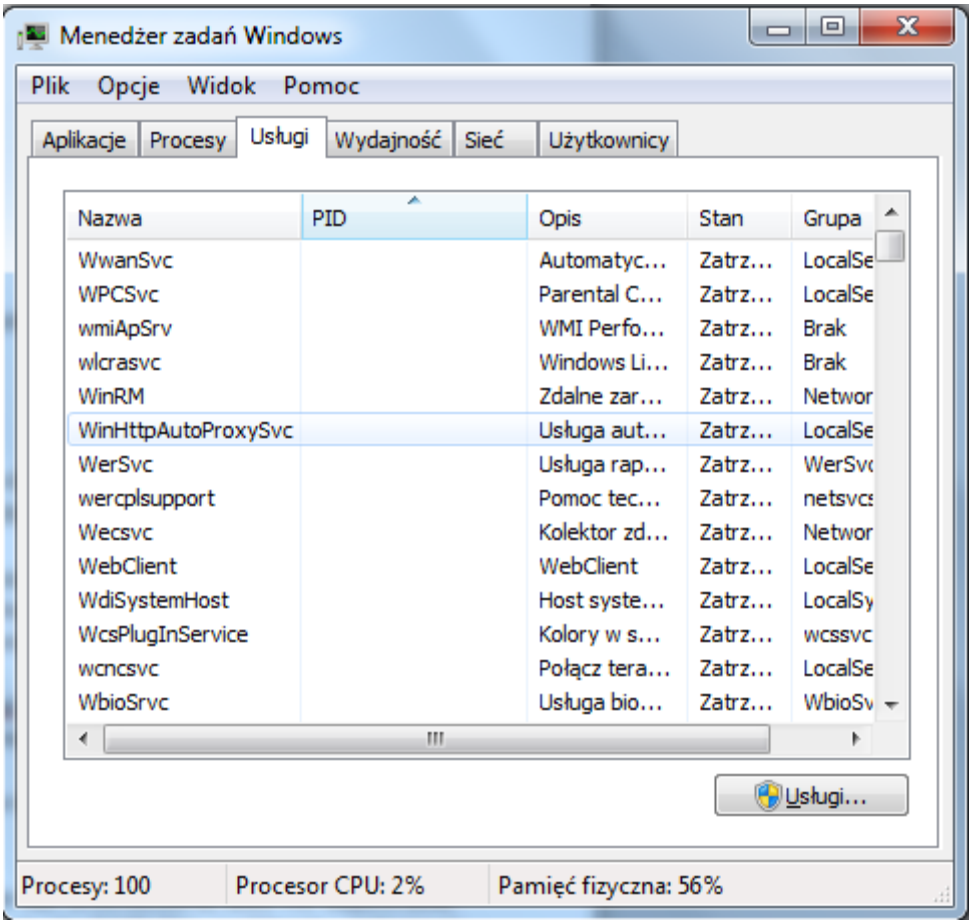
LABORATORIUM 5

Administracja systemem Windows

System Windows zapewnia szereg narzędzi umożliwiających zarządzanie nim.

Menedżer zadań



Menedżer zadań to narzędzie, które pozwala na szybkie uzyskanie informacji o bieżącym stanie systemu. Sposoby uruchamiania Menedżera zadań:

- Przez wciśnięcie kombinacji klawiszy CTRL+SHIFT+ESC
- Przez wciśnięcie kombinacji klawiszy CTRL+ALT+DEL, a następnie kliknięcie na przycisku Menedżer zadań
- Wybierając z menu Start opcję *Uruchom...*- w polu wyszukiwania wpisać polecenie *taskmgr*
- Przez kliknięcie prawym przyciskiem myszy w wolnym obszarze paska zadań, a następnie wybranie w menu kontekstowym polecenia Menedżer zadań

Menedżer zadań posiada zakładki: Aplikacje, Procesy, Usługi, Wydajność, Sieć i Użytkownicy. Każda z nich dostarcza innych informacji, a także oferuje inne opcje i kontrolki.

Zakładka Aplikacje pokazuje listę wszystkich działających w danym momencie aplikacji. Wyświetlana jest nazwa aplikacji oraz jej stan, który może być: uruchomiony albo (nie odpowiada). Aplikacja oznaczona jako uruchomiona działa bez problemów natomiast oznaczona jako nie odpowiada może być zawieszona, wykonywać niedozwolone operacje albo intensywne obliczenia, które chwilowo wstrzymały komunikację z systemem. Aby zakończyć działanie programu o takim stanie, należy odczekać kilka minut, aby aplikacja miała czas na powrót do normalnego trybu pracy. Jeśli po tym czasie program nie odpowiada, to aplikacja rzeczywiście się zawiesiła, aby przerwać jej działanie należy znaleźć ją na liście, zaznaczyć i kliknąć przycisk Zakończ działanie. Aplikacja zostanie usunięta z pamięci i kolejki procesów, zaś zasoby jakie wykorzystywała zostaną zwrócone do puli zasobów systemowych. Ponadto zakładka Aplikacje umożliwia nam także na uruchomienie nowych programów za pomocą przycisku Nowe Zadanie (można również kliknąć na liście prawym klawiszem myszy i wybrać Nowe zadanie(Uruchom…)).

Zakładka Procesy pokazuje listę wszystkich procesów działających w danej chwili w systemie. W zakładce tej znajdujemy listę wszystkich procesów działających zarówno w trybie jądra i w trybie użytkownika. Domyślnie ustawione jest wyświetlanie informacji: nazwa procesu, jego opis. użytkownik, który uruchomił proces, obciążenie CPU i zajętość pamięci.
Gdy chcemy wybrać inne kolumny korzystamy z polecenia Wybierz kolumny z menu Widok; możemy dodawać lub usuwać kolumny. Domyślnie wszystkie dane wyświetlone na zakładce Procesy są aktualizowane co sekundę. Domyślny przedział czasowy możemy zwiększać lub zmniejszać w menu Widok/Szybkość aktualizacji. Gdy proces nie ma co robić uruchamiany jest proces, który nie należy do żadnego trybu jest to tak zwany Systemowy proces bezczynny. Jeżeli konkretny proces używa przez dłuższy czas 90 i więcej procent czasu procesora, może to oznaczać, że działanie procesu jest błędne. Jednak niektóre procesy wykorzystują większą ilość czasu procesora, co oznacza że system jest przeciążony lub że pewne działania wymagają większej aktywności ze strony procesora.
Można też znaleźć proces odpowiadający aplikacji. Przykładowo Opera działa używając procesu o nazwie opera.exe. Na zakładce 'Aplikacje' znajdujemy aplikację, klikamy na niej prawym przyciskiem myszy i wybieramy 'Przejdź do procesu'; Na procesie klikamy prawym przyciskiem myszy i możemy wybrać 'Ustaw priorytet' taki, który nas interesuje. Aby zakończyć proces postępujemy tak samo, jak zmiana priorytetu tylko, że wybieramy opcję Zakończ proces.

