Rejestr systemu Windows

Mariusz Nowak 2019

Czym jest rejestr systemu Windows?

Rejestr to centralna hierarchiczna baza danych używana do przechowywania informacji, które są **niezbędne do skonfigurowania systemu.**

W rejestrze zapisane sią informacje dotyczące:

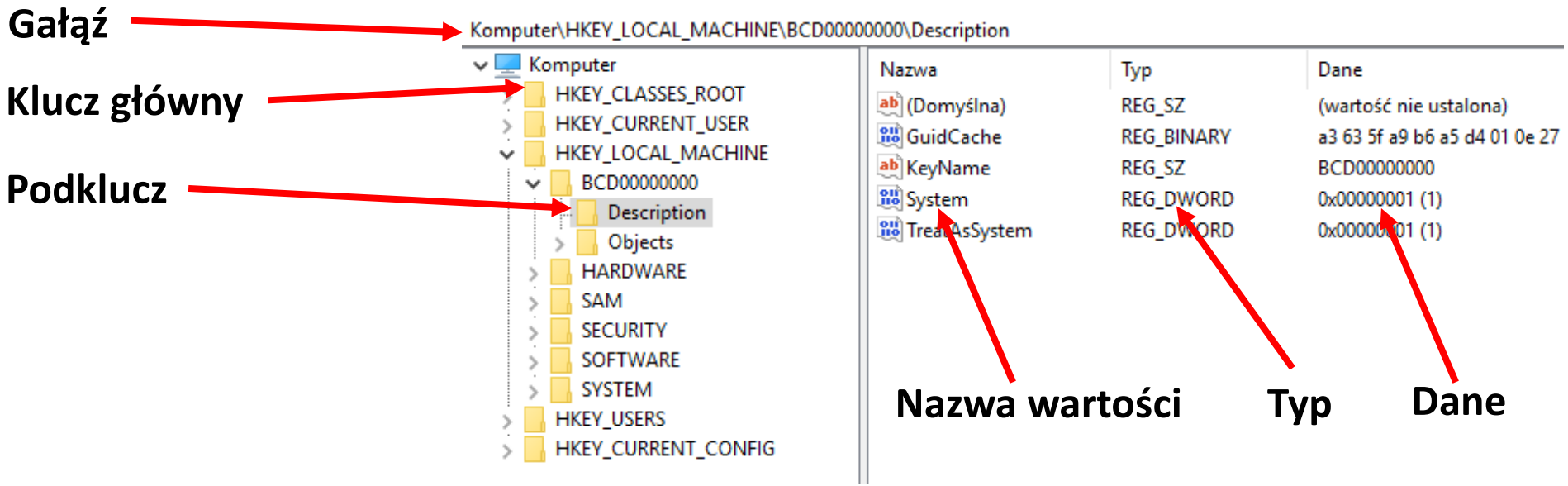
- systemu operacyjnego
- sprzętowej konfiguracji
- zainstalowanych aplikacji
- kont użytkowników
- sieci
- powiązań między typami plików a aplikacjami

System Windows zawiera narzędzie do edycje rejestru: regedit.exe

Logiczna budowa rejestru

Logiczna struktura rejestru ma postać hierarchicznego drzewa, która składa się z **kluczy, podkluczy i wartości**.

- **Klucz** to obiekt-kontener przechowujący podklucze i wartości
- **Wartości** to wpis zawierający dane konfiguracyjne określonego typu (każdy klucz ma przynajmniej jedną wartość, tzw. wartość domyślną)
- **Gałąź** to klucz główny wraz z wszystkimi podkluczami i wartościami

