

**Криминалистический  
анализ реестра  
операционной системы  
Windows**

# РЕЕСТР ОС Windows

**Реестр – это компонент операционной системы компьютера, который в иерархической базе данных хранит важнейшие установки и информацию о приложениях, системных операциях и пользовательской конфигурации.**

- Регистрационная база данных (Registration Database) Windows, в первую очередь является базой данных параметров операционной системы, приложений и драйверов оборудования. Реестр содержит огромный объем информации, начиная с параметров учетных записей пользователя и заканчивая цветами рабочего стола.

- До создания Реестра Microsoft использовала обычные текстовые файлы для управления системой. В MS-DOS конфигурация системы контролировалась двумя следующими файлами:
- **Config.sys** содержал конфигурационную информацию, необходимую для функционирования MS-DOS. В основном, это были общие параметры оборудования, используемого различными приложениями, например работа верхней и нижней памяти.
- **Autoexec.bat** был пакетным файлом, служившим для выполнения процедур автозагрузки.

## Реестр выполняет следующие основные функции:

- Отслеживает все системные устройства и их установки, включая такие ресурсы, как запросы на прерывания (IRQ) и номера каналов прямого доступа памяти (DMA).
- Работает как база данных, которая унифицирует функционирование приложений.
- Проверяет наличие необходимых драйверов для устанавливаемого оборудования. При добавлении нового периферийного устройства *Диспетчер конфигурации (Configuration manager)* операционной системы помещает конфигурационные данные устройства в реестр.
- Предоставляет системные сервисы, которые необходимы для работы многих приложений.
- Обеспечивает запуск необходимого приложения при щелчке мышью.
- Сохраняет информацию относящуюся к системным правилам, профилям пользователей и средствам администрирования.

Приложения MS-DOS самостоятельно регулировали все свои параметры и совместное с другими приложениями использование таких устройств, как принтер и звуковая карта.

Параметры хранились в текстовых файлах, называемых файлами инициализации (.INI).

- **Program.ini** - содержал параметры Менеджера программ Windows (Windows Program Manager), обеспечивающего графический интерфейс пользователя (graphical user interface - GUI), для работы в Windows.
- **Control.ini** - содержал множество пользовательских настроек Windows, включая параметры рабочего стола, звука и принтера.
- **Win.ini** -этот файл содержал информацию о визуальном оформлении Windows и параметры установленных приложений.
- **System.ini** - содержал параметры конфигурации оборудования и определял, как Windows будет с ним взаимодействовать.

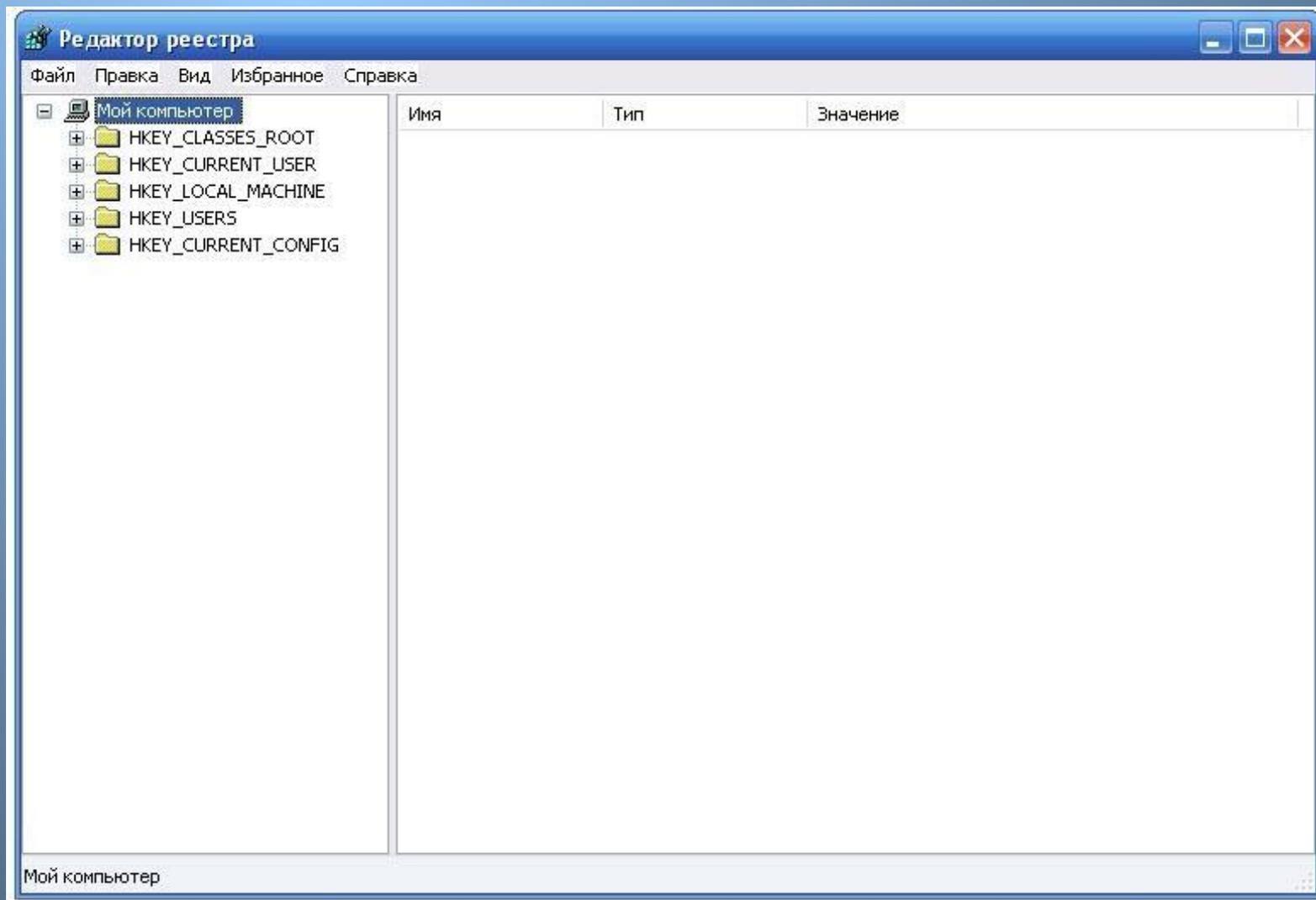
- С появлением Windows NT на свет появился новый Реестр. 64 кб ограничение было снято, и теперь Реестр мог занимать столько места, сколько ему было необходимо.
- Один файл был заменен несколькими, но при этом сохранилась единая иерархическая структура, объединяющая вместе все записи.
- С момента появления Windows NT Реестр практически не изменился.

# РЕЕСТР ОС Windows

**Реестр Windows 2000, XP, 7, 8 хранится в следующих файлах:**

- DEFAULT,
- SAM, (находятся по адресу
- SECURITY, C:\WINDOWS
- SOFTWARE, \System32\Config)
- SYSTEM
- NTUSER.DAT (по адресу C:\Documents and Settings\[Профиль пользователя])

# Ключи реестра



# HKKEY\_CLASSES\_ROOT

- В основном, HKKEY\_CLASSES\_ROOT (HKCR) обеспечивает совместимость с 16-разрядными приложениями Windows. HKCR содержит информацию об ассоциациях файлов - т.е. какие приложения открывают определенные типы файлов. Более важным для многих людей является то, что HKCR содержит определения всех объектов среды Windows XP. Ключи, контролирующие эти определения, контролируют информацию о внешнем интерфейсе объекта, как, например, команды, доступные в контекстном меню данного объекта.
- 32-битные приложения обращаются к этим данным через их копию в подкюче Software\Classes подкаталога HKKEY\_LOCAL\_MACHINE. На самом деле - это не совсем копии, а просто информация, хранящаяся в одном кусте, но рассматриваемая как бы с двух разных точек. Если изменить параметр в одном месте, то он изменится и в другом.
  - **В HKCR преобладают два следующих типа ключей:**
- **Ключи расширений** файлов названы так же, как и представляемые ими расширения (.doc, .txt и так далее). Параметры этих ключей определяют, какие приложения открывают файлы с соответствующим расширением. Эти ключи могут содержать и подключи, контролирующие дополнительные функции, такие как список программ меню Открыть с помощью (Open With).
- **Ключи определения класса** содержат информацию об объектах, соответствующих Общей модели объектов (Component Object Model - COM) - модели, позволяющей программистам разрабатывать объекты, доступные всем COM - совместимым приложениям. Технологии Внедрения и связывания объектов (Object Linking and Embedding - OLE) и ActiveX основаны на COM.

# HKEY\_USERS

Содержит информацию, определяемую пользователем (например, пользовательские настройки *рабочего стола*): установки по умолчанию (HKEY\_USERS\DEFAULT) для рабочего стола, меню Пуск (Start), приложений и т. д.

Когда новый пользователь входит в систему, установки по умолчанию копируются в отдельный подраздел, название которого совпадает с именем пользователя. Все изменения, которые пользователь в дальнейшем произведёт с этими установками сохраняются в этом подразделе.

# HKEY\_CURRENT\_USER

- Пользовательские настройки из HKEY\_USERS вступают в силу в процессе входа пользователя в систему. При этом содержимое подраздела HKEY\_USERS\name, где name - имя текущего пользователя, или подраздела HKEY\_USERS\.DEFAULT копируется в раздел HKEY\_CURRENT\_USER.

