Wybrane elementy systemu

Cechy główne

- zarządzanie serwerem
- active Directory
- bezpieczeństwo
- pamięci masowe i systemy plików
- sieci i komunikacja
- usługi aplikacyjne
- symetryczna wieloprocesorowość (smp)
- interfejs użytkownika
- kopie zapasowe

Zarządzanie serwerem

- W miejsce kilku różnych aplikacji (*User Menager, Serwer Menager, Sprinter Menager*) wprowadzono nową, wspólną powłokę zarządzającą – *Microsoft Menagement Console* (**MMC**).
- Wprowadzono możliwość zarządzania serwerem z poziomu przeglądarki internetowej WWW – *Web-Based Enterprise Menagement* (**WBEM**)

Active Directory

- Skupia w rozproszonej bazie danych wszelkie informacje na temat kont i grup użytkowników.
- Integruje się z serwerem Microsoft Exchange, pozwalając na eliminację powielających się list dystrybucyjnych poczty i kont użytkowników.
- W mechanizmie Active Directory nie ma nadrzędnego serwera sterującego, wszystkie serwery na równym poziomie mogą prowadzać i notować zmiany. Takie podejście umożliwia lepszą skalowalność systemu, większą odporność i łatwiejszą rekonfigurację.

Active Directory

- Każdy serwer może być zarówno nadrzędnym kontrolerem domeny, jak i zwykłym serwerem.
- Mechanizm wprowadzono jako rywala dla usług NDS (*Novell Directory Services*).
- Obydwa systemy wykorzystują standard **X.500**, określający typ i sposób dostępu do przechowywanej informacji i używają do obsługi swych katalogów protokołu **LDAP** (*Lightweight Directory Akces Protocol*).

Bezpieczeństwo

- Przy prawidłowo skonfigurowanej sieci system nie przesyła zaszyfrowanych haseł, lecz wykorzystuje do uwierzytelniania mechanizm *Kerberos* używający metody wezwanie-odpowiedź.
- Pliki i katalogi można zaszyfrować – system **EFS** (*Encrypted File System*). System ten jest osiągalny tylko na partycjach NTFS
- Na potrzeby szyfrowania i sprawdzania poprawności danych zaimplementowano metodę klucza publicznego

Kerberos

- Jest systemem bezpieczeństwa zaprojektowanym do użytku w transmisjach po niezabezpieczonych mediach, w których główny nacisk kładzie się na bezpieczeństwo danych
- Stacja robocza wykonuje operacje matematyczne w oparciu o hasło i pytanie postawione przez serwer, a wynik operacji odsyła z powrotem do serwera.

Kerberos

- Jest systemem bezpieczeństwa zaprojektowanym do użytku w transmisjach po niezabezpieczonych mediach, w których główny nacisk kładzie się na bezpieczeństwo danych
- Stacja robocza wykonuje operacje matematyczne w oparciu o hasło i pytanie postawione przez serwer, a wynik operacji odsyła z powrotem do serwera.

Metoda klucza publicznego

1. Do odszyfrowania danych potrzebne są dwa elementy: klucz publiczny i klucz prywatny.
2. Klucz publiczny jest publikowany i dostępny dla każdego, klucz prywatny jest utrzymywany w sekrecie.
3. Użytkownik chcąc bezpiecznie przesłać wiadomość, szyfruje ją za pomocą klucza publicznego odbiorcy.

Metoda klucza publicznego

4. Aby odbiorca był pewien, że wiadomość nie została spreparowana, nadawca może ją jeszcze zaszyfrować stosując własny klucz prywatny.
5. Odszyfrowanie takiej wiadomości wymaga klucza publicznego nadawcy do stwierdzenia jej autentyczności, oraz prywatnego odbiorcy do odszyfrowania treści wiadomości.

