно мощные и гибкие возможности аудита операций с реестром; вы можете выполнять аудит разделов, пользователей, групп и любых сочетаний. Для аудита операций с реестром нужно выполнить три шага.

- Включить аудит как групповую политику.
- Задать опции конфигурирования аудита в реестре.
- Просматривать результаты аудита в журнале Security оснастки Event Viewer

# Reg.exe

Reg.exe – это надежное и многофункциональное средство командной строки, которое вы можете использовать для управления записями реестра.

- Reg Add
- Reg Delete
- Reg Copy
- Reg Compare
- Reg Export
- Reg Import
- Reg Save
- Reg Restore
- Reg Load
- Reg Unload
- Reg Query

