Лекция №13

Администрирование операционных систем

Задачи администрирования

Генерация операционной системы

- Генерация операционной системы – процесс создания версии операционной системы (ядра ОС), учитывающей аппаратную конфигурацию компьютера, назначение системы и требования пользователя.
- В основном генерация осуществляется автоматически. Возможны запросы пользователю на выбор определённых параметров (логический диск для ОС, язык, системное время и т.д.).

Задачи сопровождения системного ПО

- Работа с системным и прикладным ПО.
- Работа с пользователями.
- Работа с устройствами.
- Работа с данными (резервирование и восстановление данных).

Работа с системным и прикладным ПО

- Настройка работы ОС и приложений.
- Контроль и восстановление работоспособности ОС и приложений.
- Модификация ОС: установка и удаление приложений, обновление ОС и приложений.

Работа с пользователями

- Управление учётными данными пользователей.
- Ограничение дискового пространства, выделяемого пользователю (дисковые квоты).

Работа с устройствами

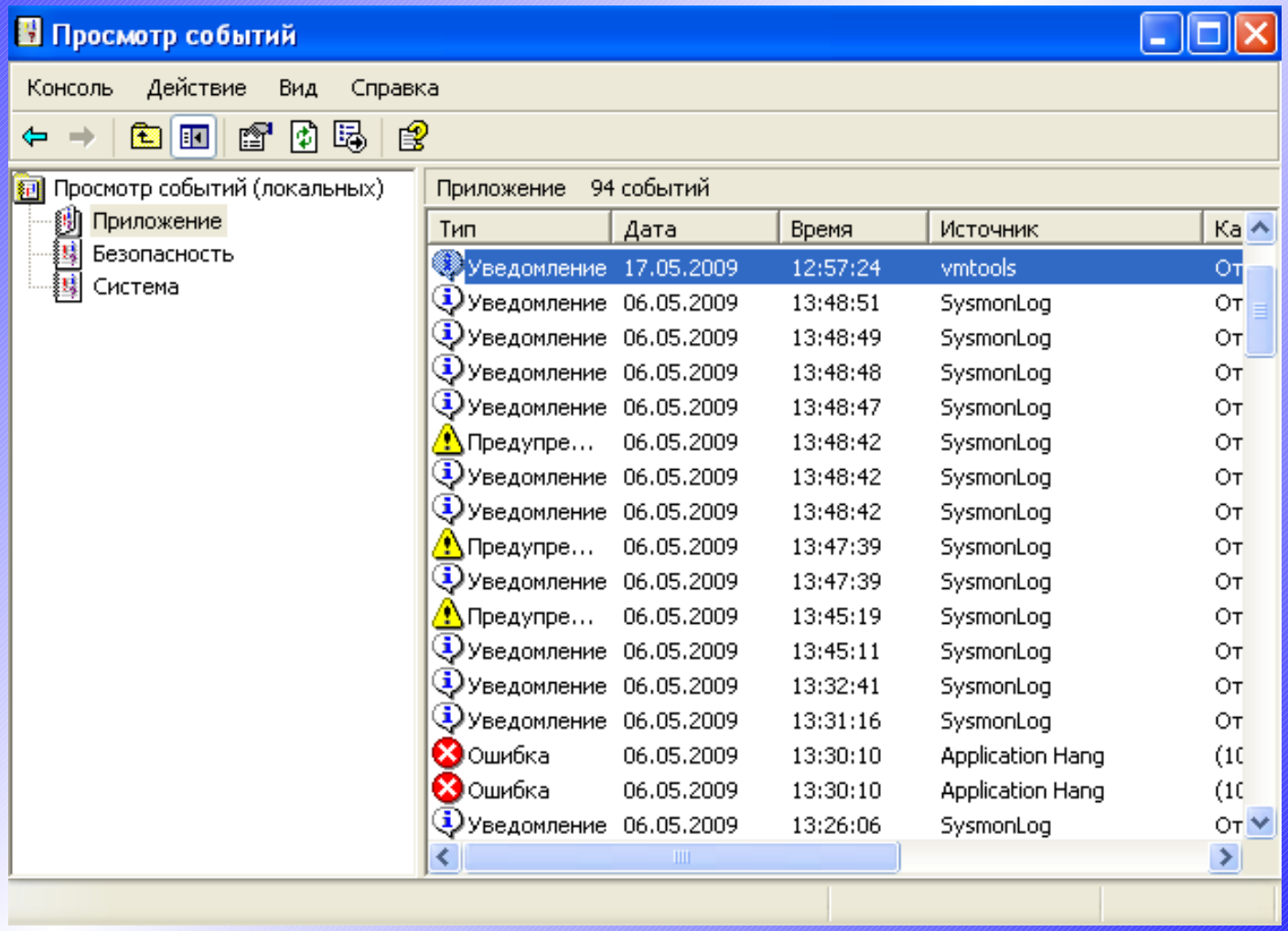
- Установка, восстановление и удаление драйверов устройств.
- Контроль производительности ОС.

Контроль работоспособности ОС и приложений

Типы событий, фиксируемые ОС:

- ошибка – событие, чаще всего приводящее к аварийной остановке работы системных или прикладных программ (например, отказ устройства);
- предупреждение – событие, генерируемое в случае возможного появления ошибки;
- уведомление – событие, описывающее ход этап выполнения системной или прикладной программы.

