

Rejestr Windows. Praca z rejestrem

Wykład: rejestr, położenie rejestru w systemie, edytor regedit, hierarchiczna budowa, klucze główne, HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG, typy wartości: REG_SZ, REG_BINARY, REG_DWORD, REG_MULTI_SZ, REG_EXPAND_SZ, uwagi praktyczne, 10 prostych ćwiczeń w edycji rejestru

Rejestr systemowy - definicja

Rejestr systemowy

to centralna, hierarchiczna baza danych, w której system operacyjny przechowuje informacje o swojej konfiguracji. Rejestr zawiera informacje o zainstalowanych aplikacjach, ustawieniach pulpitu, profilach wszystkich użytkowników komputera, składnikach sieci, zabezpieczeniach oraz informacje o sprzęcie systemu (sterownikach, urządzeniach, dostępnej pamięci). Windows podczas pracy stale odwołuje się do tych danych. Zadanie rejestru jest podobne do funkcji katalogu /etc w systemach Linux.

Rejestr systemu Windows jest następcą plików .ini, które miały poważne wady i ograniczenia, a poza tym były bardzo niewygodne w użyciu.

System operacyjny Windows NT 3.5 był pierwszym z rodziny systemów Windows, w którym występował rejestr przypominający jego obecną postać.

Kto jeszcze korzysta z rejestru?

Z Rejestru korzystają następujące komponenty Windows NT/2000/XP:

- programy instalacyjne aplikacji,
- program wykrywający urządzenia,
- jądro systemów Windows,
- menedżer PnP,
- sterowniki urządzeń,
- narzędzia administracyjne (aplety okna **Panel sterowania** i programy zawarte w grupie **Narzędzia administracyjne**, są najbezpieczniejszymi w użyciu programami umożliwiającymi modyfikowanie rejestru),
- profile użytkowników,
- profile sprzętowe (w przeciwieństwie do plików .ini, rejestr obsługuje wiele konfiguracji sprzętowych).

Gdzie zapisane są pliki rejestru?


- W Windows 95, 98 i Me wszystkie dane Rejestru znajdowały się w dwóch plikach: `system.dat` i `user.dat`
- W systemach Windows 2000 i Windows XP rejestr jest przechowywany w kilku plikach w folderach:

`\windows\system32\config`

`\Documents and Settings\[nazwa_użytkownika]`

Jeśli chcemy wykonać kopię zapasową plików Rejestru w Windows 95/98/Me, wystarczy, że skopiujemy pliki `system.dat` i `user.dat` z folderu systemowego. Jeśli jednak korzystamy z Windows 2000, XP powinno się wykorzystać odpowiedni program narzędziowy - np. Edytor rejestru `regedit`.

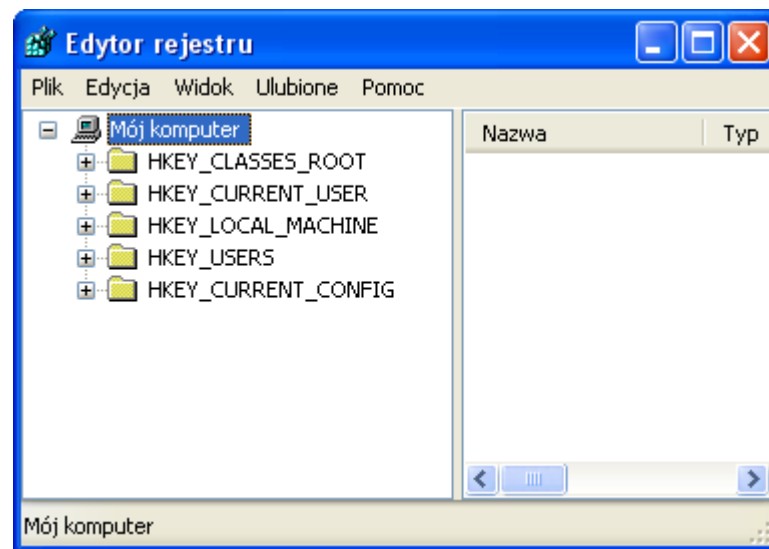
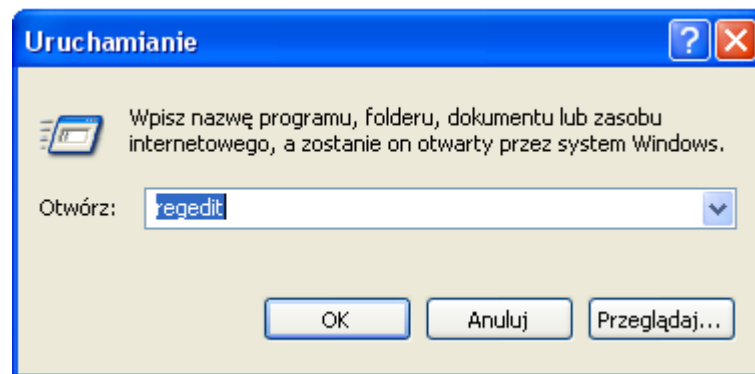
Systemowy edytor rejestru regedit