Uwaga: Wyświetlenie wszystkich uruchomionych procesów umożliwia polecenie TASKLIST.

Zakładka Usługi – zawiera listę wszystkich usług oraz ich stan (to, czy w danej chwili usługa jest włączona - aktywna, czy też wyłączona). Klikając na kolumny, możemy sortować wyświetlanie tej listy według różnych kryteriów, na przykład nazwy, PID, opisu, stanu, czy grupy.
Za pomocą przycisku **Usługi...** zlokalizowanego w dolnym prawym rogu okna, przenosimy się do panelu zarządzania usługami. Jest to jeden z elementów tzw. **narzędzi administracyjnych**. Z tego poziomu możemy zadecydować nie tylko o tym, czy chcemy włączyć lub wyłączyć usługę, ale także, czy ma się ona uruchamiać razem z systemem.
Aby uruchomić lub zatrzymać usługę z poziomu Menadżera zadań, klikamy na jej nazwę prawym przyciskiem myszy i wybieramy odpowiednie polecenie. Usługa zostanie zatrzymana lub uruchomiona do czasu kiedy zrestartujemy komputer.

Zakładka Wydajność – pozwala oszacować wydajność systemu poprzez graf działania procesora, pamięci oraz procesów. Wykres pokazuje użycie pamięci, aktualny stan pamięci, graf przedstawia stan 20 ostatnich pomiarów. Pod wykresami znajduje się informacja dotycząca 12 parametrów wydajności:

- Dojścia- ile dojść do obiektów systemowych znajduje się w użyciu (np. klucze rejestru).
- Wątki – ile ich działa w systemie
- Procesy – ile procesów działa w systemie

- Pamięć fizyczna razem – pokazuje rozmiar w kilobajtach fizycznej dostępnej pamięci RAM
- Pamięć fizyczna buforowana – wyświetla rozmiar, w KB dostępnej pamięci RAM używanej do buforowania plików.
- Pamięć zadeklarowana: razem – rozmiar całkowitej pamięci wirtualnej zaalokowanej dla procesów lub systemu
- Pamięć zadeklarowana: limit – określa jaki jest rozmiar max. ilości pamięci wirtualnej zaalokowanej dla procesów lub systemu
- Pamięć zadeklarowana: szczyt – jaka jest max ilość pamięci wirtualnej zaalokowanej dla procesów lub systemu podczas tej sesji systemu
- Pamięć jądra: razem- wyświetla ilość pamięci używanej przez jądro
- Pamięć jądra: stronicowana – wyświetla ilość pamięci używanej przez jądro, która może zostać przeniesiona do pliku stronicowania
- Pamięć jądra: niestronicowana – jaka jest ilość pamięci używanej przez jądro, która zawsze pozostaje w fizycznej pamięci RAM

Wykres przedstawia dwie linie zieloną która, określa czas wykorzystania przez procesy w trybie użytkownika oraz linię czerwoną, która określa czas procesora wykorzystanego w trybie jądra.

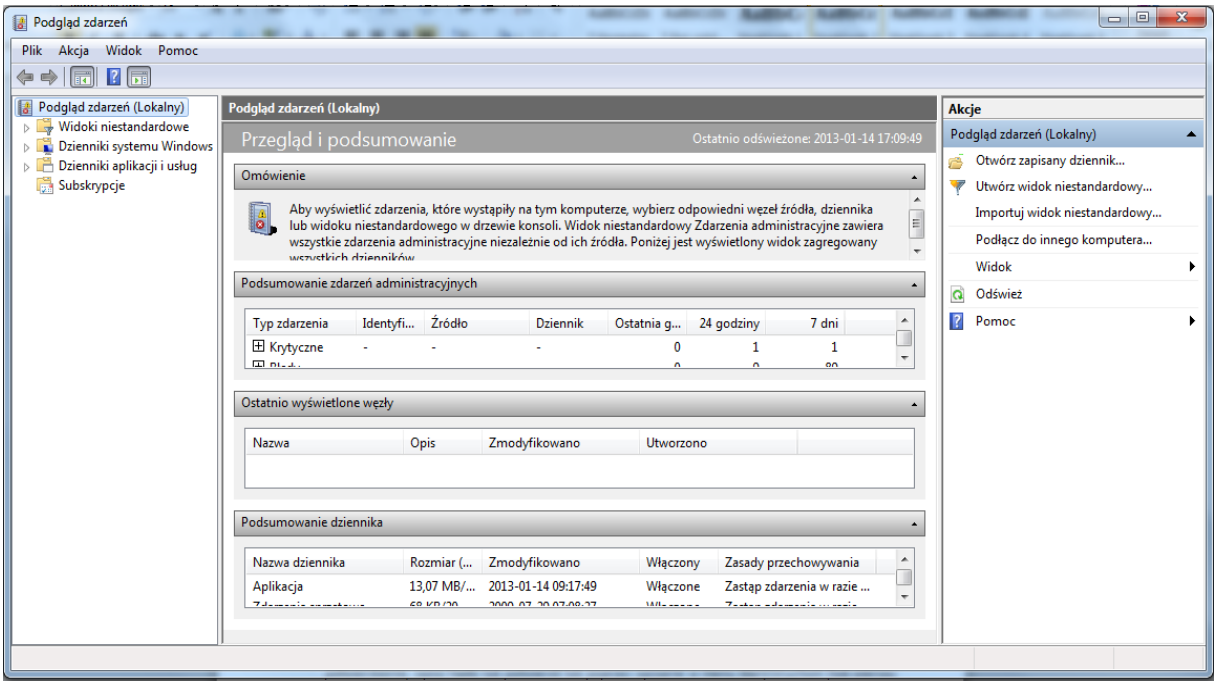
Zakładka Sieć - pozwala zobaczyć wykres pokazujący w czasie rzeczywistym wykorzystanie sieci, a dokładniej procentowy stopień wykorzystania pasma każdej karty sieciowej zainstalowanej w komputerze. Poziom wykorzystania pasma stale pozostający na bardzo wysokim poziomie, może świadczyć o wąskim gardle w komputerze bądź sieci.

