Rejestr - poznaj swojego wroga!

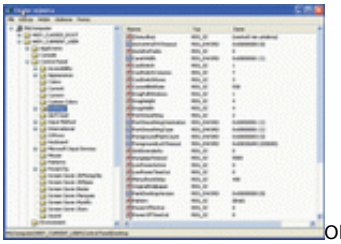
1 grudnia 2004 0:00 - Jacek Ścisławski

Rejestr to komponent systemu budzący głęboką niechęć użytkowników Windows, a często i pewną nerwowość. Jeśli myślisz, że uszkodzenie rejestru może spowodować totalną katastrofę systemu operacyjnego, masz rację. Aby uniknąć kłopotów, musisz wiedzieć, jak z nim postępować.

Rejestr to komponent systemu budzący głęboką niechęć użytkowników Windows, a często i pewną nerwowość. Jeśli myślisz, że uszkodzenie rejestru może spowodować totalną katastrofę systemu operacyjnego, masz rację. Aby uniknąć kłopotów, musisz wiedzieć, jak z nim postępować.

Microsoft dokłada wszelkich starań, aby maksymalnie uprościć konfigurację systemu Windows XP. Siadając do klawiatury, otrzymujesz wiele wygodnych, ubarwionych ilustracjami oraz animacjami kreatorów. Po otworzeniu Panelu sterowania możesz ustawić parametry ekranu, myszy lub klawiatury. Warto pamiętać, że wprowadzane zmiany trafiają do rejestru. Jeśli rejestr ulegnie uszkodzeniu, w najlepszym wypadku utracisz swoje ustawienia, w najgorszym czeka cię reinstalacja Windows.

Czym jest rejestr?

 Okno programu Regedit.Rejestr to centralna baza ustawień systemu operacyjnego, którą Windows posługuje się niemal co sekundę. Jeśli uruchomisz prosty program do monitorowania pracy rejestru, będziesz zaskoczony częstotliwością kontaktów system-rejestr. Można śmiało powiedzieć, że rejestr jest najważniejszą częścią systemu operacyjnego. Jego brak lub uszkodzenie niesie ze sobą poważne kłopoty.

Rejestr gromadzi informacje związane ze środowiskiem startowym, konfiguracją usług, urządzeń, sterowników, parametrami aplikacji, profilu użytkownika oraz zasad grupy. Centralne składowanie danych sprawia, że szybko można sięgnąć do pożądanych informacji. Równie szybko, system i aplikacje zapisują w nim odpowiednie ustawienia.

Użytkownicy Windows nie muszą ręcznie wprowadzać żadnych informacji do rejestru. Zadanie to spoczywa na Windows XP i uruchamianych w nim aplikacjach. Nie oznacza to jednak, że obsługę rejestru należy pozostawić całkowicie systemowi operacyjnemu. Sporządzanie kopii zapasowej rejestru jest pożądane, a nawet konieczne. Dodatkowo umiejętnie zarządzając rejestrem, można władać całym systemem. Modyfikacja niektórych ustawień zwiększy wydajność Windows lub uczyni pracę z systemem bardziej wygodną.

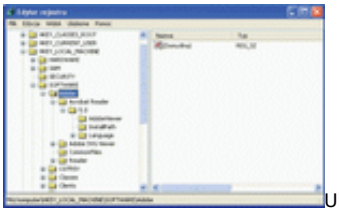
Jak to kiedyś bywało

 Wartość REG_FULL_RESOURCE_DESCRIPTOR.Pierwsze systemy operacyjne nie wykorzystywały rejestru do przechowywania informacji o swoich parametrach. Podstawowa konfiguracja systemu DOS opierała się na dwóch plikach Config.sys i Autoexec.bat. Stanowiło to proste, ale wyjątkowo ograniczone rozwiązanie. Pojawienie się "okienek" zmusiło do poszukiwania nowych sposobów na gromadzenie ustawień. System Windows we wczesnym dzieciństwie korzystał z plików INI.

Zastosowanie plików INI szybko okazało się nie najlepszym pomysłem. Podstawowym problemem tekstowych plików konfiguracyjnych była płaska struktura zapisywanych danych. Podział na sekcje, w których wprowadzano parametry i wartości, nie zawsze był efektywny. Potrzeba zróżnicowania ustawień systemu w zależności od użytkownika powodowała nie lada kłopot. Przy wielu zainstalowanych aplikacjach liczba plików INI rosła w zastraszającym tempie. Powodowało to mnożenie ustawień i ogromny bałagan. Po zainstalowaniu programu niewiele osób wiedziało, gdzie szukać plików konfiguracyjnych. Programista mógł dodać je do katalogu aplikacji, do katalogu systemu operacyjnego, a jeśli przyszło mu do głowy umieścić kolejne wpisy np. w pliku CONTROL.INI, nie stanowiło to żadnego problemu. Po wprowadzeniu ustawień do jednego pliku tekstowego pojawiały się kłopoty z modyfikacjami i szybkim wyszukiwaniem informacji. Maksymalny rozmiar pojedynczego pliku INI wynosił 64 KB.

Rejestr pojawił się razem z Windows 3.1. Od tamtej pory przeszedł wiele mniej lub bardziej istotnych modyfikacji, ale jego główne przeznaczenie nie zmieniło się. Najważniejszą, niemal rewolucyjną nowością było odrzucenie płaskiej struktury rejestru i wprowadzenie modelu podobnego do bazy danych. Ograniczenia związane z plikami INI zostały usunięte bezpowrotnie. To, co okazało się największym atutem rejestru, stało się szybko jego największą wadą. Baza konfiguracji w intensywnie eksploatowanych systemach rozrastała się szybko do monstrualnych rozmiarów. Aplikacje łatwo zaśmiecały rejestr, co powodowało bałagan. Użytkownicy Windows gubili się w gąszczu ustawień i

wpisów. Podatność na uszkodzenia i wiążące się z nimi skutki w postaci reinstalacji systemu, sprawiły, że rejestr jest wyjątkowo nielubianym komponentem Windows.


Układ wpisów do klucza SOFTWARE na przykładzie wpisów Acrobat Readera.Ewolucja rejestru, podobnie jak ewolucja systemów operacyjnych firmy Microsoft, szła dwoma drogami. Pierwszą był rozwój systemów dla użytkowników domowych. W Windows 95, 98 i Me zarządzanie rejestrem odbywało się podobnie. Wprowadzono kilka udogodnień, takich jak narzędzie SCANREG.EXE, ale po ukazaniu się Windows Me linia tych systemów odeszła w zapomnienie. Drugą rodziną systemów operacyjnych były produkty przeznaczone do firm. Miały pełnić funkcje mocnych stacji roboczych (np. Windows 2000 Professional) lub serwerów (np. Windows 2000 Server). Rejestr systemów opartych na Windows NT odznaczał się kilkoma istotnymi różnicami. Administrator mógł np. dodawać i modyfikować wartości innego typu niż w Windows 98, a dostęp do kluczy rejestru był chroniony przez uprawnienia nadawane na listach ACL (Access Control List).

Narzędzia do obsługi rejestru

Jeśli jesteś zainteresowany edycją, monitorowaniem lub innymi czynnościami związanymi z obsługą rejestru, potrzebujesz właściwych narzędzi. Najpotrzebniejsze są dostarczane bezpośrednio z systemem operacyjnym. Jeśli wymagasz bardziej zaawansowanych programów, musisz sięgnąć do Internetu.