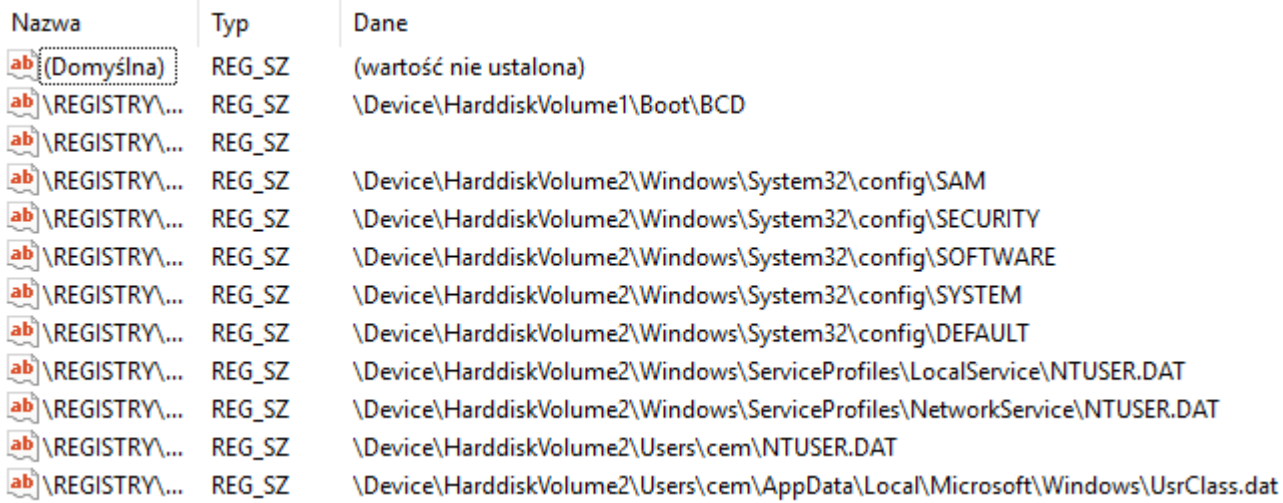


Fizyczna budowa rejestru

Gałęzie rejestru fizycznie zapisane są w **postaci plików** (Windows 10):

- C:\Windows\System32\config**SAM**
- C:\Windows\System32\config**SECURITY**
- C:\Windows\System32\config**SOFTWARE**
- C:\Windows\System32\config**SYSTEM**
- C:\Windows\System32\config**DEFAULT**
- C:\Users\Nazwa użytkownika**NTUSER.DAT**

Lokalizacja plików rejestru można sprawdzić w gałęzi:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist



Nazwa	Typ	Dane
(Domyślna)	REG_SZ	(wartość nie ustalona)
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume1\Boot\BCD
\REGISTRY\...	REG_SZ	
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SAM
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SECURITY
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SOFTWARE
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SYSTEM
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\DEFAULT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\ServiceProfiles\LocalService\NTUSER.DAT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Users\cem\NTUSER.DAT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Users\cem\AppData\Local\Microsoft\Windows\UsrClass.dat

