ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

REGISTR OS MS WINDOWS XP

Bakalářská práce

Praha 2008

Vedoucí práce: Ing. Jiří Vaněk, Ph.D.
Vypracoval: Oldřich Uhlíř

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Registr OS MS Windows XP“ vypracoval samostatně, pouze za odborného vedení vedoucího bakalářské práce.

Dále prohlašuji, že veškeré podklady, ze kterých jsem čerpal, jsou uvedeny v seznamu použité literatury.

V Praze, dne 6.5.2008 Podpis …….

Poděkování

Rád bych poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za jeho cenné připomínky, odborné vedení, ochotu a trpělivost při vedení mé bakalářské práce.

Název

Registr OS MS Windows XP

Souhrn

Práce se zabývá registrem operačního systému Microsoft Windows XP. Rozebírá jeho historii, architekturu, správu, praktické použití a zabezpečení. Na závěr se zabývá jeho srovnáním s ostatními verzemi operačních systémů Microsoft Windows a zamýšlí nad jejich budoucností.

Klíčová slova

registr, operační systém, Microsoft Windows XP, editor registru, klíč registru

Title

OS MS Windows XP Registry

Summary

This bachelor work deals with registry of operating system Microsoft Windows XP. It analyzes its history, architecture, control, practical use and security. In the end, the work compares the registry of Microsoft Windows XP with other versions of Windows operating systems and considers their future.

Key words

registry, operating system, Microsoft Windows XP, registry editor, registry key

Obsah

1. Úvod

Každý, kdo používá informační technologie, se již bezesporu setkal s produkty firmy Microsoft. Firma Microsoft je v oblasti softwaru, konkrétně operačních systémů pro PC, bezpochyby neznámější. Byla založena Williamem Henry Gatesem III (narozen 28.10.1955) v roce 1975. Jejím hlavním produktem byl tehdy interpret Basic pro počítače Altair.

Operační systém Windows XP byl poprvé uvolněn 25.10. 2001. Zkratka XP vychází z anglického slova experience, což znamená zkušenost. Vyvíjen byl pod kódovým označením Whistler. Jedná se o grafický víceúlohový (multitaskingový) operační systém, který je založen na kódovém základu systémů Windows NT a Windows 2000. Jeho architektura je 32bitová, krom variant „64-bit Edition“ a „Professional x64 Edition“, kde je 64bitová. Jedná se o první systém společnosti Microsoft, který je určen jak koncovým uživatelům, tak firmám, v závislosti na edici. Do současnosti vyšel v těchto edicích:

- **Windows XP Professional Edition** – určena zejména pro firmy
- **Windows XP Home Edition** – určena pro běžné koncové uživatele
- **Windows XP 64-bit Edition** – určena pro procesory Intel Itanium
- **Windows XP Professional x64 Edition** – určena pro procesory x86-64
- **Windows XP Media Center 2005** – určena pro HTPC (Home Theather PC) – multimediální počítače
- **Windows XP Tablet Edition** – určena pro Tablet PC
- **Windows XP Corporate** – určena pro korporace, dostupná v rámci multilicence jako předaktivovaná
- **Windows XP Embedded** – určena pro vestavěná zařízení jako např. terminály, bankomaty apod., snadno upravitelná
- **Windows Fundamentals for Legacy PCs** – určena pro starší počítače, nenáročná, snadno upravitelná
- **Windows XP Starter Edition** – určena pro trhy s velkou mírou počítačového pirátství (např. Thajsko), značně omezena o funkce
- **Windows XP Edition N** – určena všem zákazníkům, vznikla na základě nátlaku Evropské komise, došlo u ní pouze k odebrání přehrávače Windows Media Player

Od svého uvedení na trh se dočkal dvou aktualizačních balíčků (service packy), které nejen výrazně upravily jeho stabilitu, vzhled a funkce, ale opravily i

spoustu chyb (zejména v zabezpečení), které původní verze obsahovala. Poslední, třetí, balíček je již k dispozici na serveru Windows Update (únor 2008), ale pouze jako testovací, ve verzi RC1 (Release Candidate – kandidát na vydání). Jeho finální verze by se měla objevit v polovině roku 2008.

Oproti předchozím verzím Windows přináší XP spoustu nových prvků. Mezi ty hlavní patří:

- **Podpora dvou procesorů** (symetricky zapojených)
- **Podpora až 4GB RAM**
- **Režim spánku –** Umožňuje podle nastaveného času nebo na vyžádání uložit aplikace na disk a vypnout počítač od zdroje. Po obnově napájení se všechny aplikace otevřou v tom stavu, v jakém byly před vypnutím.
- **Vzdálená plocha** – Pomocí protokolu RDP (Microsoft Remote Desktop Protocol) umožňuje uživateli vytvořit virtuální relaci na vlastním počítači.
- **Vzdálená pomoc** - Umožňuje uživateli využít pro správu počítače pomoc jiné osoby v síti nebo Internetu.
- **Integrovaná podpora vypalování CD/DVD**
- **Instalační služba -** Systémová služba, která pomáhá uživateli instalovat, konfigurovat, nalézt, aktualizovat a odebrat software správným způsobem.
- **Rychlé přepínání uživatelů**
- **Služba zabezpečení protokolu IP (IPSec)** – Pomáhá chránit data přenášená v síťi, umožňuje snadné nastavení VPN (Virtual Private Network – virtuální soukromá síť).
- **Funkce Obnovení systému** – Umožňuje obnovit předchozí konfiguraci uloženou v bodech obnovení.
- **.NET** – Nové programátorské rozhraní.
- **Podpora karet SmartCard**
- **Technologie ClearType -** Nová technologie pro zobrazování textu, která ztrojnásobuje horizontální rozlišení při softwarovém vykreslování textu.
- **Zobrazení na 2 monitorech**

Došlo také k vylepšení prvků v předchozích verzích již obsažených. Z nich nejvýraznější je asi přepracování grafického rozhraní (přihlašovacího okna, nabídky start, ovládacích panelů, ikon atd.), vylepšení PnP Manageru, snadnější sdílení souborů, nové verze integrovaných programů (např. Windows Messenger, Windows Media Player), podpora nových protokolů (např. Kerberos), vylepšené ověřování ovladačů zařízení a vylepšená ochrana kódu (klíčové struktury jádra lze použít jen ke čtení). Došlo také k výraznému zrychlení bootovací sekvence

(SP3 by to měl ještě vylepšit). Výrazná změna též nastala v registru a to zejména díky přepracování jádra a vlivem nových funkcí.

V dnešní době je Windows XP, i přes vydání novějších Windows Vista, patrně stále ještě nejrozšířenějším operačním systémem pro PC.

V této práci se budu zabývat edicí Windows XP Professional, jelikož z hlediska využití registru nabízí nejširší uplatnění.

2. Cíl práce a metodika

Cílem této práce bude charakterizovat a přiblížit registr operačního systému Microsoft Windows XP. Přiblížit jeho historii, architekturu a zabezpečení, seznámit s prací v něm a poukázat na jeho změny v rámci vývoje jednotlivých operačních systémů Microsoft.

V úvodu se bude zaměřovat na historii a roli registru, a to jak z globálního hlediska, tak z hlediska operačních systémů Microsoft. Následně bude rozebírat strukturu a organizaci registru, dále správu a praktické využití registru z uživatelského hlediska. Na závěr se bude zabývat srovnáním registru v jednotlivých verzích operačních systémů Microsoft a zamýšlet se nad jejich budoucím vývojem. U většiny kapitol budou pro názornost uvedeny konkrétní příklady dané problematiky, případně rady a tipy, které by měly uživateli práci s registrem zpříjemnit.

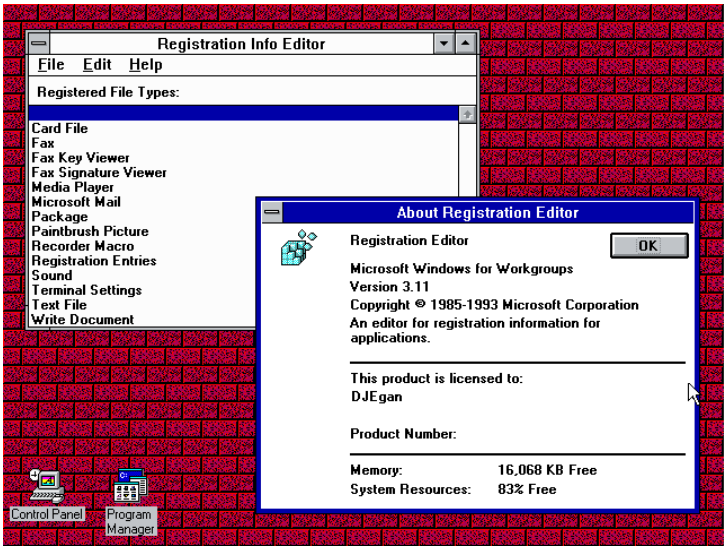
3. Historie a role registru

Slovník *Microsoft Computer Dictionary*, páté vydání, definuje registr jako: Centrální hierarchickou databázi, která se používá v operačních systémech Microsoft Windows 98, Windows CE, Windows NT a Windows 2000 a slouží k ukládání informací potřebných ke konfiguraci systému pro jednoho či více uživatelů, aplikací a hardwarových zařízení. [10]

3.1 Vznik a vývoj

Prvním systémem, který byl z hlediska vzniku registru podstatný, byl Microsoft Windows 3.1. Tento systém obsahoval 3 typy konfiguračních souborů:

- **soubory pro inicializaci systému** – *Control.ini*, *Progman.ini* (inicializační nastavení pro Windows Program Manager), *Protocol.ini* (ukládání inicializačního nastavení pro sítě Windows; přidán až ve verzi Microsoft Windows for Workgroups 3.1x), *System.ini* (ukládání systémových informací souvisejících s hardwarem), *Win.ini* (informace o konfiguraci nainstalovaného softwaru), *Winfile.ini* (nastavení Windows File Manager).
- **samotné inicializační soubory** – Soubory INI přidané nainstalovanými aplikacemi sloužící k ukládání informací souvisejících s danou aplikací.
- **soubor Reg.dat** - Přímý předchůdce dnešních registrů; soubor obsahující hierarchickou databázi s kořenovou strukturou HKEY_CLASSES_ROOT, která ukládá systémové informace pro podporu OLE (Object Linking and Embedding – jedná se o technologii, která umožňuje vkládání a spojování dokumentů s jinými objekty.Například umožňuje. editoru vyjmout část dokumentu do jiného editoru a poté ji znovu importovat. [11]) a svazky souborů. Tato databáze umožňuje upravovat chování objektů a nabízí možnost zobrazit seznam aplikací, které jsou v prostředí systému registrovány. Jedná se o binární soubor, který lze upravovat např. pomocí aplikace Registry Editor (Regedit.exe). Struktura této databáze byla podstatně jednodušší než struktura dnešních registrů. [1][15]



Obrázek č.1: Editor registru ve Windows 3.11 [28]

Registr vznikl právě jako následovník těchto souborů INI a souboru Reg.dat a jako takový byl poprvé použit v Microsoft Windows NT 3.5. Jeho vznik byl tedy dán problémy, které při používání INI souborů v systému nastaly. Zde je jejich stručný výčet:

- neustálé narůstání jejich počtu
- náročné upravování parametrů
- nedostatečná ochrana proti zápisu a smazání
- neexistence podpory pro víceuživatelské prostředí
- neexistence podpory Plug and Play

V systému Windows 98 se soubory registru nazývají *User.dat* a *System.dat*. V systému Windows Millennium Edition se soubory registru nazývají *Classes.dat*, *User.dat* a *System.dat*. [10]

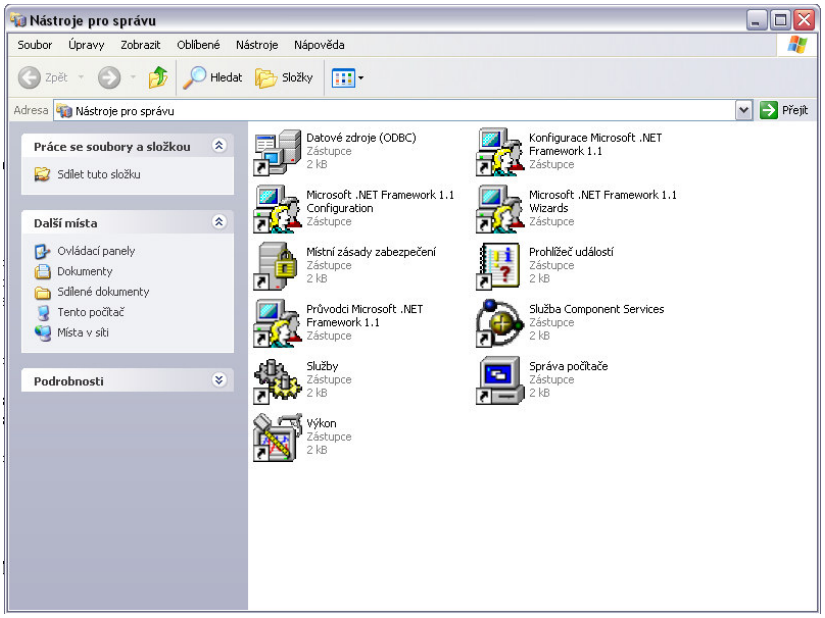
3.2 Využití v rámci OS

Z hlediska využití v rámci OS má registr klíčovou roli. Týká se hlavně 2 oblastí. První oblastí je proces zavádění systému. Druhou oblastí je pak možnost jeho úprav, ať už se jedná o systémové změny či jen kontextové. Tuto oblast podrobně rozeberou kapitoly následující.

Registr obsahuje informace, které systém Windows neustále používá během operací, jako jsou například profily jednotlivých uživatelů, aplikace nainstalované v počítači a typy dokumentů, které mohou jednotlivé aplikace vytvářet, nastavení stránek, vlastností složky a ikon aplikací, informace o hardwaru existujícím v systému a o používaných portech.

Jakožto centralizovaná databáze obsahující klíčová data je neustále využívána systémem, a to jak pro čtení, tak pro zápis. [25] Využívá ho jak jádro, tak aplikace systému. Následuje stručný popis systémových součástí Windows XP, které registr používají:

- **Instalační programy** – Při spuštění instalačního programu tento přečte informace registru, zjistí zda jsou k dispozici všechny součásti potřebné pro úspěšné dokončení instalace a následně jsou do registru přidána nová konfigurační data.
- **Rozpoznání hardwaru –** Při každém spuštění systému vytvoří seznam zjištěných zařízení a uloží jej do registru. Toto zajišťují *Ntdetect.com* a *Ntoskrnl.exe* (jádro Windows XP).
- **Jádro Windows XP –** Při spouštění systému čte registr za účelem získání informací o ovladačích zařízení a pořadí jejich zavedení.
- **PnP Manager –** Zjišťuje a identifikuje hardwarová zařízení pomocí VID (identifikátor výrobce) a DID (identifikátor zařízení). Následně požádá registr o informace o sběrnici, na níž identifikátory zařízení nalezly a zkontroluje, zda byly nainstalovány příslušné ovladače.[1][15]
- **Ovladače zařízení –** Vyměňují si spouštěcí parametry a konfigurační data s registrem (včetně přerušení a přímého přístupu do paměti). Tato data jsou pak zahrnuta do registru a jsou použitelná pro čtení programy a ovladači.
- **Nástroje pro správu –** Nástroje sloužící k upravování registru systému. Jejich výčet se může lišit v závislosti na instalovaných součástech systému.