Narzędzia do zarządzania rejestrem można podzielić na trzy grupy. Pierwsza pozwala na przeglądanie, modyfikowanie i dodawanie wpisów do bazy konfiguracyjnej systemu. W tym celu najlepiej posłużyć się wbudowanym w Windows XP edytorem REGEDIT.EXE. Drugą grupę narzędzi tworzą programy pozwalające na monitorowanie, w czasie rzeczywistym, zmian wprowadzanych do rejestru. To zadanie najlepiej powierzyć bezpłatnemu REGMON.EXE firmy SysInternals (http://www.sysinternals.com).

Ostatnią i najczęściej spotykaną grupą narzędzi są aplikacje, których celem jest porządkowanie rejestru. Jeśli instalowałeś na swoim komputerze wersje testowe i demonstracyjne gier lub oprogramowania, rejestr może zawierać nikomu niepotrzebne wpisy. Pogramy porządkujące przeprowadzą skanowanie zawartości rejestru i poinformują cię, czego należy się pozbyć. Windows XP nie oferuje narzędzi tego typu. W Internecie znajdziesz mnóstwo programów do porządkowania rejestru.

Regedit

Klucze główne i ich akronimy

NAZWA KLUCZA GŁÓWNEGO	AKRONIM
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CURRENT_USER	HKCU
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_CONFIG	HKCC

Klucze główne i ich akronimyPodstawowym narzędziem do pracy z rejestrem jest program REGEDIT.EXE. Jest to narzędzie, które pozwoli ci wykonać większość zadań związanych edycją, dodawaniem nowych wpisów, zarządzaniem zabezpieczeniami oraz importowaniem i eksportowaniem ustawień rejestru.

Poprzednie wersje systemu Windows wykorzystywały różne narzędzia. Jeśli rozpoczynałeś pracę od Windows 95 lub 98, REGEDIT.EXE nie powinien być ci obcy. W Windows NT i 2000, głównym programem do obsługi rejestru był REGEDT32.exe. Oferował kilka istotnych funkcji, np. możliwości zmiany uprawnień do kluczy rejestru. Microsoft postanowił ujednolicić zarządzanie rejestrem i w systemie Windows XP umieszczono pozbawiony uszczerbków Regedit. Co ciekawe, w XP są oba wymienione narzędzia, ale jeśli w oknie Uruchom wpiszesz REGEDT32.EXE i tak zostanie uruchomiony Regedit.

Nawigacja po programie Regedit

Programu Regedit nie znajdziesz w żadnym podmenu grupy Akcesoria lub Programy. Edytor trzeba uruchomić ręcznie z folderu Windows. Zamiast mozolnie szukać pliku za pomocą Eksploratora, najszybciej uruchomisz go, wprowadzając w oknie Uruchom nazwę Regedit. Nie musisz wprowadzać pełniej ścieżki do programu, ponieważ system operacyjny automatycznie przeszuka zawartość folderu Windows.

Po starcie programu wyświetlane są dwa panele. Panel kluczy zawiera główne klucze rejestru (patrz część "Pięć kluczy głównych"), a Panel wartości - podklucze lub wartości każdego podklucza. Nawigacja po edytorze rejestru jest niemal identyczna, jak przechodzenie pomiędzy folderami Eksploratora Windows. Główna różnica polega na tym, że zamiast plików i folderów widzisz wartości oraz podklucze. Klucze są reprezentowane przez takie same ikony jak foldery. Umieszczone przy kluczach plusy pozwalają na przechodzenie w głąb struktury rejestru. W czasie przemieszczania się między poszczególnymi kluczami warto pamiętać o możliwości wykorzystania strzałek nawigacyjnych klawiatury. Dzięki nim łatwo będziesz mógł rozwijać i zwijać każdy z obiektów. Dodatkowo, przy szybkim wprowadzaniu liter rozpoczynających nazwy podkluczy, zostaniesz przeniesiony do odpowiednich wpisów. Unikniesz wówczas żmudnego przewijania zawartości panelu albo wielokrotnego naciskania strzałki w dół. Jeśli zaznaczysz w lewym panelu jeden z podkluczy, w prawym zobaczysz jego zawartość. Panel wartości prezentuje nazwę wartości, jej typ oraz zgromadzone dane.

W czasie pracy z Eksploratorem Windows na pewno przyzwyczaiłeś się do korzystania z menu kontekstowego. Jeśli klikniesz prawym przyciskiem myszy jeden z kluczy w lewym panelu, system wyświetli menu podręczne. Zawiera ono listę najczęściej wykonywanych zadań edycyjnych, np. Utwórz nowy klucz, Usuń lub Zmień nazwę. Podobnie po kliknięciu prawym przyciskiem myszy jednej z wartości zyskasz możliwość jej modyfikacji, zmiany nazwy lub usunięcia.

Przeszukiwanie rejestru

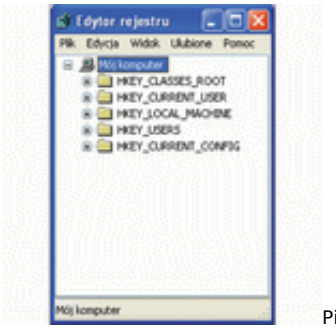
Zanim zaczniesz wprowadzać zmiany do rejestru, musisz odnaleźć interesujące cię klucze. Regedit oferuje prosty i skuteczny mechanizm penetrowania bazy konfiguracyjnej systemu. W celu rozpoczęcia przeszukiwania musisz uruchomić edytor, a następnie z menu Edycja wybrać polecenie Znajdź. Polecenie to odnajdziesz również w menu kontekstowym. Jeśli wolisz posługiwać się klawiszami skrótu, naciśnij [Ctrl F] lub [F3]. Klawisz [F3] jest dodatkowo wykorzystywany do kontynuacji przeszukiwania, gdy odnaleziona wartość nie spełnia oczekiwań.

Po wybraniu polecenia Znajdź edytor wyświetla okno, w którym należy wpisać wyszukiwany tekst. Jeśli interesują cię określone typy obiektów, możesz wybrać poszukiwanie kluczy, wartości lub danych. Zakres wybierasz, zaznaczając odpowiednie pole. Jeśli pamiętasz dokładnie ciąg znaków, który chcesz wyszukać, zaznacz opcję Uwzględnij tylko całe ciągi. Pamiętaj, że edytor rozpoczyna poszukiwania od klucza wskazanego

w lewym panelu. Jeśli chcesz przeszukać cały rejestr, zaznacz obiekt Mój komputer, a następnie naciśnij kombinację [Ctrl F].

Omówmy przeszukiwanie rejestru na prostym przykładzie. Masz zamiar wyłączyć irytującą cię opcję automatycznego uruchamiania programów po umieszczeniu płyty w napędzie CD-ROM. Za wyłączenie autostartu odpowiada wpis AutoRun o wartości 0, umieszczony w kluczu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom. Jeśli nie pamiętasz ścieżki, musisz sięgnąć do polecenia Znajdź. Rozpoczynamy od uruchomienia programu Regedit i zaznaczenia obiektu Mój komputer. Po naciśnięciu [Ctrl F] w pole edycji wpisujesz AutoRun, następnie odznaczasz opcje Klucze i Dane. Żeby uniknąć wieloznaczności poszukiwania, warto zaznaczyć Uwzględnij tylko całe ciągi. Po naciśnięciu Znajdź edytor rozpoczyna pracę. W moim komputerze pierwszym odnalezionym elementem był wpis przy kluczu Command Processor. Dalsze wyszukiwanie rozpoczynasz klawiszem [F3]. Kolejny odnaleziony ciąg znaków na pierwszy rzut oka sprawia wrażenie właściwego. Zanim wprowadzisz poprawkę, upewnij się, że jest to pożądany klucz. Najłatwiej zrobisz to, obserwując ścieżkę umieszczoną na pasku stanu (na dole okna edytora Regedit). Jeśli ścieżka będzie inna niż CurrentControlSet, np. ControlSet001, powinieneś kontynuować poszukiwania. Pamiętaj, że pasek stanu może być ukryty. Włączysz go, zaznaczając opcję Pasek stanu w menu Widok programu Regedit.