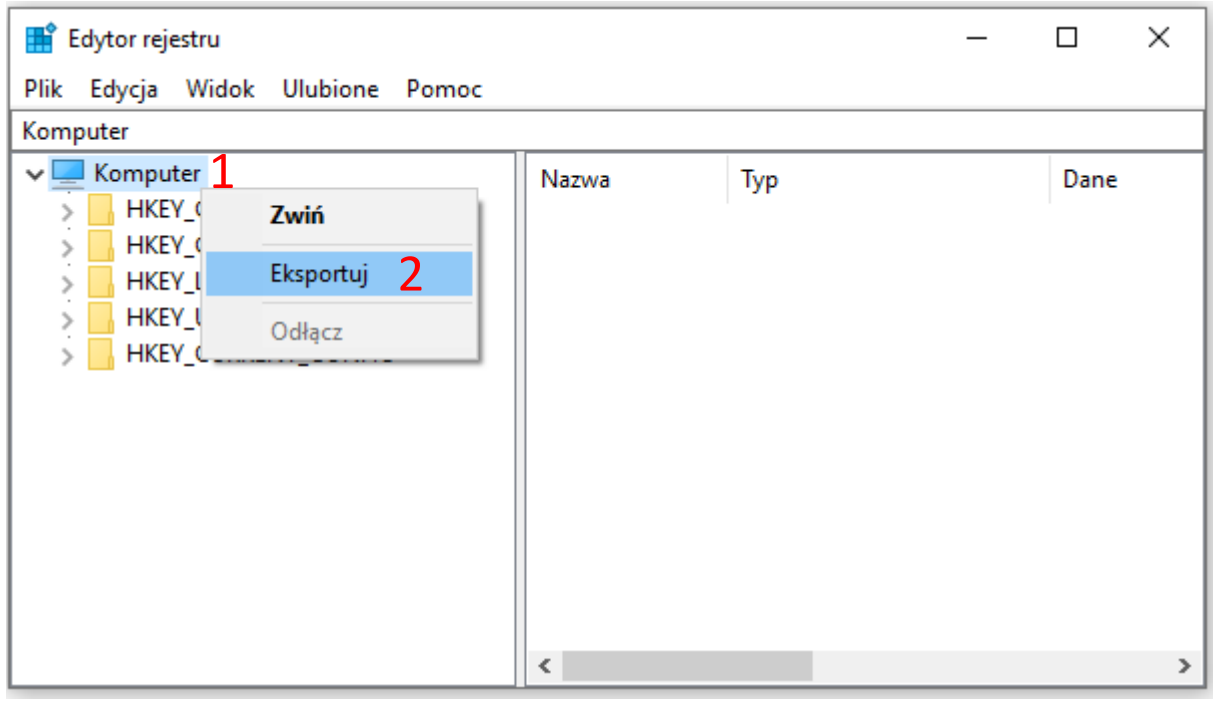
Główne klucze rejestru

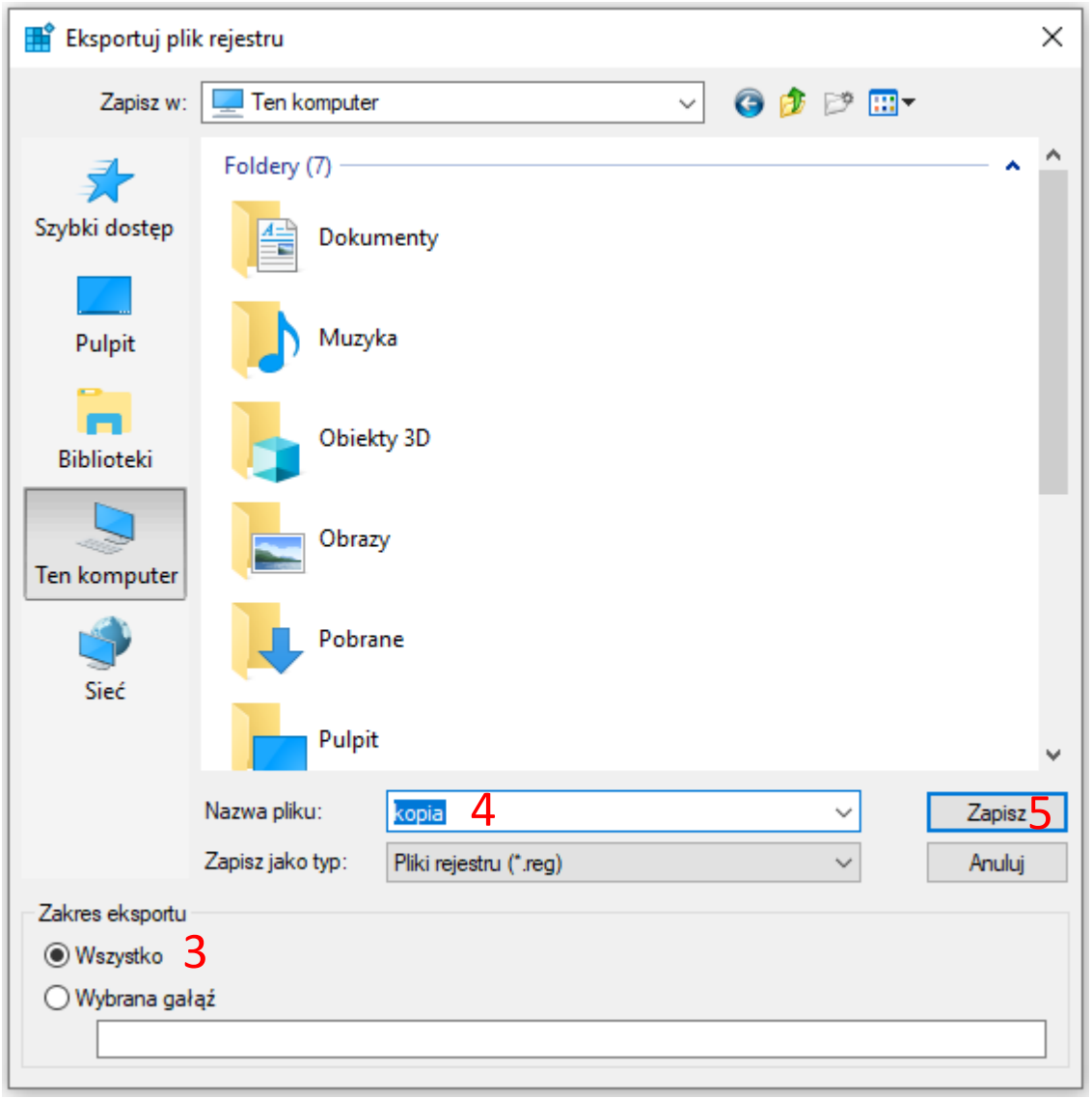
Klucz	Zadanie
HKEY_CLASSES_ROOT (HKCR)	Zapisane są tu powiązania typów plików z aplikacjami, które je obsługują
HKEY_CURRENT_USER (HKCU)	Przechowuje ustawienia profilu aktualnie zalogowanego użytkownika.
HKEY_LOCAL_MACHINE (HKLM)	Zawiera najważniejsze informacje o konfiguracji komputera niezbędne do prawidłowego uruchomienia systemu Windows
HKEY_USERS (HKU)	Są to ustawienia profili wszystkich użytkowników, którzy kiedykolwiek logowali się na dany komputer
HKEY_CURRENT_CONFIG (HKCC)	Są to dane konfiguracyjne wykorzystywane przez aktualnie używany profil sprzętowy Windows

