Rejestr systemowy

MD

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.

Rejestr systemowy

Z rejestru korzystają następujące komponenty systemu Windows:

- programy instalacyjne aplikacji,
- program wykrywający urządzenia,
- jądro systemów Windows,
- menedżer PnP (Plug and Play),
- 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

Gdzie jest rejestr?

Rejestr jest przechowywany w kilku plikach w folderach:

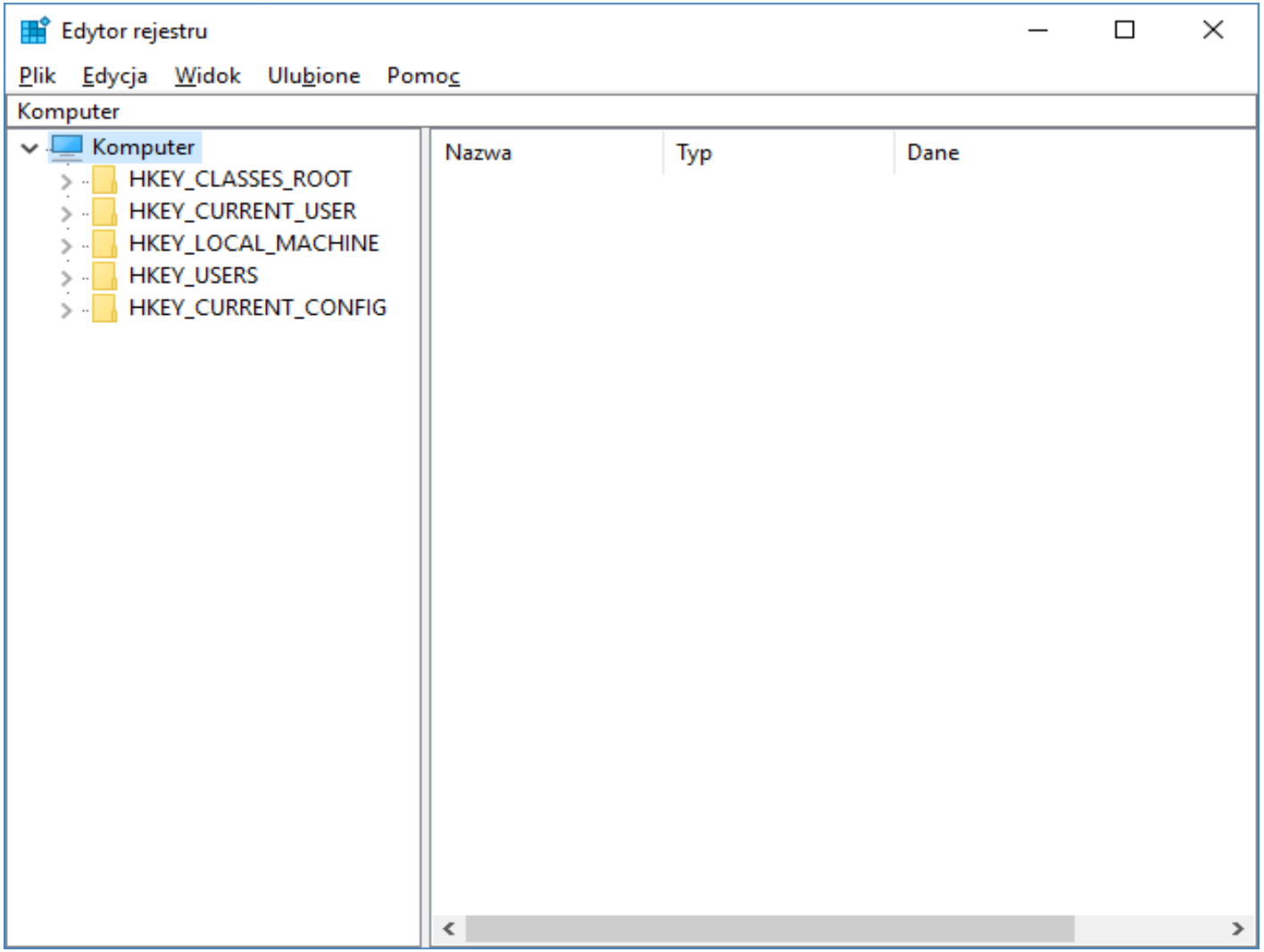
\windows\system32\config

oraz

\Documents and Settings\[użytkownik]

Program narzędziowy do edycji rejestru: **regedit**

Budowa rejestru



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).

Klucze główne rejestru

- **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 wskaźnikem do HKEY_LOCAL_MACHINE\Software\Classes.
- **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.
- **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 lokalizacji HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware\Profiles.

Co trzeba wiedzieć?

- 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 koniecznie trzeba wykonać kopię rejestru!

Typy spotykanych wartości

- 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.

- 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\[ID_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 odinstalowujemy 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 lub CCleaner.
- 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, 10bit SmartDefrag, Baku, JkDefrag

Ćwiczenia

1. Pokaż rozszerzenia plików znanych typów

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

ustawienie HideFileExt = 0

2. Pokaż wersję Windows na pulpicie

HKEY_CURRENT_USER\ControlPanel\Desktop

ustawienie PaintDesktopVersion = 1

3. Brak ustawień rozdzielczości

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System

ustawienie NoDispSettingsPage = 1

Ćwiczenia

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

[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
ustawienie LegalNoticeCaption oraz LegalNoticeText

6. Ukrywa wybrane dyski (A: 1, B: 2, itd.)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
ustawienie "NoDrives"=dword:00000004

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
ustawienie "NoDrives"=dword:00000004

Ćwiczenia

7. Wyłączenie ekranu powitalnego i użycie klasycznego okna logowania

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

8. Opóźnienie rozwinięcia menu Wszystkie programy w menu Start

HKEY_CURRENT_USER\Control Panel\Desktop
ustawienie MenuShowDelay w milisekundach

9. Pokazanie wszytkich plików, ukrytych i chronionych (jako plik .reg)

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"Hidden"=dword:00000001
"HideFileExt"=dword:00000000
"ShowSuperHidden"=dword:00000001