Раздел HKEY\_CURRENT\_USER содержит несколько подразделов:

- **AppEvents** - содержит пути звуковых файлов, используемых для озвучивания системных событий.
- **Control Panel** - содержит различные данные, которые могут быть изменены в панели управления.
- **Display** - содержит пользовательские установки экрана для текущего пользователя (этот подраздел доступен, только если разрешены *пользовательские профили (user profiles)*).
- **InstallLocationsMRU** - содержит пути, использованные в процессе последней инсталляции.
- **keyboard layout** - содержит информацию о раскладке клавиатуры. Текущая раскладка клавиатуры устанавливается с использованием пункта **Клавиатура (Keyboard)** панели управления.
- **Network** - содержит подразделы, описывающие постоянные и недавно установленные сетевые соединения, а также состояние сети.
- **RemoteAccess** - необязательный подраздел, доступный только в случае, если установлен сервис *удалённого доступа*.
- **SOFTWARE** - содержит пользовательские настройки приложений. Этот раздел ссылается на раздел HKEY\_LOCAL\_MACHINE, в которой также хранятся настройки приложений.

# HKKEY\_LOCAL\_MACHINE

Этот раздел определяет всю информацию, относящуюся к локальному компьютеру, такую как драйверы, установленное программное обеспечение, наименование портов и конфигураций программного обеспечения. Эта информация верна для всех пользователей, подключённых к системе.

## Состоит из нескольких подразделов:

- **Config** - хранит конфигурацию компьютера. Содержимое данного подраздела обновляется в процессе установки и запуска Windows.
- **Enum** - Windows использует так называемую шинную нумерацию (bus enumeration) для учёта всех установленных компонента оборудования. Данные для этих компонентов хранятся в этом подразделе и используются для построения "дерева оборудования" на вкладке **Устройства (Devices)** диалога **Система(System)**, вызываемого из панели управления.

# HKKEY\_LOCAL\_MACHINE

- **Hardware** - содержит установки для последовательных портов доступных на локальном компьютере. Подраздел Description содержит записи для устройств в системе.
- **Network** - когда Windows работает в сети, этот подраздел содержит регистрационную информацию пользователя (т. е. имя пользователя, сетевого провайдера, подтверждения регистрации и т.д.)
- **Security** - доступен для сетевых машин и содержит информацию о провайдере безопасности.
- **Software** - вся информация о программах, установленных на компьютере. Подраздел \Classes этого раздела используется для построения раздела HKKEY\_CLASSES\_ROOT.
- **System** - содержит всю необходимую информацию для запуска Windows. Здесь содержится подраздел CurrentControlSet, в котором содержатся подразделы Control и Servicer. Подраздел Control содержит такую информацию, как имя компьютера, параметры файловой системы и т.д.

# HKEY\_CURRENT\_CONFIG

- Этот ключ отвечает за устройство Plug&Play и содержит информацию о текущей конфигурации компьютера с переменным составом аппаратных средств. Установки этого раздела, соответствуют конфигурационным установкам, хранящимся в разделе HKEY\_LOCAL\_MACHINE\Config

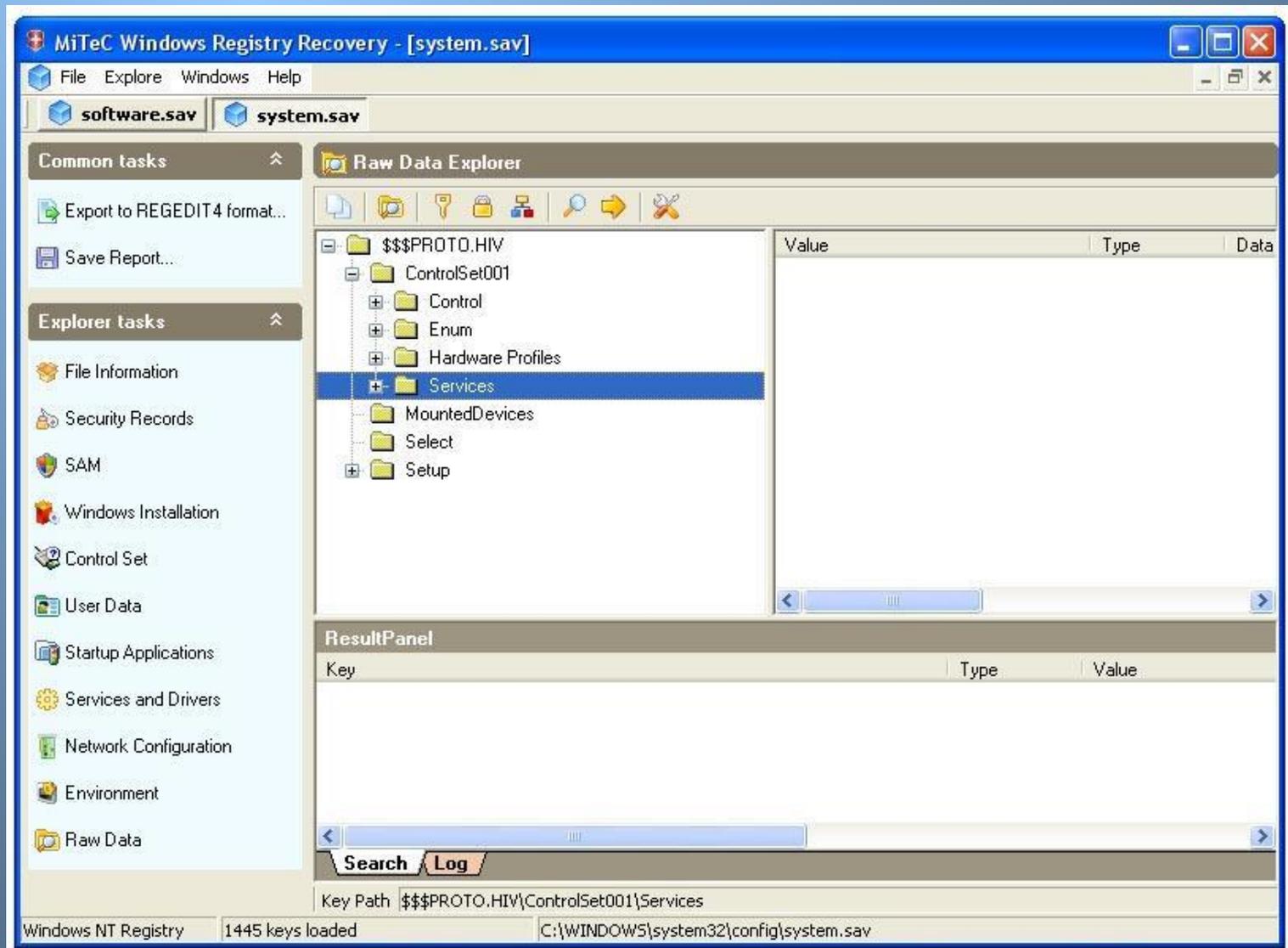
- **Hardware** - соответствует подключу HKLM\Hardware. Данный параметр не имеет своего значения, так как информация об оборудовании не хранится на диске.
- **SAM**-соответствует подключу HKLM\SAM.
- **Security** - соответствует подключу HKLM\SECURITY.
- **Software** - соответствует подключу HKLM\Software.
- **System** - соответствует подключу HKLM\System.
- **Default** - соответствует подключу HKU\Default.

Таблица 1 Ключи Реестра и файлы хранения.	
Куст реестра	Файлы
HKEY_LOCAL_MACHINE\SYSTEM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\SYSTEM\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\SYSTEM\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\SYSTEM\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