Gałęzie, klucze i wartości rejestru



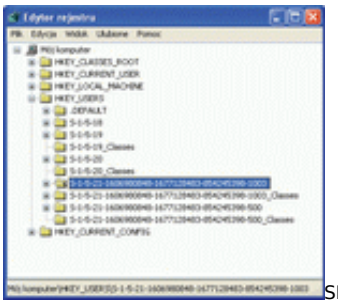
Pięć głównych kluczy.Po uruchomieniu programu Regedit można zaobserwować logiczną strukturę rejestru. Podstawowym elementem tej struktury są klucze. Edytor rejestru opisuje je ikonami folderów. Klucze rejestru mają za zadanie porządkowanie oraz gromadzenie informacji z wybranego zakresu ustawień, dokładnie tak, jak foldery gromadzą pliki związane z aplikacjami lub charakterystyką wskazaną przez użytkownika. Przykładami kluczy, które przechowują dane dotyczące zakresu ustawień będą np. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip, zawierający konfigurację protokołu TCP/IP, albo HKEY_CURRENT_USER\Control Panel\Mouse, ukrywający parametry myszy zalogowanego użytkownika.

Gałęzie to fizyczne części rejestru umieszczone na dysku. Regedit wyświetla klucze bazy konfiguracyjnej tak, że rejestr sprawia wrażenie spójnej całości. Kiedy przechodzisz od klucza do klucza, możesz przemieszczać się pomiędzy wczytanymi do pamięci komputera plikami rejestru. Istnienie gałęzi jest istotne, ponieważ Regedit pozwala na ładowanie i zwalnianie gałęzi. Odpowiednie polecenia odnajdziesz w menu Plik.

Wartości rejestru przechowują dane konfiguracyjne systemu. Klucze można porównać do folderów Windows, natomiast wartości do plików. Każda wartość rejestru ma określony typ. Tak jak system operacyjny rozpoznaje wiele typów plików, np. DOC, JPG, tak w rejestrze typ wskazuje format przechowywanych w wartościach danych. Mogą to być dane binarne lub ciągi znaków. Rejestr potrafi zgromadzić wiele rodzajów danych, ale administrator Windows XP może dodawać do rejestru wartości pięciu typów.

Struktura rejestru jest bardzo podobna do struktury przechowywania danych na dyskach. Tak jak w przypadku partycji, do każdego klucza albo wartości można się odwołać za pomocą odpowiedniej ścieżki. Ścieżki rozpoczynają się od identyfikatora jednego z głównych kluczy głównych. Kolejne elementy są rozdzielane za pomocą lewego ukośnika, przykłady ścieżki do kluczy widziałeś już przy np. wymienionych wcześniej ustawieniach myszy.

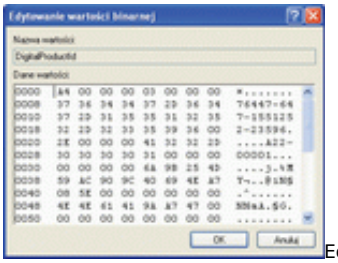
Pięć kluczy głównych


SID użytkownika i SID administratora w kluczu HKEY_USERS.Przedrostek nazwy kluczy głównych - HKEY - jest zapożyczony z języka angielskiego. Handle Key oznacza, że mamy do czynienia z dojściami (handles), które mogą zostać wykorzystane do jednoznacznej identyfikacji zasobu przez aplikacje zewnętrzne. Windows XP zawiera pięć podstawowych kluczy. Zobaczysz je zaraz po uruchomieniu edytora: HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_CURRENT_USER oraz HKEY_CURRENT_CONFIG. Klucze główne zawierają ustawienia użytkownika oraz systemu operacyjnego. W rzeczywistości możemy wyróżnić dwa podstawowe klucze, HKEY_LOCAL_MACHINE i HKEY_USERS. Pozostałe trzy klucze główne, HKEY_ CURRENT_CONFIG, HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, stanowią aliasy (skróty) do wybranych podkluczy w HKEY_LOCAL_MACHINE i HKEY_USERS. Należy pamiętać, że nie są to kopie, lecz aliasy. Jeśli zmienisz np. wartość w HKEY_USERS\SID\Control Panel\Mouse zostanie zmieniona również wartość w HKEY_CURRENT_USER\Control Panel\Mouse. Windows posługuje się aliasami ze względów systemowych. Jedną z przyczyn stosowania skrótów jest to, że aplikacje odwołujące się do ustawień użytkownika nie muszą uzyskiwać dostępu do identyfikatora konta (SID). Wystarczy, że sięgną do klucza HKEY_CURRENT_USER.

Łatwo sprawdzić, do jakich podkluczy odnoszą się HKEY_ CURRENT_CONFIG, HKEY_CLASSES_ROOT i HKEY_CURRENT_USER. Po rozwinięciu klucza HKEY_LOCAL_MACHINE przejdź do podklucza SYSTEM, a następnie do Classes. Po rozwinięciu Classes porównaj jego zawartość z kluczem głównym HKEY_CLASSES_ROOT - jest taka sama. Konto każdego użytkownika systemu Windows XP ma wygenerowany unikatowy identyfikator zabezpieczeń, tzw. SID (Security Identifier). System posługuje się nim w celu weryfikowania uprawnień dostępu użytkownika do zasobów Windows, np. systemu plików NTFS. SID rozpoczyna się od litery S, do której dodawany jest rozdzielany myślnikami ciąg cyfr. Oprócz SID wygenerowanych dla kont użytkowników, jest grupa stałych identyfikatorów, identycznych w każdym systemie. Stałe identyfikatory mają np. takie konta, jak Usługa lokalna - S-1-5-19 lub System lokalny - S-1-5-18. Po przejściu do klucza HKEY_USERS, znajdziesz w nim szereg identyfikatorów zabezpieczeń. Jednym z nich będzie SID przypisany do twojego konta. Jeśli porównasz zawartość klucza HKEY_CURRENT_USER i klucza oznaczonego SID, zobaczysz, że są takie same. Ostatni alias stanowi klucz HKEY_CURRENT_CONFIG związany z kluczem

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current. W czasie pracy z narzędziami do obsługi rejestru możesz spotkać akronimy nazw kluczy. Na przykład dostępny z wiersza poleceń program REG pozwala na odwoływanie się do klucza HKEY_LOCAL_MACHINE za pomocą skrótu HKLM. Listę akronimów kluczy głównych zawiera tabela "Klucze główne i ich akronimy".

HKEY_LOCAL_MACHINE

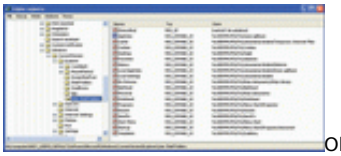


Edycja wartości typu REG_BINARY.Każdy z głównych kluczy rejestru pełni wyznaczone przez system funkcje. Najważniejszy jest HKLM. Przechowuje on informacje dotyczące konfiguracji komputera z Windows XP. Po rozwinięciu HKLM zobaczysz pięć podkluczy: HARDWARE, SAM, SECURITY, SOFTWARE oraz SYSTEM. Są to, z wyjątkiem HARDWARE, tzw. gałęzie. Gałęzie omawiamy w dalszej części artykułu, teraz pokażemy, jakie funkcje pełni każdy z wskazanych podkluczy.