Typy wartości

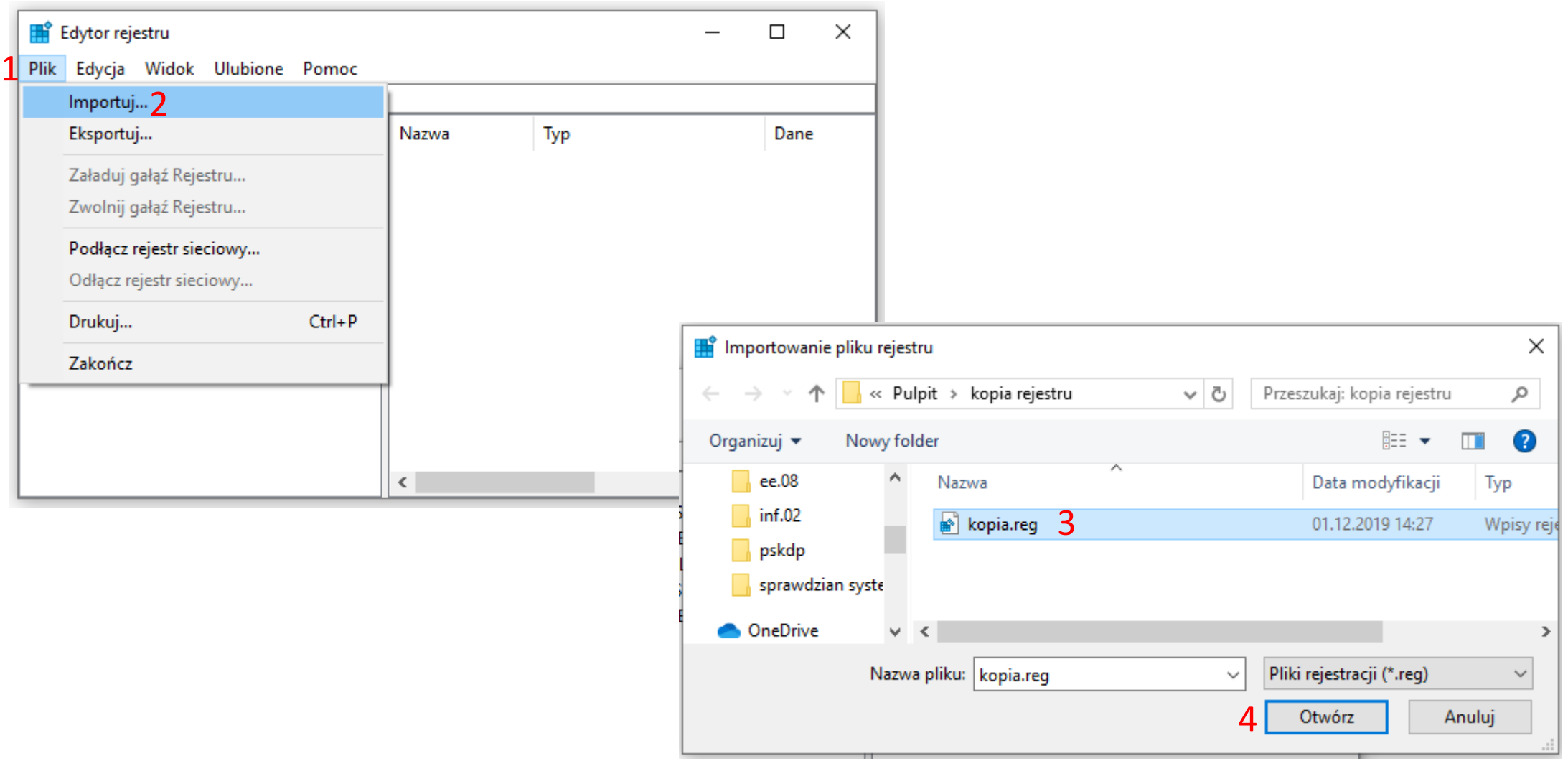
Typ (nazwa polska)	Zadanie
REG_SZ (wartość ściągu)	Łańcuch tekstowy (napis) zakończony pustym znakiem NULL "\0". Np.: **"Tekst\0"**
REG_MULTI_SZ (wartość ciągu wielokrotnego)	Wiele połączonych łańcuchów tekstowych. Każdy łańcuch tekstowy musi być zakończony znakiem pustym NULL. Na samym końcu należy dwukrotnie zapisać znak pusty NULL. Np.: **"Tekst1\0Tekst2\0Tekst3\0\0"**
REG_EXPAND_SZ (wartość ciągu rozwijalnego)	Łańcuch tekstowy zakończony znakiem pustym NULL. Może zawierać nazwy zmiennych, które zostaną zastąpiono odpowiednią wartością zmiennej. Np.: **"Nazwa użytkownika: %UserName%\0"**
REG_BINARY (wartość binarna)	Dane binarne zapisane w notacji szesnastkowej. Np.: **A3 63 5F B6**
REG_DWORD (wartość DWORD)	32-bitowa liczba całkowita zapisana w notacji szesnastkowej lub dziesiętnej. Np.: **0x0000000A** (10)
REG_QWORD (wartość QWORD)	64-bitowa liczba całkowita zapisana w notacji szesnastkowej lub dziesiętnej Np.: **0x0000000A** (10)