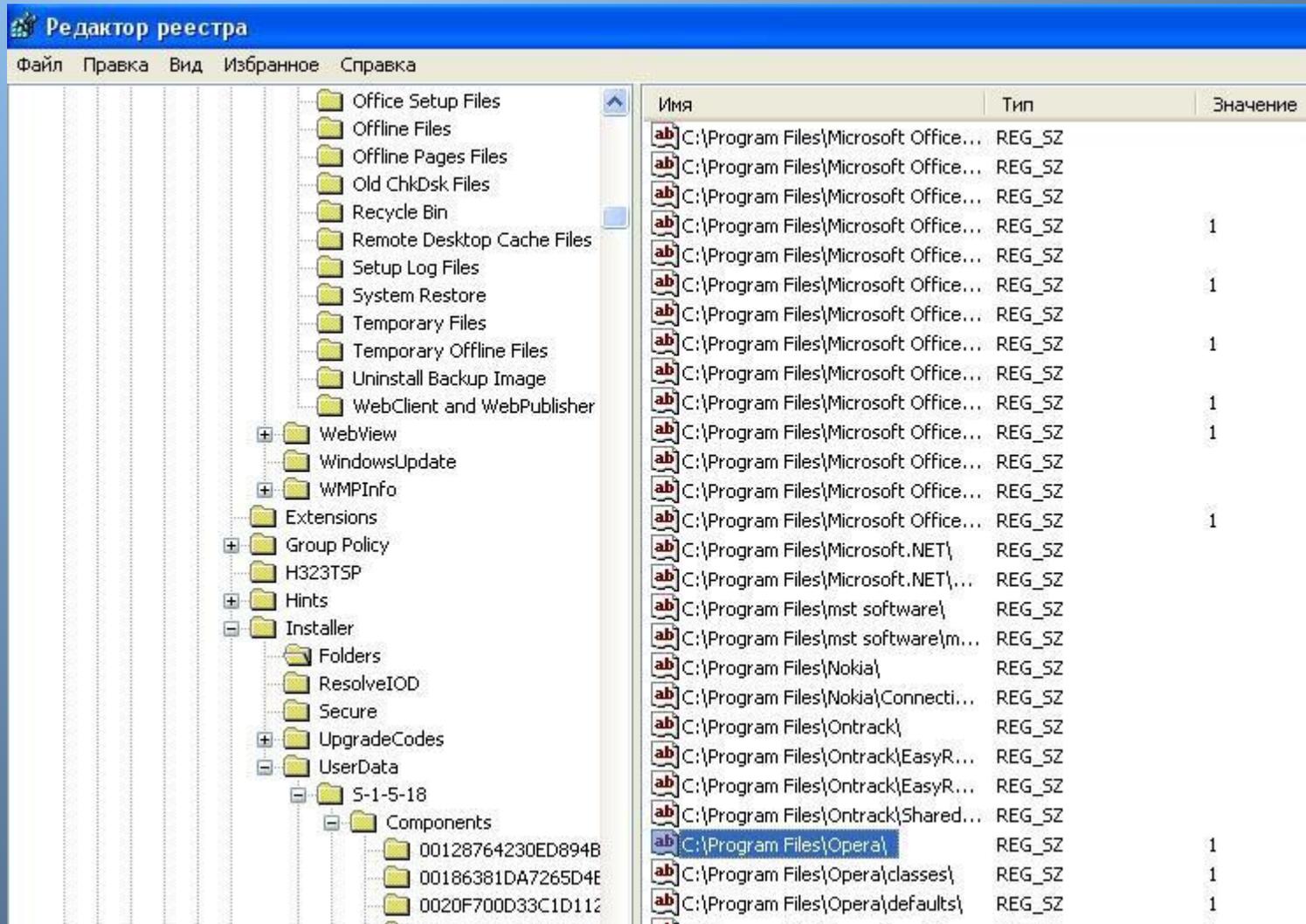
# Работа с реестром

- при обычной работе  
программа **REGEDIT**
- при исследовании отдельного накопителя  
программа **MiTEC Windows  
Registry Recovery**

# MiTEC Windows Registry Recovery



- данные реестра



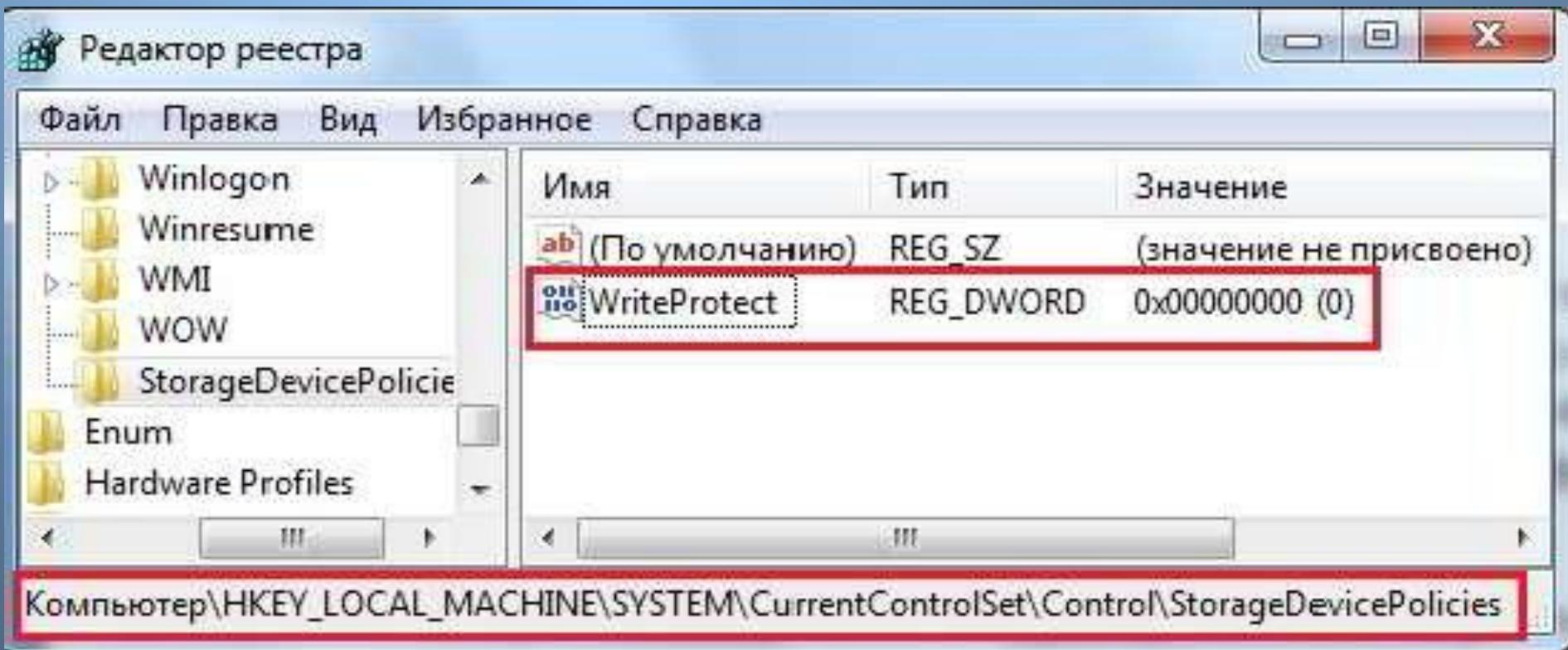
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders

# Изменения в реестре

Монитор реестра (RegMon)

# Криминалистически значимые области реестра

## 1. Блокировка/разблокировка записи через порты USB



Если раздела **StorageDevicePolicies** в разделе **Control** нет, то его необходимо создать.

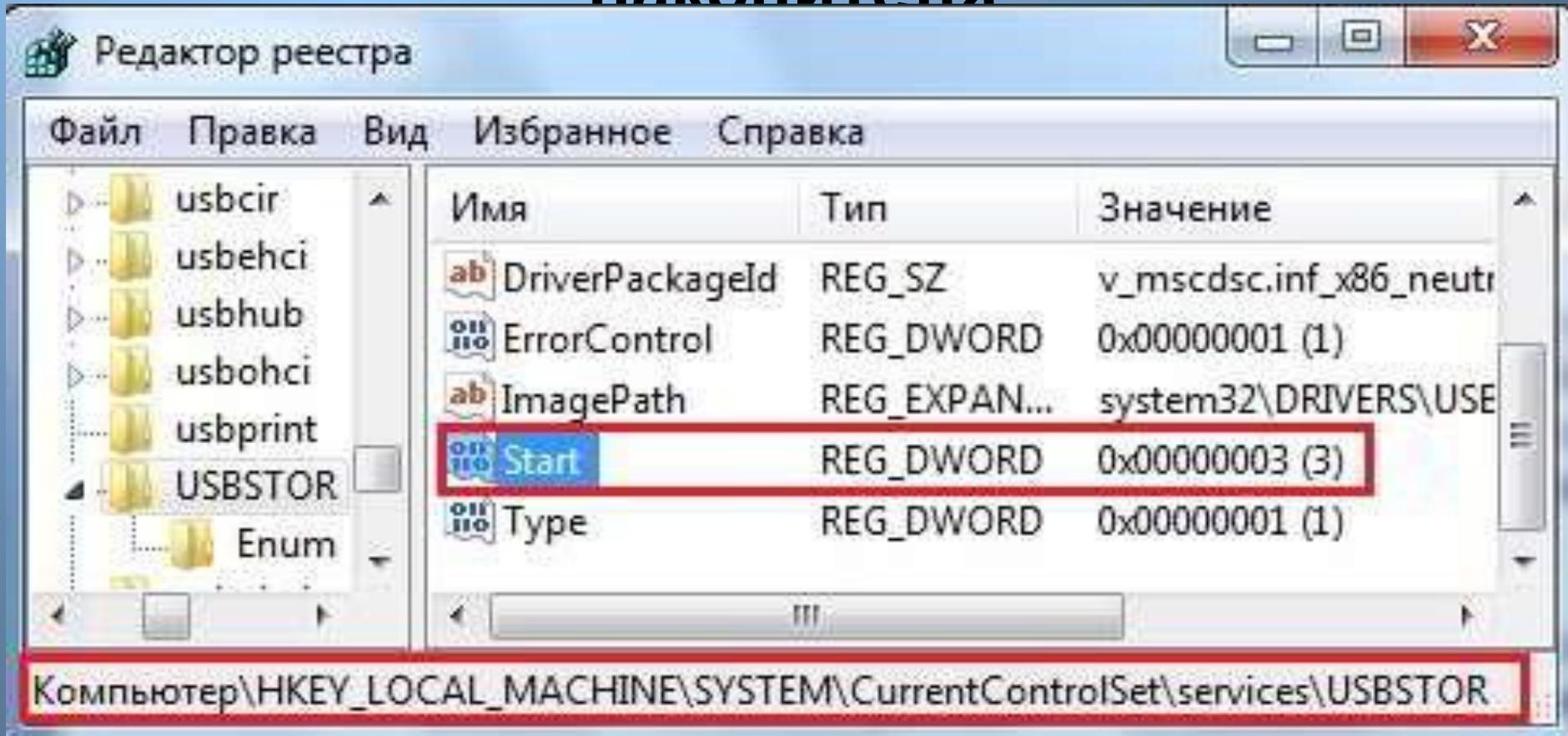
Далее создаём параметр **WriteProtect**, тип **dword**

При значении параметра **WriteProtect** :