W menu **Widok** mamy do dyspozycji kilka dodatkowych opcji, opisanych poniżej:

- **Szybkość aktualizacji -** pozwala określić jak często wykres ma być odświeżany
- **Historia karty sieciowej** - tutaj mamy możliwość włączenia opcji pokazywania bajtów przychodzących oraz wychodzących na wykresie
- **Wybierz kolumny... -** daje nam możliwość wyświetlania dodatkowych informacji w tabeli pod wykresem

Zakładka Użytkownicy- wyświetla listę użytkowników, możemy (o ile jesteśmy administratorem komputera lub członkiem grupy Administratorzy) zobaczyć informacje o sesjach innych użytkowników. Naciskając przycisk **Wyloguj** wymusimy natychmiastowe zakończenie sesji wybranego użytkownika. W rezultacie uruchomione przez niego aplikacje zostaną zamknięte, a nie zapisane dane utracone.

Podgląd zdarzeń



Narzędzie stworzone przez firmę Microsoft umożliwiające nam podgląd zdarzeń mających miejsce w systemie. Za zdarzenia uważa się zdarzenia systemu operacyjnego lub błędy spowodowane przez aplikacje lub urządzenia podłączone do komputera oraz informacje dotyczące działania systemu, które docierają do administratora (np. przepełnienie dysku).

Podgląd zdarzeń możemy uruchomić na kilka sposobów m.in. poprzez wpisanie w menu Start/Uruchom (lub wierszu poleceń) polecenia eventvwr.msc lub klikając przycisk Start, polecenie Panel sterowania, pozycję System i zabezpieczenia i pozycję Narzędzia administracyjne, a następnie klikając dwukrotnie pozycję Podgląd zdarzeń, jeśli zostanie wyświetlony monit o hasło administratora lub potwierdzenie, wpisz hasło lub potwierdź.

Podgląd zdarzeń śledzi informacje w kilku różnych dziennikach. Dzienniki systemu Windows to:

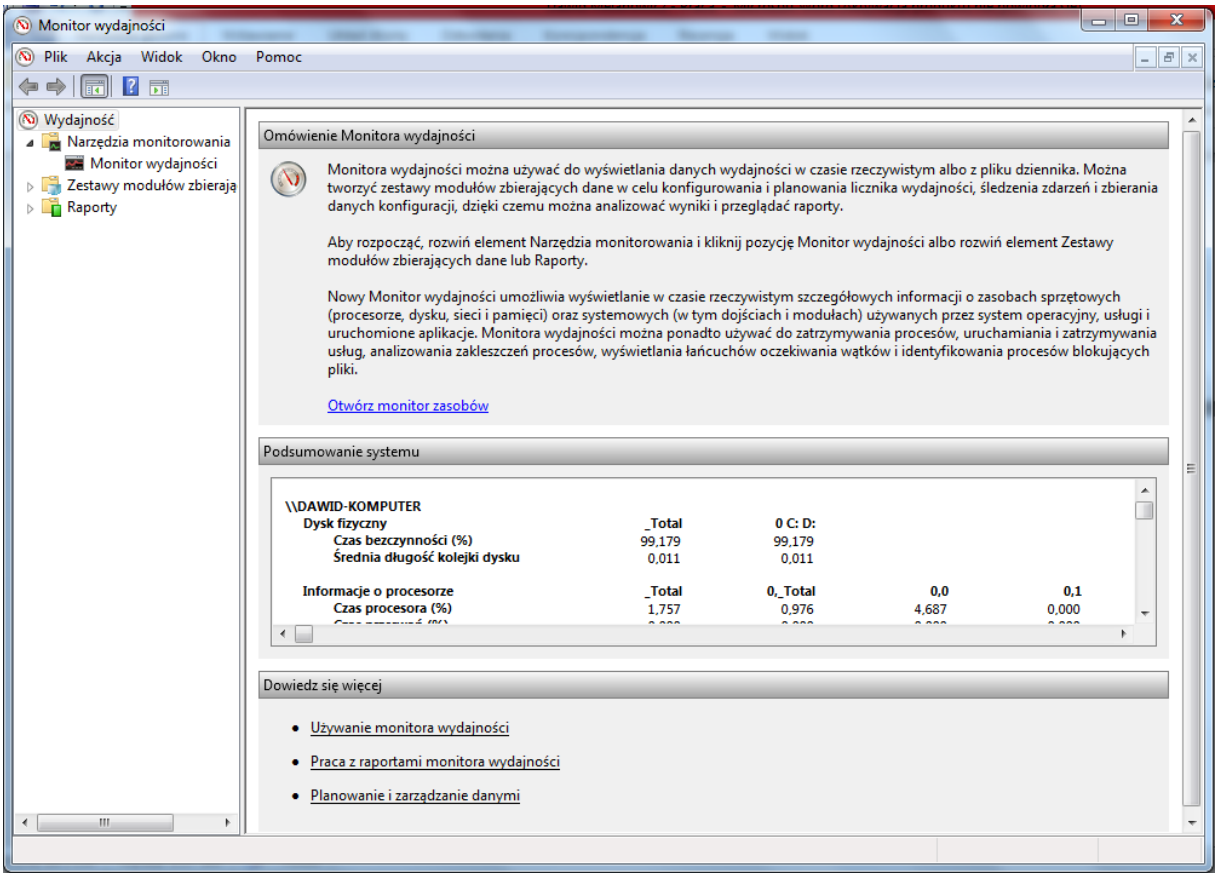
Zdarzenia aplikacji (programu). Zdarzenia są klasyfikowane jako błąd, ostrzeżenie lub informacja w zależności od ważności zdarzenia. Błąd oznacza poważny problem, taki jak utrata danych. Ostrzeżenie oznacza zdarzenie niekoniecznie znaczące, ale wskazujące możliwość wystąpienia problemu w przyszłości. Zdarzenie informacyjne opisuje prawidłowe funkcjonowanie programu, sterownika lub usługi.

Zdarzenia związane z zabezpieczeniami. Te zdarzenia są nazywane inspekcjami i są określane w zależności od zdarzenia jako zakończone powodzeniem lub niepowodzeniem. Przykładem inspekcji może być wynik próby zalogowania się użytkownika do systemu Windows.

Zdarzenia instalacji. Dla komputerów skonfigurowanych jako kontrolery domeny będą tutaj wyświetlane dodatkowe dzienniki.

Zdarzenia systemowe. Zdarzenia systemowe są rejestrowane przez system Windows i usługi systemu Windows. Są one klasyfikowane jako błąd, ostrzeżenie lub informacja.

Monitor wydajności



Pozwala sprawdzić, jak radzą sobie poszczególne podzespoły komputera. Mimo że Windows 7 radzi sobie lepiej niż jego poprzednicy, to nadal stosuje się monitor wydajności. Za pomocą wbudowanego narzędzia możesz ocenić, który komponent stanowi tak zwane wąskie gardło i które procesy sprawiają najwięcej kłopotu.