Контроль работоспособности ОС и приложений



Контроль работоспособности ОС и приложений

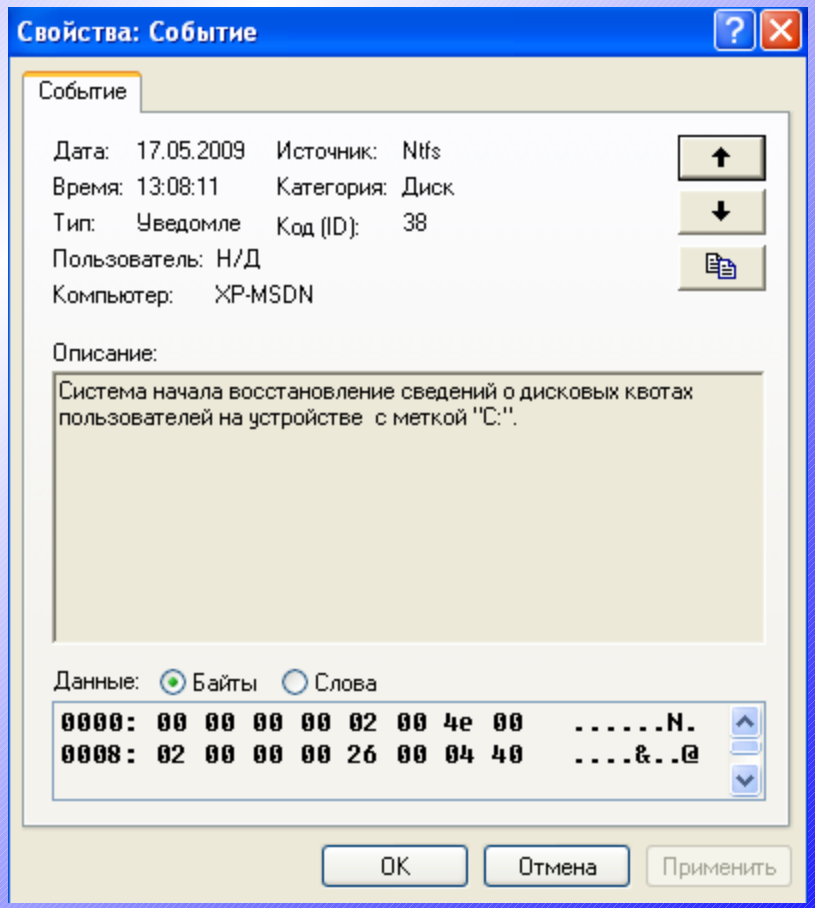
Журналы «Просмотра событий»:

- Приложение – события генерируются прикладным ПО;
- Безопасность – события генерируются системой безопасности Windows;
- Система – события генерируются системным ПО, включая драйверы устройств (в т.ч. при загрузке ОС).

Контроль работоспособности ОС и приложений

Запись каждого события содержит:

- дату и время события;
- тип и описание события;
- код, источник и категорию события;
- имя компьютера, на котором оно произошло;
- имя учётной записи, под которой оно произошло.



Настройка ОС

- Настройка ОС – изменение уполномоченным пользователем основных механизмов, политик ОС.
- Возможные цели настраивания ОС: увеличение производительности, надёжности, улучшение пользовательского интерфейса, увеличение защищённости.
- Настраивание ОС возможно на этапах генерации (для встраиваемых ОС – только на этом этапе), загрузки или работы ОС.

Варианты настройки ОС

- Метод загружаемого модуля ядра – уполномоченное лицо может загрузить в ядро модуль для модификации ОС (возможно нарушение надёжности функционирования ОС). Используется при добавлении новых драйверов и обновлении ОС.
- Изменение параметров системы – установка уполномоченным лицом необходимого режима работы ОС за счёт изменения предоставленных параметров (ограничен уровень детализации настроек).

Варианты восстановления ОС

- Автоматическое восстановление.
- Использование последней удачной конфигурации (использование сохранённой точки восстановления с работоспособными исполняемыми файлами и настройками ОС).
- Загрузка системы в безопасном режиме (восстановление или переустановка некорректно работающих драйверов и приложений).
- Откат (восстановление) драйвера устройства.

Управление учётными данными пользователей

- Регистрация пользователя – создание учётной записи с уникальным именем (включая создание пароля).
- Изменение и удаление учётной записи, сброс пароля.
- Создание групп и добавление в них пользователей.

Управление учётными данными пользователей

- Разработка групповых политик (набора ограничений и привилегий пользователя).
- Управление профилями пользователей.

  Профиль – совокупность папок и данных, в которых хранятся текущее окружение пользователя (содержимое рабочего стола, параметры настройки приложений и личные данные).

Контроль производительности операционной системы

Факторы, влияющие на производительность ОС:

- аппаратные средства (частота процессора, объём память и т.д.);
- конфигурация операционной системы (настройки GUI, количество событий, подлежащих регистрации);
- установленное прикладное программное обеспечение.