Obsługa pamięci masowych i systemów plików

- *Remote Storage Server* (**RSS**) umożliwia korzystanie ze zdalnych taśm i dysków optycznych, tak jakby były one dostępne lokalnie.
- RSS kataloguje i śledzi kasety i taśmy, umożliwiając ich późniejszą lokalizację, a wszystko to działa wspólnie z nowym ulepszonym programem obsługi kopii zapasowych.

Obsługa pamięci masowych i systemów plików

- Wprowadzono zintegrowany system limitowania dysków, dzięki czemu możliwe jest przydzielanie użytkownikom miejsca na dysku z uwzględnieniem ograniczeń i ostrzeżeń dla osób zajmujących zbyt wiele przestrzeni dyskowej..

Obsługa pamięci masowych i systemów plików

- Rozproszony system plików (*Distributed File System*) umożliwia rozproszenie ważnych i często używanych plików w całej sieci, przy czym są one osiągalne dla użytkowników poprzez mechanizm pojedynczego dostępu.

Plik taki może być przechowywany na kilku różnych serwerach, a wszyscy użytkownicy będą się odwoływać do niego przez tę samą nazwę, korzystając z jego najbliżej położonej reprezentacji.

Sieci i komunikacja

- Zaimplementowano zestaw najczęściej używanych protokołów (TCP/IP, IPX/SPX a nawet NetBEUI), inne (rzadko stosowane) zaimplementowano w formie składników do opcjonalnej indywidualnej instalacji.
- System zawiera mechanizm wieloprotokołowego trasowania (*routing*) co oznacza, że komputer wyposażony w kilka kart sieciowych może funkcjonować jako router przekazując dane z sieci do sieci.

Sieci i komunikacja

- Wprowadzono obsługę jakości usług (*Quality of Service*), pozwalającą na nadawanie pewnym typom adresów i pakietów wyższych priorytetów niż pozostałym rodzajom przesyłu.

Usługi aplikacyjne

- Usługa *Windows Scripting Host* (**WSH**) - skrypty uruchamia się zdalnie, a serwer wykonuje zadania dla stacji klienckich.
- Usługa indeksująca (*Indexing Service*) - stanowi centralny punkt przeglądania dużych dysków w poszukiwaniu dokumentów zawierających specyficzne informacje.

Symetryczna wieloprocesorowość_

- *Symmetric Multiprocessing* (**SMP**) - program wykorzystujący wiele procesorów nie musi znać liczby procesorów zainstalowanych w systemie i będzie działał poprawnie nawet na komputerze z jednym procesorem.

Interfejs użytkownika

- Nowy interfejs użytkownika oparto na technologii zastosowanej w programie *Internet Explorer 5* i zastosowano konsekwentnie we wszystkich wersjach Windows Server
- Windows Server redukuje liczbę ponownych startów systemu związanych ze zmianą konfiguracji.
- Zapewnia obsługę technologii *Plug-and-Play* począwszy od PCMCIA i USB a kończac na gniazdach PCI typu *Hot-Plug* (umożliwiających podłączenie urządzeń w czasie pracy).