1 - режим чтения (readonly)

0 - режим записи

## 2. Запрет на использование USB накопителя

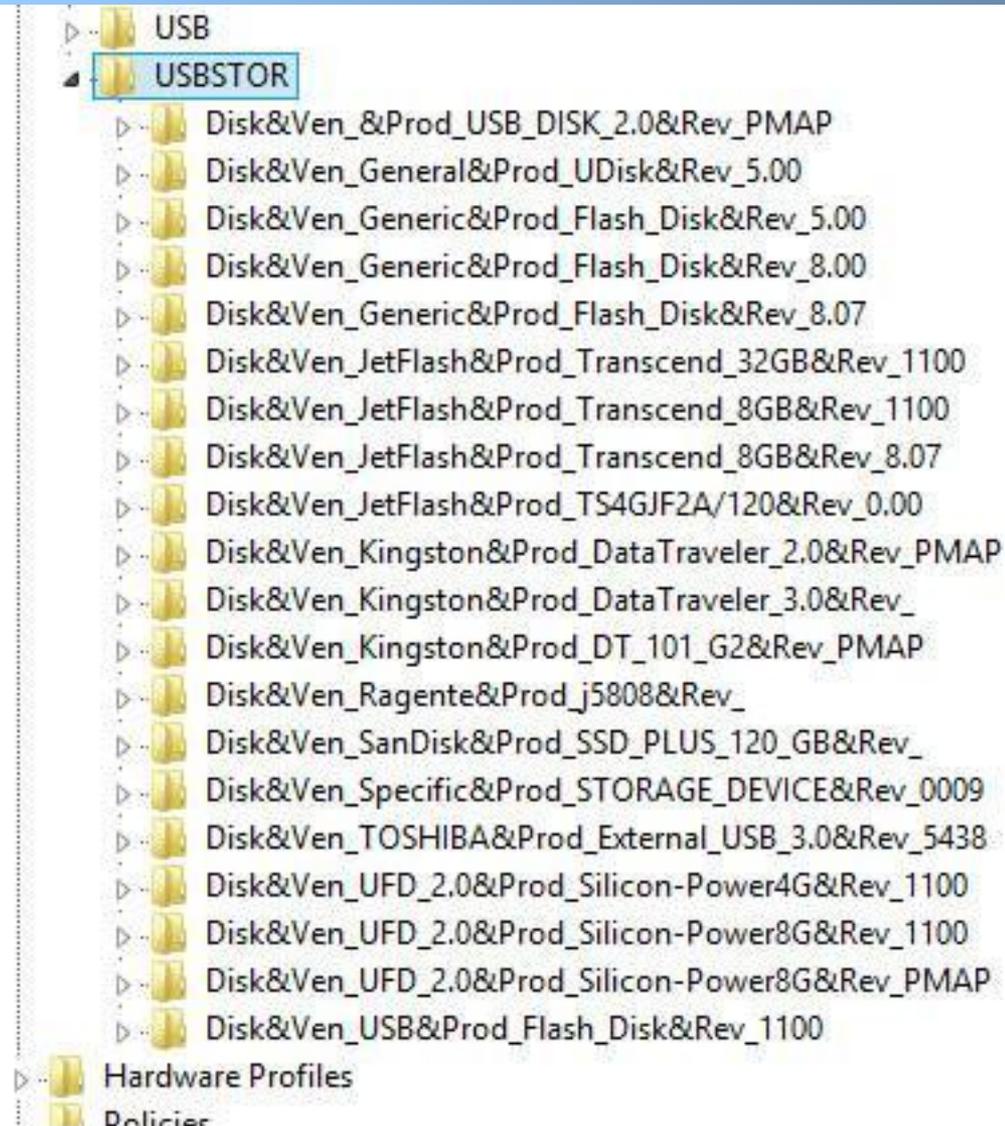


При значении параметра **Start** :

4 - блокировка USB накопителя

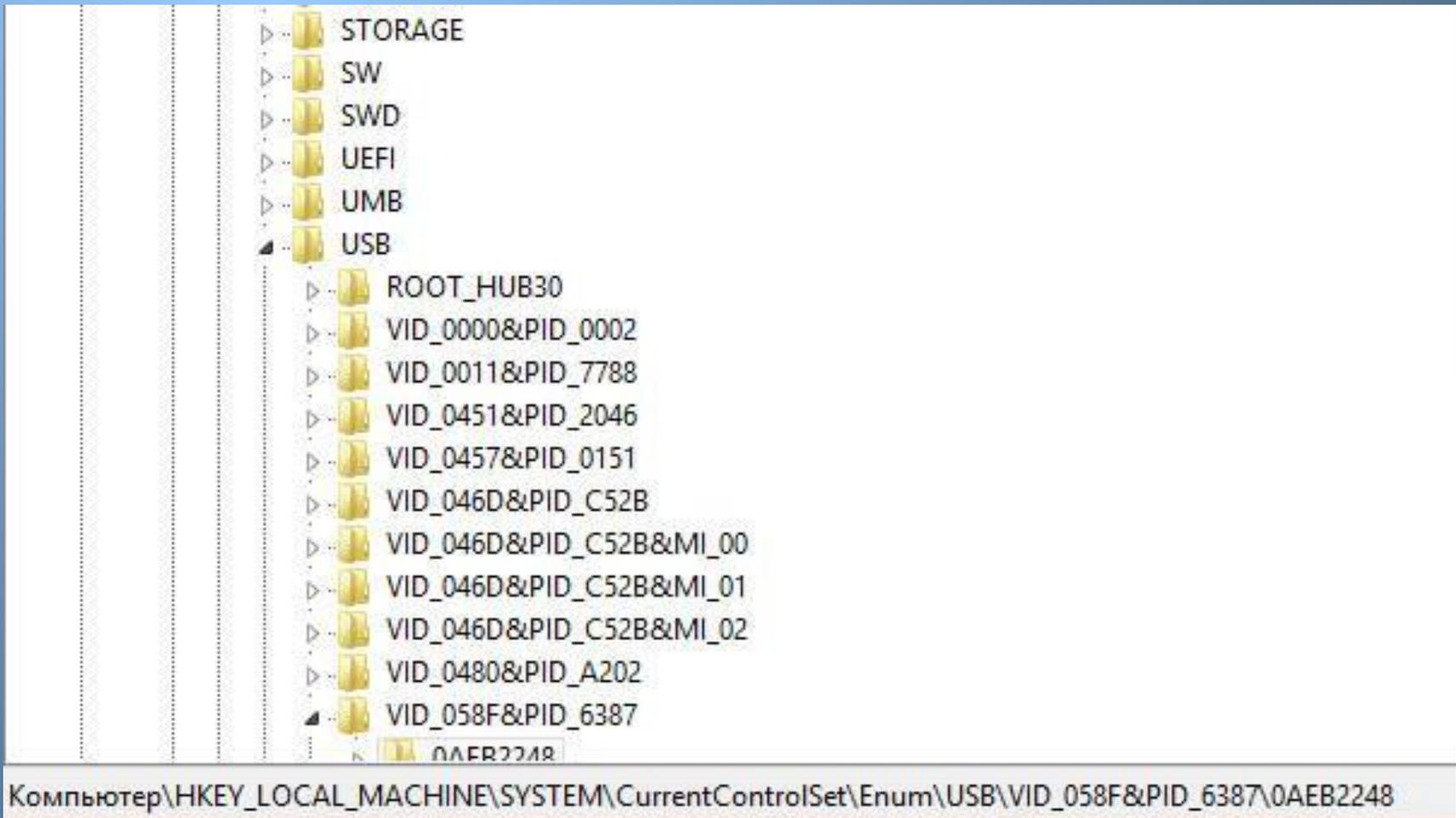
3 - стандартный режим (без блокировок)

### 3. Подключенные через USB накопители



Компьютер\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

# 4. Устройства USB



**Сведения об устройстве по VID и PID на сайтах:**

- [flashboot.ru](http://flashboot.ru)
- [driverslab.ru](http://driverslab.ru)

# driverslab.ru

Поиск устройства USB\VID\_058F&PID\_6387

Поиск по ID Добавить в закладки!

Введите имя устройства, например, GeForce GTX 1060 , usb 3.0  
или ID оборудования, например, PCI\VEN\_10EC&DEV\_8168&SUBSYS\_99EB1019

Вы искали драйвер для : **USB\VID\_058F&PID\_6387**

Выберите драйвер для своей операционной системы и ее разрядности. Рекомендуется устанавливать более позднюю версию драйвера (смотрите на дату выхода).  
Для перехода к скачиванию файла нажмите на ссылку.