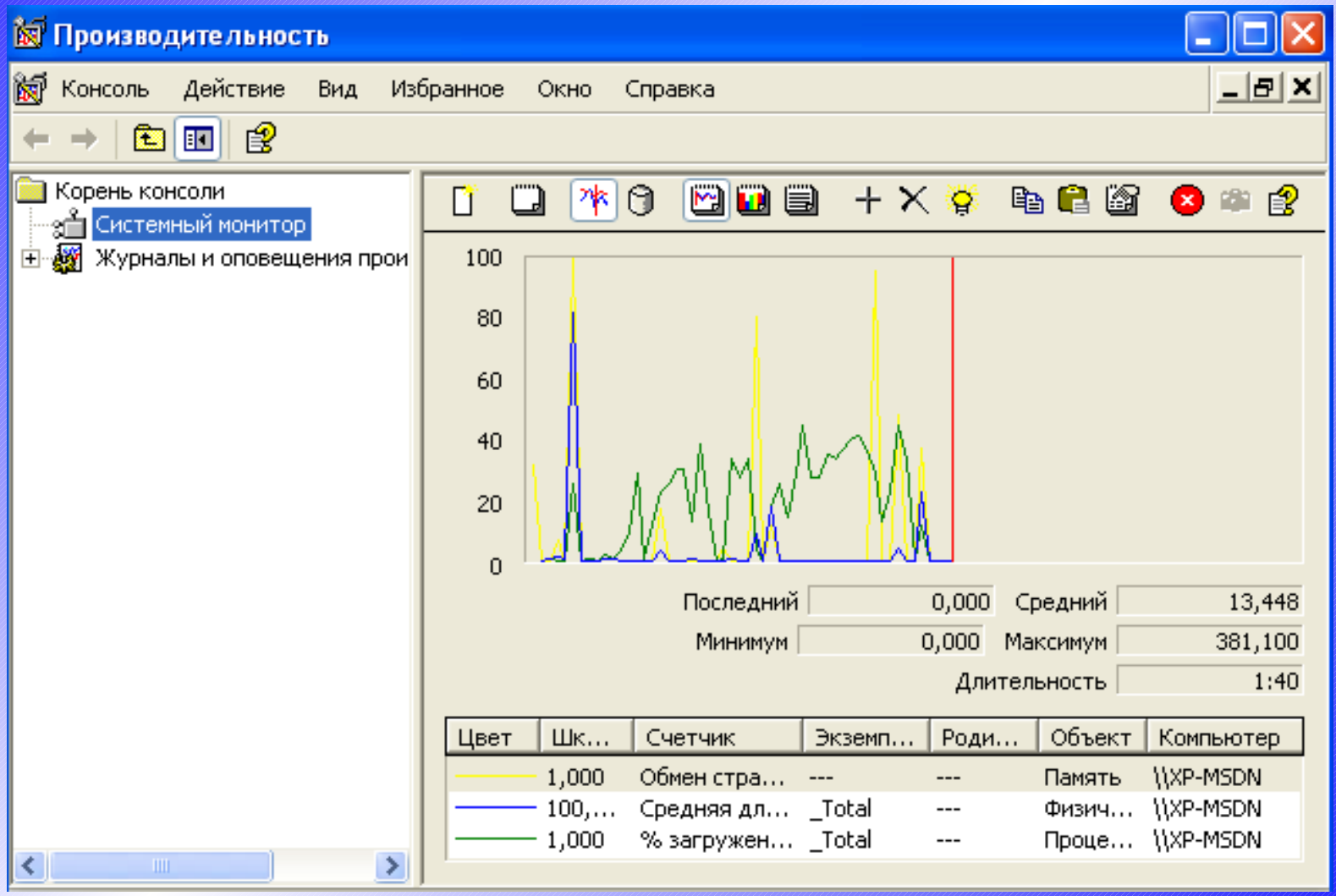
Категории аппаратных средств, влияющих на производительность

- Память.
- Центральный процессор.
- Дисковая подсистема.
- Сетевой адаптер.
- Видеоадаптер.
- Системная шина.

Инструменты для контроля производительности

- Системный монитор – инструмент для отображения информации о производительности.
- Журналы счётчиков – инструмент для регистрации производительности заданных компонентов системы.
- Журналы трассировки – инструмент для регистрации производительности при наступлении заданного события.
- Оповещения – выполняют определённые пользователем действия при превышении заданного порога производительности.