Kopie zapasowe i odtwarzanie danych

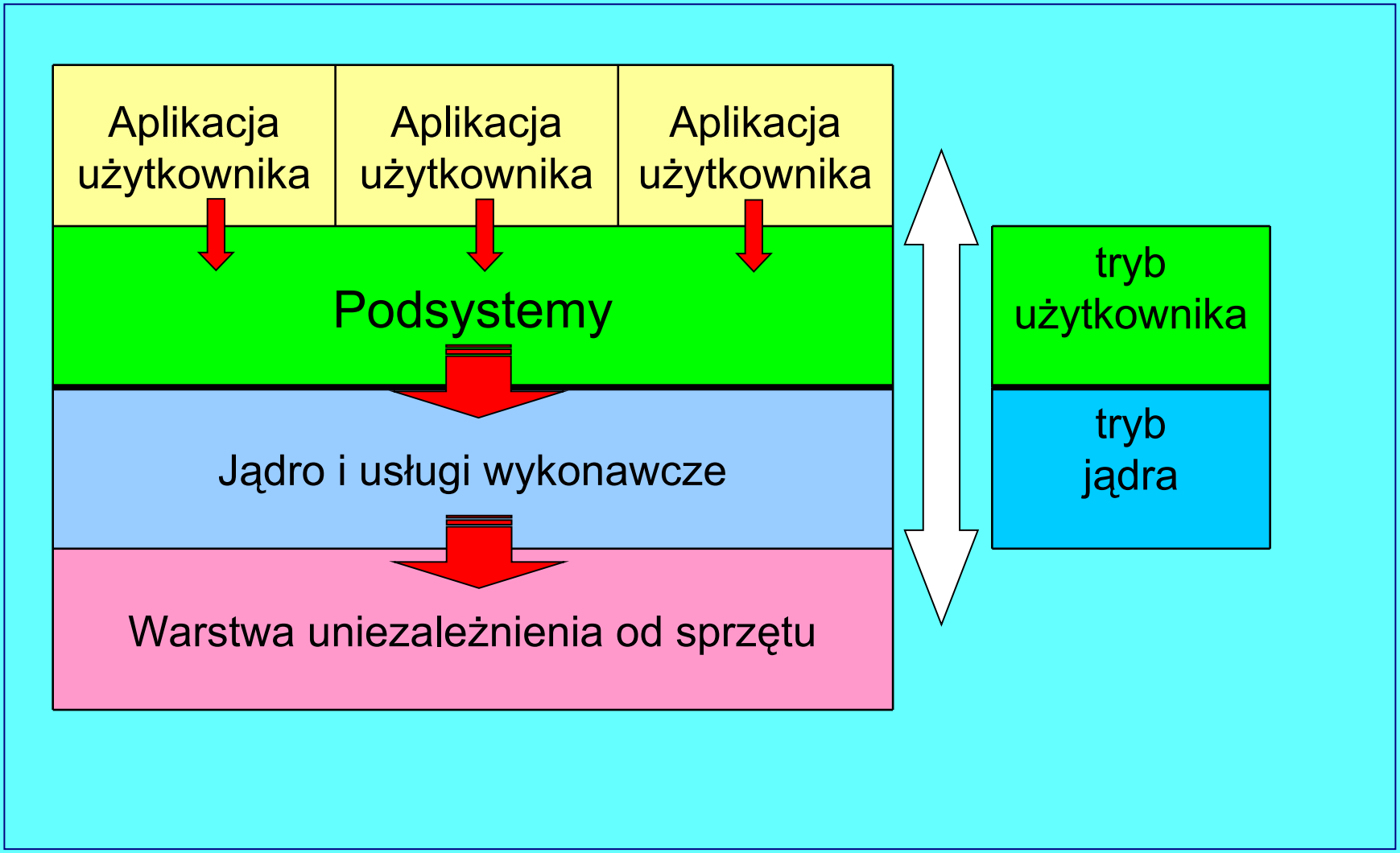
- Zaimplementowano całkiem nowy program do wykonywania i odtwarzania kopii zapasowych.

Program ten charakteryzuje się wysoką wydajnością, obsługą zmieniaczy taśm i możliwością wykonywania pełnych, przyrostowych lub różnicowych kopii zapasowych.

Tryb użytkownika i tryb jądra

- Windows używa dwóch różnych trybów procesora:
  - *tryb jądra* uruchamia usługi wykonawcze
  - *tryb użytkownika* uruchamia programy użytkownika
- Usługi trybu jądra są chronione przez procesor, a usługi użytkownika przez system operacyjny

Architektura systemu



Tryb użytkownika i tryb jądra

- Realizacja ochrony polega na:
  - Uniemożliwieniu programom działającym w trybie użytkownika zapisu do obszaru pamięci wykorzystywanego przez programy trybu jądra,
  - procesor z kolei zapobiega zapisywaniu do obszaru pamięci aplikacji trybu użytkownika