Kika sposobów uruchomienia Monitora Wydajności:
• W wierszu poleceń wpisz perfmon
• Start \ Uruchom wpisz polecenie monitor
• Start \ Panel sterownia \ Narzędzia administracyjne \ Monitor Wydajności
• Start \ Uruchom wpisz polecenie perfmon

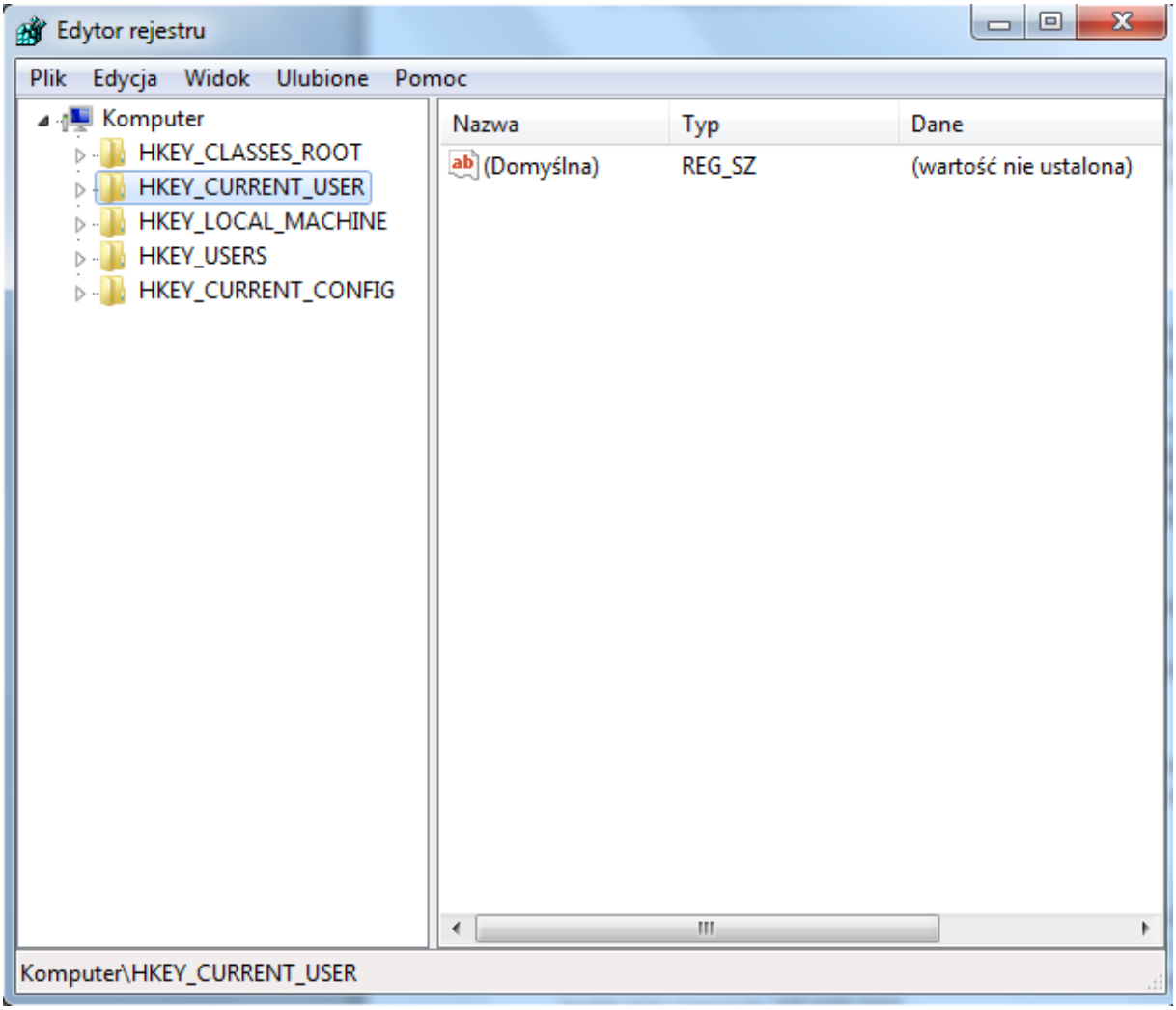
Monitor wydajności domyślnie nie wyświetla żadnych liczników. Aby umieścić w oknie Monitora wydajności licznik, musimy wykonać następujące kroki:

1. Prawym klawiszem myszy (PPM) klikamy w dowolnym miejscu okna Monitora Wydajności i z menu wybieramy dodaj licznik. Wyświetli się okno Dodawanie Liczników.
2. Z Listy Dostępne Liczniki wyświetl listę dostępnych liczników.
3. Wybierz licznik który ma być wykorzystany. Jeżeli licznik posiada wiele wystąpień, pojawią się one na liście. Klikamy Dodaj.
4. Potwórz wcześniejsze kroki, aby dodać inne liczniki.
5. Klikamy przycisk OK.

Narzędzie Monitora wydajności powinno zostać skonfigurowane tak, aby użytkownik widział interesujące go aspekty (rozmiar pliku stronicowania, ilość wolnej pamięci itp.). Jeśli pojawią się

problemy z wydajnością systemu operacyjnego, możemy sprawdzić za pomocą tego programu, czy wystąpiły jakiekolwiek wąskie gardła lub zakłócenia.

Rejestr Windows 7



Rejestr jest bazą ustawień konfiguracyjnych, aplikacji i sterowników urządzeń. Rejestr zawiera różnego rodzaju informacje, począwszy od koloru tła pulpitu, ustawień kont użytkowników po domyślne ustawienia aplikacji. Rejestr jest przechowywany w bazie hierarchicznej, która może być bezpośrednio zmieniana za pomocą wbudowanego edytora rejestru Windows - **Regedit**, aby go uruchomić użyj start>uruchom>**regedit.**
Każdy wpis rejestru jest oznaczony ścieżką i wartością. Ścieżka składa się z poddrzewa, gałęzi, klucza i podkluczy. Wartość składa się z nazwy wartości, typu danych i danych. Główne składniki tego drzewa to:

- Poddrzewa. Poddrzewa są węzłami podstawowymi, które zawierają klucze, podklucze i wpisy wartości
- Klucze – klucz odpowiada folderowi widocznemu w oknie Eksploratora Windows. Może zawierać wpisy podkluczy i wartości
- Podklucze – są to klucze wewnątrz kluczy

- Wpis wartości – ciąg danych, który pojawia się w prawym oknie Rejestru i definiuje wartość zaznaczonego klucza. Wpis wartości ma trzy części; nazwę, typ danych i wartość. Te wpisy będą edytowane za pomocą Edytora rejestru.