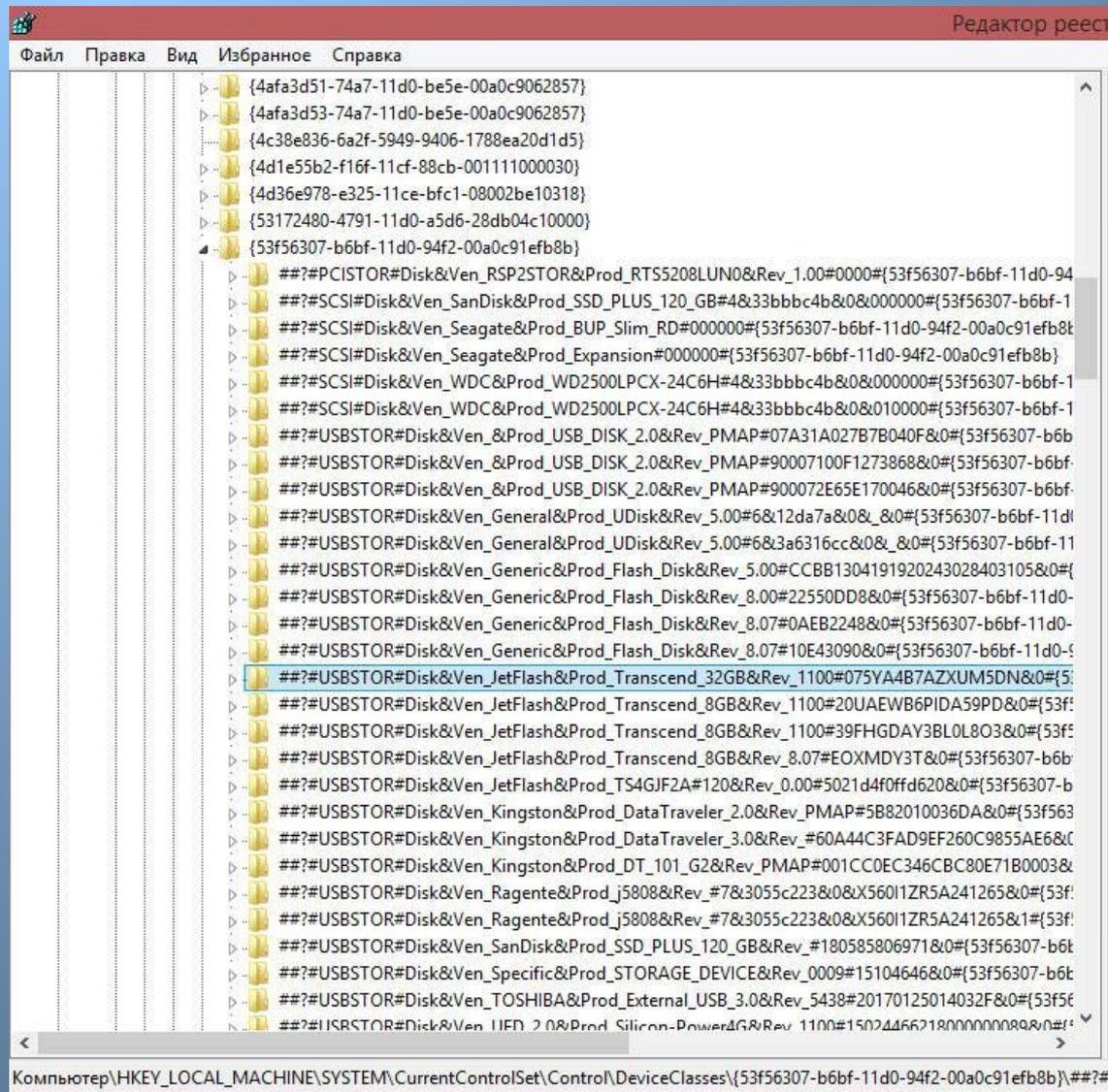
Результаты поиска:

VID	PID	Производитель	Устройство	Драйвер
058f	6387	Alcor Micro Corp.	Flash Drive USB\VID_058f&PID_6387	

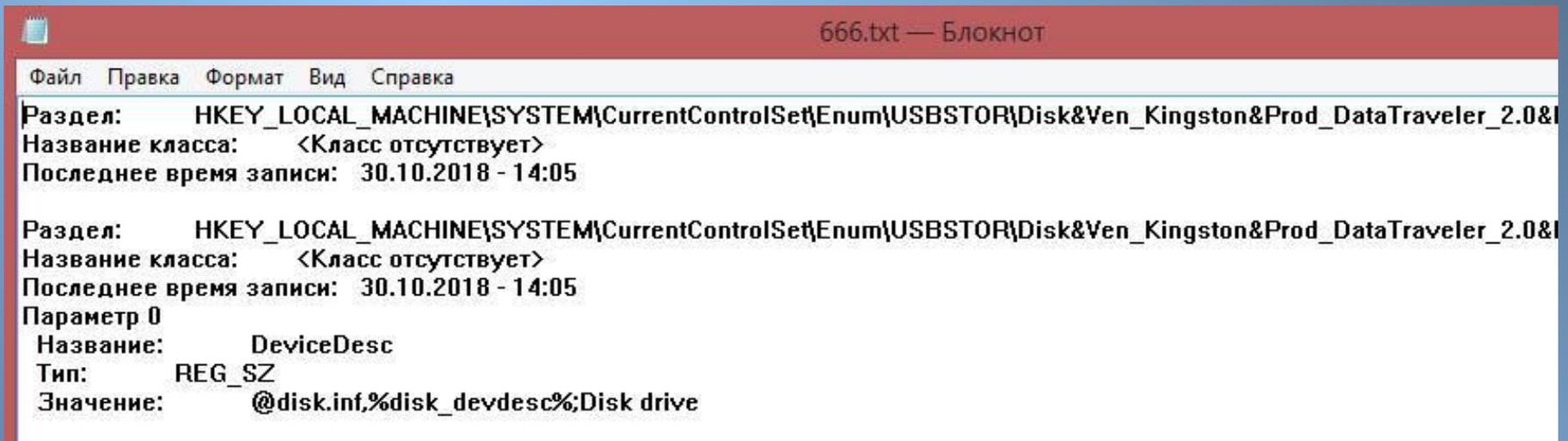
# 5. Временные метки

- Все ключи реестра содержат временную метку (timestamp, last write value), аналогично дате последнего изменения для файлов.
- Это значение хранится в структуре FILETIME и показывает дату и время того, когда ключ реестра был изменен. Это значение обновляется, когда ключ был создан, изменен или удален. Временная метка есть только у ключей реестра, значения реестра такого поля не содержат.

# Обнаружение метки



# Экспорт



666.txt — Блокнот

Файл Правка Формат Вид Справка

Раздел: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven\_Kingston&Prod\_DataTraveler\_2.0&I  
Название класса: <Класс отсутствует>  
Последнее время записи: 30.10.2018 - 14:05

Раздел: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven\_Kingston&Prod\_DataTraveler\_2.0&I  
Название класса: <Класс отсутствует>  
Последнее время записи: 30.10.2018 - 14:05

Параметр 0

Название: DeviceDesc  
Тип: REG\_SZ  
Значение: @disk.inf,%disk\_devdesc%;Disk drive

Экспортируем ключ реестра  
в файл формата \*.txt

## 6. Иные сведения

Параметр	Путь к ключу	Название ключа
Имя компьютера	\ControlSet00X\Control\ComputerName\ComputerName	LENOVO-PC
Время последнего выключения компьютера	\ControlSet00X\Control\Windows	ShutdownTime
Сетевые шары	\ControlSet00X\Services\LanmanServer\Shares	
Сетевые адаптеры, и их параметры	\ControlSet00X\Services\Tcpip\Parameters\Interfaces	
Разрешение входящих подключений по протоколу RDP	\ControlSet00X\Control\Terminal Server	

## Раздел реестра HKEY\_LOCAL\_MACHINE\SYSTEM

### Настройки времени (текущий часовой пояс)

\ControlSet00X\Control\TimeZoneInformation

The screenshot shows the Windows Date and Time Properties dialog box with the Time Zone tab selected. The current time zone is set to (GMT-08:00) Pacific Time (US & Canada). A world map is displayed on the left, and the checkbox for "Automatically adjust clock for daylight saving changes" is checked. The Time Zone Information registry view is shown on the right, listing various registry values for the selected time zone.

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0x000001e0 (480)
Bias	REG_DWORD	0x000001e0 (480)
DaylightBias	REG_DWORD	0xfffffc4 (4294967236)
DaylightName	REG_SZ	Pacific Daylight Time
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	Pacific Standard Time