Jeżeli ochrona zawiedzie to następuje tzw. wyjątek trybu jądra, a system sygnalizuje tę sytuację niebieskim ekranem **BSOD** (*Blue Screen of Death*)

Tryb użytkownika i tryb jądra

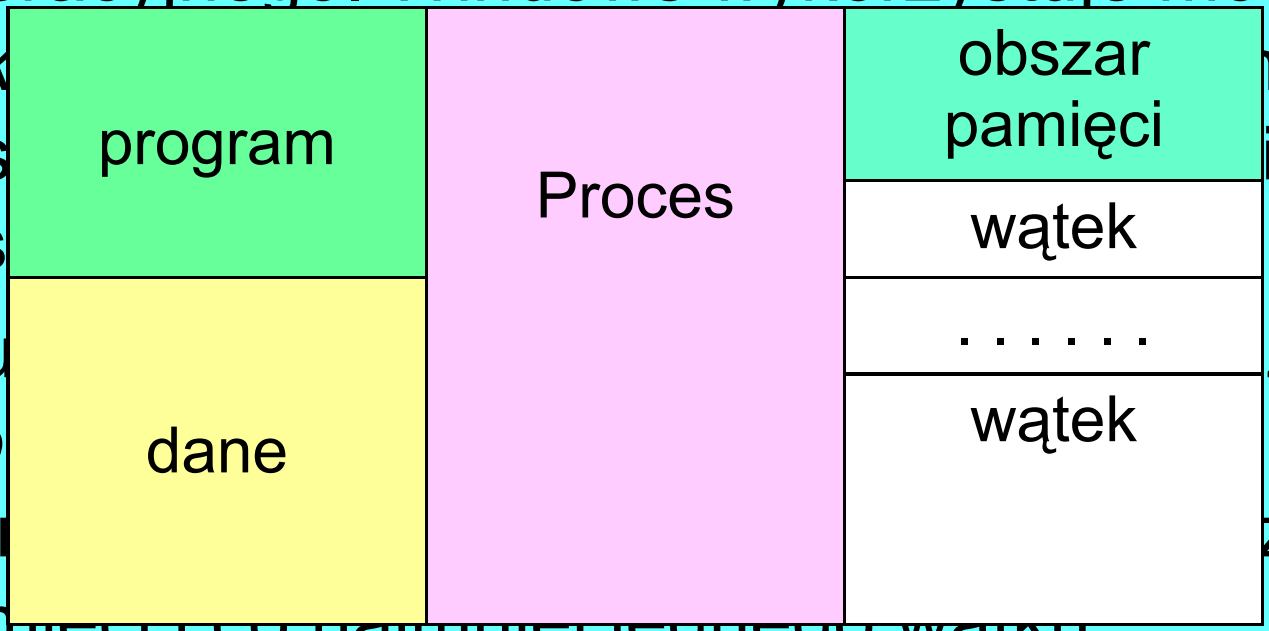
- Programy trybu użytkownika komunikują się z jądrem poprzez interfejsy programowe aplikacji (*Application Programming Interface* – **API**)
- Reszta trybu jądra podzielona jest na trzy części:
  - warstwę uniezależnienia od sprzętu (Hardware Abstraction Layer – HAL),
  - procesy jądra,
  - usługi wykonawcze (NT Executive Services)

Warstwa uniezależnienia od sprzętu (HAL)

- Na warstwę HAL składają się elementy systemu napisane w języku niskiego poziomu (języku procesora).
- Warstwa HAL działa jako stały interfejs dla jądra umieszczonego powyżej i jednocześnie jako maska przysłaniająca zawiłości sprzętu leżącego poniżej.
- Praca warstwy HAL polega na odbieraniu żądań jądra i tłumaczeniu ich na instrukcje rozumiane przez procesor.