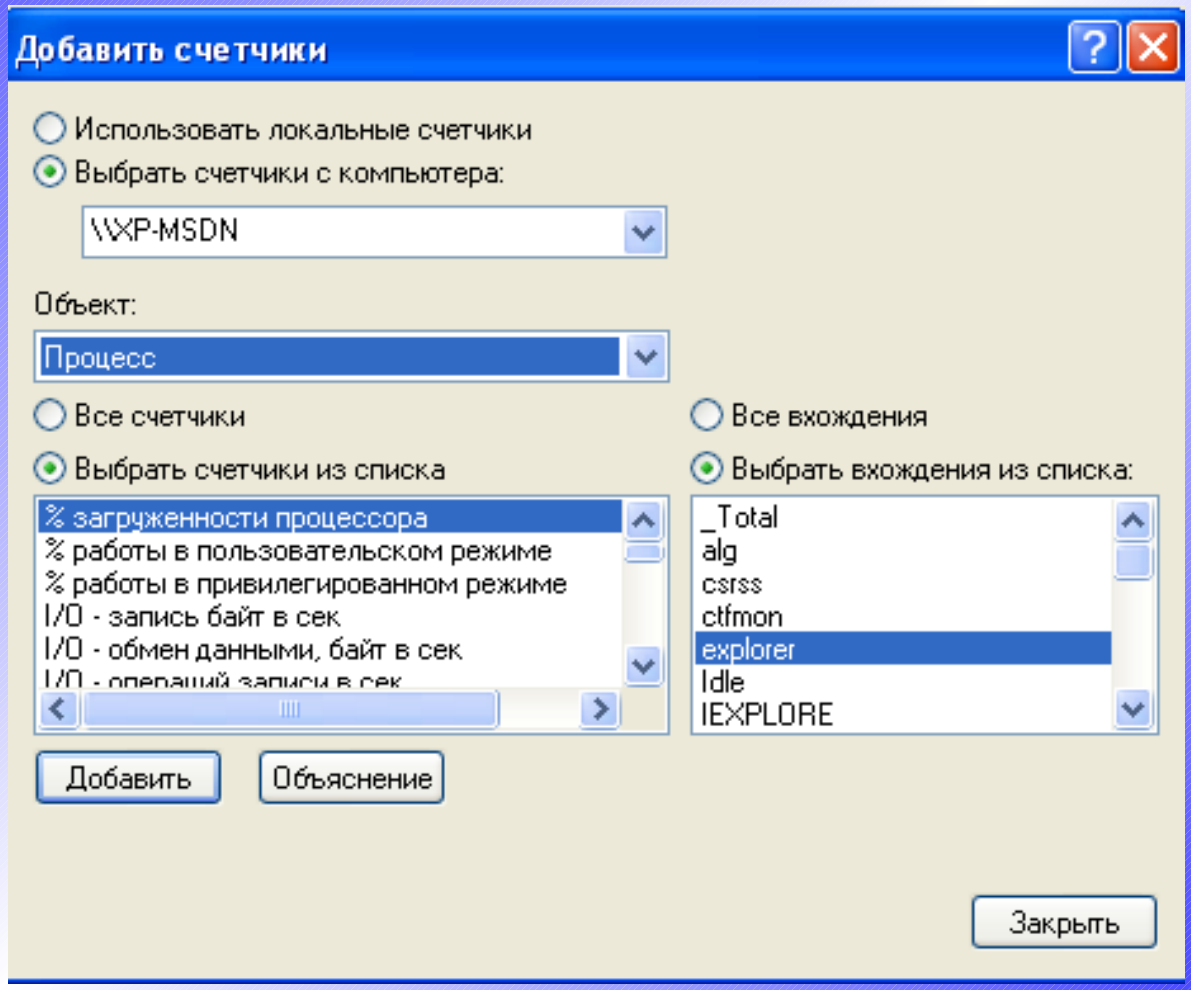
Системный монитор Windows



Принцип сбора информации Системным монитором

- Объект – физический или логический ресурс ОС (физический диск, процессор; логический диск, процесс).
- Экземпляр объекта – один из нескольких объектов одного типа (1-й процессор в многопроцессорной системе, процесс «explorer», логический диск D:\).
- Счётчик производительности – параметр, который может быть измерен; у каждого объекта свой набор счётчиков.

Окно добавления счётчиков



Базовый уровень производительности

- Базовый уровень – измерение производительности в течение обоснованно длительного периода времени, который охватывает различные периоды использования компьютера.
- Необходим для получения данных о нормальной производительности.

Периодический анализ производительности

- Периодический анализ – периодическая проверка производительности и сравнение полученных результатов с базовым уровнем.
- Необходим для выявления компонентов, которым требуется улучшение.
- Для проведения базового и периодического анализа могут использоваться журналы производительности.

Использование оповещений

- Возможно задание порогового значения счётчика, превышение которого вызовет определённое действие (запуск программы или журнала производительности, отправку сообщения администратору).
- Например, увеличение количества расщеплений ввода-вывода при работе с логическим диском может свидетельствовать о сильной фрагментации. В ответ на превышение заданного порога может быть вызвана утилита дефрагментации диска.

Администрирование логических дисков

- Форматирование диска.
- Изменение размера файла подкачки.
- Дефрагментация диска.
- Проверка на наличие неисправных кластеров.
- Очистка диска от ненужных файлов.

Принципы сопровождения системного ПО

- Непрерывность.
- Минимизация используемого прикладного ПО.
- Комплексность.
- Своевременное реагирование.
- Адекватность.
- Непротиворечивость.
- Выполнение организационно-правовых документов.
- Подконтрольность.