**Edit String**

Value name:  
StandardName

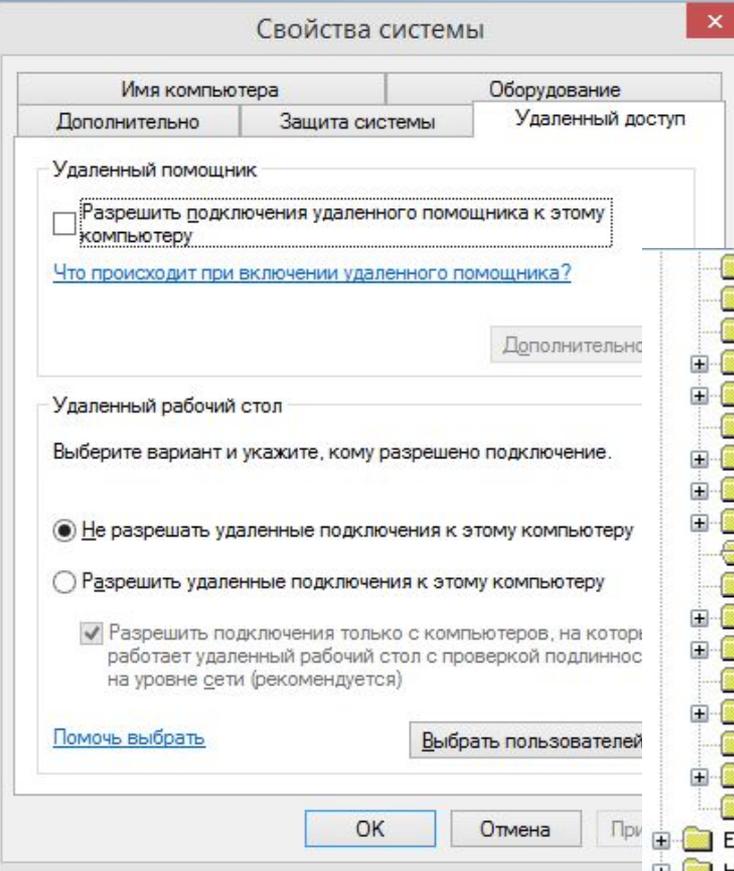
Value data:  
Pacific Standard Time

OK Cancel

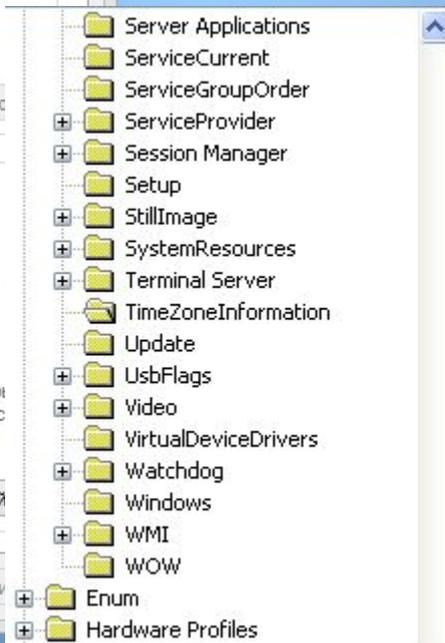
## Раздел реестра HKEY\_LOCAL\_MACHINE\SYSTEM

### Запрет на входящие подключения по протоколу RDP

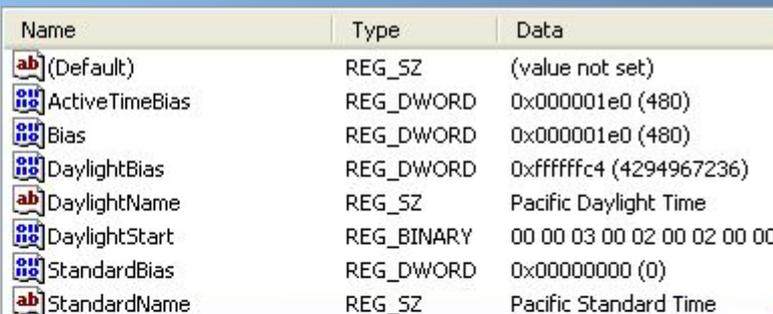
`\ControlSet00X\Control\Terminal Server`



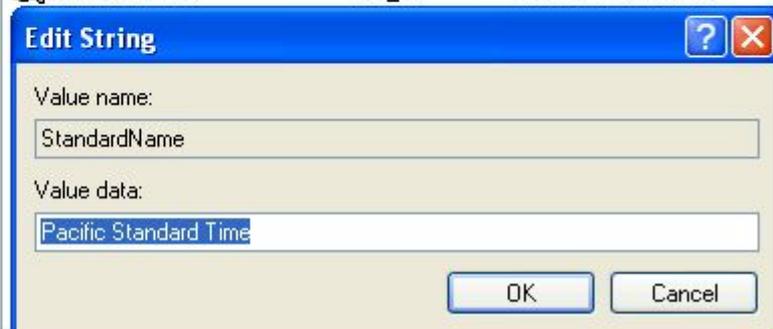
The screenshot shows the 'Свойства системы' (System Properties) dialog box. The 'Удаленный доступ' (Remote) tab is active. Under 'Удаленный помощник' (Remote Assistance), the checkbox 'Разрешить подключения удаленного помощника к этому компьютеру' (Allow remote assistance connections to this computer) is unchecked. Under 'Удаленный рабочий стол' (Remote Desktop), the radio button 'Не разрешать удаленные подключения к этому компьютеру' (Do not allow remote connections to this computer) is selected.



The Registry Editor shows the path `ControlSet00X\Control\Terminal Server` expanded in the left pane.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0x000001e0 (480)
Bias	REG_DWORD	0x000001e0 (480)
DaylightBias	REG_DWORD	0xfffffc4 (4294967236)
DaylightName	REG_SZ	Pacific Daylight Time
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	Pacific Standard Time

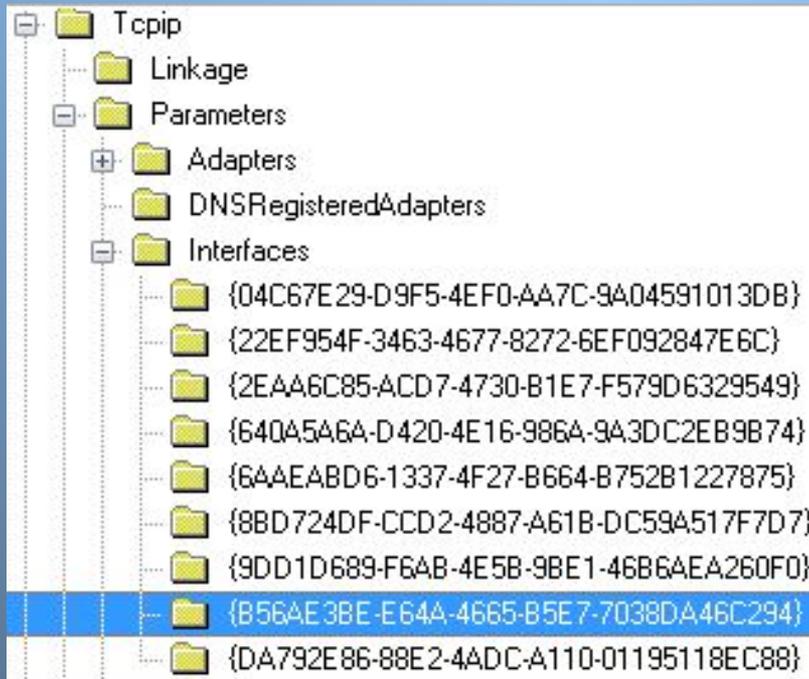


The 'Edit String' dialog box shows the 'Value name' field containing 'StandardName' and the 'Value data' field containing 'Pacific Standard Time'.

# Раздел реестра HKEY\_LOCAL\_MACHINE\SYSTEM

## Сетевые настройки

\ControlSet00X\Services\Tcpip\Parameters\Interfaces



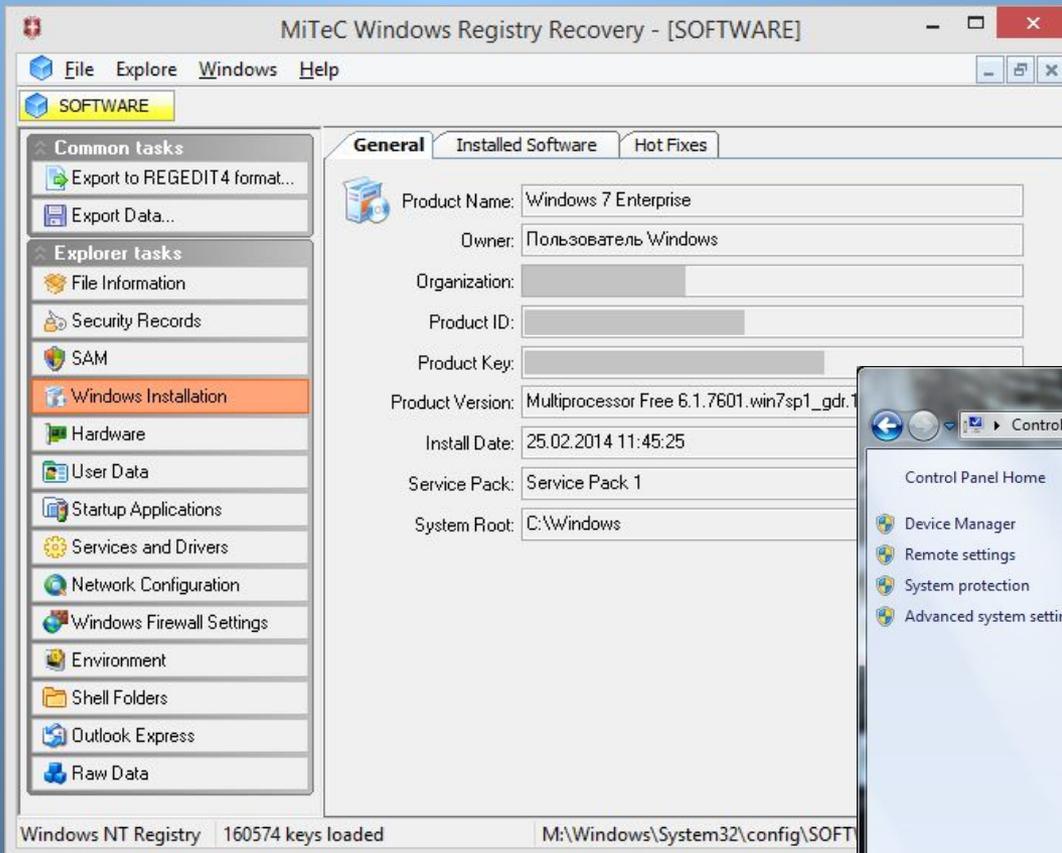
Value	Type	Data
DhcpDefaultGateway	REG_MULTI_SZ	101.24.10.24
DhcpDomain	REG_SZ	<u>netbynet.ru</u>
DhcpIPAddress	REG_SZ	101.24.38.34
DhcpNameServer	REG_SZ	212.1.224.34
DhcpServer	REG_SZ	10.39.16.111
DhcpSubnetMask	REG_SZ	255.255.192.0
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.192.0
Domain	REG_SZ	
EnableDeadGwDetect	REG_DWORD	0x00000001
EnableDHCP	REG_DWORD	0x00000001
IPAddress	REG_MULTI_SZ	0.0.0.0
IPAutoconfigurationAddress	REG_SZ	0.0.0.0
IPAutoconfigurationMask	REG_SZ	255.255.0.0
IPAutoconfigurationSeed	REG_DWORD	0x00000000
NameServer	REG_SZ	
NTEContextList	REG_MULTI_SZ	0x00000002
RawIPAllowedProtocols	REG_MULTI_SZ	0
RegisterAdapterName	REG_DWORD	0x00000000
RegistrationEnabled	REG_DWORD	0x00000001
SubnetMask	REG_MULTI_SZ	0.0.0.0