Program regedit.exe - kopia rejestru

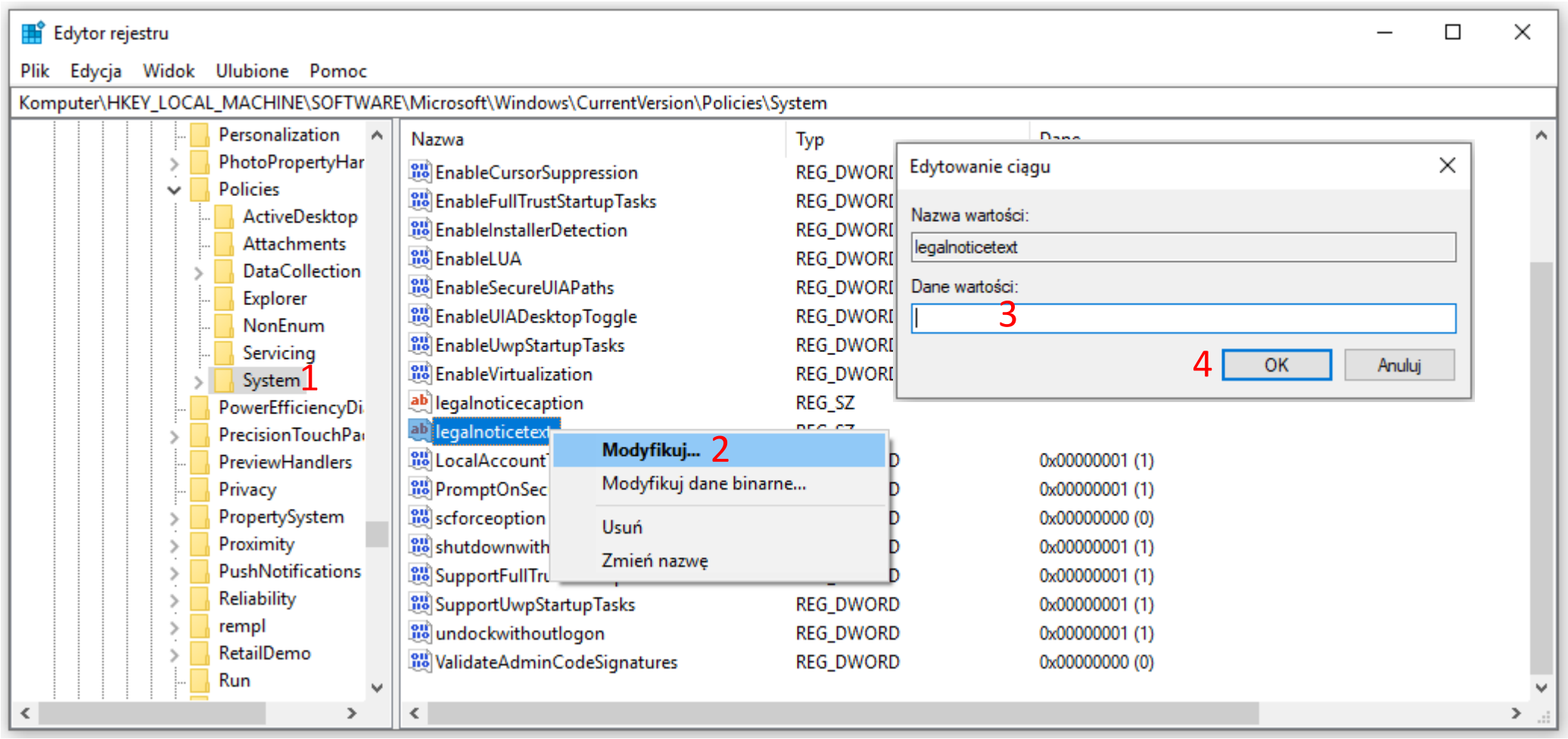