Средства настройки ОС семейства Windows NT

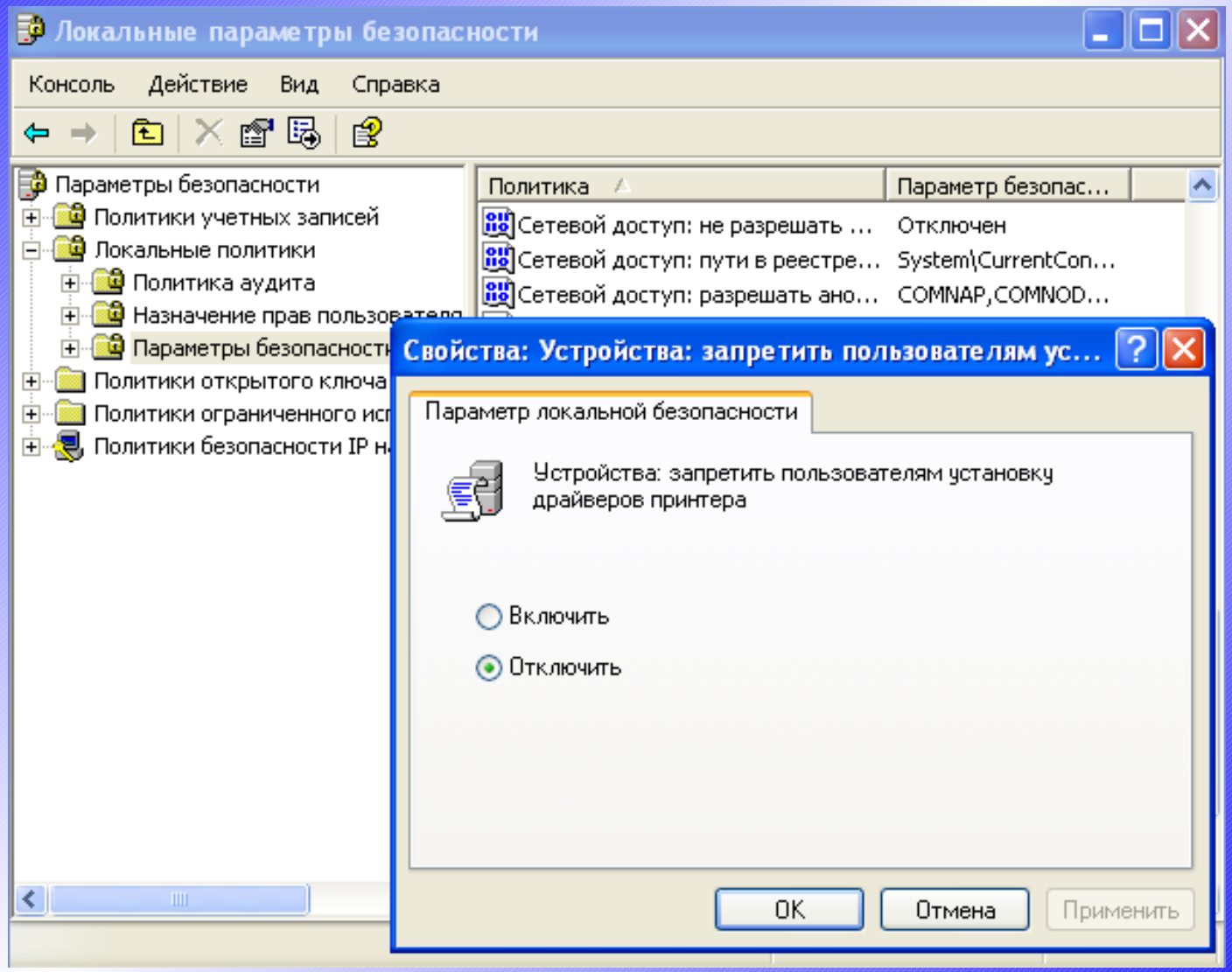
Средства настройки ОС семейства Windows NT

- MMC (Microsoft Management Console) – консоль управления.
- Реестр.

Структура MMC

- Функции администрирования объединены в единую древовидную структуру.
- Функции предоставляются различными оснастками, являющимися подключаемыми модулями с единым интерфейсом.
- В левой части окна содержатся объекты-контейнеры, а в правой – параметры, входящие в контейнере.
- У каждого параметра есть настраиваемые свойства.

Структура MMC



Microsoft Management Console

Примеры оснасток:

- групповая политика (конфигурация компьютера, пользователя);
- журналы и оповещения производительности;
- локальные пользователи и группы;
- общие папки;
- просмотр событий (приложения, безопасность, система);
- службы;
- управление дисками.

Реестр Windows

- Реестр – хранилище общесистемных и пользовательских параметров операционной системы.
- Утилита для редактирования – regedit.exe.