Rejestr składa się siedmiu plików, sześć z nich znajduje się w folderze Windows: COMPONENTS, DEFAULT, SAM, SECURITY, SOFTWARE, SYSTEM. Siódmy plik przechowuje ustawienia osobiste użytkowników. Znajduje się on w folderze danego konta jego nazwa to NTUSER.DAT.

Rozszerzenia plików, w których przechowywane są informacje Rejestru to :

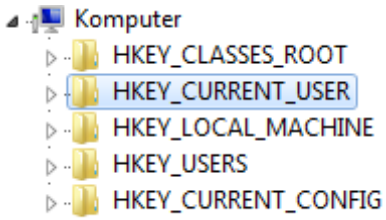
- Brak rozszerzenia – plik taki jest pełną kopią danych katalogu
- .alt – kopia zapasowa katalogu HKEY_LOCAL_MACHINE\System.
- .log – plik przechowujący dokonane zmiany w danym katalogu
- .sav – podczas instalacji systemu operacyjnego program instalacyjny używa plików o tym rozszerzeniu do przechowywania katalogów opisujących aktualny stan w chwili zakończenia procesu instalacji w trybie tekstowym. Jeśli wystąpi błąd podczas trybu graficznego procesu instalacji systemu Windows 7, pliki o rozszerzeniu .sav są wykorzystywane do przywrócenia informacji z katalogów.

• Typy danych rejestru

REG_BINARY - przechowuje binarnie 16-bitową wartość dwubajtową
REG_DWORD - przechowuje wartość szesnastkową o długości słowa, 8 cyfr szesnastkowych. Rozmiar owej wartości wynosi 32 bity czyli 4 bajty
REG_SZ - wartość łańcuchowa, która, umożliwia zapisanie w rejestrze wartości najmniej obciążającej pamięć np. pojedynczego znaku lub bajtu.
REG_EXPAND_SZ - wartość łańcuchowa, która, umożliwia obsługę zmiennych środowiskowych
REG_MULTI_SZ - wartość łańcuchowa, która, umożliwia z obsługę kilku wartości.

Wpisy rejestru umieszczone są w strukturze hierarchicznej, gdzie najwyższy poziom składa się z poddrzewa.

Głównym elementem Rejestru są klucze główne :



HKEY_CLASSESS_ROOT - jest to najbardziej rozbudowany z kluczy, Windows przechowuje w nim informacje o typach plików, np. o formacie graficznym .gif. Klucz determinuje również programy, które mają służyć do otwierania plików danego typu.
HKEY_CURRENT_USER zapisane tutaj ustawienia dotyczą tylko aktualnie aktywnego konta użytkownika.
HKEY_LOCAL_MACHINE - zapisane ustawienia dotyczące komputera, np. sterowników do sprzętu i ich ustawień.

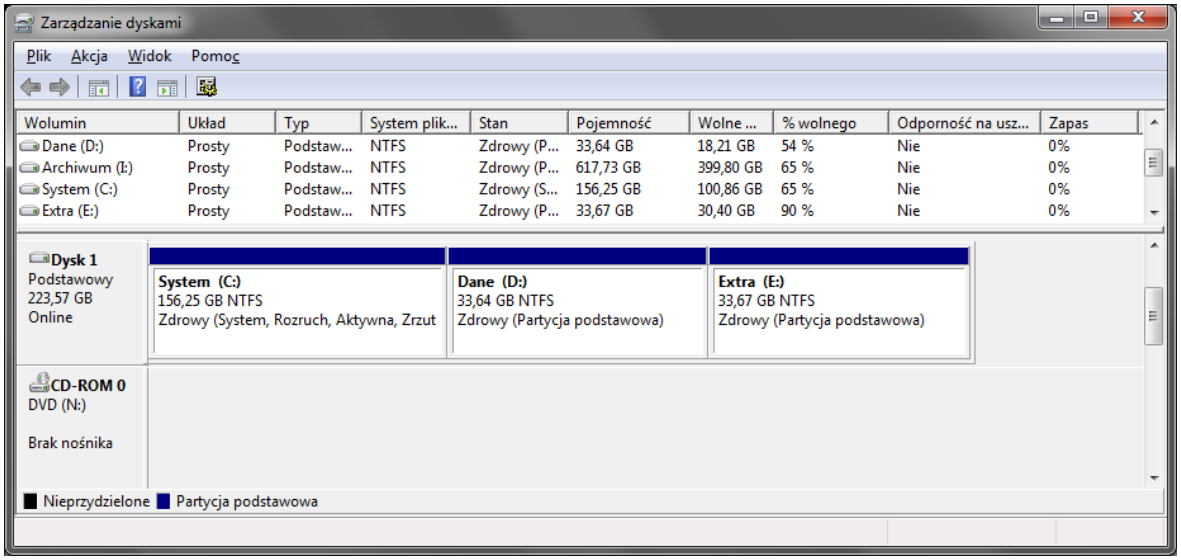
HKEY_USERS - w tym kluczu zapisane są ustawienia wszystkich użytkowników komputera. Kiedy do komputera zaloguje się zupełnie nowy użytkownik, to właściwe podklucze zostaną automatycznie przesunięte do klucza.
HKEY_CURRENT_CONFIG - klucz zawiera aktualne ustawienia wszystkich wbudowanych i podłączonych do komputera urządzeń.

Główne podklucze występują poniżej kluczy głównych :

HKLM\HARDWARE – jest tworzony podczas pierwszego uruchomienia systemu zawierają się w nim konfiguracje sprzętowe systemu.
HKLM\SAM- ten podklucz zawiera informacje o bazach danych użytkowników. W Windows 7 są one przechowywane w aktywnej kartotece.
HKLM\SECURITY – zawiera informacje o zabezpieczeniach systemu m.in. uprawnienia aktualnie zalogowanego użytkownika, czy zasady zabezpieczeń. Nie można modyfikować tego podklucza.
HKLM\SOFTWARE – przechowywane są tu informacje o oprogramowaniu zainstalowanym w systemie.
HKLM\SYSTEM – zawiera informacje które, dotyczą bieżącej sesji.

Uwaga: ZMIANY W REJESTRZE MOGĄ DOPROWADZIĆ DO NIESTABILNOŚCI SYSTEMU. EDYTUJ REJESTR TYLKO W OSTATECZNOŚCI, MAJĄC JEGO KOPIĘ ZAPASOWĄ I DOKŁADNIE WIEDZĄC, CO CHCESZ ZMIENIĆ.