HARDWARE jest jedynym podkluczem HKLM, którego zawartość nie jest przechowywana w pliku na dysku. XP tworzy go dynamicznie w czasie każdego startu systemu. Jak wskazuje nazwa, klucz ten gromadzi informacje opisujące sprzęt komputera. Umieszczono w nim rzadko spotykane w rejestrze typy danych, takie jak REG_FULL_RESOURCE_DESCRIPTOR i REG_RESOURCE_LIST. Odtwarzanie klucza podczas każdego uruchomienia ma ułatwić zbieranie informacji o nowo dodanych urządzeniach i zmianie konfiguracji sprzętowej.

SAM to skrót od Security Account Manager. W kluczu tym Windows XP przechowuje informacje o utworzonych w systemie kontach użytkowników i grup. Jeśli będziesz chciał podejrzeć zawartość klucza SAM, otrzymasz komunikat o braku dostępu. Ponieważ SAM zawiera krytyczne informacje, dostępu do niego nie mają nawet członkowie grupy Administratorzy. Jeśli będziesz chciał koniecznie zobaczyć, co ukrywa klucz SAM, możesz zmienić uprawnienia, korzystając z opcji Uprawnienia w menu Edycja. Klucz SECURITY, tak jak SAM, przechowuje zaszyfrowane informacje związane z zabezpieczeniami komputera - o prawach, lokalnych zasadach haseł oraz o członkostwie grup lokalnych. Jeśli chcesz zobaczyć zawartość klucza SECURITY, także musisz zmienić uprawnienia domyślne. Do modyfikacji zawartości kluczy SAM i SECURITY trzeba stosować odpowiednie narzędzia, takie jak Zasady zabezpieczeń lokalnych czy moduł Zarządzanie komputerem. Ręczna ingerencja w zawartość bazy kont i zabezpieczeń jest zabroniona i najczęściej przyniesie więcej szkody niż pożytku.

Zgodnie z nazwą, klucz SOFTWARE służy do gromadzenia informacji o oprogramowaniu zainstalowanym w Windows XP. Dane programów powinny być przechowywane zgodnie ze standardem PRODUCENT\PROGRAM\WERSJA. Jeśli masz aplikację do odczytywania plików PDF (Acrobat Reader), możesz zobaczyć, że korzysta ona dokładnie z takiego sposobu porządkowania danych. Ważnym podkluczem gałęzi SOFTWARE jest Classes. Odnajdziesz w nim dane dotyczące powiązań rozszerzeń plików z aplikacjami (np. pliki DOC Worda) oraz rejestracji klas obiektów COM (Component Object Model).


Okno rejestru z wartościami typu REG_EXPAND_SZ.Ostatnim z podkluczy HKEY_LOCAL_MACHINE jest SYSTEM. Windows XP przechowuje w nim informacje o zestawach kontrolnych. Są oznaczane przez ControlSet NUMER. Każdy zestaw kontrolny zawiera parametry startowe systemu operacyjnego, ale tylko jeden z nich jest wykorzystywany podczas uruchamiania Windows. O numerze bieżącego zestawu kontrolnego poinformuje cię zawartość klucza Select. Aktualny zestaw będzie oznaczony takim numerem, jaki znajduje się przy wpisie Current. Po naciśnięciu klawisza [F8] w czasie uruchamiania systemu, możesz określić opcje startowe Windows. Jedną z nich jest tzw. Ostatnia znana dobra konfiguracja, czyli zestaw rozruchowy zapisany w momencie ostatniego poprawnego logowania do XP. W kluczu Select rozpoznasz jego numer po wpisie LastKnownGood. Ostatniej dobrej konfiguracji możesz użyć wtedy, gdy zawiedzie rozruch z wykorzystaniem zestawu domyślnego.

HKEY_USERS

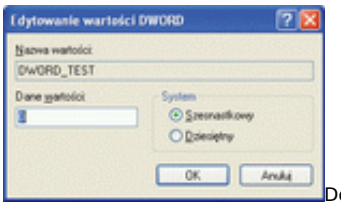
HKEY_USERS gromadzi dane obejmujące ustawienia środowiska użytkowników. Dotyczą one spersonalizowanych parametrów systemu operacyjnego, takich jak: konfiguracja pulpitu, ekranu lub aplikacji. Oprócz informacji związanych z profilem aktualnie zalogowanego użytkownika HKEY_USERS zawiera parametry usługowych kont systemowych np. System lokalny, Usługa lokalna i Usługa sieciowa. Konta systemowe i użytkowników są reprezentowane przez opisywane już Identyfikatory zabezpieczeń (SID). Podklucz .DEFAULT służy do określania ustawień obowiązujących wtedy, kiedy nikt nie jest zalogowany do systemu. Można to łatwo sprawdzić, podłączając się do rejestru przez sieć.


Najpopularniejsze typy wartości spotykane w rejestrze Windows XPJeżeli w kluczu HKEY_USERS odnajdziesz dwa identyfikatory zabezpieczeń, będzie to oznaczać, że jedno z okien zostało otwarte z użyciem usługi Logowanie pomocnicze. Podczas codziennej pracy nie powinieneś korzystać z konta należącego do lokalnej grupy Administratorzy. Stwarza to potencjalne ryzyko niejawnego uruchamiania skryptów modyfikujących ważne ustawienia systemu operacyjnego. Do logowania pomocniczego sięgaj wtedy, gdy zamierzasz wykonać zadania związane z administracją systemu. W celu uruchomienia programu na wyższym poziomie uprawnień musisz kliknąć ikonę aplikacji prawym przyciskiem myszy, a następnie wybrać Uruchom jako. Po wprowadzeniu nazwy konta i hasła Windows uruchomi aplikację z alternatywnymi poświadczeniami.

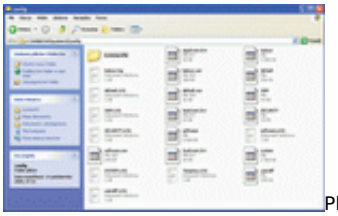
Parametry użytkownika są podzielone na dwie grupy. Pierwszą reprezentuje SID konta, drugą - SID plus przyrostek _Classes. Pod kluczem reprezentowanym przez identyfikator zabezpieczeń ukryte są parametry profilu użytkownika. W czasie przeglądania podkluczy SID znajdziesz między innymi ustawienia Panelu sterowania, konsoli oraz właściwe dla konta zmienne środowiskowe. Klucz z zakończeniem Classes zawiera rejestracje klas i powiązania rozszerzeń plików indywidualnych zalogowanego użytkownika.

Wpisy do rejestru

Administrator komputera może edytować oraz dodawać do rejestru nowe wpisy. Każdy musi mieć nazwę, typ danych oraz wartość. Typ danych określa rodzaj przechowywanych informacji. Rejestr może przechowywać informacje w niemal dwudziestu formatach. W czasie przeglądania bazy konfiguracyjnej systemu może się to wydawać nieco zaskakujące, gdyż zdecydowana większość wpisów opiera się na pięciu typach: REG_DWORD, REG_BINARY, REG_EXPAND_SZ, REG_SZ i REG_MULTI_SZ.