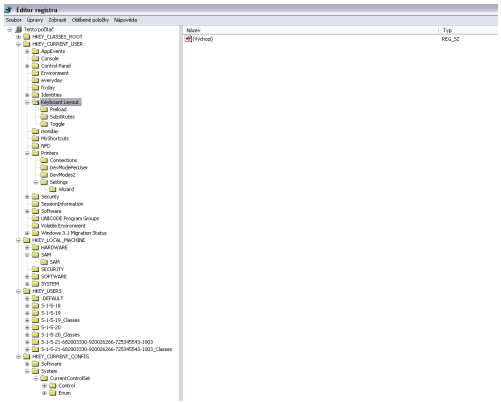
Obrázek č.2 : Nástroje pro správu systému Windows XP

- **Profily uživatelů –** Slouží k vytváření a upravování uživatelských profilů. Každý profil obsahuje uživatelské jméno a přiřazená práva. Tyto informace jsou uloženy v registru.
- **Hardwarové profily –** Jedná se o sady instrukcí použitých k definování ovladačů zařízení, které musí být zavedeny při spuštění systému. Při instalaci systému je vytvořen standardní hardwarový profil, který zahrnuje informace o veškerém hardwaru zjištěném v době instalace. Registr podporuje více konfigurací hardwaru, resp. hardwarových profilů. [1]

4. Struktura registru

Struktura registru je velmi podobná struktuře systému souborů Windows. Jedná se o strukturu hierarchickou, která je rozdělena na klíče, jejich hodnoty a datové typy.

Obsah registrů ve dvou různých počítačích se může zásadně odlišovat podle toho, jaké programy, zařízení a služby jsou v těchto počítačích instalovány.



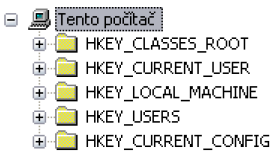
Obrázek č.3: Struktura registru zobrazená pomocí editoru registru

4.1 Klíče

Při zachování příměru ke struktuře systému souborů, lze klíče přirovnat ke složkám. Platí pro ně stejná pravidla jako pro přidělování názvů souborů. Tato podobnost se týká i cest k jednotlivým klíčům.

Základní rozdělení klíčů je na:

- **Kořenové** (umístěny na vrcholu hierarchické struktury) – obrázek č. 4
- **Podklíče** (klíče podřazené klíčům jiným, např. kořenovým)



Obrázek č. 4: Kořenové klíče registru

Názvy všech kořenových klíčů začínají předponou HKEY_. Tato předpona slouží vývojářům softwaru jako označení popisovačů, které mohou jejich programy používat. Popisovač je hodnota používaná k identifikaci prostředku, se kterým mají pracovat programy. Někdy bývají kořenové klíče též označovány pojmem podstromy. [1][15]

Podle stavu v systému je rozdělení klíčů na:

- **Stálé –** zůstávají neměnné při spouštění systému
- **Nestálé –** přepisují se při každém spuštění systému

Pro každý klíč platí jasně definovaná specifika:

- Lze vkládat jeden či více klíčů do jiného klíče, pokud názvy zůstanou v daném klíči jedinečné.
- Počet znaků v názvu klíče je omezen na 512 v případě normy ANSI (American National Standards Institute – soukromá nezisková organizace, která dohlíží na vývoj dobrovolných konvenčních standardů pro produkty, služby, procesy a systémy a zaměstnance v USA [12]) či na 256 v případě normy Unicode (jde o původně šestnáctibitovou tabulku znaků všech existujících abeced, která byla později rozšířená na 31 bitů. Jejím autorem je *Unicode Consortium* [13]).
- Název může obsahovat jakýkoli znak vyjma zpětného lomítka (/), hvězdičky (*) a otazníku (?)
- Názvy začínající tečkou jsou vyhrazeny systémem pro vlastní použití.

Jakýkoli klíč registru může být navzájem propojen s jiným. Pokud k tomu dojde, pak mají oba stejné podklíče a hodnoty, a nazývají se klíči propojenými.

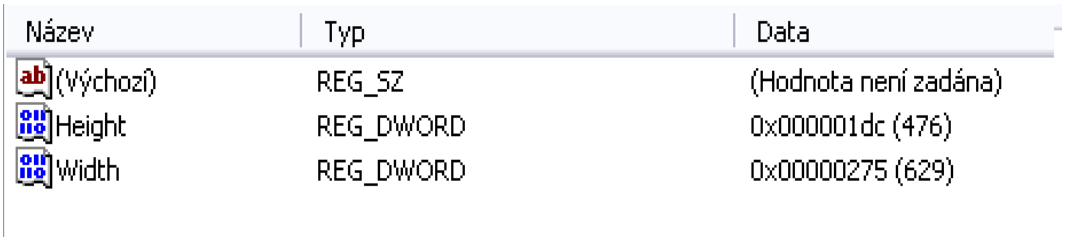
4.2 Hodnoty klíčů

Každý klíč obsahuje jednu či více hodnot a současně alespoň jednu hodnotu výchozí. Výchozí hodnotou je téměř vždy řetězec, avšak některé programy mohou tento typ změnit. Většinou je nulová a při náhledu jsou její data zobrazena jako (Hodnota není zadána).

Každá hodnota se skládá ze tří částí:

- **Název –** Musí být jedinečný, odlišné klíče však mohou obsahovat hodnoty se stejným názvem. Platí zde stejná pravidla jako pro názvy klíčů, viz podkapitola 4.1.
- **Typ –** Určuje druh obsažených dat. Přehled typů zmiňuje kapitola 4.3.
- **Data –** Mohou mít maximální velikost 32 767B, skutečný limit je ale 2KB. Obvykle odpovídají typu, pouze binární hodnoty mohou obsahovat řetězce, čísla či cokoli jiného.
  [15]

  Výše zmíněné údaje ukazuje obrázek č. 5:



Obrázek č.5: Ukázka hodnoty klíče HKEY_CURRENT_USER

4.3 Datové typy

Datový typ popisuje formát údajů obsažených v hodnotě klíče. Typy dat od 0 do 0x7FFFFFFF jsou rezervovány pro definiční potřeby systému. V programech lze tyto datové typy používat, kromě toho jsou však pro ně rezervovány typy od 0x80000000 do 0xFFFFFFFF. [14]

Systém podporuje následující typy dat v registru [1][14][15]:

- **REG_BINARY -** Neformátovaná binární data. Většina informací o hardwaru je ukládána ve formě binárních dat a Editor registru je zobrazuje v šestnáctkovém formátu.
- **REG_DWORD -** Údaje reprezentované číslem o délce 4 bajty. Tento typ je využíván velkým množstvím parametrů ovladačů zařízení a služeb. Editor registru je zobrazuje v binárním, šestnáctkovém nebo desítkovém formátu.

- **REG_EXPAND_SZ -** Datový řetězec proměnné délky. K tomuto typu dat patří proměnné vyhodnocované v okamžiku, kdy si program nebo služba příslušná data vyžádá.
- **REG_MULTI_SZ -** Řetězec s více než jednou hodnotou. Tohoto typu jsou zpravidla hodnoty tvořené seznamem několika údajů určených k přímému zobrazování v uživatelském rozhraní. Jednotlivé položky jsou odděleny mezerami, čárkami nebo jinými znaky.
- **REG_SZ -** Textový řetězec pevné délky.
- **REG_FULL_RESOURCE_DESCRIPTOR -** Sada vnořených polí určená k ukládání seznamu prostředků hardwarové součásti nebo ovladače.
- **REG_DWORD_BIG_ENDIAN –** Čtyřbajtové hodnoty. Jako první se do paměti ukládají nejvýznamnější bajty. K tomu dochází v obráceném pořadí, než v jakém se ukládá hodnota *REG_DWORD*.
- **REG_DWORD_LITTLE_ENDIAN –** Čtyřbajtové hodnoty. Jako první se do paměti ukládají nejméně významné bajty. Shoduje se s typem *REG_DWORD*, díky čemuž nelze v editoru registru vytvářet. Jedná se o nejčastěji používaný číselný typ.
- **REG_LINK –** Propojení. Hodnoty *REG_LINK* nelze vytvářet.
- **REG_NONE –** Hodnoty bez definovaného typu.
- **REG_QWORD –** Osmibajtové hodnoty. Tento typ je podporován pouze systémem Windows XP Professional x64 Edition. Lze ho zobrazovat a upravovat v desítkovém či šestnáctkovém formátu.
- **REG_QWORD_BIG_ENDIAN –** Osmibajtové hodnoty. Jako první se do paměti ukládají nejvýznamnější bajty. K tomu dochází v obráceném pořadí, než v jakém se ukládá hodnota *REG_QWORD*.
- **REG_QWORD_LITTLE_ENDIAN -** Osmibajtové hodnoty. Jako první se do paměti ukládají nejméně významné bajty. Shoduje se s typem *REG_QWORD*, díky čemuž nelze v editoru registru vytvářet.
- **REG_RESOURCE_LIST –** Seznam hodnot *REG_FULL_RESOURCE_DESCRIPTOR*. V editoru registru jej lze zobrazovat, nikoli však upravovat.
- **REG_RESOURCE_REQUIREMENTS_LIST –** Seznam prostředků vyžadovaných zařízením. V editoru registru jej lze zobrazovat, nikoli však upravovat.

Za většinu nastavení v registru odpovídají typy dat REG_BINARY, REG_DWORD a REG_SZ.

4.4 Podregistry a soubory registru

Pojem podregistr označuje skupinu klíčů, podklíčů a hodnot, jejíž kořen je umístěn na vrcholu hierarchické struktury registru. Obsah podregistru je popsán jedním souborem a souborem s příponou *LOG*. Tyto soubory jsou uloženy ve složkách %SystemRoot%\System32\Config a %SystemDrive%\Documents and Settings\UserName. Řetězec *%SystemRoot%* zastupuje název adresáře, který obsahuje soubory systému Windows. Řetězec %SystemDrive% zastupuje označení diskového oddílu, který obsahuje soubory systému Windows. Jsou-li například soubory systému Windows přiřazené uživateli se jménem User uloženy do adresáře Windows v diskovém oddílu C:, což je výchozí název složky při instalaci, budou soubory podregistru uloženy ve složkách C:\Windows\System32\Config a C:\Documents and Settings\User. Podregistry se nazývají také soubory registru nebo soubory s protokolem registru.[15]

Většina souborů registru (DEFAULT, SAM, SECURITY, SOFTWARE a SYSTEM) je standardně uložena ve složce %SystemRoot%\System32\Config. V jednotlivých operačních systémech řady Windows se může umístění profilů jednotlivých uživatelů počítače včetně souborů *Ntuser.dat* a *Ntuser.dat.log* záviset na tom, zda byl operační systém instalován do nového počítače, nebo zda se jednalo o aktualizaci ze systému staršího. [1][3]

Každému podregistru systému Windows XP je přiřazena standardní sada souborů. V následující tabulce jsou uvedeny standardní podregistry a jejich soubory.

Podregistr	Názvy souborů
HKEY_LOCAL_MACHINE\SAM	Sam a Sam.log
HKEY_LOCAL_MACHINE\SECURITY	Security a Security.log
HKEY_LOCAL_MACHINE\SOFTWARE	Software a Software.log
HKEY_LOCAL_MACHINE\SYSTEM	System a System.log
HKEY_CURRENT_CONFIG	System a System.log
HKEY_CURRENT_USER	Ntuser.dat a Ntuser.dat.log
HKEY_USERS\.DEFAULT	Default a Default.log

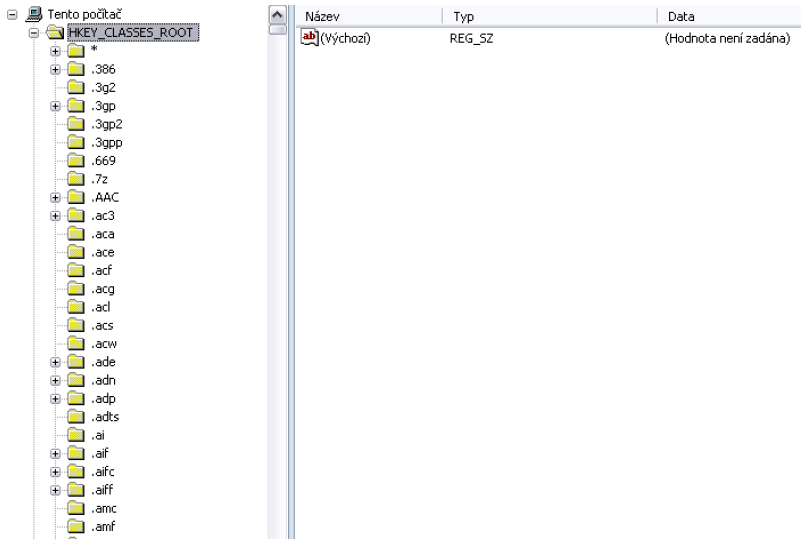
Tabulka č. 1: Soubory standardních podregistrů [14]

5. Organizace registru

Jak bylo již uvedeno, má registr 5 kořenových klíčů (ve skutečnosti jich je 6, ale dynamický klíč *HKEY_DATA_DYN* zobrazující systémové informace, není v editoru registru zobrazen, proto ho autor záměrně neuvádí). Dělí se na dva hlavní: *HKEY_LOCAL_MACHINE* a *HKEY_USERS*, přičemž zbylé tři jsou aliasy jiných částí registru. [14] Tato kapitola se podrobněji zaměřuje právě na tyto jednotlivé kořenové klíče (podstromy) a jejich nejdůležitější podklíče.