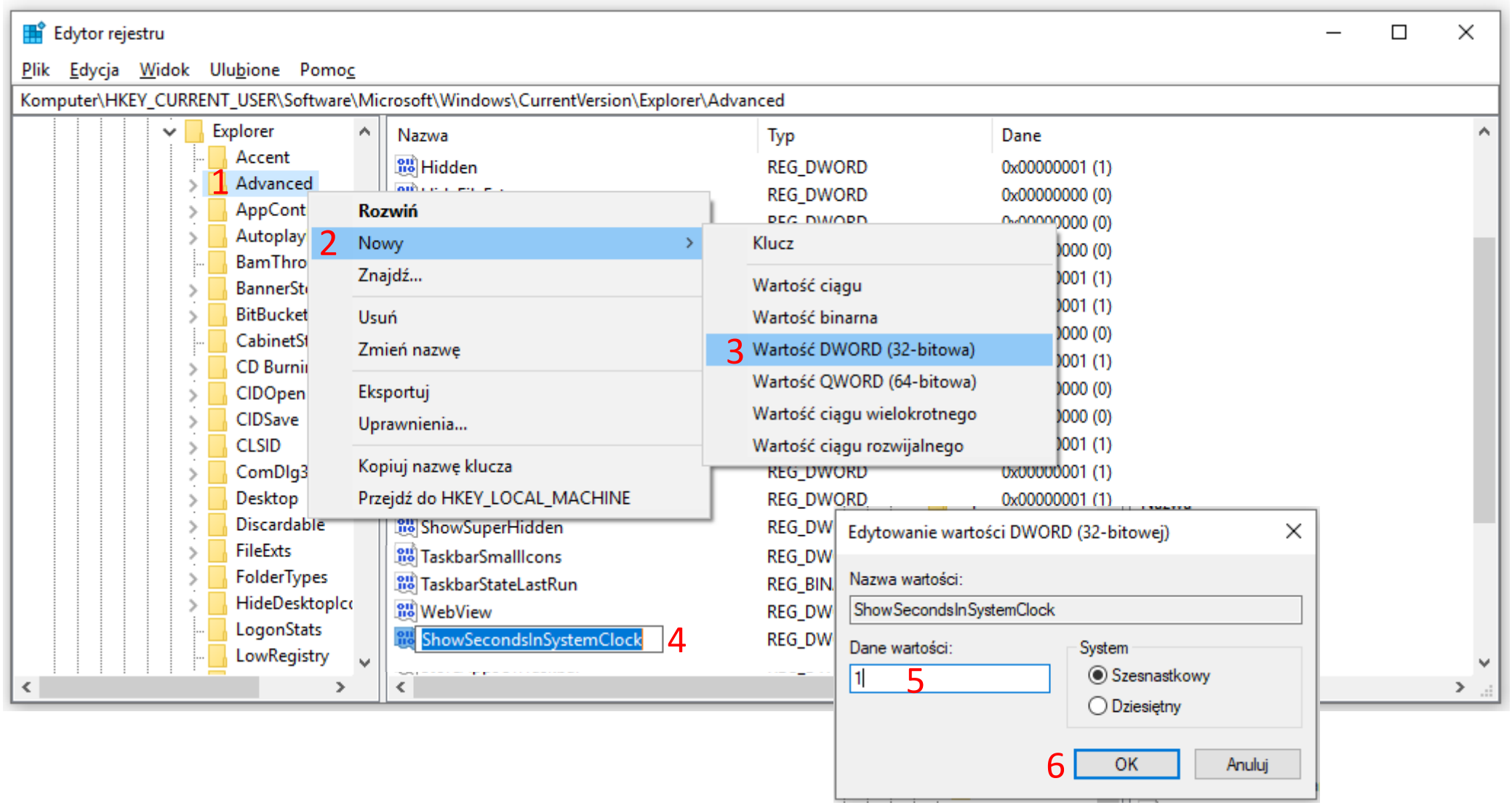
Program regedit.exe - przywracanie rejestru