Jądro systemu

- Jądro stanowi centralną część systemu operacyjnego. Windows wykorzystuje model *mik* malny zes i sys
- Uru z nim *pro* jedr zaru pam ego wątku.
- Wątek to „kawałek programu” wykonywany w danej chwili przez procesor.



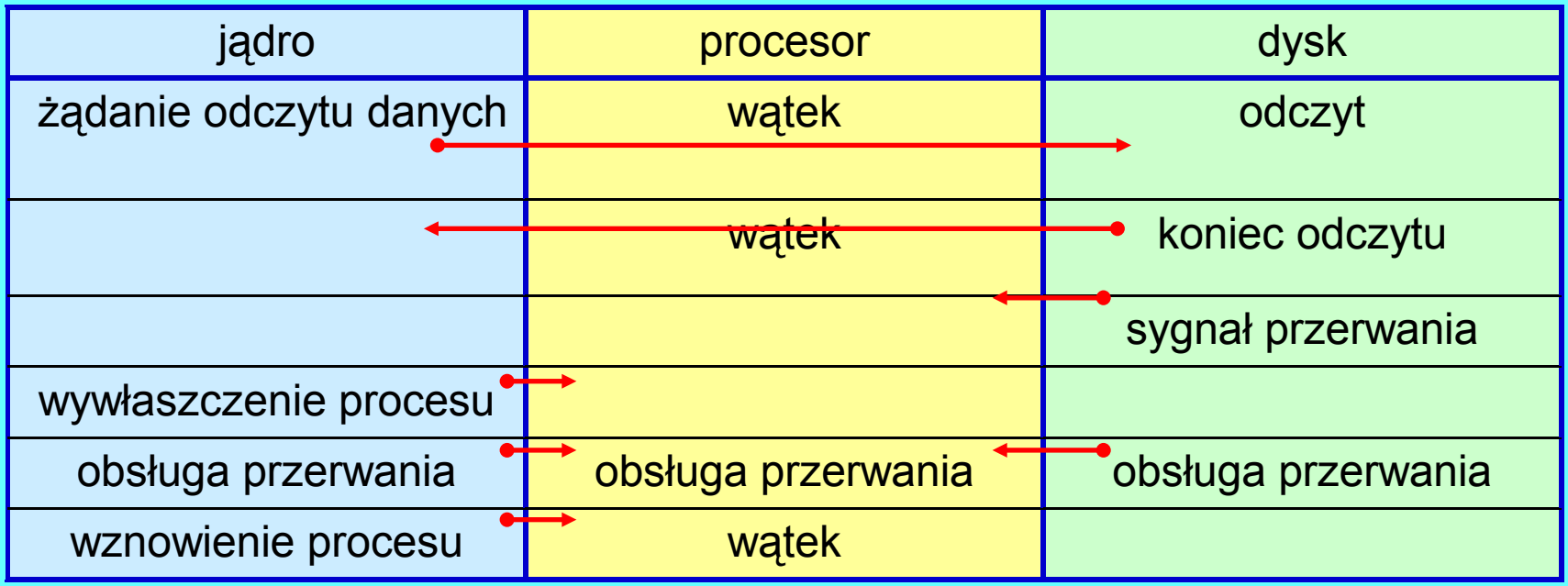
Jądro systemu

- Jądro realizuje trzy typy zadań:
  1. określa harmonogram wykonywania wątków
     - każdy z nich otrzymuje priorytet od 0 do 31,
     - jądro pobiera na krótki czas wątek o najwyższym priorytecie i zleca jego wykonanie przez procesor,
     - gdy przydzielony czas minie ponownie pobiera po jednym wątku dla każdego procesora.

Jądro systemu

2. obsługuje przerwania
   - jeżeli urządzenie (np. dysk) ma odczytać dane to wysyłane jest do niego żądanie,
   - dysk po wykonaniu żądania zawiadamia jądro, generując sygnał przerwania do procesora,
   - jądro wywłaszcz wykonywany proces, obsługuje przerwanie i wraca do uprzednio wywłaszczonego procesu.