5.1 HKEY_CLASSES_ROOT (HKCR)

Kořenový klíč *HKEY_CLASSES_ROOT* zahrnuje informace o všech existujících spojeních souborů a datech spojených s objekty COM (Component Object Model – jedná se o standardní rozhraní pro tvorbu softwaru představené společností Microsoft v roce 1993. Používá se k umožnění komunikace mezi procesy a tvorbě dynamických objektů v jakémkoli jazyce, který tuto technologii podporuje) [9] . Obsahuje data, která spojují typy souborů podle přípony s konkrétními aplikacemi, s kterými jsou tyto typy souborů asociovány. Jeho účelem je poskytování zpětné kompatibility s databází registru Windows 3.1x. [15][1]

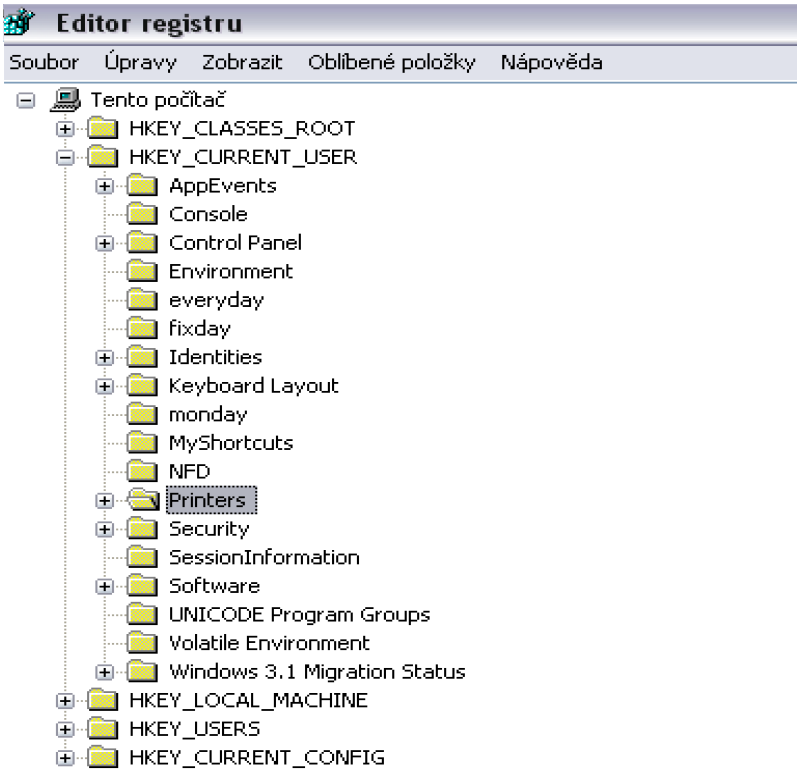


Obrázek č.6: Kořenový klíč HKCR zobrazený pomocí editoru registru

5.2 HKEY_CURRENT_USER (HKCU)

Klíč *HKEY_CURRENT_USER* obsahuje data, která popisují uživatelský profil pro uživatele přihlášené k místnímu systému (nikoli vzdálené uživatele) a veškeré informace potřebné pro nastavení pracovního prostředí konkrétních uživatelů. V uživatelském profilu jsou informace definující individuální nastavení daného uživatele. Jedná se o nastavení pracovní plochy, síťového připojení, proměnného prostředí a zabezpečení. Příkladem je například informace o nastavení pozadí pracovního prostředí. Tento klíč obsahuje celou řadu podklíčů, z nichž nejdůležitější jsou:

- **AppEvents** – Definuje události aplikací, zvuková schémata a sady relací mezi uživatelskými akcemi a zvuky produkovanými počítačem jako relace.
- **Console** – Definuje nastavení konzole (rozhraní mezi uživatelským a znakovým režimem aplikací) systému; jako například velikost a barva okna. Také zahrnuje nastavení možnosti příkazového řádku včetně způsobu použití těchto nastavení (každá či pouze aktuální relace).
- **Control Panel** – Obsahuje informace o nastavených parametrech v nabídce Ovládací panely.
- **Environment** – Obsahuje nastavení proměnných definovaných pro jednotlivého přihlášeného uživatele. Jejich hodnoty lze nastavit přes Ovládací panely.
- **Keyboard Layout** – Definuje jazyk použitý k aktuálnímu rozvržení klávesnice.
- **Printers** – Popisuje aktuálně nainstalované tiskárny, které jsou přihlášenému uživateli k dispozici.
- **Software** – Popisuje konfigurační nastavení pro nainstalovaný software.
- **UNICODE Program Groups** – Slouží pro zpětnou kompatibilitu v případě aktualizace z nižší verze Windows. Neobsahuje klíčová data pro systém.
- **Windows 3.1 Migration Status** – V případě přechodu z nižší verze Windows obsahuje data o tomto procesu aktualizace. V případě nové instalace je tento podklíč prázdný.



Obrázek č.7: Podklíče kořenového klíče HKCU

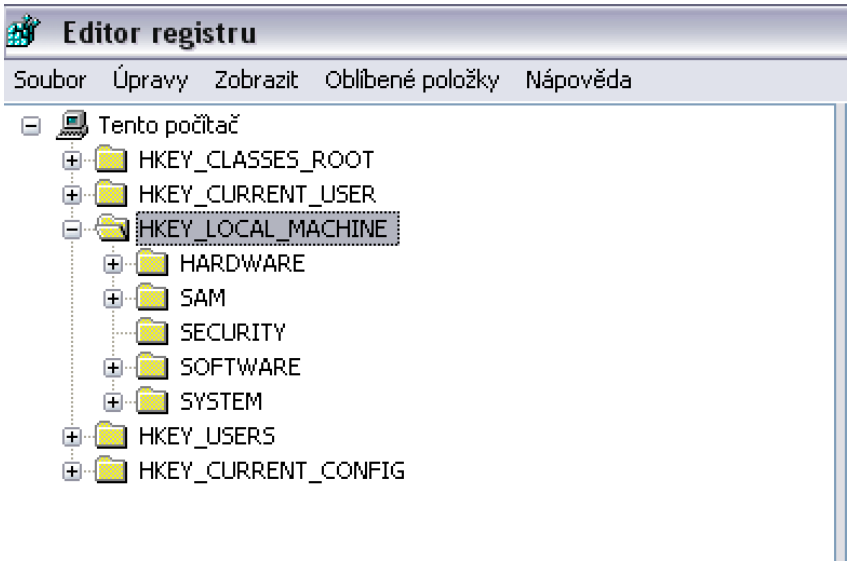
5.3 HKEY_LOCAL_MACHINE (HKLM)

Jak bylo již uvedeno v předchozí kapitole, *HKEY_LOCAL_MACHINE* je jedním z nejdůležitějších kořenových klíčů registru. Obsahuje konfigurační data pro místní počítač, které jsou využívány aplikacemi, ovladači zařízení a v neposlední řadě samotným systémem. Tento klíč je složen z pěti podklíčů [1][15][5]:

- **HARDWARE –** Tento podklíč ukládá data popisující hardware zjištěný systémem Windows při spuštění. Operační systém vytváří tento klíč při každém spuštění a zahrnuje do něj informace o zařízeních a k nim přiřazených ovladačích.
- **SAM –** Obsahuje místní databázi zabezpečení Windows – SAM (Security Accounts Manager). Systém Windows ukládá do klíče SAM místní uživatele a skupiny. Seznam řízení přístupu (ACL – Access Control List) tohoto klíče neumožňuje jeho prohlížení ani administrátorům, jelikož

informace v tomto klíči jsou šifrovány. Klíč SAM je propojením ke klíči *HKLM\Security\SAM*.

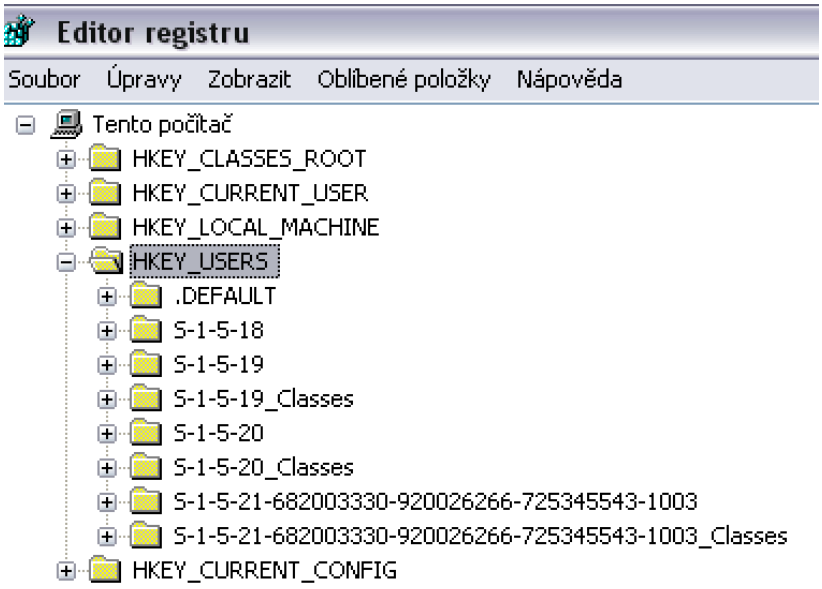
- **SECURITY –** Obsahuje místní zásady zabezpečení, včetně uživatelských práv a oprávnění. Obsahuje například informace, které definují, zda jednotliví uživatelé mohou restartovat počítač, spustit nebo zastavit ovladače zařízení, zálohovat/obnovit soubory nebo mají přístup k počítači prostřednictvím sítě. Informace v tomto klíči jsou šifrovány.
- **SOFTWARE –** Obsahuje informace o nainstalovaném softwaru na lokálním počítači včetně konfiguračních dat.
- **SYSTEM –** Zahrnuje informace o řízení spouštění operačního systému, pořadí zavedení ovladačů zařízení, systémových služeb a chování operačního systému.



Obrázek č.8 Podklíče kořenového klíče HKLM

5.4 HKEY_USERS (HKU)

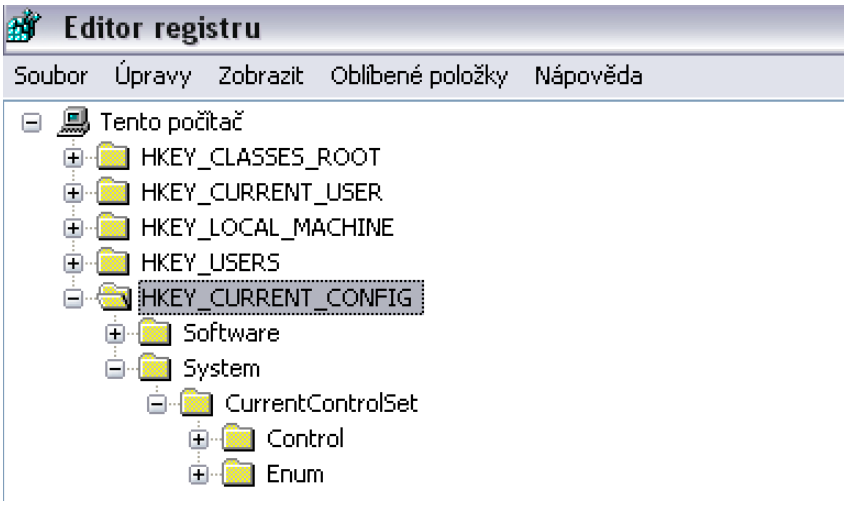
Klíč *HKEY_USERS* zahrnuje všechny aktivně zavedené uživatelské profily. Obsahuje dva podklíče. Podklíč *.DEFAULT*, jehož data jsou použita v případě, že není v systému přihlášen žádný uživatel, a podklíč <*Security ID*>, který obsahuje data uživatele aktuálně přihlášeného. Na obrázku č.9 je tímto <*Security ID*> například podklíč S-1-5-18. [1]



Obrázek č.9: Účty v kořenovém klíči HKU

5.5 HKEY_CURRENT_CONFIG (HKCC)

Klíč *HKEY_CURRENT_CONFIG* obsahuje konfigurační data pro aktuálně používaný hardwarový profil. Poprvé se objevil ve verzi Windows NT 4.0. Odkazuje se na klíč *HKCC\System\CurrentControlSet\HardwareProfiles\Current.*



Obrázek č.10: Podklíče kořenového klíče HKCC

6. Správa a práce s registrem

S registrem lze pracovat dvěma způsoby. Buď přímo, prostřednictvím editoru registru, či nepřímo prostřednictvím některé aplikace. Práci pomocí editoru registru podrobně rozebírá kapitola 6.1.1. Aplikace může komunikovat s registrem dvěma způsoby:

- **soubory s příponou REG** – spustitelné textové soubory, které mohou obsahovat jeden nebo více klíčů stromu registru a hodnoty s daty. Po jejich spuštění přidají do registru všechny obsažené klíče.
- **programové nástroje v API** – REG soubory jsou vhodné jen pro přidání klíčů, hodnot a dat do registru. Aplikace však potřebují s těmito údaji dále pracovat, především číst a měnit. K tomu slouží některé API funkce v knihovnách Windows, ale všechny moderní programovací jazyky pro Windows obsahují pro tento účel propracovanější podporu, obvykle jde o třídy a z nich odvozené objekty. V každém programovacím jazyce se tyto třídy nazývají jinak, obsahují však ve svém názvu vždy podřetězec REGISTERY nebo alespoň REG (například v Delphi existuje TRegistery), proto lze tyto třídy a jejich definice jednoduše vyhledat v nápovědě. [15]
- **soubory s příponou INF** – speciálně strukturované soubory pomocí nichž lze pracovat (vkládat i mazat) s registrem. Jedná se ale o natolik těžkopádnou možnost v porovnání s programovými nástroji, že se dnes prakticky nepoužívá.

Existuje mnoho dalších nástrojů pro práci s registrem (viz následující kapitola 6.1), z nichž některé jsou přítomny v operačním systému (různé v závislosti na verzi Windows, ve Windows 95 prakticky jen regedit, v dalších verzích je přítomen například nástroj scanreg pro optimalizaci a obnovu registru). Další nástroje, které slouží buď k optimalizaci nebo opravení registru, a nebo k práci s obsahem registru (optimalizace Windows apod.), je možné sehnat buď jako komerční software nebo freeware či shareware.

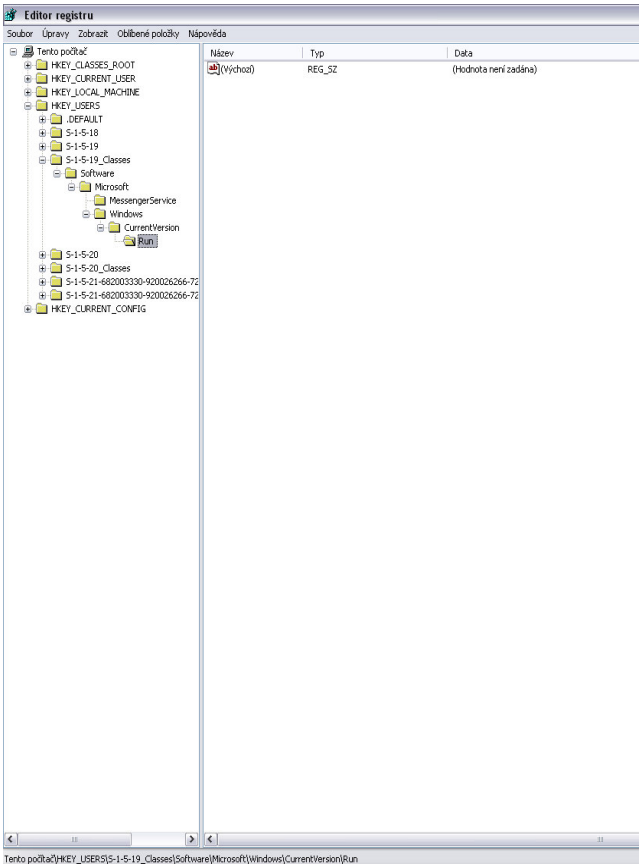
6.1 Nástroje pro práci s registrem

Tato kapitola se zabývá nejpoužívanějšími nástroji pro práci s registrem, ať už se jedná o software Microsoft či jiných firem. Konkrétní možnosti práce a úprav jsou blíže popsány zde [6][8].