Menedżer dysków (Zarządzanie dyskami)



Istnieje kilka sposobów uruchomienia menadżera dysków m. in. klikając menu ***Start | Uruchom***, wpisać **diskmgmt.msc** i wcisnąć [Enter].

Narzędzie Zarządzanie dyskami służy do wykonywania zadań:
• Tworzenie partycji
• Usuwanie partycji
• Formatowanie woluminów
• Zarządzanie dyskami lokalnymi i zdalnymi
• Skanowanie i naprawa błędów dyskowych
• Monitorowanie i wyświetlanie informacji o woluminie
• Rozciąganie woluminów poprzez dodawanie obszarów wolnej przestrzeni.

Użytkownicy i grupy

Proces logowania

Rozpoczynając prace z systemem operacyjnym na danym komputerze lokalnym Windows 7 musimy w oknie logowania wybrać użytkownika oraz podać prawidłowe hasło dostępu, gdy zostaniemy o to poproszeni. Windows sprawdza czy informacje podane są zgodne z danymi o autoryzowanych użytkownikach, zapisanymi w wewnętrznej bazie danych. Jeśli wszystko jest prawidłowe użytkownik zostanie zalogowany. Jeżeli poda błędne dane i na ekranie pojawi się komunikat o błędzie, to zostanie poproszony o wprowadzenie ich jeszcze raz.

Stosując takie rozwiązanie na danym komputerze :
• Chronimy swoje dane przechowywane na dyskach przed dostępem do nich osób niepowołanych, które nie znają prawidłowego identyfikatora użytkownika oraz hasła dostępu.
• Umożliwiamy korzystanie z tego samego komputera kilku autoryzowanym użytkownikom bez konieczności dzielenia się obszarem danych, bądź korzystania ze wspólnych programów oraz ustawień.
Logując się do sieci domenowej oprócz standardowo nazwy użytkownika i hasła należy podać dodatkowo nazwę serwera lub nazwę domeny (w polu nazwa użytkownika wpisujemy Identyfikator użytkownika@nazwa domeny). Aby wywołać okno logowania naciska się klawisze Ctrl+Alt+Del.

Konta użytkowników

Konta użytkowników służą w szczególności do identyfikacji poszczególnych użytkowników w systemie operacyjnym i uzyskania dostępu do zasobów. Nazwa konta użytkownika musi być niepowtarzalna i składać się maksymalnie z 64 znaków (zalecane jest używanie nazw krótszych niż 15 znaków), ale może zawierać dowolną kombinację liter, cyfr oraz większości symboli (wyjątkami są znaki: @, /, \, <, >, [,], :, ;, +, =, *, |,,, ?,.). Windows 7 dopuszcza stosownie spacji w nazwie konta.

Po zainstalowaniu Windows 7 ma dwa wbudowane konta użytkowników Administrator oraz Gość. Administrator ma pełną kontrolę, posiada specjalne uprawnienia(): nie można go wyłączyć, usunąć, czy zablokować. Konto Administrator umożliwia m.in.
• tworzenie nowych kont użytkowników i zarządzanie nimi
• instalację oprogramowania i sprzętu
• tworzenie praw dostępu do folderów, plików i drukarek
• tworzenie lokalnych grup domeny i zarządzanie nimi

Konto Gość jest jednym z predefiniowanych kont systemu operacyjnego Windows 7. Logując się jako Gość, uzyskujemy dostęp do systemu przez podanie identyfikatora użytkownika oraz dowolnego hasła dostępu.

Domena Windows 7

To zbiór komputerów w sieci, których zasoby i bezpieczeństwo są kontrolowane przez wyznaczony serwer, nazwany głównym kontrolerem domeny. System Windows 7 korzysta z usługi Active Directory (ADS – Active Directory Services) w strukturze tego typu konta użytkowników, grup i komputerów są grupowane w jednostkach organizacyjnych, co pozwala na łatwiejszą administrację. Użytkownicy Windows 7 logują się do kontrolera domeny, który sprawdza istnienie danego konta dla danego użytkownika w bazie danych katalogu ADS, poprawność podanego hasła dla danego

użytkownika, a następnie pozwala na zalogowanie się do domeny. Żaden komputer w Windows 7 nie pełni roli podstawowego kontrolera domeny. Tylko serwery działają jako kontrolery domeny Windows 7. Administratorzy domeny mają możliwość definiować zasady bezpieczeństwa dla wszystkich komputerów w domenie.

Grupa robocza

Połączenie grupy komputerów, które umożliwia wymianę danych, współużytkowanie drukarek, dysków i innych zasobów. Każdy komputer w grupie z osobna jest odpowiedzialny za bezpieczeństwo zgromadzonych w nim danych. Aby udostępnić innym członkom grupy roboczej swoje zasoby należy utworzyć folder lokalny oraz nadać mu odpowiednie prawa dostępu dla określonej grupy. Do danej grupy może podłączyć się każdy, kto zna nazwę folderu i odpowiednio skonfiguruje ustawienia sieciowe swojego komputera.

Zadania grupy

Konta użytkowników mogą korzystać z tych samych uprawnień wystarczy tylko zorganizować je w odpowiednie grupy, co pozwala na łatwiejszą pracę administratora, gdyż nie musi nadawać uprawnień pojedynczym kontom tylko jednorazowo grupie kont użytkowników. Stając się członkiem grupy, nowy użytkownik dziedziczy wszystkie jej uprawnienia oraz aplikacje i dane. Dwa typy grup kont użytkowników są na poziomie domeny: grupy dystrybucyjne oraz zabezpieczeń. Każdy z tych typów dzieli się na Grupy uniwersalne, globalne oraz grupy domeny. Windows 7 Professional posługuje się grupami zabezpieczeń, które służą do nadawania uprawnień kontom użytkowników. Administrator może organizować konta użytkowników w lokalne grupy domeny w sieciach domenowych lub w grupy lokalne w środowiskach grup roboczych.

Grupy wbudowane

W Windows 7 jest sześć wbudowanych grup lokalnych :
• Administratorzy
• Goście
• Użytkownicy - członkowie tej grupy mogą uruchamiać oprogramowanie już zainstalowane, nie mogą instalować nowego oprogramowania oraz zmieniać konfiguracji systemu.
• Użytkownicy zaawansowani – nie mają dostępu do plików innych użytkowników, nie mogą zmieniać konfiguracji systemu natomiast mogą instalować oprogramowanie i sterowniki.
• Operatorzy kopii zapasowych – użytkownicy do niej należący mają dostęp do wszystkich plików przechowywanych w danym komputerze, ale tylko jeśli posiadają oprogramowanie do wykonywania kopii zapasowych.
• Replikator – grupa ta ściśle służy replikacji i nie powinna zawierać żadnych użytkowników z wyjątkiem konta używanego do wykonywania usługi replikacji. Standardowo grupa ta jest używana przy replikacji domeny.