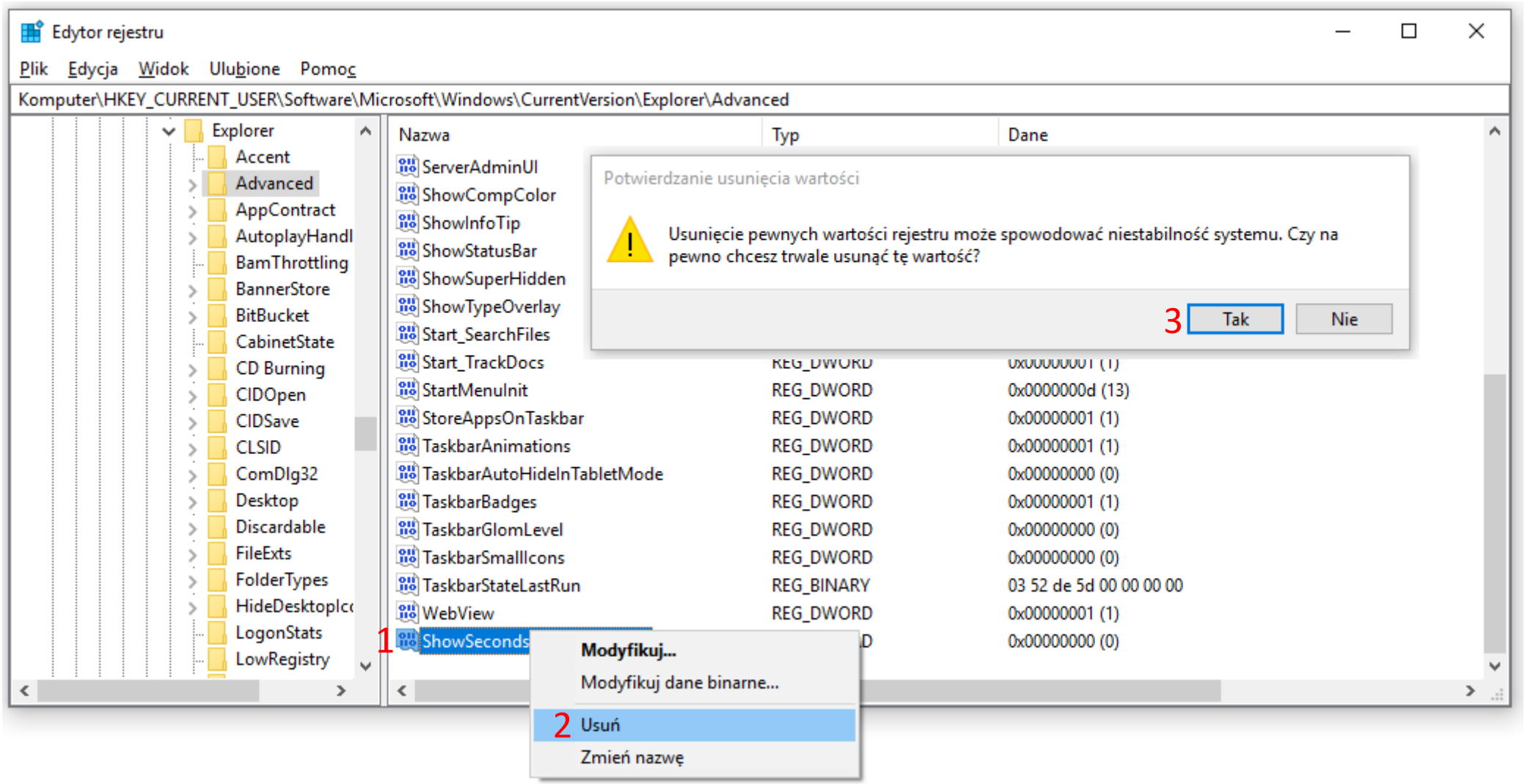
Program regedit.exe - modyfikacja wartości (REG_SZ)