6.1.1 Editor registru (regedit.exe)

Editor registru je nástroj, jehož prostřednictvím lze přímo upravovat registr. Pomocí něj lze upravit nastavení bez pomoci uživatelského rozhraní. Díky tomu je tento nástroj jedním z nejvýkonnějších a zároveň nejvíce nebezpečných v operačním systému. A to především díky tomu, že žádný jiný nástroj nekontroluje uživatelem změněná nastavení, která jsou po uzavření okna editoru ihned použita. Současně nelze tyto změny v editoru automaticky vrátit na původní. Nesprávné nastavení může vést k softwarovým chybám či způsobit havárii systému a zabránit úspěšnému spuštění systému. V takovém případě je potřeba použít jednu z možností funkce *Obnovení systému*, neboť je v tu chvíli nemožné se do editoru registru dostat a chyby opravit.

Jak již bylo uvedeno v předchozích kapitolách, lze editor registru spustit pomocí *regedit.exe*, který je při instalaci systému implicitně uložen do složky *%SystemRoot%*. Po jeho spuštění se zobrazí okno rozdělené na 2 části a 4 hlavní oblasti (obrázek č.11):

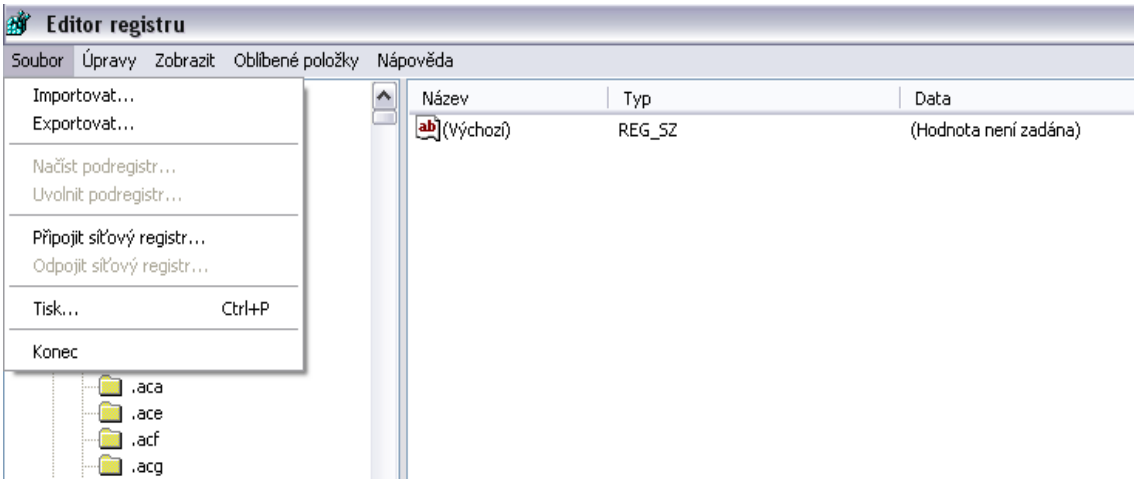


Obrázek č.11: Editor registru

- **Panel nabídek** – Obsahuje položky *Soubor*, *Úpravy*, *Zobrazit*, *Oblíbené položky* a *Nápověda.*
- **Levé podokno** – Zobrazuje hierarchii registru.
- **Pravé podokno** – Zobrazuje hodnotové položky obsažené ve vybraném klíči.
- **Stavový řádek** – Zobrazuje cestu vybrané položky registru.

Příkazy nabídky *Soubor* umožňují uživateli importovat či exportovat soubory registru, připojit či odpojit síťový registr, načíst nebo uvolnit podregistr, vytisknout libovolnou část registru a ukončit práci s editorem registru.

Nabídka *Soubor* obsahuje tyto položky (viz obrázek č.12):



Obrázek č.12: Příkazy nabídky Soubor v editoru registru

- **Importovat** – Umožňuje importovat dříve exportované soubory registru (viz kapitola 6.2.2).
- **Exportovat** – Umožňuje exportovat celý registr či pouze jeho část (viz kapitola 6.2.2).
- **Připojit síťový registr** – Umožňuje upravit registr vzdáleného počítače. Je k dispozici pouze v případě, kdy je počítač s programem Regedit součástí sítě, která obsahuje servery Windows NT/2000 nebo Novell Netware. Pro samotné připojení ke vzdálenému registru je třeba definovat název počítače, na kterém je vzdálený registr. [1]
- **Odpojit síťový registr** – Umožňuje odpojit připojený síťový registr (viz předchozí bod).
- **Načíst podregistr** – Umožňuje načíst soubory registru, které byly dříve z registru exportovány a uloženy ve formátu podregistru. Tento příkaz je použitelný pouze pro klíče HKU a HKLM a je k dispozici pouze tehdy,

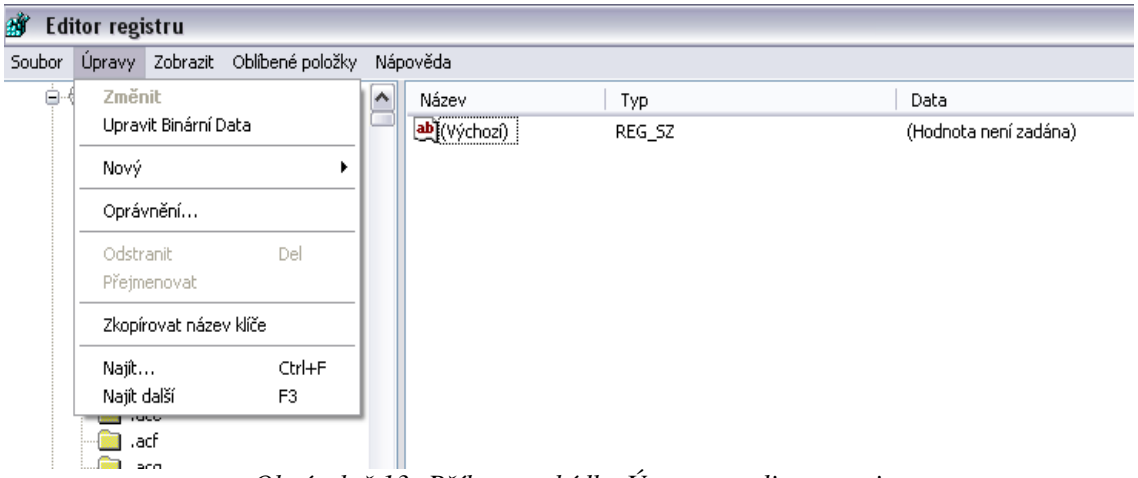
když je vybrán jeden z těchto klíčů. Načtený podregistr se stane jedním z podklíčů výše uvedených kořenových klíčů. [1]

- **Uvolnit podregistr** – Umožňuje uvolnit podregistry, které byly dříve načteny do registru (viz předchozí bod).
- **Tisk** – Umožňuje tisk vybrané oblasti registru.
- **Konec** – Slouží k ukončení práce s editorem registru.

Pro provedení většiny těchto příkazů musí být uživatel připojen jako Administrator nebo jako uživatel náležející do skupina Administrators.

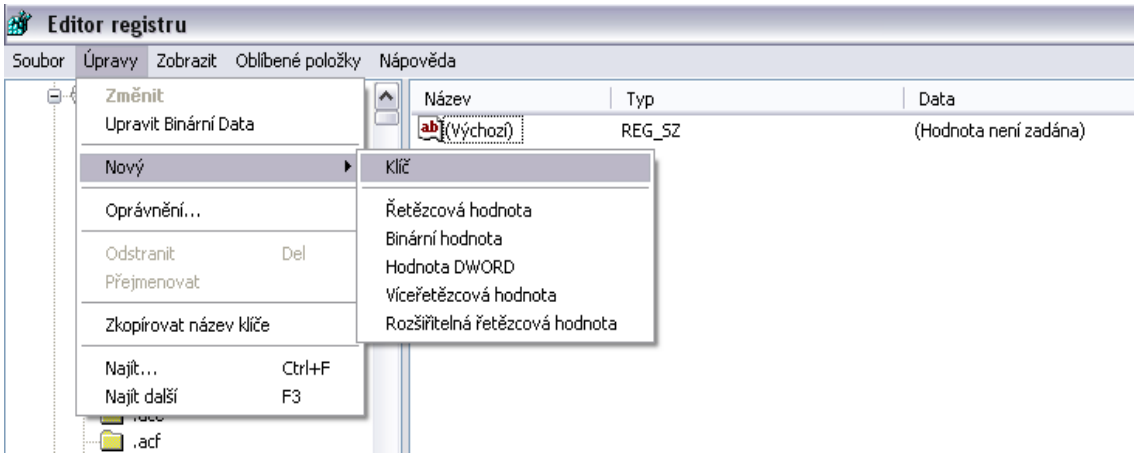
Příkazy nabídky *Úpravy* umožňují uživateli vytvářet, kopírovat, upravovat a měnit oprávnění položek registru.

Nabídka *Úpravy* obsahuje tyto položky (obrázek č.13):



Obrázek č.13: Příkazy nabídky Úpravy v editoru registru

- **Změnit** – Umožňuje upravit data obsažená v položkách registru. Tento příkaz lze použít pouze v případě, že je vybrána jedna z položek v pravém podokně editoru registru.
- **Upravit Binární Data** – Umožňuje upravit jakákoli data (včetně jiných datových typů) v okně editoru binárních hodnot. [1]
- **Nový** – umožňuje přidávat nové položky klíčů a hodnot (obrázek č.14)

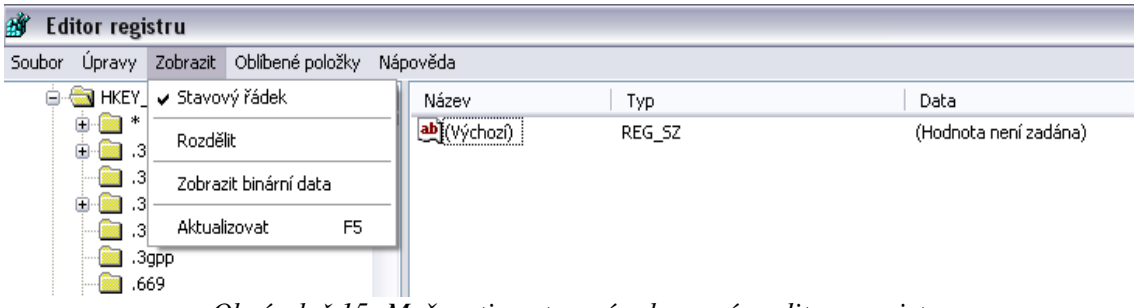


Obrázek č.14: Možnosti vytvoření nového klíče či hodnoty

- **Oprávnění** – Umožňuje provádět správu oprávnění klíčů registru a auditovat akce s nimi souvisejícími. Mohou být přiřazena nezávisle na typu systému souborů na systémovém oddílu. [1]
- **Odstranit** – Umožňuje odstranit hodnotové položky.
- **Přejmenovat** – Umožňuje přejmenovat hodnotové položky.
- **Zkopírovat název klíče** – Umožňuje zkopírovat název vybraného klíče do schránky pro další použití.
- **Najít** – Slouží k vyhledávání klíčů a hodnotových položek registru. Vyhledávat lze jednak pouze celý zadaný řetězec, ale i pouze samotné klíče, hodnoty či data.
- **Najít další** – Slouží k samotnému vyhledání zadaného řetězce (viz předchozí bod).

Příkazy nabídky *Zobrazit* umožňují uživateli nastavit zobrazení stavového řádku, binárních dat, podoken editoru registru a změn v něm provedených.

Nabídka *Zobrazit* obsahuje tyto položky (obrázek č.15):



Obrázek č.15: Možnosti nastavení zobrazení v editoru registru

- **Stavový řádek** – Umožňuje zobrazení či skrytí stavového řádku.

- **Rozdělit** – Umožňuje nastavit velikost obou podoken editoru registru pomocí oddělovače.
- **Zobrazit binární data** – K dispozici pouze po vybrání konkrétní hodnotové položky. Umožňuje zobrazit vybranou datovou položku ve formátech *Bajt*, *Word* a *DWord*. [1].
- **Aktualizovat** – Umožňuje obnovit zobrazení provedených změn, které se nezobrazily ihned.

Nabídka *Oblíbené položky* umožňuje přidávat (vytvářet seznam) a odebírat (mazat ze seznamu) klíče, které uživatel používá nejčastěji. Po vytvoření takovéto položky lze pak pouhými dvěma kliknutími přejít i do nejvíce zanořeného klíče, což uživateli práci s registrem značně ulehčí.

Nabídka *Nápověda* umožňuje uživateli zjistit informace o verzi registru a vyhledat konkrétní jednoduché postupy, jak pracovat s příkazy registru. [15][1]

6.1.2 Nástroje jiných společností

Nástrojů na sledování, úpravu a práci s registrem je celá řada. Většina z nich nabízí oproti editoru registru množství dalších funkcí. Tato kapitola se zaměřuje na tři nejpoužívanější a uživateli nejoblíbenější.

6.1.2.1 TweakNow Regcleaner

Nástroj od společnosti TweakNow sloužící pro údržbu systému. Je vydávána ve dvou verzích.