Dodawanie wartości DWORD.Pięć głównych typów wpisów pozwala na przechowywanie najpotrzebniejszych ustawień Windows XP. REG_BINARY jest wykorzystywany do gromadzenia danych binarnych. Są one wyświetlane i wprowadzane do rejestru w formacie szesnastkowym. REG_DWORD służy do przechowywania danych numerycznych. Jego nazwa - DWORD - jest skrótem określenia "double word", co oznacza, że w tym formacie możemy przechowywać cztery bajtowe liczby. Z typem REG_DWORD spotkasz się najczęściej przy okazji wpisów oznaczających prawdę lub fałsz, tak lub nie oraz włączenie albo wyłączenie wybranej opcji. Dodając nową wartość DWORD, możesz się posłużyć formatem szesnastkowym lub dziesiętnym. Kolejne trzy typy danych są przeznaczone do przechowywania ciągów znaków. Najbardziej popularny REG_SZ pozwala na wpisywanie pojedynczego ciągu, np. 'PC WORLD KOMPUTER'. Jego kuzyni: REG_MULTI_SZ i REG_EXPAND_SZ różnią się tym, że pierwszy pozwala na wprowadzanie wielu wierszy ciągów (list), a drugi może zawierać zmienne dynamicznie zastępowane rzeczywistymi wartościami przez sięgające do rejestru aplikacje. Przykładowo wpis %USERPROFILE% jest zastępowany przez ścieżkę do profilu tego użytkownika, który aktualnie pracuje z systemem.


Pliki rejestru umieszczone w folderze \System32\Config.Jeśli korzystasz z edytora Regedit, dodawanie wpisu rozpoczyna się od wskazania typu danych. Po odnalezieniu klucza, w którym chcesz dodać nową wartość, należy kliknąć menu Edycja. Następnie wskaż Nowy i wybierz rodzaj wartości. Regedit wyświetli bardziej zrozumiałe nazwy typów. Możesz wybrać jedną z opcji: Wartość ciągu (REG_SZ), Wartość binarna (REG_BINARY), Wartość DWORD (REG_DWORD), Wartość wielociągu (REG_MULTI_SZ) i Wartość ciągu rozwijalnego (REG_EXPAND_SZ). Po kliknięciu odpowiedniej opcji system dodaje wpis i czeka na wprowadzenie nazwy wartości. Gdy wpiszesz nazwę, musisz ponownie sięgnąć do menu Edycja i wybrać Modyfikuj. Lepszym rozwiązaniem jest naciśnięcie klawisza [Enter] po zaznaczeniu wartości. Edytor wyświetli wówczas okno do wprowadzania danych. Jeśli określiłeś typ danych jako REG_SZ, trzeba wpisać wymagany ciąg znaków. Przy wartościach DWORD możesz wybrać dziesiętny lub szesnastkowy sposób zapisu. Dla REG_BINARY dane musisz wpisywać szesnastkowo. Chcąc usunąć wartości i klucze bazy konfiguracji systemu, wybierz menu Edycja | Usuń lub naciśnij klawisz [Delete].

Gdzie ten rejestr?

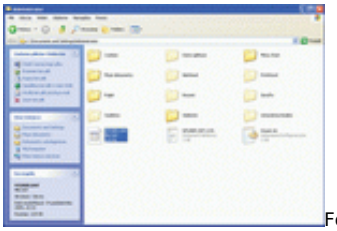
Nazwa "rejestr" sugeruje, że baza konfiguracyjna Windows to jeden plik. Niestety, tak nie jest. Rejestr obejmuje nie tylko ustawienia komputera, ale również informacje o środowisku pracy każdego użytkownika systemu. Jest to jednym z powodów przechowywania bazy ustawień Windows w grupie plików. Nie zapomnij o tym, że część rejestru jest budowana dynamicznie podczas każdego uruchamiania komputera.

Lista plików rejestru zawierająca ustawienia systemuPodział na ustawienia użytkowników oraz systemu w sposób naturalny dzieli miejsce przechowywania plików rejestru na dwie lokalizacje. Część związana z ogólną konfiguracją komputera umieszczona jest w folderze %systemroot%\system32\config, co dla zainstalowanych w sposób domyślny systemów operacyjnych oznacza C:\WINDOWS\system32\config. Jeśli wyświetlisz zawartość tego folderu, możesz być nieco zaskoczony - powinien się tam znajdować jeden plik, a nie ponad dwadzieścia. Pełną zawartość folderu \System32\Config, zobaczysz dopiero po zmianie domyślnych ustawień Eksploratora Windows. W tym celu musisz uruchomić Eksplorator, przejść do menu Narzędzia i wyświetlić Opcje folderów. Następnie przejdź do karty Widok i odznacz Ukryj chronione pliki systemu operacyjnego, dodatkowo należy przenieść zaznaczenie opcji Nie pokazuj ukrytych plików i folderów, na Pokazuj ukryte pliki i foldery. Odznacz również opcję Ukryj rozszerzenia dla plików znanych typów.

Takie pliki, jak AppEvent.evt, SecEvent.evt i SysEvent.evt, to dzienniki programu Podgląd zdarzeń i z punktu widzenia rejestru nie są dla nas interesujące. O wiele ważniejsze są takie pliki, jak System, SAM, software, SECURITY itp. Listę plików i ich przeznaczenie zawiera tabela powyżej.

Pora wskazać miejsce rejestru z danymi użytkownika. Windows pozwala na personalizację ustawień pulpitu. Dzięki tej funkcji możesz zdefiniować własną tapetę, przełączyć ustawienia myszy na układ dla leworęcznych, zmienić zawartość menu Start itp. Wskazane parametry są określane przez odpowiednie aplety Panelu sterowania i zapisywane w profilu użytkownika. Każdy użytkownik Windows XP ma tworzony indywidualny profil podczas pierwszego logowania do systemu. Listę wszystkich profili możesz uzyskać, klikając kolejno: Start | Ustawienia | Panel sterowania | System. Po otworzeniu apletu System przejdź do karty Zaawansowane i kliknij Profile użytkownika | Ustawienia. Jeśli chcesz zobaczyć, gdzie Windows przechowuje profile, musisz otworzyć Eksplorator Windows i odnaleźć folder Dokumenty i ustawienia. Znajduje się w nim grupa podfolderów, których nazwy są nazwami kont użytkowników komputera lokalnego. Jeśli stacja pracuje w sieci, znajdziesz tam również konta domeny systemów Windows NT, 2000 lub 2003. Każdy z folderów użytkowników zawiera ukryty plik NTUSER.DAT, który jest częścią rejestru odpowiedzialną za przechowywanie informacji o konfiguracji każdego z kont.

Zabezpieczanie rejestru


Folder profilu użytkownika Administrator z plikiem rejestru NTUSER.DAT.Bezpieczeństwo rejestru jest jednym z fundamentów ochrony systemu Windows XP. Biorąc pod uwagę możliwość zdalnego dostępu do bazy ustawień, zagrożenie należy uznać za poważne. Nieuprawniony dostęp do bazy konfiguracji komputera może prowadzić do odczytu lub zmiany znaczących informacji. Jeśli nie wykonałeś kopii zapasowej systemu, celowe uszkodzenie rejestru kończy się reinstalacją Windows. Niestety, nieprzemyślana lub zbyt restrykcyjna modyfikacja uprawnień jest również bardzo niebezpieczna. System operacyjny nieustannie komunikuje się ze swoją bazą ustawień i jeśli zabronisz kontom i usługom systemowym sięgać do rejestru, Windows może przestać funkcjonować poprawnie.

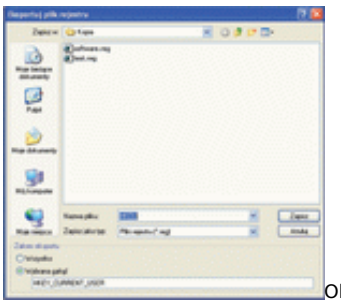
Windows XP chroni rejestr przez nadawanie uprawnień do kluczy i wartości. Jeśli kiedykolwiek konfigurowałeś uprawnienia do systemu plików NTFS, praca z modelem zabezpieczeń stosowanym dla rejestru nie będzie niczym trudnym. Okna i zasady konfiguracji są identyczne, różnicę stanowią typy uprawnień. Windows pozwala na przypisanie dwóch standardowych rodzajów uprawnień, są to Odczyt oraz Pełna kontrola. W czasie instalacji systemu jest nadawana domyślna pula ustawień zabezpieczeń grup systemowych (np. SYSTEM) oraz wbudowanych (np. Administratorzy).