Edytor rejestru uruchomimy wybierając z menu  opcję Uruchom i wpisując nazwę edytora: regedit

Łatwo zauważyć podobieństwo edytora do Eksploratora Windows. Nawyki z niego wyniesione można tutaj z powodzeniem wykorzystać.

Lewy obszar okna możemy potraktować tak jak drzewo folderów, a prawy podobnie jak listę plików.

Szczegółowe informacje możemy wyszukiwać rozwijając kolejne gałęzie drzewa lub korzystając z dostępnego polecenia **Znajdź**.



Hierarchiczna budowa rejestru

Logiczną strukturę Rejestru, dla lepszego zrozumienia, można porównać z drzewem folderów na dysku. Rejestr zawiera **klucze** przypominające foldery i **wartości**, które można porównać do plików zapisanych na dysku.

Klucze Rejestru są obiektami-kontenerami przechowującymi **podklucze** i **wartości**. Wartości Rejestru - podobnie jak pliki - zawierają dane. Klucze najwyższego poziomu takiej hierarchicznej struktury są nazywane wstępnie zdefiniowanymi kluczami głównymi (**root keys**).

Rejestr składa się z 5 kluczy głównych. Nazw kluczy głównych nie można edytować. Są to:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG



Klucze główne rejestru (1,2,3)

Klucz główny	Zadanie
HKEY_CLASSES_ROOT	Zapisane są tu powiązania typów plików z aplikacjami, które je obsługują (np. dzięki informacjom w tym kluczu system wie, że format pliku .doc otwierany jest przez np. Worda). W rzeczywistości klucz ten jest wskaźnikiem do: <code>HKEY_LOCAL_MACHINE\Software\Classes</code>
HKEY_CURRENT_USER	Ten klucz przechowuje ustawienia profilu aktualnie zalogowanego użytkownika, np. schemat kolorów, zastosowane czcionki, dokonane personalizacje
HKEY_LOCAL_MACHINE	Zawiera najważniejsze informacje o konfiguracji komputera niezbędne do prawidłowego uruchomienia systemu Windows - zainstalowany sprzęt i programy oraz parametry systemu. Dane dotyczą wszystkich użytkowników danego systemu

Klucze główne rejestru (4,5)

Klucz główny	Zadanie
HKEY_USERS	Zawiera ustawienia profili wszystkich użytkowników, którzy kiedykolwiek logowali się na danym komputerze w kluczach odpowiadających ich numerom identyfikacyjnym w systemie (Security ID)
HKEY_CURRENT_CONFIG	Przechowuje dane konfiguracyjne o aktualnie używanym profilu sprzętowym Windows. Dane tak naprawdę pobierane są z: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware\Profiles

Co należy wiedzieć o edytorze?

- Edytor zapisuje wprowadzone zmiany natychmiast do rejestru
- Nie posiada polecenia COFNIJ
- Nie posiada polecenia PLIK | ZAPISZ, zmiany dokonywane są natychmiast po ich wpisaniu
- **Przed dokonaniem jakichkolwiek zmian konieczne trzeba wykonać kopię rejestru!**

Aby skopiować na inne komputery wprowadzone do Rejestru parametry powinniśmy skorzystać z dostępnej w Rejestrze funkcji **eksportu**.

Edytor Rejestru pozwala bowiem na skopiowanie wybranych gałęzi bazy do pliku o rozszerzeniu ***.reg**.

W celu zapisania odpowiednich parametrów wybieramy odpowiednią gałąź i uaktywniamy funkcję Rejestr | Eksportuj plik Rejestru. Warto przy tym zwrócić uwagę, czy chcemy eksportować cały rejestr, czy może lepiej tylko wybraną, interesującą nas gałąź.