Считывание конфигурационных данных из реестра

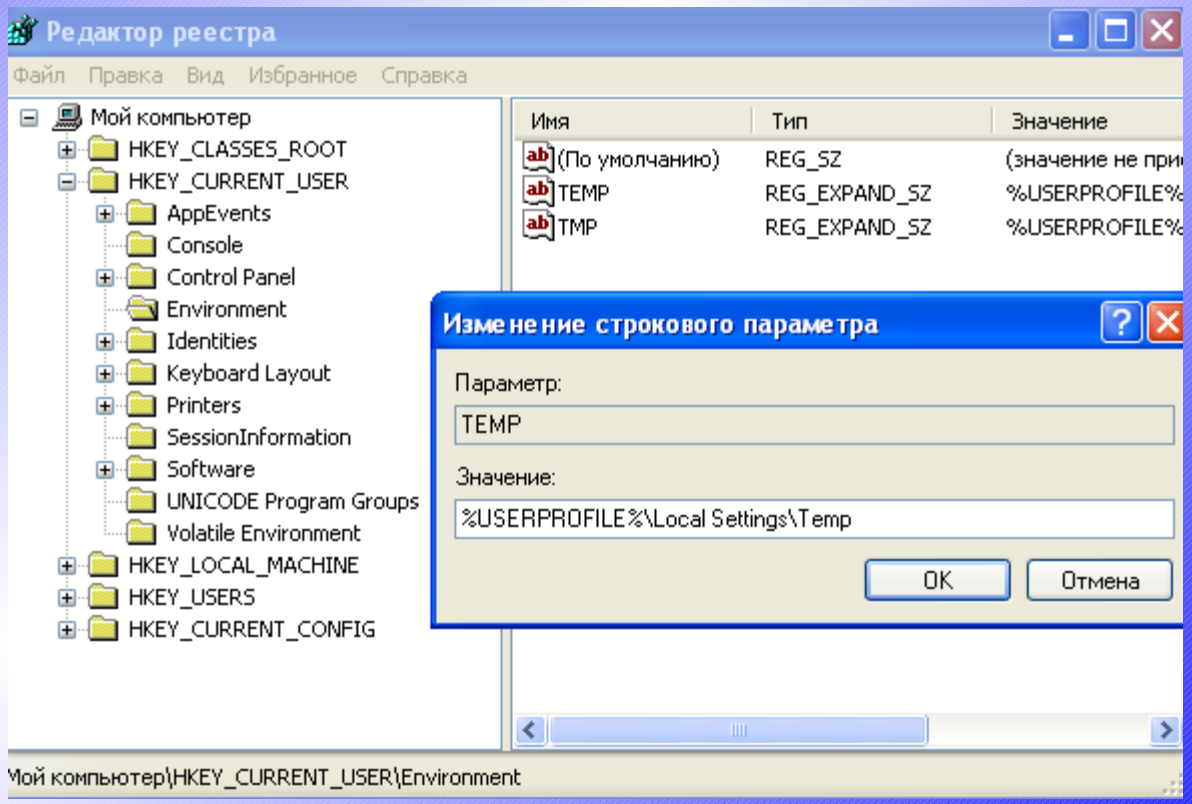
- При загрузке ОС – информацию о драйверах устройств, которые нужно загрузить; параметры для настройки различных подсистем (диспетчера памяти, процессов и др.).
- При входе пользователя – предпочтения пользователя (буквы подключенных сетевых дисков, настройки рабочего стола и др.).
- При запуске приложений – общесистемные параметры, информацию о лицензировании, настройки пользователя.

Модификация реестра

- Исходная структура и настройки по умолчанию определяются его прототипной версией, поставляемой с дистрибутивом ОС.
- Программы установки приложений создают для них настройки по умолчанию и настройки, выбранные пользователем во время установки.
- Подсистема Plug and Play при установке драйвера устройства сохраняет информацию о настройках этого драйвера и способах работы с ним.
- Изменение настроек приложений и системы через пользовательский интерфейс или при помощи reg-файлов.

Структура реестра

- 6 корневых разделов.
- Подразделы.
- Параметры.
- Все разделы и подразделы содержат один параметр «по умолчанию».



Типы данных

- REG_NONE – нетипизированный параметр.
- REG_SZ – Unicode-строка фиксированной длины.
- REG_EXPAND_SZ – Unicode-строка переменной длины.
- REG_LINK – символьная ссылка на другой раздел или параметр реестра в формате Unicode.
- REG_MULTI_SZ – массив Unicode-строк с завершающим нулём.
- REG_RESOURCE_LIST – описание аппаратного ресурса.
- REG_FULL_RESOURCE_DESCRIPTOR – описание аппаратного ресурса.
- REG_RESOURCE_REQUIREMENTS_LIST – список требований к ресурсам.

Типы данных

- REG_BINARY – двоичные данные произвольной длины.
- REG_DWORD – 32-битное число.
- REG_DWORD_LITTLE_ENDIAN – 32-битное число, в котором первый – младший байт; эквивалентно REG_DWORD.
- REG_DWORD_BIG_ENDIAN – 32-битное число, в котором первый – старший байт.
- REG_QWORD – 64-битное число.
- REG_QWORD_LITTLE_ENDIAN – 64-битное число, в котором первый – младший байт; эквивалентно REG_QWORD.
- REG_QWORD_BIG_ENDIAN – 64-битное число, в котором первый – старший байт.

Логическая структура реестра

- HKEY_CURRENT_USER – содержит данные, сопоставленные с пользователем, который локально вошёл в систему на данный момент.
- HKEY_USERS – хранит информацию обо всех учётных записях на компьютере.
- HKEY_CLASSES_ROOT – хранит сопоставления файлов и регистрационную информацию COM-объектов.
- HKEY_LOCAL_MACHINE – содержит информацию, специфичную для системы.
- HKEY_CURRENT_CONFIG – включает некоторые сведения о текущем профиле оборудования.
- HKEY_PERFORMANCE_DATA – хранит сведения о производительности.