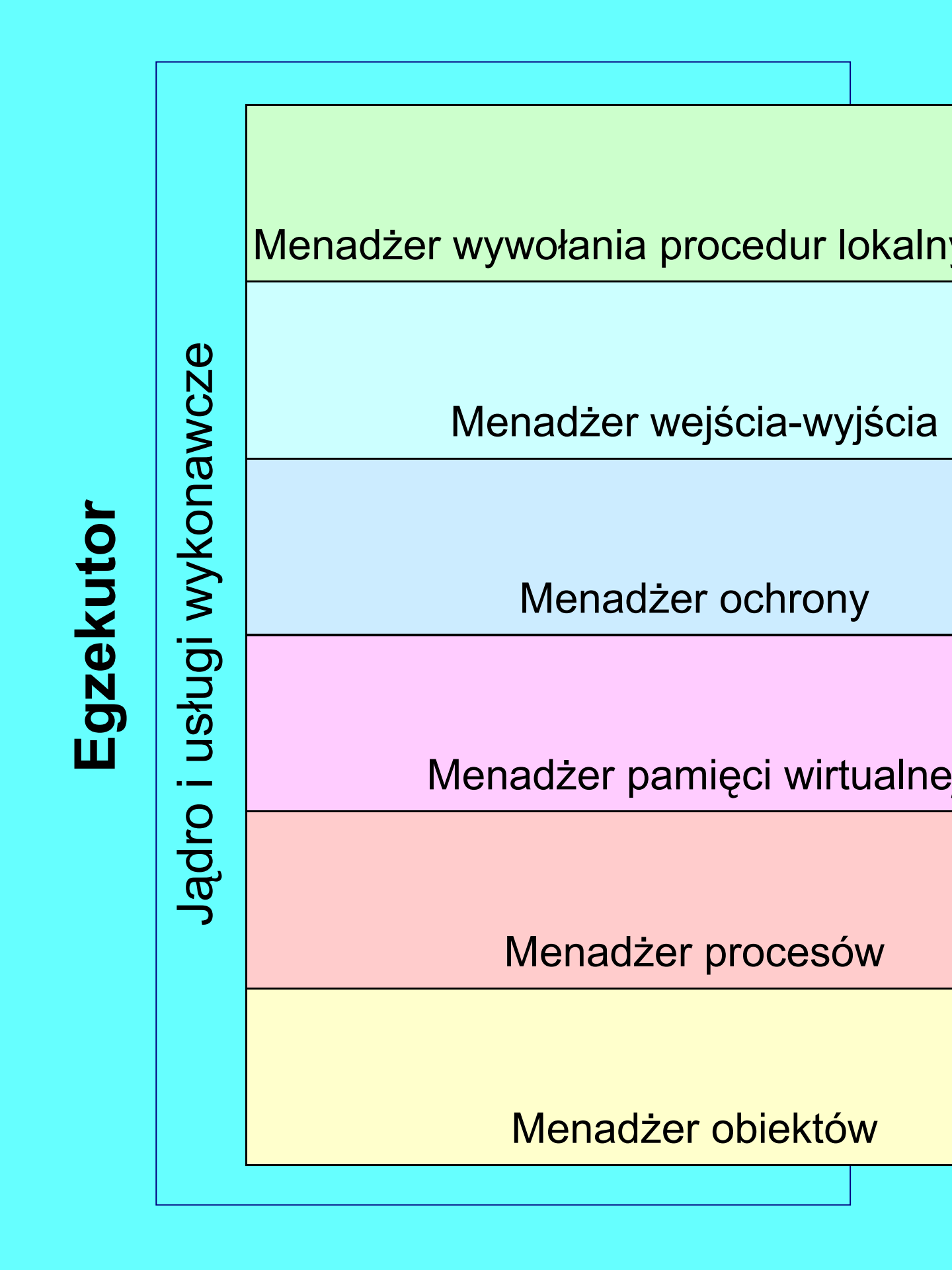
Jądro systemu



3. obsługa wyjątków jądra
   - jeżeli program uruchomiony w trybie jądra spowoduje błąd ochrony lub inny jądro próbuje się z nim uporać.