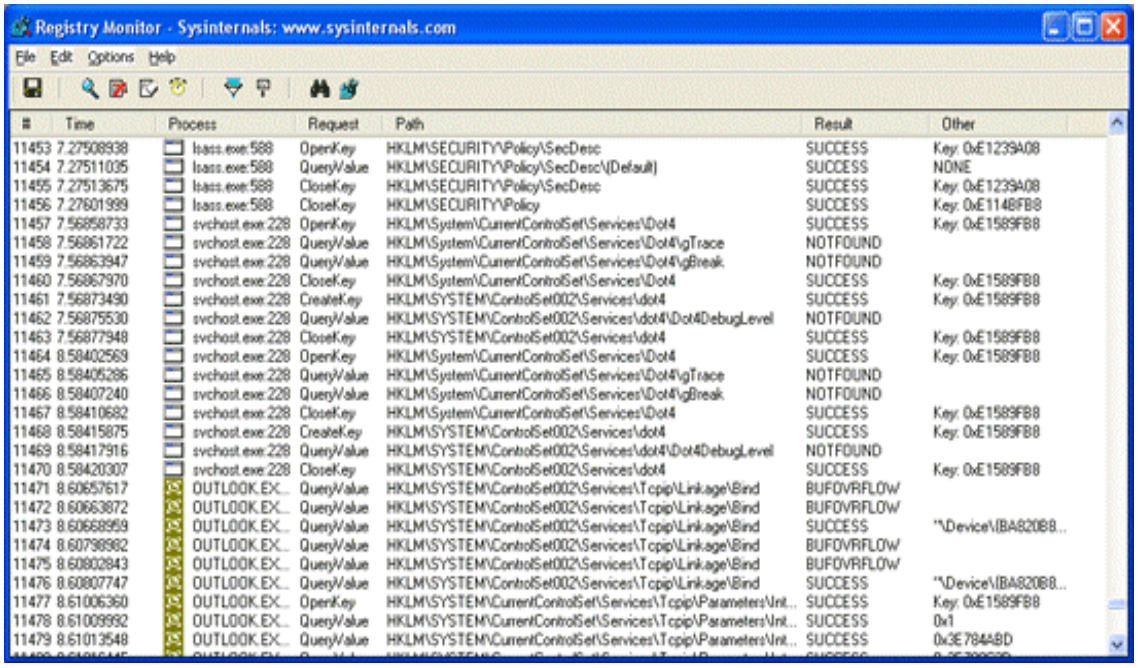
Verze *Standard* je zdarma a obsahuje nástroj na vyhledávání neplatných údajů v registru (položky nepoužívané žádným programem). Po vyhledání doporučí uživateli, které položky mohou být odstraněny. Standardně vytváří zálohu registru, takže veškeré změny mohou být vráceny zpět.

Verze *Professional* je placená a obsahuje oproti verzi *Standard* navíc ještě nástroj na odstranění stop zanechaných po činnosti různých aplikací, nástroj na defragmentaci registru a nástroj na optimalizaci systému. [16][27]

Obrázek č.16: Program TweakNow RegCleaner Professional Edition [17]

6.1.2.2 Registry Monitor

Nástroj Registry Monitor byl vyvinut Markem Russinovichem a Brycem Cogswellem. Slouží ke sledování a zobrazení všech informací týkajících se přístupu k registru v celém systému. Je implementován jako kombinace ovladače zařízení a grafického uživatelského rozhraní. Podporuje filtrování procesů, umožňuje ukládat výstupy v souboru ASCII a sledovat aktivitu registru během spouštění. Tento nástroj je zdarma a navíc k němu autoři nabízejí technické informace o implementaci a zdrojový kód. [1]



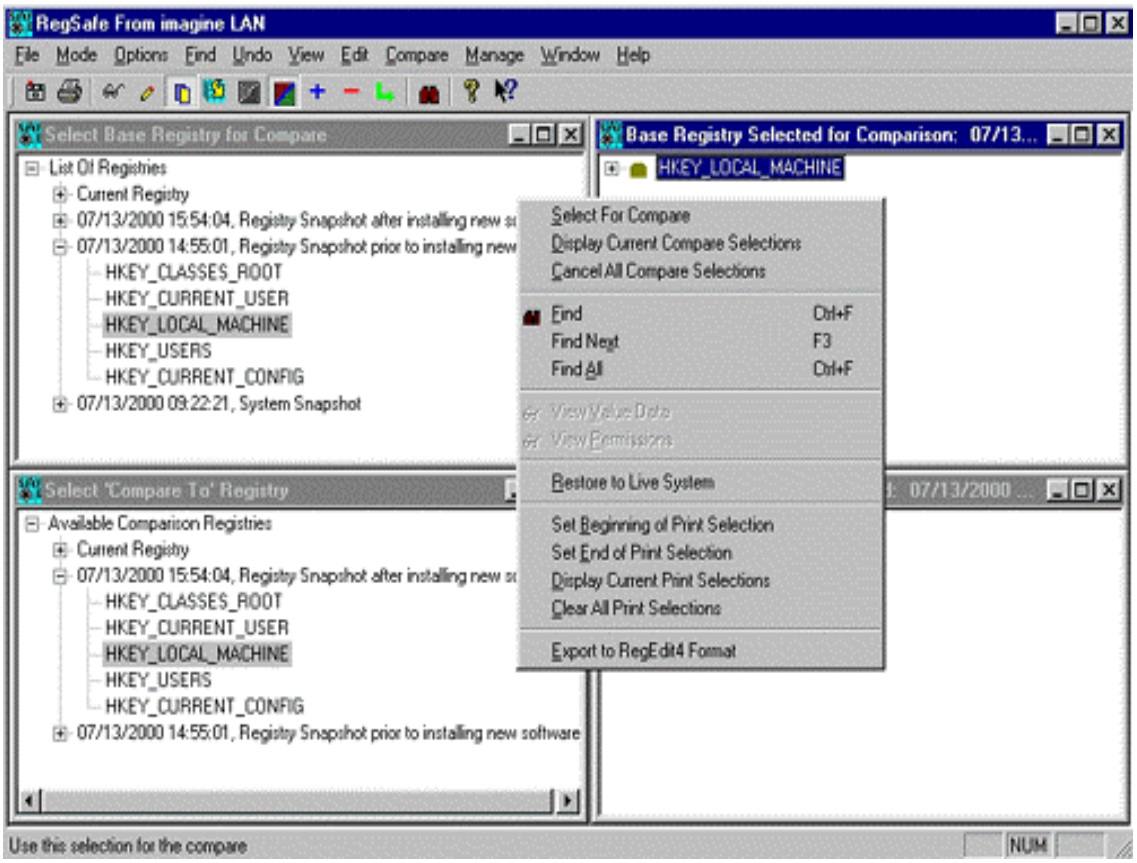
Obrázek č.17: Program Registry Monitor [18]

6.1.2.3 RegSafe

Nástroj RegSafe slouží k pokročilé správě a upravování registru. Jeho nejzajímavější funkce jsou:

- **Chráněné prostředí** – automaticky ukládá kopii registru před uplatněním jakýchkoli změn
- **Porovnání registru** – porovnává klíče, hodnoty či celé registry
- **Exportování** – exportace částí registru nebo výsledků porovnání do souboru s příponou REG
- **Částečné či úplné obnovení registru**
- **Obnovení registru pro nespouštěné systémy** – umožňuje obnovit systém na všech existujících verzích Windows (pomocí technologie Command Prompt SOS či pomocí konzoly systému Windows XP) [1]

Dříve byl distribuován ve dvou verzích, zdarma ve verzi *Editor Only* a v placené verzi *Professional*. V dnešní době je však distribuován pouze ve verzi *Professional*.



Obrázek č.18: Program RegSafe [19]

6.2 Záloha a obnovení registru

Při provádění změn v registru je vhodné si ho zálohovat. Záloha je praktická také v případě instalace zkušební verze některého programu, při níž je možné, že program bude přidávat do registru „nevyhledatelné“ položky. [7]

Windows XP nabízí různé možnosti zálohování a obnovení registru, spolu se zdokonalením spolehlivosti. Některé z těchto vlastností byly získány z Windows NT/2000 a některé jsou zde představeny poprvé. Tato kapitola nastiňuje nejčastěji používané metody.

6.2.1 Ruční záloha a obnovení registru

Pokud je spouštěcí oddíl Windows XP formátován pomocí systému souborů FAT, lze systém snadno zálohovat ručně zkopírováním souborů registru na

záložní médium spuštěním počítače pod alternativním operačním systémem nebo pomocí spouštěcí diskety. Používá-li spouštěcí oddíl systém souborů NTFS, je doporučována společností Microsoft paralelní instalace Windows NT nebo Windows XP a pomocí této instalace následné zkopírování souborů registru z instalace původní.

Soubory registru, které je nutno zkopírovat, se nacházejí ve složce %SystemRoot%\System32\Config. Jsou to:

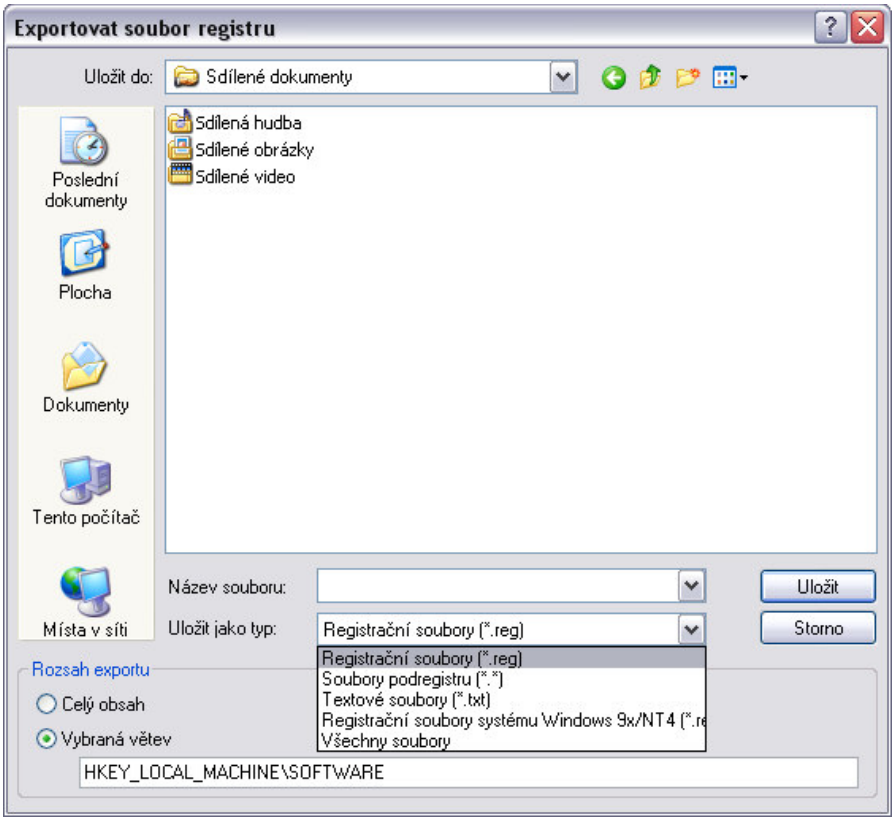
- Appevent.evt
- Default
- Default.log
- Default.sav
- Sam
- Sam.log
- Secevent.evt
- Security
- Security.log
- Software
- Software.log
- Software.sav
- Sysevent.evt
- System
- System.log
- System.sav
- Userdiff

Obnovení registru ze záložní kopie, která byla vytvořena touto metodou vyžaduje spuštění počítače pod alternativním systémem. Po spuštění stačí zkopírovat soubory registru ze zálohovacího média zpět do složky %SystemRoot%\System32\Config. [1][15]

6.2.2 Export a import registru

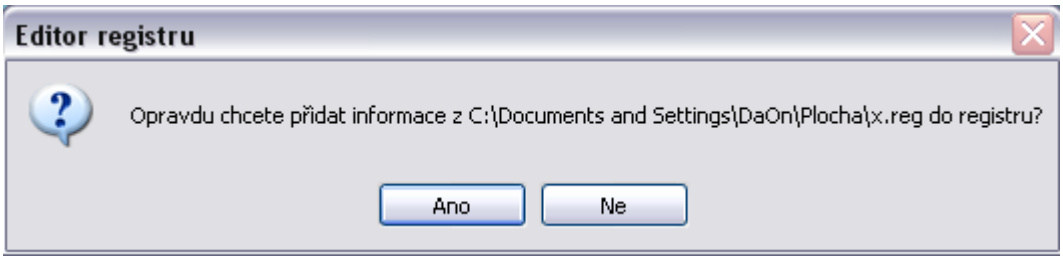
Export registru patří mezi nejjednodušší metody jeho zálohy. Slouží k zálohování nastavení registru, která lze pak snadno obnovit. Je také vhodný pro sdílení nastavení s jinými uživateli či počítači. Exportovat lze buď část či celý registr a to na jakékoli zařízení nainstalované na místním systému. Provádí se prostřednictvím editoru registru. Ten umí exportovat do čtyř druhů souborů (obrázek č.19):

- Registrační soubory (přípona REG)
- Soubory podregistru
- Textové soubory (přípona TXT)
- Registrační soubory systému Windows 9x/NT4 (přípona REG)



Obrázek č.19: Možnosti formátů pro export registru

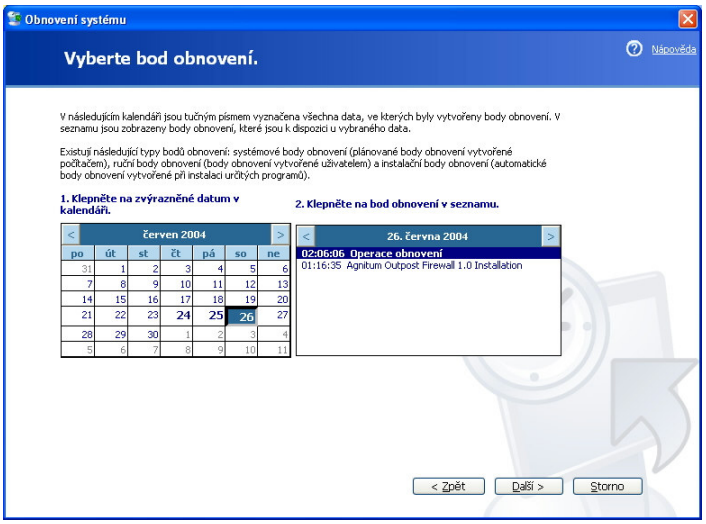
Import registru slouží k obnovení registru či jeho klíčů nebo pro přidání nových klíčů, většinou konfiguračních nastavení některé z aplikací. Provádí se primárně pomocí editoru registru. Druhou možností je spuštění souboru s příponou REG, po kterém se automaticky zobrazí dialogové okno s nabídkou potvrzení importu informací ze souboru do registru (obrázek č.20), neboť je toto implicitně podporováno systémem Windows.



Obrázek č.20: Potvrzovací dialog pro import REG souboru do registru

6.2.3 Nástroj Obnovení systému

Nástroj *Obnovení systému* sleduje změny v konfiguraci operačního systému. Při změnách konfigurace automaticky vytváří body obnovy. V podstatě jde o systém souborů, do něhož se změny uloží. V případě poruchy systému je možné prostřednictvím záznamů v bodech obnovy Windows XP zrestaurovat, tzn. uvést do stavu, kdy byl stabilní a pracoval správně. Výhodou tohoto nástroje je uživatelsky příjemné prostředí a možnost rychlého obnovení poškozeného systému. Body obnovy lze zaznamenat ručně, ale většinou se využívá automaticky vytvořených údajů. To ukazuje obrázek č.21:



Obrázek č.21 Nástroj Obnovení systému [20]

Obnovení systému obsahuje dvě následující součásti:

- **Nástroj pro sledování souborů –** Sleduje všechny změny v nadefinované sadě systémových souborů a v souborech aplikací; prováděno ovladačem systému souborů na úrovni jádra. Seznam souborů, které jsou sledovány, je uložen v souboru Filelist.xml umístěném v adresáři %SystemRoot%\System32\restore. Následující soubory a složky jsou vyloučeny z procesu sledování:
    - **Stránkovací soubor virtuální paměti**
    - **Uživatelská data** (včetně obsahu složek Dokumenty, Koš, Temporary Internet Files, Temp a Historie)
    - **Grafické soubory** (včetně souborů s příponou *JPG, BMP, EPS*, ad.)