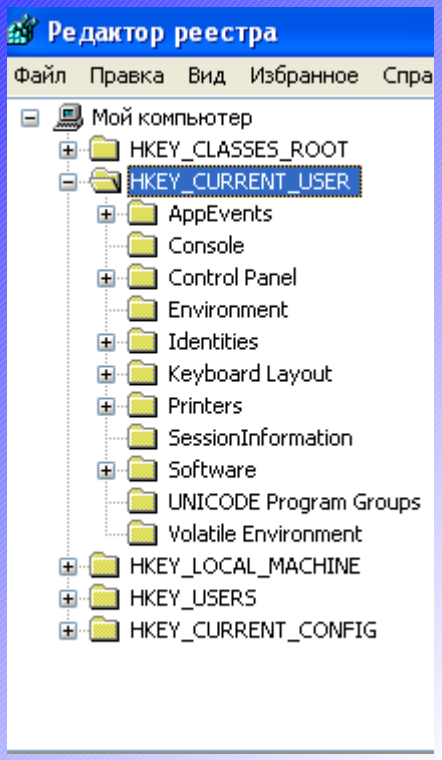
Логическая структура реестра

- HKCU – ссылка на подраздел в HKEY_USERS, соответствующий текущему вошедшему в систему пользователю.
- HKU – не является ссылкой.
- HKCR – ссылка: HKLM\SOFTWARE\Classes.
- HKLM – не является ссылкой.
- HKCC – ссылка: HKLM\SYSTEM\CurrentControlSet\ HardwareProfiles\Current.
- HKPD – не является ссылкой.

Подразделы в HKCU

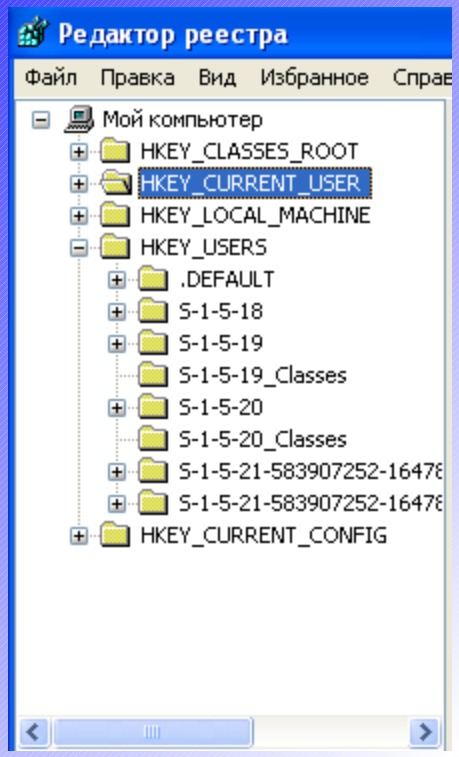
- AppEvents – сопоставление звуковых сигналов с событиями.
- Console – параметры окна командной строки (ширина, высота, цвет и т.д.).
- Control Panel – текущая экранная заставка, оформление рабочего стола, параметры клавиатуры и мыши, настройки специальных возможностей, язык и региональные стандарты.
- Environment – определение переменных окружения.
- Keyboard Layout – раскладки клавиатуры.

Подразделы в HKCU



- Network – имена и параметры подключённых сетевых дисков.
- Printers – параметры подключения принтеров.
- Software – настройки программ, специфичные для пользователя.
- Windows 3.1 Migration Status – данные о состоянии файлов для систем, обновляемых с версии 3.x до 2000и выше.

Подразделы в HKU



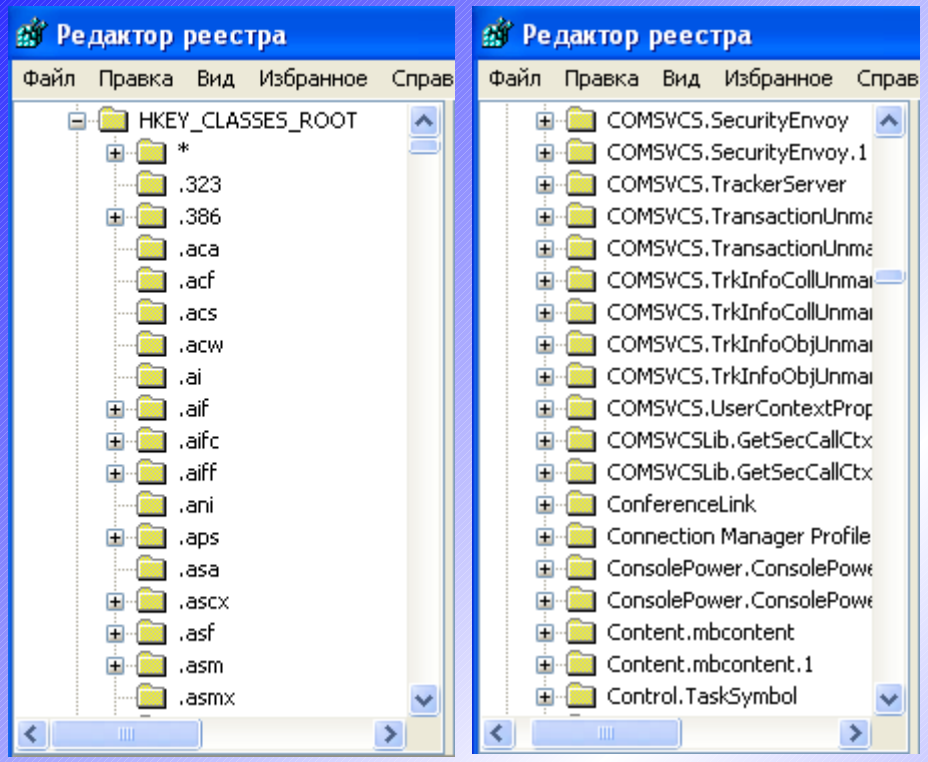
- Подразделы для каждого загруженного профиля пользователя (%SystemDrive %\Documents and Settings\...).
- Регистрационная база данных классов.
- .Default – профиль пользователя по умолчанию ((%SystemDrive%\Documents and Settings\Default User).