Egzekutor

- Przyjęty w systemie model mikrojądra powoduje, że pozostałe usługi realizowane są poza jego obszarem – jedną z nich jest egzekutor
- Egzekutor pracuje w całości w trybie jądra i posiada pełny dostęp do jądra oraz urządzeń wejscia-wyjścia.
- Różne części egzekutora wspólnie realizują podstawowe usługi systemu operacyjnego.


Egzekutor
Jądro i usługi wykonawcze
Menadżer wywołania procedur lokaln
Menadżer wejścia-wyjścia
Menadżer ochrony
Menadżer pamięci wirtualne
Menadżer procesów
Menadżer obiektów

Menadżer obiektów

- *Object Menager* używany jest do tworzenia, zarządzania i usuwania obiektów wykorzystywanych przez system.
- Ponadto menadżer obiektów opiekuje się porzuconymi obiektami.

Jeżeli program korzystający np. z portu szeregowego, załamał się, menadżer obiektów odpowiada za odnalezienie uchwytu portu i zamkniecie go w celu przywrócenia jego dostępności dla innych procesów.

Menadżer procesów

- Jest pośrednikiem między użytkownikiem a menadżerem obiektów.
- Do głównych jego zadań należy tworzenie procesów i zarządzanie nimi.
- Odpowiada za odbieranie żądań tworzenia procesów, wzywanie menadżera obiektów do budowy obiektu i jego wątków oraz za utrzymanie listy dostępnych procesów.

Menadżer pamięci wirtualnej

- Po utworzeniu proces otrzymuje 4 GB przestrzeni adresowej– 2 GB przeznaczane są na obszar użytkownika i 2 GB na system.
- Menadżer pamięci wirtualnej (*Virtual Memory Manager* – **VMM**) utrzymuje tablicę, śledząc za jej pomocą, które z części procesu są dostępne w danej chwili w pamięci fizycznej, a które nie.
- Jeżeli proces chce odczytać dane, których nie ma w pamięci VMM zarządza ściągnięcie ich z dysku.

Menadżer ochrony

- *Security Reference Manager* (**SRM**) jest podstawą bezpieczeństwa systemu Windows.
- W trakcie logowania użytkownika, proces logujący generuje do niego żeton ochrony. Gdy użytkownik żąda dostępu do jakiegoś obiektu, menadżer obiektów prosi SRM o sprawdzenie żetonu i określenie poziomu dostępu użytkownika do tego obiektu. Następnie menadżer obiektów zwraca uchwyt obiektu z wyznaczonym poziomem dostępu.

Menadżer wejścia-wyjścia

- Menadżer wejścia-wyjścia (*I/O Manager*) zajmuje się wszystkimi urządzeniami we/wy używanymi przez system.
- Dostarcza usług zarówno sterownikom sprzętowym jak i samym aplikacjom, przez co sterowniki nie muszą wiedzieć, jak wykorzysta je aplikacja, ani aplikacja nie zna sposobu użycia sterowników.
- Menadżer we/wy tłumaczy odwołania do urządzeń na postać zrozumiałą przez sam sprzęt.

Funkcje wywołania procedur lokalnych

- Windows 2003 jest systemem typu klient-serwer (procesy klienta i serwera działają na tym samym komputerze).
- Możliwości takie stwarza mechanizm zdalnego wywołania procedur (*Remote Procedure Call* – **RPC**) – jest to jednak proces pracochłonny.
- Mechanizm wywołania procedur lokalnych (*Local Procedure Call* – **LPC**), umożliwia wykorzystanie tego samego interfejsu, lecz przy znacznie mniejszych nakładach.