    - **Datové soubory** (včetně souborů s příponou *DOC, XLS, MDB, PST, PDF*, ad.)
- **Body obnovení –** viz dále

Obnovení systému vytváří různé typy bodů obnovení:

- **Úvodní systémové kontrolní body –** Vytvářeny při prvním spuštění systému. Při jejich obnovení dojde k návratu do stavu po instalaci systému.
- **Systémové kontrolní body** – Implicitně vytvářeny každých 24 hodin nezávisle na systémových změnách. Je-li počítač vypnut po delší dobu než 24 hodin, pak jsou vytvořeny při následném spuštění systému.
- **Instalační kontrolní body** – Vytvářeny při instalaci programů. Umožňují obnovu do stavu před instalací daných programů.
- **Kontrolní body automatické aktualizace** – Vytvářeny před aktualizací systému prostřednictvím Automatic Update (Automatická inovace) či Windows Update.
- **Ručně vytvořené kontrolní body** – Vytvářeny uživatelem pomocí nástroje *Obnovení systému* nebo pomocí vlastního skriptu.
- **Kontrolní body před obnovením** – Vytvářeny před obnovou kontrolního bodu. Umožňují rychlý návrat do stavu před poslední obnovou.
- **Kontrolní body nepodepsaných ovladačů zařízení** – Vytvářeny při instalaci nepodepsaného ovladače zařízení. Umožňují obnovu do stavu před instalací tohoto ovladače.
- **Kontrolní body zotavení nástroje Zálohování (BackUp)** – Vytvářeny před použitím nástroje Zálohování k provedení zotavení.

Funkce *Obnovení systému* vyžaduje alespoň 200MB volného prostoru na disku. Implicitně je přidělováno 12% velikosti pevného disku (nebo 400MB na discích s menší kapacitou než 4GB). Více nemůže systém funkci *Obnovení systému* přidělit. Není-li však tento prostor k dispozici, pak systém tuto funkci zakáže. Velikost tohoto prostoru může být nakonfigurována i samotným uživatelem, ale pouze v souladu s již uvedenými omezeními. Pokud uživatel velikost prostoru zmenší, dojde k omezení počtu bodů obnovení, které může funkce *Obnovení systému* současně spravovat. Tato funkce může být uživatelem i zcela zakázána, což je ovšem doporučováno pouze v případě instalace systému na pomalých počítačích či při odvirovávání systému.

Samotný program je uložen v *%SystemRoot%\System32\restore\rstrui.exe.* [26]

6.2.4 Nástroj Automatické obnovení systému (ASR)

Funkce *ASR (Automated System Recovery) Automatické obnovení systému* byla poprvé představena až v systému Windows XP. Má dvě hlavní funkce:

- **Zálohování** - To se provádí pomocí *Průvodce automatickým obnovením systému,* který je součástí zálohovacího programu *Backup.* Průvodce zálohuje stav systému, systémové služby a veškeré disky, které jsou spojeny se součástmi operačního systému. Vytváří rovněž soubor obsahující informace o záloze, konfiguraci disku (včetně běžných a dynamických svazků) a o způsobech obnovení. [21]
- **Obnovení** - To přečte z dříve vytvořeného záložního souboru konfiguraci disku a obnoví veškeré podpisy, svazky a oddíly alespoň na discích, které jsou vyžadovány pro spuštění počítače. Pak nainstaluje Windows a automaticky zahájí obnovení systému s využitím zálohy (vytvořené *Průvodcem automatickým obnovením systému).* [21]

Vytvoření kompletní zálohy (všech dat) je relativně snadné, ale pro uložení zálohy je nutné:

- Zařízení s dostatečnou kapacitou (kam se budou záložní data ukládat). Záložní soubor se komprimuje, ale jeho zmenšení oproti originálu se podle typu zálohovaných dat pohybuje zhruba mezi 1/2 a 1/3 originálu. Například při zálohování dnes relativně malé velikosti dat 20 GB se bude velikost zálohy pohybovat zhruba okolo 13 GB.
  Záložní data musí být navíc umístěna na médiu, které bude dostupné během instalace Windows XP. Není tedy možné použít ani síťové disky (na vzdálených PC), ani média CD a DVD (navíc je kapacita médií CD z hlediska ASR velmi malá). Pro zálohu ASR je velmi vhodné zařízení pásková jednotka (která je však k použití v PC velmi drahá), praktičtější a levnější je pak uložení zálohy na jiný pevný disk.
- Disketa, kam si ASR uloží údaje nutné ke spuštění procesu obnovy ASR. Nejdříve je tedy nutné rozvážit, zda je ASR tím správným řešením (zda neprovést pouze částečnou zálohu, která je kapacitně méně náročná).

O postupu zálohování jsou podávány průběžné informace. Od velikosti zálohovaných dat se odvíjí doba trvání zálohy (od desítek minut až po hodiny). Odhadovaný čas, velikost záložního souboru a počet zálohovaných souborů

ukazuje okno *Průběh zálohování.* Zálohu ASR končí vytvořením spouštěcí *Diskety automatické obnovy.* [21]

Záloha ASR se používá v případě havárie systému, kdy s její pomocí lze rychle vrátit systém do původního stavu. K úspěšné obnově je třeba:

- Instalační CD Windows XP
- Disketu automatické obnovy, vytvořenou během ukládání zálohy ASR
- Vlastní zálohu na dostupném médiu

7. Ochrana a zabezpečení registru

Samotný operační systém Windows XP odpovídá požadavkům zabezpečení třídy C2 pro chráněné operační systémy. Sada kritérií požadovaných pro jednotlivé třídy zabezpečení byla vyvinuta úřadem U.S. National Security Agency (NSA) a samotná certifikace je prováděna pomocí TCSEC (Trusted Computer System Evaluation Criteria). Kritérium TCSEC poskytuje specifikace procedur vyhodnocování úrovně zabezpečení informačních systémů pro státní organizace. Třída C2 je považována za nejvyšší třídu zabezpečení pro obecně použitelné operační systémy. Certifikace a testování operačního systému na třídu zabezpečení C2 zahrnuje vyhodnocení a testování zabezpečovacích funkcí implementovaných operačním systémem. Toto testování stanoví, zda jsou tyto funkce dostatečně implementovány a pracují správně. [1] Mezi požadavky úrovně zabezpečení C2 patří:

- Vyžadovaná identifikace a ověření všech uživatelů operačního systému
- Libovolné řízení přístupu
- Možnosti auditování – systém musí mít možnost auditovat všechny prováděné akce
- Ochrana systémových objektů proti znovupoužití – systém musí být schopen zabránit uživateli v přístupu k prostředkům již uvolněným (např. čtení odstraněných souborů)

Podrobnější informace ohledně úrovní zabezpečení a samotné certifikace lze nalézt na internetové adrese http://radium.ncsc.mil. [1]

Windows XP poskytuje tyto funkce ochrany systému a zabezpečení správy:

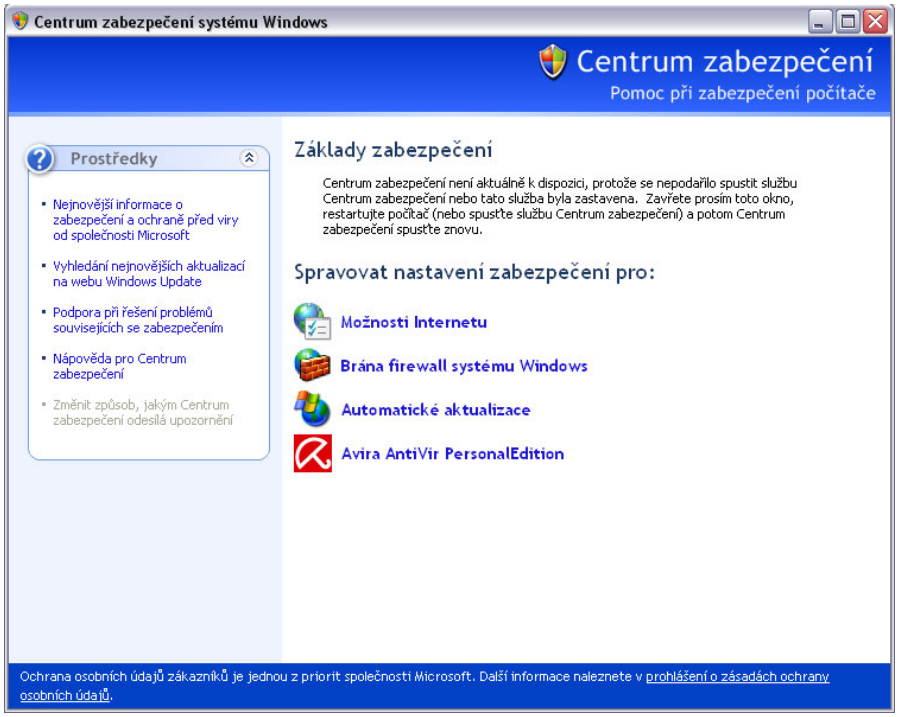
- Kontrola veškerého přístupu k systémovým prostředkům
- Registrace všech operací, které přistupují k systémovým prostředkům v protokolu zabezpečení
- Heslo pro přístup k systému
- Možnost protokolování operací přistupujících k systému [1]

7.1 Správa zabezpečení registru

Kromě výše uvedených funkcí zabezpečení nabízí Windows XP po instalaci druhého opravného balíčku (SP2) nová rozšíření zdokonalující správu a možnosti

zabezpečení klíčů. K hlavním rozšířením patří nová komponenta, kterou je *Centrum zabezpečení Windows* (obrázek č.22). K jejím funkcím patří následující:

- Oznamuje stav třech hlavních součástí zabezpečení (Brána Firewall systému Windows, Automatické aktualizace a Antivirová ochrana)
- Určuje zda jsou funkce zabezpečení klíčů zapnuté a aktuální
- Oznamuje nutnost aktualizací, případně doporučuje provedení dalších kroků pro zdokonalení zabezpečení počítače



Obrázek č.22: Centrum zabezpečení systému Windows XP

Správu centra zabezpečení Windows lze provádět prostřednictvím nastavení Active Directory Group Policy. V doménových prostředích je tento nástroj implicitně vypnutý. [15]

7.1.1 Skupiny zabezpečení

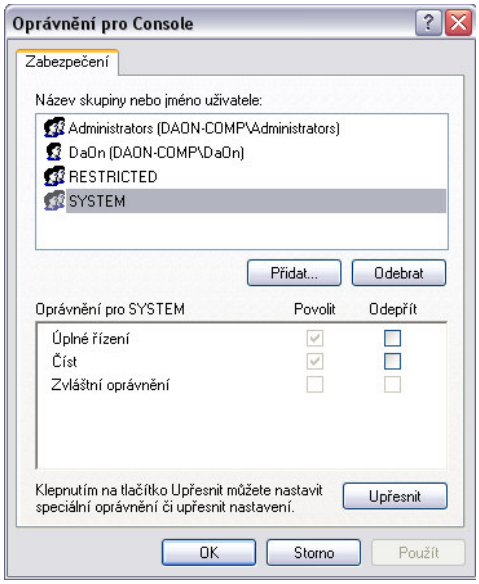
Standardní nastavení zabezpečení ve Windows XP jsou definována výchozími právy pro přístup, která jsou nastavena pro následující vestavěné skupiny zabezpečení:

- **Administrators** – Tato skupina poskytuje úplnou kontrolu nad celým počítačem. Její členové mohou změnit soubory operačního systému a aplikací, všechna nastavení v registru a také mohou převzít vlastnictví nad klíči a změnit seznam ACL klíče. [15] Tato skupina bude implicitně zahrnovat první uživatelský účet vytvořený při instalaci operačního systému. [1] Podle společnosti Microsoft by měl být účet typu Administrator využíván co nejméně z důvodu minimalizace rizika poškození konfigurace počítače. I správce by měl pro běžnou práci využívat účet s nižším oprávněním, pokud právě nepotřebuje vykonávat činnost, ke které je účet typu Administrator nutný. [21]
- **Power Users** – Tato skupina poskytuje zpětnou kompatibilitu pro spuštěné programy, které nejsou certifikovány pro systém Windows. [15] Členové této skupiny mají kromě svých uživatelských profilů implicitně oprávnění pro čtení a zápis i v dalších částech operačního systému. Mohou provádět omezenou sadu úkolů, včetně nastavení systémového data a času, definování nastavení obrazovky, instalace tiskáren a konfigurace správy výkonu. [1]
- **Users** – Tato skupina má nejvyšší úroveň zabezpečení, protože její výchozí oprávnění neumožňují členům měnit data operačního systému nebo jiná uživatelská nastavení. [15] Uživatelé mají přístup pro čtení a zápis pouze k vlastním uživatelským profilům. Microsoft doporučuje do této skupiny řadit koncové uživatele z důvodu ochrany integrity systému. [1]
- **Guests** – Tato skupina má při výchozím nastavení odepřen přístup k protokolům událostí aplikací a systému. Ve všech dalších aspektech mají členové stejná oprávnění pro přístup jako členové skupiny *Users*. Primárně slouží pro příležitostné uživatele.
- **Backup Operators –** Členové této skupiny mohou zálohovat a obnovovat soubory na počítači, bez ohledu na oprávnění, která dané soubory chrání. Také se mohou k počítači přihlásit a vypnout jej, nemohou však měnit nastavení zabezpečení.
- **Replicators –** Členové této skupiny mohou replikovat soubory v doméně.
- **Network Configuration Operators –** Členové této skupiny mají omezená oprávnění pro správu, která jim umožňují konfigurovat vlastnosti sítí, např. přiřazení IP adresy.
- **HelpServiceGroup –** Členové této skupiny mohou využít pomocných aplikací k rozpoznání použití systému. Tento účet může být použit členy služeb nápovědy a odborné pomoci Microsoft pro přístup k počítači ze sítě a místní přihlášení.

- **Remote Desktop Users –** Členové této skupiny mají právo pro místní přihlášení.