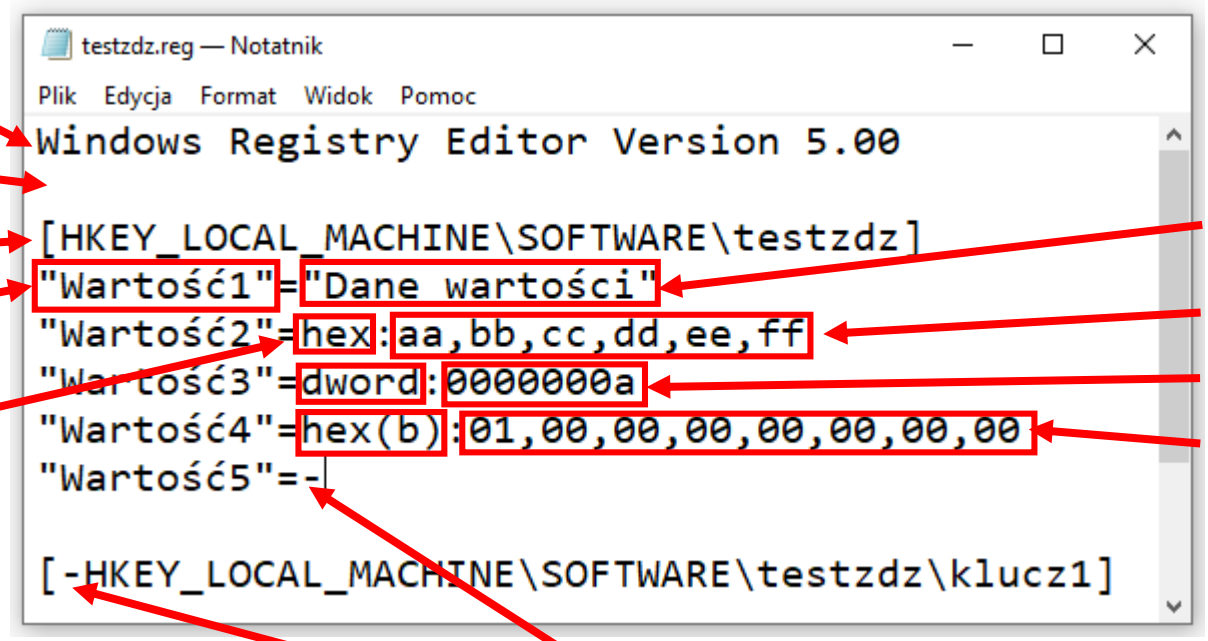
regedit.exe - dodawanie nowej wartości (REG_DWORD)



regedit.exe - usuwanie wartości



Składnia plików **.reg**



Wersja edytora rejestru

Pusta linia

Ścieżka do danego klucza

Nazwa wartości

Deklaracja typu właściwości

Dane typu REG_SZ

Dane typu REG_BINARY

Dane typu REG_DWORD

Dane typu REG_QWORD

Znak minus (-) usuwa dany klucz lub wartość

Scalanie plików .reg