## Раздел HKEY\_LOCAL\_MACHINE\SOFTWARE

Полный путь к ключу	Название ключа
<b>Сведения об установленном ПО</b>	
\Microsoft\Windows NT\CurrentVersion\Uninstall	-
<b>Сведения об установленной ОС</b>	
\Microsoft\Windows NT\CurrentVersion	

# Сведения об установленной ОС

## \\Microsoft\Windows NT\CurrentVersion



MiTeC Windows Registry Recovery - [SOFTWARE]

File Explore Windows Help

SOFTWARE

Common tasks

- Export to REGEDIT4 format...
- Export Data...

Explorer tasks

- File Information
- Security Records
- SAM
- Windows Installation
- Hardware
- User Data
- Startup Applications
- Services and Drivers
- Network Configuration
- Windows Firewall Settings
- Environment
- Shell Folders
- Outlook Express
- Raw Data

General

Product Name: Windows 7 Enterprise

Owner: Пользователь Windows

Organization: [REDACTED]

Product ID: [REDACTED]

Product Key: [REDACTED]

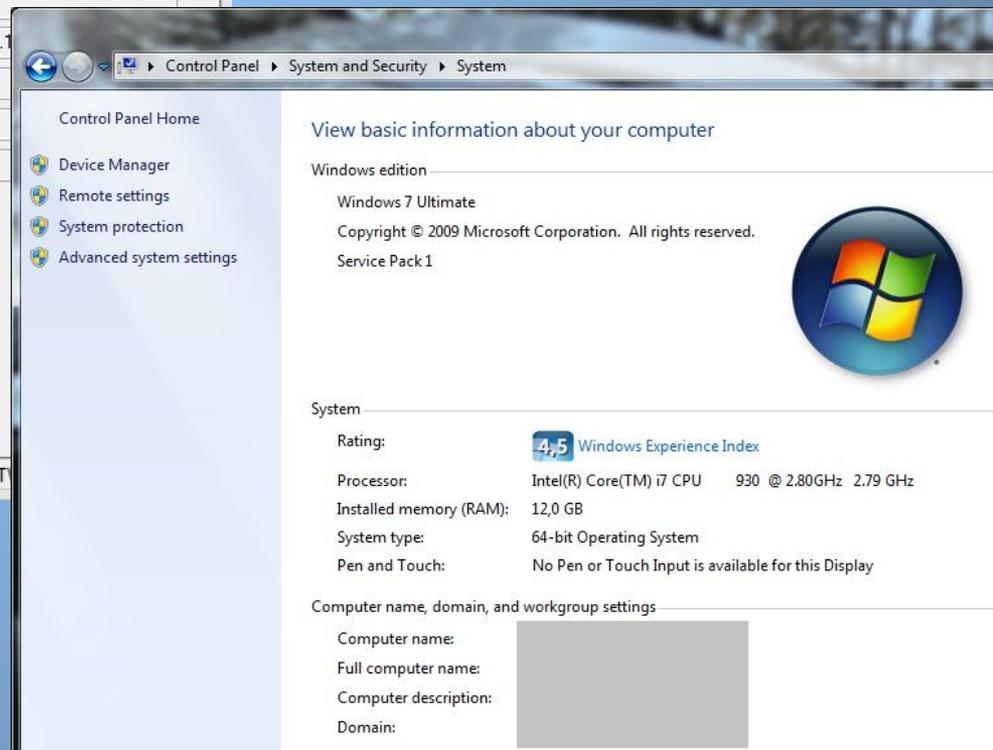
Product Version: Multiprocessor Free 6.1.7601.win7sp1\_gdr.1

Install Date: 25.02.2014 11:45:25

Service Pack: Service Pack 1

System Root: C:\Windows

Windows NT Registry 160574 keys loaded M:\Windows\System32\config\SOFT



Control Panel > System and Security > System

Control Panel Home

- Device Manager
- Remote settings
- System protection
- Advanced system settings

View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

Rating: **4.5** Windows Experience Index

Processor: Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2.79 GHz

Installed memory (RAM): 12,0 GB

System type: 64-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: [REDACTED]

Full computer name: [REDACTED]

Computer description: [REDACTED]

Domain: [REDACTED]

# Сведения об установленной ОС

\\Microsoft\Windows NT\CurrentVersion

AccessData Registry Viewer (Demo Mode) - [SOFTWARE]

File Edit Report View Window Help

VSTAHostConfig  
VSTO Runtime Setup  
WAB  
WBEM  
WIMMount  
Windows  
Windows CE Services  
Windows Defender  
Windows Desktop Search  
Windows Mail  
Windows Media Device Manager  
Windows Media Foundation  
Windows Media Player NSS  
Windows Messaging Subsystem  
Windows NT  
CurrentVersion  
Windows Photo Viewer  
Windows Portable Devices  
Windows Script Host  
Windows Search  
Wisp  
Workspaces  
WwanSvc  
MozillaPlugins  
Notepad++

Name	Type	Data
CurrentVersi...	REG_SZ	6.1
CurrentBuild	REG_SZ	7601
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x530C8255 (1393328725)
RegisteredO...	REG_SZ	[REDACTED]
RegisteredO...	REG_SZ	Пользователь Windows
SystemRoot	REG_SZ	C:\Windows
InstallationT...	REG_SZ	Client
EditionID	REG_SZ	Enterprise
ProductName	REG_SZ	Windows 7 Enterprise
ProductId	REG_SZ	[REDACTED]
DigitalProdu...	REG_BINARY	A4 00 00 00 03 00 00 00 30 30 33 39 32 2D 39 31 38 2D 35 30 30 30 30 32 2D 3
DigitalProdu...	REG_BINARY	F8 04 00 00 04 00 00 00 30 00 30 00 33 00 39 00 32 00 2D 00 30 00 30 00 31 00 37
CurrentBuild...	REG_SZ	7601
BuildLab	REG_SZ	[REDACTED]
BuildLabEx	REG_SZ	[REDACTED]
BuildGUID	REG_SZ	[REDACTED]
CSDBuildNu...	REG_SZ	1130
PathName	REG_SZ	C:\Windows
CSDVersion	REG_SZ	Service Pack 1

**Key Properties**

Last Written Time	16.10.2014 3:51:01 UTC
OS Install Date (UTC)	Tue Feb 25 11:45:25 2014
OS Install Date (Local)	Tue Feb 25 11:45:25 2014

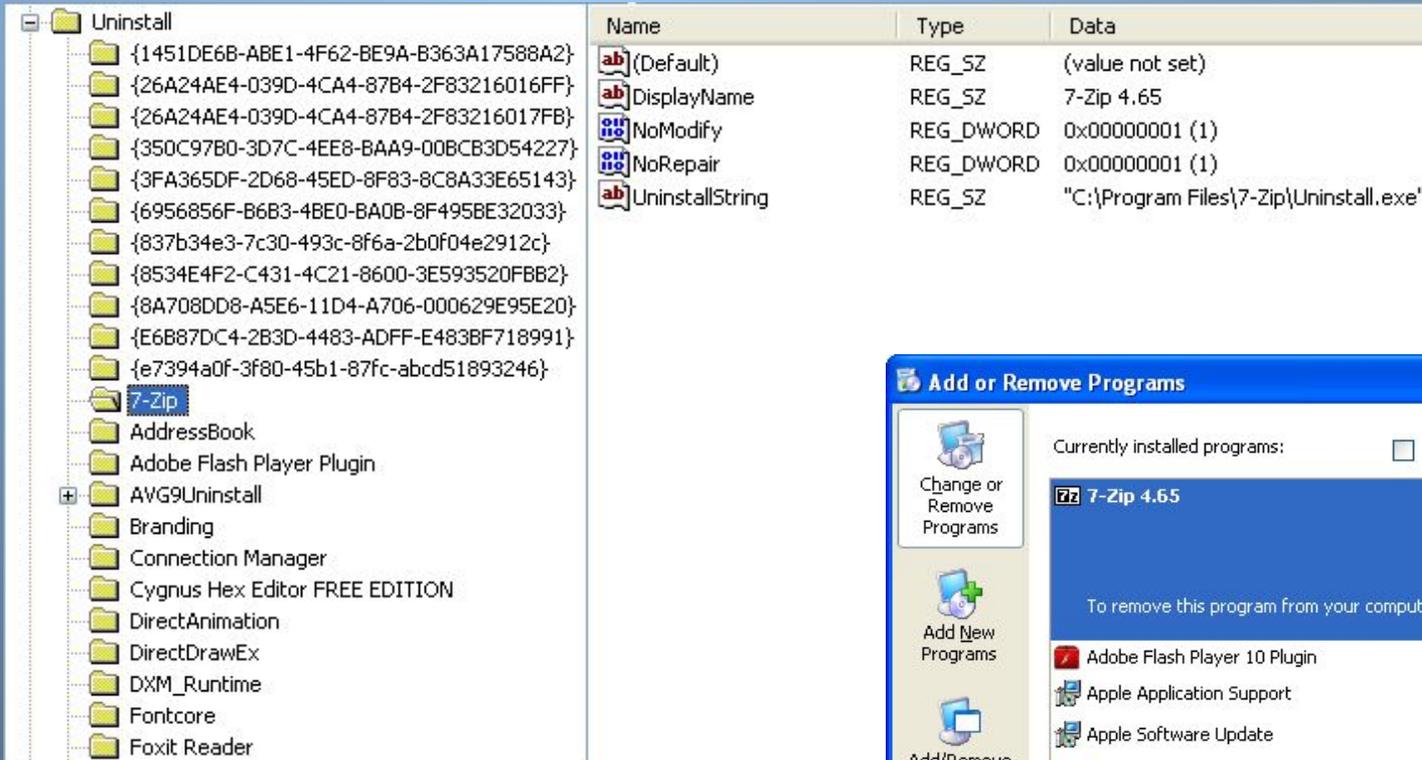
00 57 00 69 00 6E 00 64 00-6F 00 77 00 73 00 20 00 W-i-n-d-o-w-s-  
10 37 00 20 00 45 00 6E 00-74 00 65 00 72 00 70 00 7- -e-n-t-e-r-p-  
20 72 00 69 00 73 00 65 00-00 00 r-i-s-e-...