Do przeglądania i zarządzania uprawnieniami wykorzystaj program Regedit. Po uruchomieniu edytora zaznacz klucz, którego właściwości chcesz obejrzeć, następnie w menu Edycja kliknij opcję Uprawnienia. W nowym oknie wyświetlane są grupy kont systemu Windows oraz przypisane im standardowe uprawnienia. Jeśli pola wymienione w kolumnie Zezwalaj lub Odmów są szare, oznacza to, że uprawnienia zostały odziedziczone po jednym z kluczy nadrzędnych. Dziedziczenie umożliwia łatwiejsze zarządzanie zabezpieczeniami. Wystarczy wskazać typ zabezpieczeń na najwyższym kluczu, a uprawnienia automatycznie przeniosą się na wszystkie podklucze rejestru. Dostęp do uprawnień specjalnych uzyskujesz po naciśnięciu przycisku Zaawansowane. W oknie Zaawansowane ustawienia uprawnień możesz dodawać lub edytować pojedyncze rodzaje zabezpieczeń, zarządzać inspekcją, przypisywać nowego właściciela i sprawdzać uprawnienia efektywne. Lista specjalnych zasad dostępu zawiera dziesięć typów uprawnień: Pełna kontrola, Badanie wartości, Ustawianie wartości, Tworzenie podklucza, Wyliczanie podkluczy, Powiadamianie, Tworzenie łącza, Usuń, Zapisywanie DAC, Zapisywanie właściciela oraz Kontrola odczytu. Po zaznaczeniu jednej z opcji i zamknięciu okna system sygnalizuje nadanie pojedynczego uprawnienia przez wyświetlenie znacznika w polu Uprawnienia specjalne.


Okno zabezpieczeń kluczy rejestru.W zaawansowanych opcjach zabezpieczeń odnajdziesz karty Inspekcja, Właściciel oraz Czynne uprawnienia. Służą do zarządzania specyficznymi cechami ochrony rejestru. Jeśli będziesz chciał monitorować dostęp do poszczególnych informacji gromadzonych w rejestrze, inspekcja odda ci nieocenione usługi. W zależności od wybranych ustawień i obiektów, możesz sprawdzać, kto, kiedy i w jaki sposób sięgał do kluczy rejestru. Implementacja inspekcji jest dwuetapowa. Na początku musisz wyedytować Zasady zabezpieczeń lokalnych. Odnajdziesz je, klikając Narzędzia administracyjne w Panelu sterowania. Po uruchomieniu konsoli Zasad należy wybrać Ustawienia zabezpieczeń | Zasady lokalne | Zasady zabezpieczeń. Na wyświetlonej liście musisz odnaleźć i włączyć Zasady dostępu do obiektów. Po zamknięciu wszystkich okien dalsze zarządzanie inspekcją wykonujesz na karcie Inspekcja edytora Regedit. Naciskając przycisk Dodaj, wskazujesz, kogo i w jakim zakresie chcesz obserwować. Wyniki inspekcji dostępu do rejestru są zapisywane w dzienniku Zabezpieczenia programu Podgląd zdarzeń. Pamiętaj, że za szeroki zakres monitorowania będzie powodował wiele wpisów w dzienniku i może doprowadzić do spadku wydajności systemu.

Karta Właściciel jest przeznaczona do zmiany właściciela kluczy w rejestrze. Domyślnie właścicielami są członkowie lokalnej grupy Administratorzy. Modyfikacja tej opcji powinna być wykonywana jedynie wtedy, gdy chcesz uzyskać dostęp do kluczy rejestru, które zostały założone przez innych użytkowników, a twoje konto nie ma do nich uprawnień. Przeglądanie zawartości karty Czynne uprawnienia jest bardzo przydatne w przypadku serwerów sieci komputerowych. Weryfikacja czynnych uprawnień w systemach z wieloma grupami i użytkownikami pozwala na szybkie ustalenie, jakie są efektywne możliwości każdego z kont.

Więcej kopii, mniej zmartwień


Okno dialogowe eksportowania kluczy rejestru.W systemie Windows XP nie możesz bezkarnie bawić się rejestrem. Musisz być ostrożny jak saper, bo jeśli popełnisz błąd, skutki mogą być natychmiastowe i często nieodwracalne. W przypadku uszkodzenia rejestru konsekwencje będą równie poważne. Na szczęście system operacyjny oferuje mnóstwo sposobów na skuteczne zabezpieczenie się przed awarią zawinioną przez sprzęt lub użytkownika.

Zanim zabierzesz się za wykonywanie kopii zapasowej, zdecyduj, o jaką ochronę danych ci chodzi. W przypadku drobnych modyfikacji

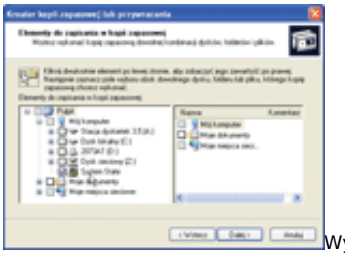
wystarczy prosta kopia fragmentu bazy systemowej. Jeśli liczysz się z możliwością poważnego uszkodzenia systemu, wykonaj kopię stanu systemu lub Windows XP.

Do każdego ze sposobów zabezpieczania się przed awarią system oferuje różne narzędzia. Do nieskomplikowanych czynności ochrony wybranych kluczy możesz wykorzystać mechanizmy wbudowane w Regedit. Gdy potrzebujesz bardziej zaawansowanych kopii, trzeba skorzystać z innych narzędzi Windows. Niekiedy do szybkiej reanimacji komputera potrzebne będą narzędzia zewnętrzne, które można pobrać z Internetu.

Podstawowa ochrona kluczy rejestru


Odtwarzanie punktu przywracania systemu.Zabezpieczenie się przed skutkami błędów to podstawa działania. Czasami wystarczy nie zwrócić uwagi na ścieżkę do klucza i kłopot gotowy. Jeżeli modyfikujesz rejestr po to, żeby wprowadzić drobne zmiany parametrów Windows XP, przeważnie nie potrzeba pełnej archiwizacji danych komputera. Wystarczy sięgnąć do programu Regedit, który pozwala na kopiowanie danych oraz eksportowanie kluczy rejestru.

Zanim zmodyfikujesz wartość dowolnego klucza, zrób jej kopię. Uwaga ta dotyczy przede wszystkim wartości typów innych niż DWORD. Zmiana 0 na 1 jest prosta do odtworzenia. Gorzej, gdy zmienisz wartość REG_BINARY, jej odtworzenie z pamięci, jest raczej trudne. W celu skopiowania nazwy wartości musisz wykonać kilka prostych operacji edycyjnych. Na początek należy zmienić nazwę oryginalnej wartości na taką, która będzie wskazywać, że jest to kopia, np. DigitalProductId na DigitalProductId_bak. Następnie dodajesz nowy wpis tego samego typu, co zmodyfikowana wartość np. REG_BINARY. Nazwa wprowadzanej wartości również powinna być taka sama, w naszym przykładzie DigitalProductId. Pamiętaj, że wpisując nazwę, zawsze można popełnić błąd, dlatego do edycji nazwy lepiej użyć klawisza [F2], a do skopiowania - standardowej kombinacji [Ctrl+C]. Po nadaniu nazwy należy skopiować jej zawartość. I w tym wypadku można wykorzystać kombinację klawiszy. Okno zawierające dane obsługuje stosowanie skrótów [Ctrl C], [Ctrl X] i [Ctrl V], a w menu podręcznym znajduje się opcja Zaznacz wszystko. Gdy kopiowanie wartości zostanie zakończone, możesz przejść do modyfikacji parametru rejestru.