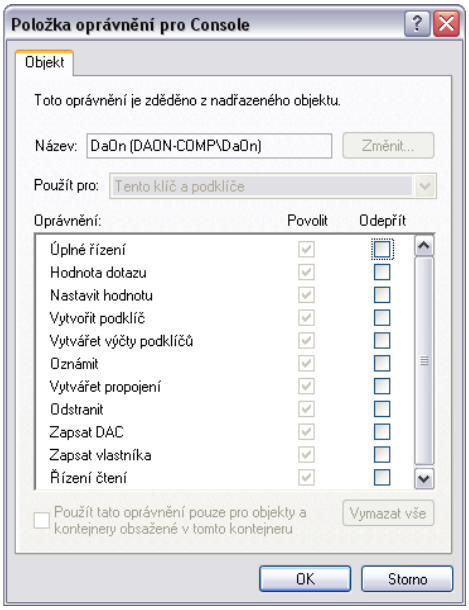
7.1.2 Typy oprávnění klíčů registru

Pro nastavení typu oprávnění klíčů registru slouží příkaz *Oprávnění* v editoru registru. Využívá se zejména pro klíče přidané kvůli optimalizaci softwaru nebo pro jiné typy upravování systému. Možnost nastavení oprávnění klíče nezávisí na systému souborů použitém k formátování oddílu, který obsahuje soubory Windows XP. Společnost Microsoft doporučuje v součinnosti se změnou oprávnění klíčů auditovat přístup k těmto klíčům, neboť takováto změna může mít závažné důsledky.Jednotlivé typy oprávnění ukazuje obrázek č.23 a jsou to:



Obrázek č.23: Okno Oprávnění pro konzolu Windows

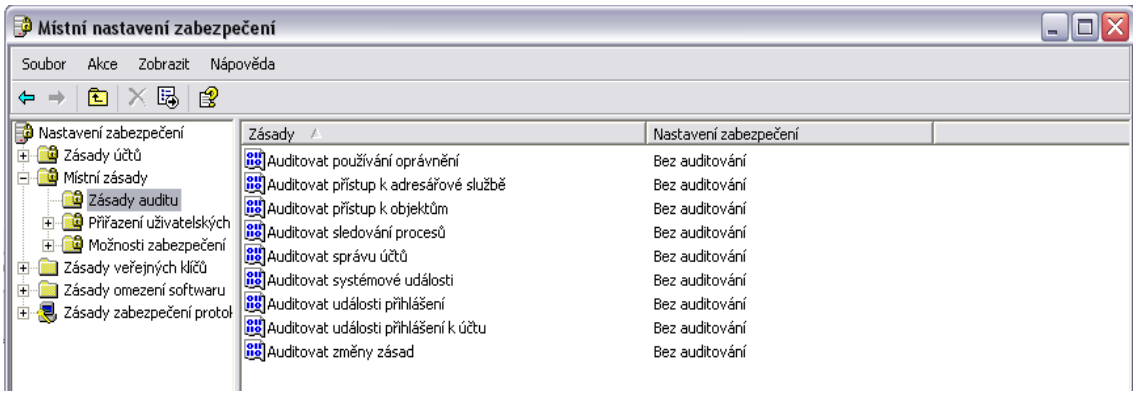
- **Číst** – Povoluje či zakazuje uživateli nebo skupině zobrazovat obsah klíče, ale nedovoluje ukládat žádné změny.
- **Úplné řízení** – Povoluje či zakazuje uživateli nebo skupině otevřít, uložit, upravit obsah a úroveň přístupu pro daný klíč.
- **Zvláštní oprávnění** – Povoluje či zakazuje uživateli nebo skupině speciální kombinaci oprávnění (obrázek č.24). Tato kombinace nabízí větší kontrolu přístupu než základní oprávnění.



Obrázek č.24: Typy Oprávnění pro uživatele DaOn

7.1.3 Auditování registru

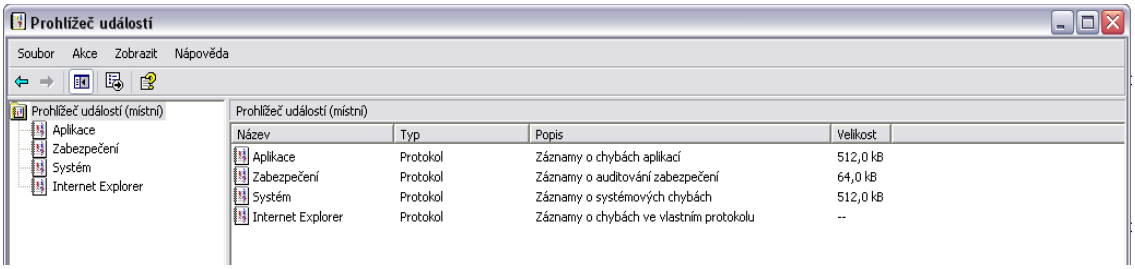
Auditace je proces používaný systémem Windows XP ke zjišťování a protokolování událostí souvisejících se zabezpečením. Těmito událostí je například každý pokus o vytvoření nebo odstranění systémových objektů nebo každý pokus o přístup k nim. Všechny události související se zabezpečením jsou registrovány v protokolu zabezpečení. Auditace není v systému implicitně aktivována (obrázek č.25).



Obrázek č.25: Možnosti zásad auditu v konzoly Místní zásady zabezpečení

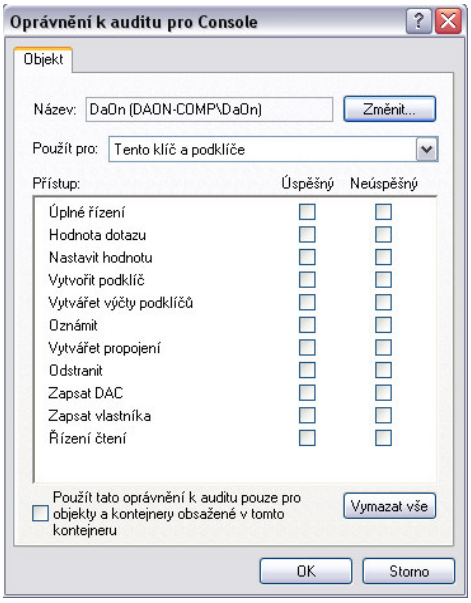
Aktivovat auditování lze pouze jako Administrator nebo člen skupiny Administrators. Po její aktivaci zahájí systém protokolování událostí. Informace

registrované v protokolu zabezpečení lze zobrazit pomocí *Prohlížeče událostí* (obrázek č.26).



Obrázek č.26: Okno Prohlížeče událostí v Nástrojích pro správu systému Windows XP

Při zahájení auditace lze definovat typy událostí, které budou registrovány v protokolu zabezpečení a operační systém vytvoří záznam pokaždé, když se stanovený typ událostí objeví v systému. Záznam zapsaný do protokolu zabezpečení obsahuje popis události, jméno uživatele, který akci provedl a datum a čas. Auditovat lze úspěšné a neúspěšné pokusy, protokol zabezpečení zobrazuje jména uživatelů. Možnosti auditování jsou velmi podobné možnostem *Oprávnění* (obrázek č.27).



Obrázek č.27: Možnosti Oprávnění auditování pro uživatele DaOn

7.1.4 Zásady skupiny

Nástroj *Zásady skupiny* byl poprvé představen v systému Microsoft Windows 2000. Systém Windows XP ukládá tyto zásady odděleně od uživatelských

nastavení. Existuje-li zásada, operační systém použije nastavení definované v této zásadě. Pokud zásada v registru není, operační systém použije uživatelské nastavení, případně výchozí nastavení. Daná zásada však nezmění příslušné uživatelské nastavení. Nejedná se tedy o trvalou změnu v registru.

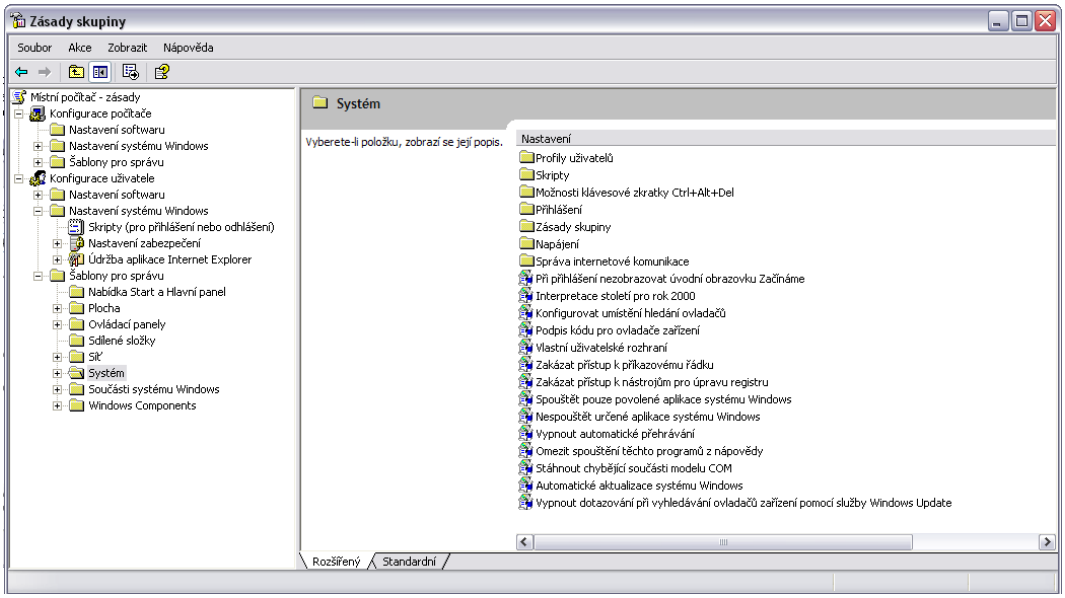
Systém Windows slučuje zásady do objektu zásad skupiny (GPO – Group Policy Object). Ve Windows XP je pouze jeden objekt GPO – *Místní GPO*. Nastavení v tomto objektu GPO platí pro místní počítač a pro každého uživatele, který se do systému na tomto počítači přihlásí. Mezi objekty GPO patří nastavení pro konfiguraci počítačů i uživatelů a obsahují následující větve:

- **Konfigurace počítače** – Nastavení zásad týkajících se počítače, které definují chování operačního systému, chování pracovní plochy, nastavení zabezpečení, skripty pro spouštění a vypínání počítače, aplikace přiřazené k počítači a nastavení aplikací. Windows uplatňuje tyto zásady při spuštění operačního systému a v pravidelných intervalech. [15]
- **Konfigurace uživatele** – Nastavení zásad týkajících se uživatelů, které definují chování operačního systému, nastavení pracovní plochy, nastavení zabezpečení, přiřazené a publikované aplikace, nastavení přesměrování složek, skripty pro přihlašování a odhlašování uživatele a nastavení aplikací. Windows uplatňuje tyto zásady při přihlášení uživatele a v pravidelných intervalech. [15]

Nástroj *Zásady skupiny* nabízí několik rozšíření, jejichž přehled uvádí následující seznam:

- **Skripty** – K uživatelům lze přiřadit skripty, které se spustí při přihlášení nebo odhlášení ze systému Windows. K počítačům pak skripty, které poběží při spouštění a vypínání systému. Toto rozšíření je ve složce *Nastavení systému Windows*.
- **Nastavení zabezpečení** – Toto rozšíření umožňuje provádět správu nastavení zabezpečení (včetně zásad hesel, auditu a uzamčení), správu uživatelských práv a omezení aplikací, které může uživatel spouštět. Je ve složce *Nastavení systému Windows*.
- **Šablony pro správu** – Toto rozšíření umožňuje zavedení nastavení registru (klíče HKCU nebo HKLM), které bylo pomocí *Zásad skupiny* uloženo do souboru *Registry.pol*, při spuštění systému a po přihlášení uživatele k počítači.[1]

Místní objekt GPO lze upravovat pomocí *editoru Zásad skupiny*. Ten lze otevřít zadáním příkazu *gpedit.msc* v dialogovém okně *Spustit* v nabídce *Start*. Sám editor je velmi podobný editoru registru jak ukazuje obrázek č. 28:



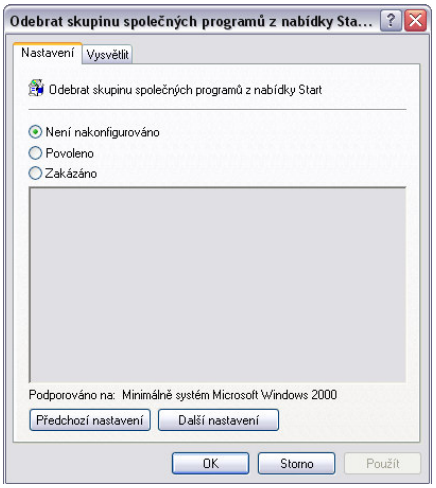
Obrázek č.28: Konzole Zásad skupiny v systému Windows XP

7.1.4.1 Zásady pro správu

Zásady pro správu, někdy též nazývané zásady založené na registru, jsou nastavení registru, která potlačují uživatelská nastavení, aby je uživatelé nemohli měnit. Úprava těchto zásad je prováděna pomocí *šablon pro správu* v *editoru zásad skupiny*. Systém Windows poskytuje následující šablony pro správu:

- **System.adm** – Základní nastavení a primární soubor *šablon pro správu* definující většinu nastavení
- **Wmplayer.adm** – Nastavení přerávače Windows Media Player
- **Conf.adm** – Nastavení komunikačního softwaru NetMeeting
- **Inetres.adm** – Nastavení prohlížeče Internet Explorer
- **Wuau.adm –** Nastavení služby Automatické aktualizace

U všech *zásad pro správu* je nastaven jeden ze tří stavů: Povoleno, Zakázáno, Není nakonfigurováno (obrázek č.29). [15]



Obrázek č.29: Možnosti nastavení zásady Odebrat skupinu společných programů z nabídky Start v systému Windows XP

Možnosti *Povoleno/Zakázáno* zapínají/vypínají nastavení zásad. Možnost *Není nakonfigurováno* odstraní nastavení z registru a následně je použito uživatelské nastavení.

Zásady pro správu jsou v registru přednostně ukládány do podregistru HKLM\Software\Policies (pro počítač) a HKCU\Software\Policies (pro uživatele). V systému souborů jsou uloženy ve složce %SystemRoot%\System32\GroupPolicy, která je implicitně skrytá. Tato složka obsahuje následující podsložky:

- **\Adm** – Obsahuje všechny soubory ADM pro místní objekt GPO.
- **\User** – Zde je umístěn soubor *Registry.pol*, který obsahuje zásady platné pro uživatele založené na registru.
- **\User\Scripts** – Obsahuje uživatelské skripty místního objektu GPO. Skripty ve složce \Logon se spouští při přihlášení uživatele k systému Windows a skripty ve složce \Logoff se spouští při odhlášení ze systému Windows.
- **\Machine** – Zde je umístěn soubor *Registry.pol*, který obsahuje zásady platné pro tento počítač.
- **\Machine\Scripts** – Obsahuje skripty místního objektu GPO pro počítač. Skripty ve složce \Startup běží při spuštění systému a skripty \Shutdown se spouští při vypínání systému.