SOFTWARE\Microsoft\Windows NT\CurrentVersion Offset: 0

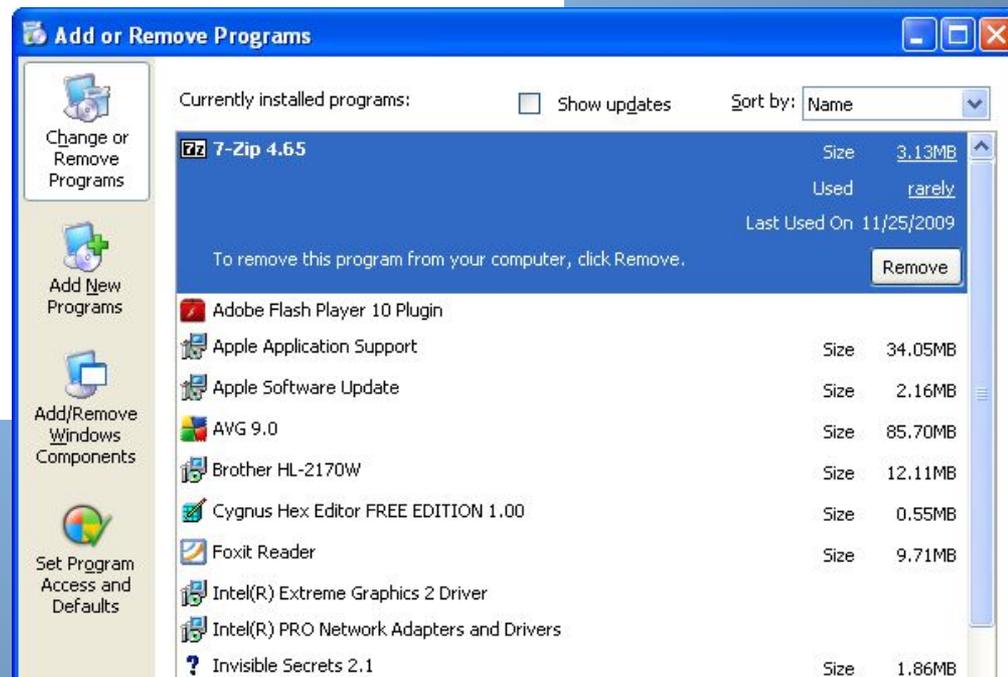
# Сведения об установленном ПО

## Раздел реестра HKEY\_LOCAL\_MACHINE\SOFTWARE

### \Microsoft\Windows NT\CurrentVersion\Uninstall



Name	Type	Data
{1451DE6B-ABE1-4F62-BE9A-B363A17588A2}	(Default)	REG_SZ (value not set)
{26A24AE4-039D-4CA4-87B4-2F83216016FF}	DisplayName	REG_SZ 7-Zip 4.65
{26A24AE4-039D-4CA4-87B4-2F83216017FB}	NoModify	REG_DWORD 0x00000001 (1)
{350C97B0-3D7C-4EE8-BAA9-00BCB3D54227}	NoRepair	REG_DWORD 0x00000001 (1)
{3FA365DF-2D68-45ED-8F83-8C8A33E65143}	UninstallString	REG_SZ "C:\Program Files\7-Zip\Uninstall.exe"
{6956856F-B6B3-4BE0-BA0B-8F495BE32033}		
{837b34e3-7c30-493c-8f6a-2b0f04e2912c}		
{8534E4F2-C431-4C21-8600-3E593520FBB2}		
{8A708DD8-A5E6-11D4-A706-000629E95E20}		
{E6B87DC4-2B3D-4483-ADFF-E483BF718991}		
{e7394a0f-3f80-45b1-87fc-abcd51893246}		



Currently installed programs:  Show updates Sort by: Name

Name	Size	Used	Last Used On
<b>7-Zip 4.65</b>	3.13MB	rarely	11/25/2009
To remove this program from your computer, click Remove.			
Adobe Flash Player 10 Plugin			
Apple Application Support	34.05MB		
Apple Software Update	2.16MB		
AVG 9.0	85.70MB		
Brother HL-2170W	12.11MB		
Cygnus Hex Editor FREE EDITION 1.00	0.55MB		
Foxit Reader	9.71MB		
Intel(R) Extreme Graphics 2 Driver			
Intel(R) PRO Network Adapters and Drivers			
Invisible Secrets 2.1	1.86MB		

# Сведения о об учетных записях в ОС

## Раздел реестра HKEY\_LOCAL\_MACHINE\SAM

The screenshot displays the MiTeC Windows Registry Recovery tool interface. The title bar reads "MiTeC Windows Registry Recovery - [SAM]". The main window is divided into several sections:

- Navigation:** Includes "File", "Explore", "Windows", and "Help" menus. Below are tabs for "SOFTWARE", "SYSTEM", and "SAM" (which is currently selected).
- Left Panel (Tasks):** Contains "Common tasks" (e.g., "Export to REGEDIT4 format...", "Export Data...") and "Explorer tasks" (e.g., "File Information", "Security Records", "SAM", "Windows Installation", "Hardware", "User Data", "Startup Applications", "Services and Drivers", "Network Configuration", "Windows Firewall Settings", "Environment", "Shell Folders", "Outlook Express", "Raw Data").
- Right Panel (Groups and Users):** Shows a tree view with "Users" and "Groups" folders. Under "Users", the "Администратор" (Administrator) user is selected. Below the tree is a table of properties for the selected user.

Property	Value
SID	S-1-5-21-1159259651-1992089595-3254878985-500
Comment	Встроенная учетная запись администратора компьютера/дом...
Last logon	05.11.2014 16:33:14
Last password set	25.02.2014 11:44:53
Last incorrect password	05.11.2014 11:32:07

At the bottom of the window, the status bar shows "Windows NT Registry 70 keys loaded" and the path "M:\Windows\System32\config\SAM".

# Сведения о об учетных записях в ОС

## Раздел реестра HKEY\_LOCAL\_MACHINE\SAM

The screenshot displays the MiTeC Windows Registry Recovery application window. The title bar reads "MiTeC Windows Registry Recovery - [SOFTWARE]". The interface is divided into several sections:

- Left Panel:** Contains navigation tabs for "SOFTWARE", "SYSTEM", and "SAM". Below these are "Common tasks" (Export to REGEDIT4 format..., Export Data...) and "Explorer tasks" (File Information, Security Records, SAM, Windows Installation, Hardware, User Data, Startup Applications, Services and Drivers, Network Configuration, Windows Firewall Settings, Environment, Shell Folders, Outlook Express, Raw Data).
- Tree View:** Shows the registry tree structure. The "ProfileList" folder is expanded, showing a list of user profile folders. The folder "S-1-5-21-1159259651-1992089595-3254878985-500" is selected and highlighted in blue.
- Right Panel:** Displays the values for the selected key. It is a table with columns "Value", "Type", and "Data".
- Bottom Panel:** A "Result Panel" with a search bar and a "Log" button. Below it, the "Key Path" is shown as: "CMI-CreateHive{3D971F19-49AB-4000-8D39-A6D9C673D809}\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1159259651-1992089595-3254878985-500".
- Status Bar:** At the bottom left, it shows "Windows NT Registry" and "160574 keys loaded". At the bottom right, it shows the path "M:\Windows\System32\config\SOFTWARE".

Value	Type	Data
ProfileImagePath	REG_EXPANDED_STRING	C:\Users\Администратор
Flags	REG_DWORD	0x00000000
State	REG_DWORD	0x00000100
Sid	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 03 E6 18 45 FB D
ProfileLoadTimeLow	REG_DWORD	0x00000000
ProfileLoadTimeHigh	REG_DWORD	0x00000000
RefCount	REG_DWORD	0x00000001
RunLogonScriptSync	REG_DWORD	0x00000000
NextLogonCacheable	REG_DWORD	0x00000001

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**

Содержит до 26 записей  
командной строки