Grupy specjalne

System Windows 7 automatycznie tworzy kilka dodatkowych grup.

• **Interakcyjna** ta grupa zawiera użytkownika aktualnie zalogowanego na komputerze. Podczas aktualizacji do systemu Windows 7, członkowie tej grupy zostaną dodani do grupy Użytkownicy zaawansowani, dzięki czemu starsze aplikacje będą działać tak samo, jak przed aktualizacją.

• **Sieć.** Grupa ta zawiera wszystkich użytkowników, którzy mają aktualnie dostęp do systemu przez sieć. Podczas gry serwery terminali są instalowane w trybie obsługi aplikacji, ta grupa zawiera wszystkich użytkowników, którzy są aktualnie zalogowani w systemie za pomocą serwera terminali. Programy uruchomione przez użytkownika w systemie Windows NT 4.0 będą działały dla użytkownika serwera terminali w systemie Windows 7. Domyślne uprawnienia przypisane do grupy umożliwiają użytkownikowi serwera terminali uruchamianie większości starszych programów.

Profile użytkownika

Zastosowano to rozwiązanie w celu zachowania środowiska konkretnego użytkownik nawet wtedy, kiedy dany profil loguje się poprzez różne systemy w sieci. Kiedy logujemy się po raz pierwszy do systemu zostaje tworzony profil użytkownika zawierający zestaw folderów i plików przeznaczonych do wyłącznej dyspozycji danego użytkownika tzn. jest to miejsce gdzie system zapisuje wszystkie osobiste dane użytkownika i informacje o różnych ustawieniach (np. zawartość folderu Moje dokumenty) w folderze Documents and Settings.

Windows 7 pozwala na stosowanie trzech rodzajów profilu użytkownika :
• **Profil lokalny** –tworzony jest automatycznie podczas pierwszego logowania użytkownika w danym komputerze. Jest umieszczony w pod folderze Documents and Settings i ma posiada taką samą nazwę, jak nazwa konta użytkownika.
• **Profil mobilny** –administrator sieci tworzy profil jest i przechowywany na serwerze Windows 7 lub Windows NT. Wszystkie zmiany profilu są zapisywana na serwerze i dlatego, gdy użytkownik loguje się w różnych komputerach, otrzymuje zawsze ten sam profil użytkownika.
• **Profil obowiązkowy** – jest to odmiana profilu mobilnego. Zawiera ustawienia użytkownika, których on nie może zmienić. Zastosowanie ma w dużych sieciach w których użytkownicy mogą tylko wykonywać operacje i uruchamiać programy zatwierdzone przez administratorów. Podczas każdego logowania się do systemu, profil użytkownika jest lokalnie buforowany, a dokładniej mówiąc podczas kolejnego logowania użytkownik zaloguje się do tego samego systemu, poprzez sieć zostaną pobrane tylko te elementy profilu, które uległy zmianie. Podczas logowania się na konto Gość, które jako jedyne nie posiada własnego unikalnego profilu, jest przypisany domyślny profil użytkownika. Nie będą zapisywane żadne zmiany dokonywane przez użytkownika Gość i nie będzie tworzona korekta dla tego profilu.

Katalog macierzysty

Katalog danego użytkownika, który zawiera jego własne dane, co za tym idzie jest to obszar przydzielony każdemu użytkownikowi, w którym może on przechowywać swoje pliki. Do swojego katalogu macierzystego użytkownik może przydzielać uprawnienia.

Mapowanie dysków

Technika umożliwiająca na przypisanie liter dysków poszczególnym udziałom sieciowym, czyli komputerom, folderom, dyskom to mapowanie dysków. Głównym zadaniem jest traktowanie udziałów sieciowy tak jakby to były dyski lokalne.

Jak dokonać mapowania ?

Otwieramy Eksploratora Windows potem Narzędzia / Mapuj dysk sieciowy. Na ekranie pojawi się kreator mapowania dysków. Rozwiń listę Dysk i wybierz literkę, jaką będzie oznaczony wybrany udział sieciowy. W polu Folder wpisz nazwę udziału w formacie UNC (czyli \\nazwa_serwera\nazwa udziału) lub naciśnij przeglądaj, aby wyszukać i zaznaczyć żądany udział.

Zabezpieczenia w Windows 7

W Windows 7 został wprowadzony nowy moduł o nazwie Centrum akcji - zastępuje on Centrum zabezpieczeń znane z poprzednich wersji systemów Windows. W Centrum akcji wyświetlana jest lista komunikatów dotyczących ustawień zabezpieczeń i konserwacji, które wymagają uwagi użytkownika. W przypadku wykrycia problemu Centrum akcji wyświetla alerty o dwóch poziomach ostrzeżenia:

- **Pomarańczowy** - Program Centrum akcji systemu Windows wykrył możliwy problem w tym obszarze. Program Centrum akcji systemu Windows wyświetla informacje na temat potencjalnego problemu wraz z zalecanym rozwiązaniem.
- **Czerwony** - Program Centrum akcji systemu Windows wykrył poważny problem w tym obszarze. Problem ten może wpłynąć na zabezpieczenia systemu. Program Centrum akcji systemu Windows wyświetla informacje na temat problemu wraz z zalecanym rozwiązaniem.

Aby otworzyć Centrum Akcji

- Start > Panel sterowania, a następnie w obszarze System i zabezpieczenia klikając pozycję Zapoznaj się ze stanem komputera.

Pozwolenia dostępu do katalogów

Windows 7 współpracuje z systemami plików : FAT, FAT32, NTFS. Pierwsze dwa nie zawierają mechanizmów zabezpieczających. Nadają się jedynie dla starszych systemów operacyjnych, przeznaczonych dla stacji roboczych Windows 3.x, Windows 95, czy Windows 98. NTFS jest systemem bezpiecznym pozwalającym nadawać uprawnienia dostępu do plików i katalogów.