Параметры хранения профилей

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList – список всех профилей.
- Информация о каждом профиле хранится в подразделе с именем, отражающим SID учётной записи для данного профиля.
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

  Параметр ProfilesDirectory – каталог для хранения профилей.

Подразделы в HKCR



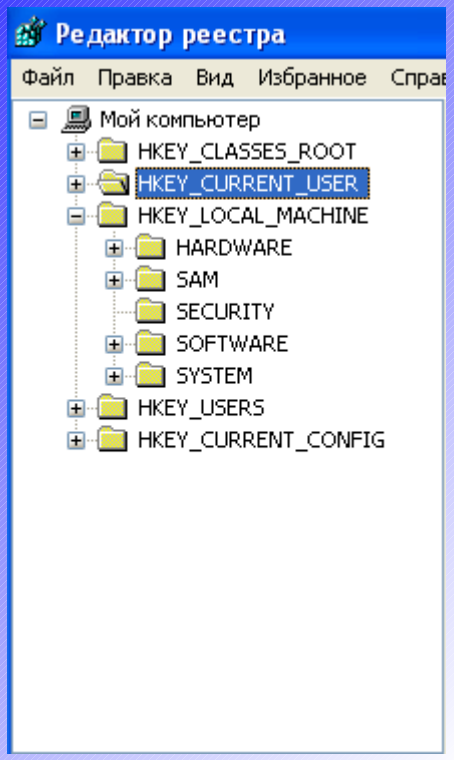
- Сопоставления расширений файлов (подразделы с названиями, соответствующими типам файлов, содержат ссылки на другие разделы с информацией о сопоставлении классов файлов).

- Регистрационные данные COM-классов.

Формирование HKCR

- Специфичные для пользователя регистрационные данные классов (HKCU\Software\Classes).
- Общесистемные регистрационные данные классов (HKLM\SOFTWARE\Classes).

Подразделы в HKLM



- HARDWARE – описание аппаратного обеспечения системы и все сопоставления драйверов с устройствами.
- SAM – информация о локальных учётных записях и группах (пароли, определения групп, сопоставления с доменами); по умолчанию не имеет доступ даже администратор.

Подразделы в HKLM

- SECURITY – данные об общесистемных политиках безопасности, о правах пользователей.
- SOFTWARE – общесистемная конфигурационная информация, не требующаяся при загрузке системы и настройки приложений сторонних разработчиков.
- SYSTEM – общесистемная конфигурационная информация, необходимая при загрузке системы (списки загружаемых драйверов, сервисов, список смонтированных устройств); создаётся копия раздела, называемая последней удачной конфигурацией.

HKPD

- Обратиться напрямую к информации о производительности можно только программно через API-функции реестра типа RegQueryValueEx. Через regedit доступ невозможен – хранится не сама информация, а ссылки на источники этих данных.
- Информация о производительности доступна через API-функции Performance Data Helper.

Физическая структура реестра

- Куст – один из файлов, из которых состоит реестр.
- В кусте содержится дерево реестра со своим разделом, являющимся корнем.
- При загрузке путь к каждому кусту отмечается в HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist.
- Ограничение размера куста SYSTEM – 200 МБ или четверть объёма физической памяти (в Windows 2000 – 12 МБ).

Дисковые файлы

- HKLM\SYSTEM – \WINDOWS\system32\config\System.
- HKLM\SAM – \WINDOWS\system32\config\Sam.
- HKLM\SECURITY – \WINDOWS\system32\config\Security.
- HKLM\SOFTWARE – \WINDOWS\system32\config\Software.
- HKLM\HARDWARE – изменяемый куст.
- HKLM\SYSTEM\Clone – изменяемый куст (только в Windows 2000).
- HKU\<SID_пользователя> – \Documents and Settings\<имя_пользователя>\Ntuser.dat.
- HKU\<SID_пользователя>_Classes – \Documents and Settings\<имя_пользователя>\Local Settings\Application Data\Microsoft\Windows\Usrclass.dat.
- HKU\.DEFAULT – \WINDOWS\system32\config\Default.

Недостатки реестра

- Реестр подвержен фрагментации, из-за чего доступ к нему постепенно замедляется
- Размер реестра значительно увеличивается по мере использования операционной системы из-за хранения различной информации системы и приложений (например, список недавно открытых файлов).
- Невозможен перенос настроек системы путём копирования реестра, т.к. в нём хранятся не все настройки системы.

Рассмотренные вопросы

- Задачи и принципы сопровождения системного ПО.
- Механизмы управления и конфигурирования Windows.
- Структура MMC.
- Логическая и физическая структура реестра.
- Назначение разделов реестра.

Всем спасибо – все свободны,

если нет вопросов