Wybór opcji System State podczas wykonywania kopii zapasowej.Innym sposobem na uniknięcie kłopotów jest wyeksportowanie kluczy rejestru do pliku. Po wprowadzeniu nieudanych zmian, będziesz mógł szybko przywrócić zawartość klucza. Istotną różnicą między kopiowaniem a eksportem jest to, że eksport jest wykonywany w odniesieniu do kluczy, a nie wartości. Oznacza to, że możesz wyeksportować niewielki wskazany zakres albo całą gałąź rejestru. Po uruchomieniu programu Regedit zaznacz klucz do skopiowania, następnie z menu Plik wybierz Eksportuj. W nowym oknie dialogowym podaj lokalizację, nazwę, zakres eksportu oraz format zapisywanego pliku - REG, REG w trybie zgodności z Windows NT i 95, gałąź rejestru lub TXT. Jeśli chcesz zachować fragment ustawień, posłuż się formatem REG. Choć edytor rejestru pozwala na wyeksportowanie całości ustawień do pliku tekstowego, nie jest to zalecane ze względu na wydajność. Eksportując więcej danych, należy się posłużyć formatem gałęzi. Typ wykorzystywany do zapisu kluczy ma istotne znaczenie w czasie odtwarzania informacji z zapisanych plików. Podczas importu danych z plików REG system posługuje się ustaloną logiką scalania, zależną od tego, czy plik zawiera wartości znajdujące się w rejestrze, czy nie. Wartości znajdujące się w bazie są zastępowane przez dane z pliku, jeżeli mają taką samą nazwę i typ. Wartość, której nie ma w pliku, a jest w rejestrze, będzie pozostawiona w stanie nienaruszonym. Natomiast gdy wpisów znajdujących się w importowanym pliku nie ma w bazie, zostaną dodane do rejestru. Jeśli zapomnisz o wymienionych zależnościach, może się okazać, że eksport danych i ich późniejszy import nie przywróci rejestru do stanu pierwotnego. Opisywany problem nie ma znaczenia podczas eksportu i importu dla typu gałęzi.

Punkty przywracania systemu

Regedit nie oferuje nic więcej ponad podstawowe sposoby unikania kłopotów z rejestrem. Bardziej zaawansowane metody rozwiązywania problemów są zawarte w innych komponentach systemu Windows XP. Jednym z najwygodniejszych jest Przywracanie systemu. Zamiast poświęcać czas na ręczne kopiowanie kluczy lub manipulowanie wprowadzanymi wartościami, możesz szybko utworzyć punkt przywracania. Cały kłopot w tym, aby punkt przywracania powstał, zanim rejestr ulegnie destrukcji.

Jeśli jeszcze nie korzystałeś z Przywracania systemu, zdziwisz się, jak niewiele trzeba, aby się zabezpieczyć przed potencjalnymi problemami. Wystarczy nieco miejsca na dysku, standardowo 12 procent jego pojemności. Jeśli masz mały dysk, każda ilość jego przestrzeni ma fundamentalne znaczenie i kilkaset megabajtów to dużo. Jednak dyski poniżej 4 GB to odległa przeszłość, a 12 procent można spokojnie zredukować na karcie Przywracanie systemu we właściwościach apletu System.

Utworzenie punktu przywracania to operacja wykonywana za pomocą prostego kreatora. W menu Akcesoria kliknij Narzędzia systemowe, a następnie Przywracanie systemu. Pierwsze okno kreatora służy do wskazania rodzaju zamierzonych zadań. Możesz przywrócić komputer do poprzedniego stanu lub ręcznie utworzyć nowy punkt przywracania. System został tak zaprojektowany, aby automatycznie tworzyć punkty przywracania. Jeśli będziesz miał trochę szczęścia, wycofasz zmiany nawet bez ręcznego utworzenia punktu. Realizacja szybkiej kopii bazy ustawień Windows polega na zaznaczeniu opcji Utwórz punkt przywracania. Po naciśnięciu Dalej wprowadź czytelną nazwę punktu i kliknij Utwórz. Te proste czynności umożliwiają niemal bezpieczne modyfikacje rejestru. Odtwarzanie danych przez usługę przywracania, jest wykonywane za pomocą tego samego kreatora. Po uruchomieniu Przywracania systemu zaznacz opcję Przywróć system do wcześniejszego stanu i naciśnij przycisk Dalej. W nowym oknie wybierz jeden z proponowanych przez system punktów, następnie potwierdź proponowany wybór. System rozpocznie odtwarzanie.

Kopia zapasowa i konsola odzyskiwania systemu

Przywracanie systemu ma jedną poważną słabość. Jeśli po naniesionych przez ciebie zmianach lub na skutek uszkodzeniu rejestru XP się nie

uruchomi, wykonane punkty przywracania są mało przydatne. Tak czy tak, będziesz musiał poświęcić sporo czasu na powtórną instalację systemu operacyjnego. Rozwiązaniem, które może wyeliminować ten kłopot, jest wykonanie kopii zapasowej stanu systemu lub kopii automatycznego odzyskiwania systemu. Na pierwszy rzut oka jest to propozycja bez większego sensu. Jeśli uszkodzenie systemu będzie na tyle poważne, że Windows się nie uruchomi, szybkie odtworzenie danych wydaje się niemożliwe. Aby odtworzyć rejestr, trzeba zainstalować powtórnie system. Twierdzenie to jest jak najbardziej prawdziwe, gdy pominiemy jedną istotną funkcję backupu. W czasie wykonywania kopii zapasowej stanu systemu Windows realizuje dodatkowe czynności, o których nie informuje użytkowników. Jedną z nich jest automatyczne sporządzenie kopii plików rejestru.

Bezpośrednio w katalogu Windows możesz odnaleźć folder Repair. Jest to miejsce, do którego kopiowany jest rejestr systemu. Jeśli nigdy nie wykonasz kopii zapasowej, w katalogu będzie się znajdować archiwum rejestru z momentu instalacji Windows. Po sporządzeniu kopii stanu systemu lub automatycznego odzyskiwania systemu, zawartość folderu Repair jest uaktualniana. Dzięki temu możesz odtworzyć rejestr bez reinstalacji Windows. Jeżeli uszkodzenie systemu będzie na tyle poważne, że archiwum rejestru nie wystarczy do naprawy XP, to kopia stanu Windows pomoże wrócić do ustawień sprzed awarii.

Wykonanie kopii stanu systemu jest bardzo proste. Rozpocznij od uruchomienia narzędzia Kopia zapasowa. W tym celu po kolei wybierz Start | Wszystkie programy | Akcesoria | Narzędzia systemowe | Kopia zapasowa. W oknie powitalnym Kreatora kopii zapasowej lub przywracania naciśnij Dalej. Wybierz polecenie Wykonaj kopię zapasową plików i ustawień, a następnie Pozwól mi wybrać, co ma zawierać kopia zapasowa. W oknie Elementy do zapisania w kopii zapasowej rozwiń obiekt Mój komputer i zaznacz System State. Po naciśnięciu Dalej musisz wskazać lokalizację i nazwę kopii. Jeśli chcesz natychmiast rozpocząć sporządzanie archiwum, naciśnij Zakończ. Ponieważ kopia stanu Windows zajmuje dużo miejsca, szybkość twojego komputera będzie jednym z czynników wyznaczających czas jej trwania. Gdy archiwizacja zostanie zakończona, możesz sprawdzić zawartość folderu Repair. Znajdziesz w nim uaktualnione kopie plików rejestru.