Zásady pro správu lze upravit pomocí již zmíněných existujících šablon nebo vytvořením nových. Vytváření nových je však doporučováno pouze zkušeným uživatelům, neboť je velmi složité a primárně určeno pro vývojáře. [1][15]

7.2 Druhy ochrany registru

Nejjednodušším způsobem ochrany registru je zamezení přístupu uživatelů do registru. Toho lze docílit na systémech Windows XP nainstalovaných na oddílu NTFS nastavením oprávnění k důležitým souborům, včetně editoru registru, podregistrů a uživatelských profilů. Pokud je použit systém souborů FAT, nelze tento způsob použít. Microsoft oficiálně uvádí, že nejlepším způsobem ochrany Windows XP je ochrana hesel pro správu. Existuje však mnoho způsobů jak registr chránit. Mezi nejdůležitější patří:

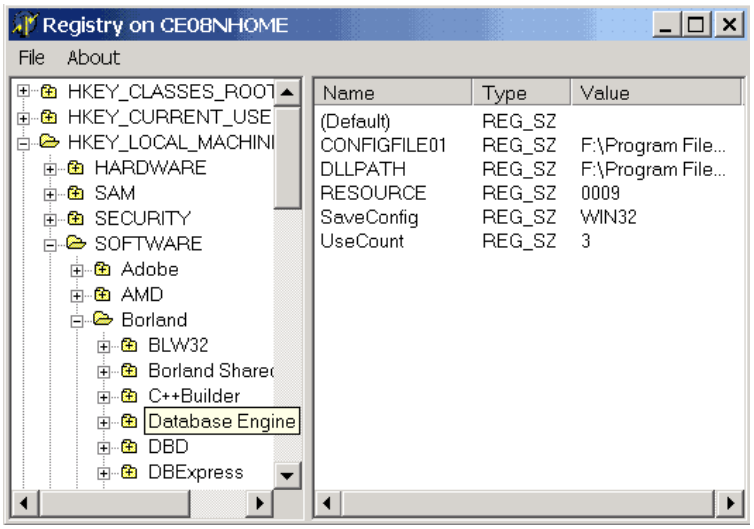
- **Ochrana před neautorizovaným vzdáleným přístupem** – Pomocí seznamu ACL v klíči HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg lze stanovit uživatele, kteří mají k registru vzdálený přístup. Pokud tento klíč v registru není nebo nemá nastaven seznam ACL, bude mít každý vzdálený uživatel přístup do registru, což je z hlediska ochrany a zabezpečení silně nedoporučováno. [15]
- **Ochrana SAM a podregistrů –** Podregistr SAM obsahuje uživatelská hesla, podregistr Security ukládá informace o zabezpečení pro místní systém, včetně uživatelských práv a oprávnění, zásad hesel a členství ve skupinách. Z tohoto důvodu jsou informace v podregistru SAM za účelem dosažení maximální ochrany šifrovány. [15]
- **Omezení anonymního přístupu k počítači** – Pro zamezení přístupu osobám, které nemají vytvořen svůj vlastní uživatelský účet, je možné učinit dva základní kroky. Každému uživatelskému účtu je vhodné přiřadit dostatečně silné heslo, aby bylo zajištěno, že k účtu bude mít přístup pouze jeho vlastník. Druhým krokem je zakázání uživatelského účtu pro anonymní přístup *Guest*.

8. Srovnání registru Win NT 4.0, 2K a Vista

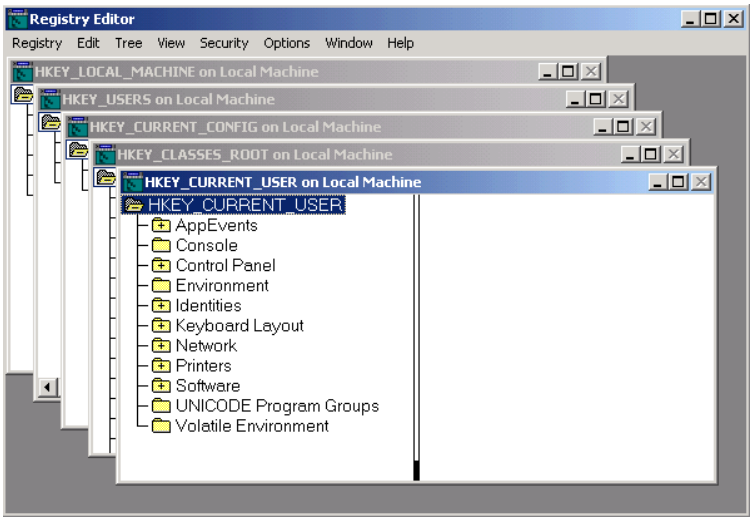
Registr Windows se v jednotlivých verzích operačního systému značně liší. Těchto odlišností je velké množství, proto se tato kapitola snaží poukázat jen na ty nejvýznamnější.

8.1 Vzhled

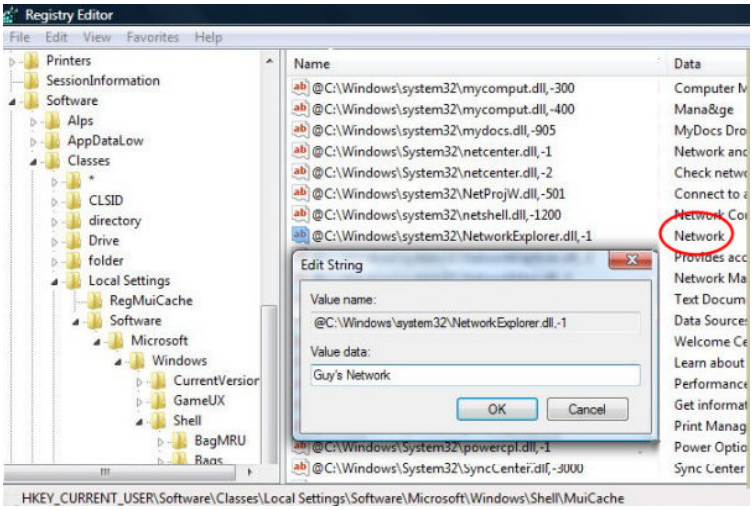
Vzhled editoru registru Windows se od Windows 3.11 značně změnil. Vzhled editoru registru v jednotlivých verzích Windows liší stejně jako se liší celé uživatelské grafické rozhraní. Zatímco ve Windows NT se jednotlivé klíče zobrazují v jednom okně nad sebou, ve Windows 2000 se jednotlivé klíče zobrazují v samostatných oknech. Panel nástrojů ve Windows NT je oproti ostatním verzím Windows značně chudší, obsahuje jen dvě položky a to *Soubor* a *O programu*.



Obrázek č.30: Editor registru Windows NT 4.0 [22]



Obrázek č.31: Editor registru Windows 2000 [23]



Obrázek č.32: Editor registru Windows Vista [24]

8.2 Ostatní

Struktura registru se od Windows NT až po verzi Vista dosti liší. Nejenže narůstala její složitost a přibylo šifrování některých klíčů, ale od verze Windows 2000 již není zobrazován klíč HKEY_DATA_DYN. Další významnější změnou je nová možnost způsobu práce s registrem pod Windows Vista. Windows Vista nově umožňuje změny klíčů nebo jejich hodnot nejen jednotlivě, ale i hromadně, což může znamenat výrazné zjednodušení a zrychlení práce. Novinkou ve Windows Vista jsou i nové podklíče, které umožňují správu nastavení grafického rozhraní včetně mnoha vizuálních efektů, které nebylo v předchozích verzích Windows pomocí registru možné měnit. Změny nastaly i v ukládání registru

v jednotlivých verzích. Data podregistrů ve Windows NT 4.0 jsou ukládána ve složkách %SystemRoot%\System32\Config a %SystemRoot%\Profiles\UserName. Ve Windows 2K, XP a Vista do %SystemRoot%\System32\Config a %SystemDrive%\Documents and Settings\UserName. [4] Velmi významnou změnou, mezi verzemi Windows NT/2000 a Windows XP/Vista, je odebrání omezení velikosti registru, což má dvě hlavní výhody. Možnost větší velikosti registru a rychlejší dotazování.

V souvislosti s přechodem z 32-bitového na 64-bitový systém byly ve Windows Vista přidány i nové 64bitové klíče registru. 32-bitové klíče běžící v 64-bitovém módu jsou uloženy v podklíči HKEY_LOCAL_MACHINE\Software\WOW6432node. Implicitní 64-bitové podklíče jsou uloženy v podklíči HKEY_LOCAL_MACHINE\Software, který slouží pro ukládání nativních klíčů dané verze Windows.

9. Závěr

Na počátku vývoje registru systémů Microsoft Windows byly INI soubory, které se ukládaly téměř všude po celém pevném disku, a nepřinášely uživatelům mnoho možností pro správu a úpravu registru. V průběhu vývoje se registr zdokonalil a stal se nedílnou součástí každých Windows. Možnosti jeho nastavení se s vývojem operačních systémů výrazně zlepšily a v dnešní době poskytuje nejen odborníkům a správcům systému, ale i běžným uživatelům spousty možností jak si Windows optimalizovat a přizpůsobit svým potřebám. Jeho složitost a malé množství informací poskytovaných firmou Microsoft způsobila odpor a neznalost běžných uživatelů, které však již díky aplikacím a editorům registru jiných společností pomalu opadají. Díky neustálému vývoji v oblasti operačních systémů se dá předpokládat, že i registr dozná do budoucna velkých změn, které již předeslal registr systému Windows Vista novými možnostmi. Zda se bude jednat o novinky zásadní a pozitivní ukáže až čas a schopnosti vývojářů, ale vzhledem ke stále se zvyšujícím nárokům uživatelů lze předpokládat, že tomu tak bude.

10. Seznam literatury

1. KOKOREVA, Olga, *Registr Microsoft Windows XP.* 2.vyd.Brno: Computer Press, 2004. 393 s. ISBN 80-7226-783-3.
2. SIMPSON, Alan. *Windows XP Bible*. [eBook]. Hungry Minds, 2001. 902 s. ISBN 0-764548-60-3.
3. HONEYCUTT, Jerry. *Windows XP Registry Guide*. [eBook]. Microsoft Press, 2003. 440 s. ISBN 0-735617-88-0.
4. MICROSOFT. *Rozdíly mezi nástroji Regedit.exe a Regedt32.exe*. [online]. [cit. 2007-05-04]. <http://support.microsoft.com/kb/141377/>.
5. WINDOWS IT LIBRARY. *How the registry is architected*. [online]. [cit. 2007-11-09]. <http://www.windowsitlibrary.com/Content/224/toc.html>.
6. THE ELDER GREEK. *Registry edits for Windows XP*. [online]. [cit. 2007-11-09]. <http://www.theeldergeek.com/registry_edits.htm>.
7. MICROSOFT. *Zálohování, úpravy a obnovení registru v systémech Windows XP a Windows Server 2003*. [online]. [cit. 2007-11-09]. <http://support.microsoft.com/kb/322756/cs>.
8. KELLYS KORNER. *Registry edits for Windows XP*. [online]. [cit. 2007-11-09]. <http://www.kellys-korner-xp.com/xp_tweaks.htm>.
9. WIKIPEDIA. *Component Object Model.* [online]. [cit. 2008-04-28]. <http://en.wikipedia.org/wiki/Component_Object_Model>.
10. MICROSOFT. *Informace o registru systému Windows pro pokročilé uživatele.* [online]. [cit. 2007-04-28]. <http://support.microsoft.com/kb/256986/cs>.
11. WIKIPEDIA. *Object Linking and Embedding.* [online]. [cit. 2008-04-29]. <http://en.wikipedia.org/wiki/Component_Object_Model>.
12. WIKIPEDIA. *American National Standards Institute.* [online]. [cit. 2008-04-30]. <http://en.wikipedia.org/wiki/American_National_Standards_Institute>.
13. WIKIPEDIA. *Unicode.* [online]. [cit. 2008-05-01]. <http://cs.wikipedia.org/wiki/Unicode>.
14. MICROSOFT WINDOWS SERVER TECHCENTER. *Struktura registru.* [online]. [cit. 2008-05-01]. <http://technet2.microsoft.com/windowsserver/cs/library/28e3337c-70ff-41e1-86ef-2581350712a91029.mspx?mfr=true>.
15. HONEYCUTT, Jerry. *Windows XP Registry Guide*. 1.vyd: . Computer Press, 2006. 546 s. ISBN 80-251-1265-9.

16. STUDNA. *TweakNow RegCleaner Professional.* [online]. [cit. 2008-05-04]. <http://www.studna.cz/8495/systemove-nastroje/programy-pro-optimalizaci-a-opravu-systemu/tweaknow-regcleaner-professional/>.
17. STUDNA. *TweakNow RegCleaner Professional.* [online]. [cit. 2008-05-05]. <http://www.studna.cz/pictures_small/84/95.jpg>.
18. MICROSOFT TECHNET. *RegMon for Windows.* [online]. [cit. 2007-05-05]. <http://www.microsoft.com/technet/sysinternals/processesandthreads/regmon.mspx>.
19. IMAGINELAN. *Product Tour.* [online]. [cit. 2008-05-03]. <http://www.imaginelan.com/images/screens/3selcomp.gif>.
20. MACICH. *Obnovení systému.* [online]. [cit. 2008-05-03]. <http://blog.macich.net/screenshoty/obnova.jpg>.
21. HORÁK, Jaroslav. *Hardware učebnice pro pokročilé*. [eBook]. 3 vyd. Brno: CP Books, 2005. 902 s. ISBN 80-251-0647-0.
22. ONLINE-ADMIN. *Registry Component.* [online]. [cit. 2008-05-05]. <http://www.online-admin.com/images/RegEditor_demo.gif>.
23. PETRI. *Windows 2000 Regedit.* [online]. [cit. 2008-05-05]. <http://www.petri.co.il/images/w2k_regedt32.gif>.
24. COMPUTERPERFORMANCE. *Vista Registry.* [online]. [cit. 2008-05-05]. <http://www.computerperformance.co.uk/images/Vista/network_icon_reg.jpg>.
25. REGEDIT.SK. *Úvod a história registra.* [online]. [cit. 2008-05-04]. <http://www.regedit.sk/index.php?action=zobraz&id=1049740665>.
26. MICROSOFT. *Špuštění nástroje Obnovení systému z příkazového řádku v systému Windows XP.* [online]. [cit. 2007-05-04]. <http://support.microsoft.com/kb/304449/>.
27. TWEAKNOW. *Products.* [online]. [cit. 2008-05-05]. <http://www.tweaknow.com/products.html>.
28. WIKIPEDIA. *Windows Registry.* [online]. [cit. 2008-05-05]. <http://upload.wikimedia.org/wikipedia/en/thumb/b/bb/Registration_Editor.png/180px-Registration_Editor.png>.

11. Seznam obrázků