Pozwolenia dostępu służą ograniczeniu dostępu użytkowników do takich katalogów jak Windows, Windows\System, czy Windows\Repair. Sterują również poziomem dostępu użytkowników do plików i katalogów

Tabela Uprawnienia do katalogów

UPRAWNIENIE	OPIS
Pełna kontrola	Użytkownik posiadający to prawo może zmienić właściciela katalogu oraz usuwania wszystkich plików i katalogów.
Wyświetlenie zawartości folderu	Umożliwia użytkownikowi przeglądanie zawartość katalogu
Odczyt	Umożliwia na oglądanie zawartości katalogów, włącznie z pozwoleniami dostępu, nazwami właścicieli oraz atrybutami.
Zapis	Umożliwia tworzenie plików i katalogów, zmieniać atrybuty katalogu oraz przeglądać pozwolenia dostępu do folderu i nazwę właściciela.
Odczyt i wykonanie	Pozwala przeglądanie wszystkich katalogów podrzędnych, obejmuje prawo Przeglądanie zawartości folderu oraz Czytanie
Modyfikacja	Obejmuje uprawnienia Czytanie i Wykonanie, Pisanie, a także pozwala na usunięcie katalogu.

Pozwolenia dostępu do plików
Umożliwiają sterowanie dostępem do takich plików jak NTLDR, NTDETECT.COM.

Tabela Uprawnienia do plików

UPRAWNIENIE	OPIS
Pełna kontrola	Użytkownik, który posiada to prawo może zmienić właściciela pliku. Obejmuje ono wszystkie uprawnienia zamieszczone poniżej
Odczyt	Umożliwia odczytanie zawartości plików
Zapis	Umożliwia nadpisywanie plików
Odczyt i wykonanie	Pozwala na uruchamianie plików wykonywalnych, dodatkowo obejmuje wszystkie uprawnienia związane z pozwoleniem na czytanie
Modyfikacja	Obejmuje takie uprawnienia jak : Czytanie i Wykonanie, Pisanie, a także pozwala na zmianę i usunięcie pliku.

Pozwolenia do katalogów współdzielonych

Współdzielenie katalogów używamy gdy potrzebujemy udostępnić zasoby sieciowe użytkownikom, grupom oraz obiektom specjalnym.

Uprawnienia do katalogów współdzielonych to :

Czytanie (Read)	Umożliwia użytkownikom wyświetlić nazwę katalogu, nazwy plików oraz ich atrybuty, uruchomić pliki wykonywalne, zmieniać katalogi wewnątrz wspólnego folderu.
Zmiana (Change)	Umożliwia tworzenie katalogów, dodawanie plików do katalogów, dodawanie danych do plików, zmienianie danych w plikach, modyfikacje atrybutów plików a także usuwanie plików i katalogów. Dodatkowo obejmuje wszystkie przywileje określone pozwoleniem Czytanie.
Pełna kontrola (Full Control)	Pozwalana zmianę pozwoleń dostępu do plików oraz przejęcie ich własności. Dodatkowo obejmuje wszystkie uprawnienia określone pozwoleniem Zmiana

Zagadnienia do przemyślenia

1. Uprawnienia co to są i do czego służą?
2. Prawa dostępu dla plików i katalogów, do jakiego celu wykorzystujemy?
3. Co to jest domena, wymień jej charakterystyczne cechy.
4. Co jest bezpieczniejsze zgromadzenie komputerów w domenie czy grupie roboczej
5. Jakie są różnice między kontem Użytkownik i Użytkownik zaawansowany.
6. W jakim celu tworzymy grupy?
7. Co nazywamy dziedziczeniem uprawnień ?
8. Co to jest mapowanie i jakie ma zalety.
9. Wymagania stawiane kontom użytkowników.
10. Co to jest autoryzacja użytkowników.
11. Do czego wykorzystywane są narzędzia administracyjne.
12. Zadania rejestru i dlaczego trzeba obchodzić się z nim bardzo ostrożnie.
13. Zastanów się co zrobić kiedy zawiesiła się aplikacja na której pracowałeś.
14. Który z priorytetów procesu jest zarezerwowany dla administratora
15. Kiedy przydatne okazuje się narzędzie podgląd zdarzeń i dlaczego?
16. W jakim celu wykorzystujemy narzędzie zarządzanie dyskami.
17. Jak myślisz co jest lekarstwem na polepszenie problemów wydajnościowych wynikających z obserwacji monitora wydajności

Zadania do samodzielnego wykonania

1. Uruchom Menedżer zadań, odczytaj jakie programy i procesy są aktualnie uruchomione
2. Uruchom nowe zadanie np. calc.exe potem je zakończ. Cały czas obserwuj co dzieje się w panelu wydajność Menedżera zadań
3. Uruchom cztery programy naraz jakie jest wykorzystanie procesora w stosunku do stanu kiedy otwarty jest jeden program.
4. Sprawdź jakie są czasy aktualizacji procesów w Menedżerze zadań
5. Zaobserwuj z jakimi priorytetami są uruchomione procesy w systemie.
6. Który proces zużywa najwięcej czasu procesora
7. Uruchom edytor rejestru. Po uruchomieniu sprawdź w menu Opcje czy zaznaczony jest punkt Tylko do odczytu, jeśli nie zaznacz tę opcję.
8. Wyszukaj w rejestrze datę zainstalowanego BIOS-u HKEY_LOCAL_MACHINE/HARDWARE/DESCRIPTION\SYSTEM\SYSTEMBIOSDATE oraz wersję zainstalowanego BIOS-u
9. Sprawdź typ procesora oraz szybkość procesora HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\CENTRALPROCESSOR
10. Sprawdź numer wersji Windows HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWSNT\CURRENTVERSION
11. Sprawdź czy możesz połączyć się z innym rejestrem
12. Uruchom Menedżer dysków. Nie dokonując żadnych zmian w parametrach dysku, zapoznaj się z opcjami dostępnymi w poszczególnych menu. Odczytaj dostępne informacje na temat organizacji dysku w systemie.
13. Przejdź do podglądu zdarzeń i poprzez menu Akcja / Podłącz do innego komputera, wybierz komputer, którego dziennik chcesz oglądać. Zanotuj jakie zdarzenia powodują błędy.
14. Sprawdź jaki rozmiar ma plik stronicowania i na jakim dysku się znajduje, wyraź swoją opinie na temat jego wielkości?
15. Sprawdź czy twój komputer należy do domeny Windows

16. Sprawdź właściwości konta Gość.
17. Utwórz folder z dowolną zawartością. Udostępnij do w sieci. Nadaj uprawnienie tylko do odczytu. Inni użytkownicy mają sprawdzić czy twój folder jest widoczny w sieci i czy można coś do niego zapisać.
18. Za pomocą usługi Telnet podłącz się na inny komputer i stworzony przez twojego sąsiada katalog spróbuj usunąć. Jakie wnioski Ci się nasuwają, do czego służy ta usługa?
(Start / Uruchom wpisz Telnet nazwa komputera lub adres IP komputera zdalnego)
19. Zmapuj katalog udostępniony studentom .....