Najczęściej spotykane wartości

Wartość	Funkcja
Ciąg znaków (REG_SZ)	Przechowuje dane, które mają postać tekstu (tzn. znaków alfanumerycznych)
Wartość binarna (REG_BINARY)	Do zapamiętania danych binarnych (0, 1)
Wartość "podwójne słowo" (REG_DWORD)	32-bitowa (czterobajtowa) liczba całkowita
Wielokrotny ciąg znaków (REG_MULTI_SZ)	Tzw. "wielociąg", czyli kilka ciągów znaków rozdzielonych znakami NULL
Rozwijany ciąg znaków (REG_EXPAND_SZ)	W odróżnieniu od zwykłego ciągu znaków, rozwijany ciąg zawiera w sobie jedną lub kilka zmiennych systemowych. Po pobraniu przez aplikację takiego ciągu, w miejsce ich nazw zmiennych systemowych wstawiane wartości.

Uwagi praktyczne (1)

- Wszędzie w edytorze gdzie nazwa klucza zaczyna się od `HKEY_LOCAL_MACHINE` wprowadzone zmiany obowiązują u wszystkich użytkowników!
- Aby zmiany dotyczyły tylko aktualnego użytkownika należy je wprowadzać w kluczu `HKEY_CURRENT_USER` dla aktualnie zalogowanego lub `HKEY_USERS\[SID_usera]` dla danego usera.
- Pamiętaj również, że przy wpisywaniu ścieżek dostępu w rejestrze zamiast znaku `\` używamy `\\`. Np. `C:\\Windows\\System32`
- Instalator każdego programu wprowadza do Rejestru systemu dane. Gdy odinstalujemy taki program, deinstalator powinien usunąć te wpisy. Dość często zdarza się jednak, że programy pozostawiają w rejestrze klucze, które nie służą do niczego. Pozostawione wpisy spowalniają system, ponieważ Windows musi analizować wiele kluczy, które nic nie oznaczają. Dostępne są programy, które czyszczą Rejestr z tego typu "śmieci". Jednym z nich jest aplikacja `RegCleaner`

Uwagi praktyczne (2)

- Szybkość pracy naszego systemu zależy między innymi od rozmiarów rejestru. Im większy rejestr, tym wolniejszy system. Z tego też względu powinniśmy optymalizować zawartość tej bazy, poprzez tzw. **defragmentację rejestru**.
- Dzięki defragmentacji znacznie zmniejszą się rozmiary rejestru. W tym celu można posłużyć się którymś z programów do defragmentacji rejestru. Dostępne w Internecie są na przykład: Auslogics Registry Defrag 4.1.6.75, 10bit SmartDefrag, Baku, JkDefrag

10 prostych ćwiczeń (1)

1. Pokaż rozszerzenia plików znanych typów

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced  
HideFileExt = 0
```

2. Pokaż wersję Win na pulpicie

```
HKEY_CURRENT_USER\ControlPanel\Desktop  
PaintDesktopVersion = 1
```

3. Brak ustawień rozdzielczości

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System  
NoDispSettingsPage = 1
```

4. Brak ustawień rozdzielczości jako fix z rozszerzeniem *.reg:

```
Windows Registry Editor Version 5.00  
[HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System]  
"NoDispSettingsPage"=dword:00000001
```

5. Okno z własnym komunikatem podczas logowania

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\WinLogon  
lub HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\policies\system  
LegalNoticeCaption  
LegalNoticeText
```

10 prostych ćwiczeń (2)

6. Ukrywa wybrane dyski (A: 1, B: 2, C: 4, D: 8, E: 16, itd.)

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDrives"=dword:00000004
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDrives"=dword:00000004
```

7. Zmiana nazwy Kosza

Znajdź: @C:\WINDOWS\system32\SHELL32.dll i zamień nazwę kosza na dowolną

8. Wyłącza ekran powitalny i używa klasycznego okna logowania

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"LogonType"=dword:00000000
```

9. Opóźnienie rozwinięcia menu "Wszystkie programy" w menu Start

```
HKEY_CURRENT_USER\Control Panel\Desktop
MenuShowDelay w milisekundach
```

10. Pokazuje wszystkie pliki, ukryte i chronione (jako plik .reg)

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"Hidden"=dword:00000001
"HideFileExt"=dword:00000000
"ShowSuperHidden"=dword:00000001
```

Źródła

Systemy operacyjne i sieci komputerowe.
Cz. 1. WSIP. Krzysztof Pytel, Sylwia Osetek

Systemy operacyjne i sieci komputerowe.
Cz. 2. WSIP. Krzysztof Pytel, Sylwia Osetek