Jeżeli Windows działa na tyle poprawnie, że pozwala na zalogowanie użytkownika, do odtworzenia kopii stanu systemu wykorzystaj narzędzie Kopia zapasowa. Jeśli każda próba startu zakończy się niepowodzeniem, będziesz musiał odtworzyć rejestr z Konsoli odzyskiwania. Najszybszym sposobem na uruchomienie konsoli jest start systemu z płyty instalacyjnej. W oknie powitalnym instalatora musisz nacisnąć klawisz [R]. XP przerwie instalację i przełączy cię w tryb tekstowy. Po wskazaniu, do którego systemu chcesz się podłączyć, należy podać hasło Administratora. Jeśli podasz je poprawnie, system uruchomi odpowiednik wiersza poleceń. Dalsze czynności polegają na zastąpieniu uszkodzonej gałęzi rejestru tą, która jest przechowywana w katalogu Repair. Jeśli np. zostanie uszkodzona gałąź System, należy po kolei wpisać następujące polecenia: REN C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM.BAK, COPY C:\WINDOWS\REPAIR\SYSTEM C:\WINDOWS\SYSTEM32\CONFIG\. Pierwsze służy do zmiany nazwy starej gałęzi SYSTEM na SYSTEM.BAK, drugie kopiuje gałąź z folderu Repair do folderu C:\WINDOWS\SYSTEM32\CONFIG. Jeśli otrzymasz komunikat o poprawnym skopiowaniu pliku, możesz wpisać polecenie EXIT i system zostanie ponownie uruchomiony. Pamiętaj, że konsola odzyskiwania może zostać zainstalowana na stałe. W czasie każdego uruchamiania systemu będziesz mógł wybrać, czy chcesz uruchomić Windows XP, czy konsolę odzyskiwania. Konsolę dodasz, uruchamiając z płyty instalacyjnej polecenie i386\Winnt32.exe /cmdcons.

UWAGA!
W edytorze Regedit nie znajdziesz opcji Cofnij. Wszystkie działania są wykonywane bezpośrednio na lokalnym rejestrze komputera. Jeśli przez przypadek usuniesz jeden z kluczy, nie będziesz miał możliwości szybkiego i prostego odzyskania utraconych wpisów. Zanim zaczniesz pracę z edytorem, koniecznie wykonaj kopię zapasową. Brak aktualnego archiwum może się zakończyć małą katastrofą, czyli reinstalacją Windows XP.

UWAGA!
Jeśli chcesz szybko się dowiedzieć, jaki identyfikator SID ma twoje konto, możesz skorzystać z wbudowanego w Windows XP narzędzia wiersza poleceń WHOAMI. WHOAMI oferuje wiele interesujących przełączników, które wyświetlą informacje o użytkowniku aktualnie zalogowanym do Windows XP. Po wprowadzeniu polecenia WHOAMI /USER /SID, otrzymasz swój identyfikator, np. S-1-5-21-1645522239-706699826-1060284298-1003. Pełną listę informacji zwracanych przez WHOAMI uzyskasz po wpisaniu WHOAMI /? lub WHOAMI /HELP.

UWAGA!
Jeśli chcesz zabronić dostępu do rejestru swojego komputera, wykonaj kilka prostych czynności. Użytkownicy innych komputerów w sieci mogą się łączyć z twoją stacją, jeśli spełnione są dwa warunki. Po pierwsze, muszą mieć odpowiednie uprawnienia, czyli konto, na którym pracują, musi należeć np. do grupy Administratorzy. Po drugie, za umożliwienie dostępu do rejestru odpowiada usługa Rejestr zdalny. Jeśli ją wyłączysz, tylko użytkownicy zalogowani lokalnie będą mogli przeglądać i modyfikować zawartość rejestru. W celu wyłączenia usługi należy po kolei kliknąć Start | Ustawienia | Panel sterowania | Narzędzia administracyjne | Usługi, następnie na liście usług odnaleźć Rejestr zdalny i z menu Akcja wybrać Właściwości. W wyświetlonym oknie rozwiń listę przy opcji Tryb uruchamiania i wybierz Wyłączony. Jeśli w czasie modyfikacji usługa jest uruchomiona, dodatkowo możesz ją zatrzymać naciśnięciem przycisku Stop.

Uprawnienia do rejestru
Bez istotnego powodu nie należy zmieniać uprawnień do rejestru. Modyfikacja będzie konieczna wtedy, gdy zainstalowane w Windows aplikacje wymagają dodatkowych uprawnień. Zanim przejdziesz do zmiany ustawień, zapoznaj się dokładnie z dokumentacją lub zaleceniami producenta programu oraz bezwzględnie wykonaj kopię zapasową rejestru! Zabranianie dostępu przy użyciu opcji Odmów jest wyjątkowo niebezpieczne. Jeśli odmówisz pełnej kontroli jednej z grup systemowych, np. Wszyscy, możesz sam paść ofiarą swoich nieprzemyślanych działań.

Przykładowa modyfikacja rejestru (1)
Jeśli Windows XP ma zainstalowany interfejs sieciowy, domyślnie włączana jest usługa Udostępnianie plików i drukarek w sieciach Microsoft. System automatycznie tworzy tzw. udostępnienia administracyjne, które pozwalają na dostęp przez sieć do wszystkich partycji dysków komputera. Jeśli np. twój dysk będzie podzielony na dwie partycje C i D, wówczas zostaną utworzone udostępnienia C$ i D$. Możesz to łatwo sprawdzić: w Panelu sterowania przejdź do Narzędzi administracyjnych, następnie dwukrotnie kliknij Zarządzanie komputerem i kolejno Narzędzia systemowe | Foldery udostępnione | Udziały. Wyświetlona w prawym panelu lista udostępnień powinna zawierać pozycje C$ i D$. Udziały te gwarantują pełny dostęp do zasobów partycji wszystkim członkom grupy Administratorzy. Najważniejsze, że udostępnień tych nie można w prosty sposób wyłączyć. Gdy chcesz trwale wyeliminować udostępnienia administracyjne, należy zmienić odpowiednią wartość w rejestrze. Zacznij od odnalezienia właściwego klucza. Dla XP będzie to HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters. Po odszukaniu klucza należy dodać wpis typu DWORD o nazwie AutoShareWks z wartością 0. Po restarcie usługi Serwer automatyczne udostępnienia administracyjne znikną. Restart możesz wykonać, korzystając z modułu Usługi w Narzędziach administracyjnych lub po wpisaniu

w wierszu poleceń NET STOP server i NET START server.

Przykładowa modyfikacja rejestru (2)
UWAGA! Jeśli tęsknisz za widokiem ekranu wyświetlającego błąd zatrzymania, tzw. Blue Screen, możesz go wywołać w dowolnym momencie. Wystarczy dodać odpowiednie wpisy w rejestrze. Po uruchomieniu programu Regedit przejdź do klucza HKLM\System\CurrentControlSet\Services\i8042prt\Parameters\.

Następnie dodaj wartość typu Dword CrashOnCtrlScroll i wprowadź 1. Po restarcie systemu naciśnij kombinację klawiszy [Ctrl] i dwukrotnie [Scroll Lock]. Jeśli nie popełniłeś błędu, wpisując nazwę klucza, system powinien wygenerować błąd zatrzymania.