Systemy operacyjne w środowisku sieciowym*

System komputerowy i system operacyjny

Rys. 1.1. Model systemu komputerowego

Budowa systemu operacyjnego i jego zadania

W systemie operacyjnym można wyróżnić trzy warstwy, które zajmują się odrębnymi zadaniami:

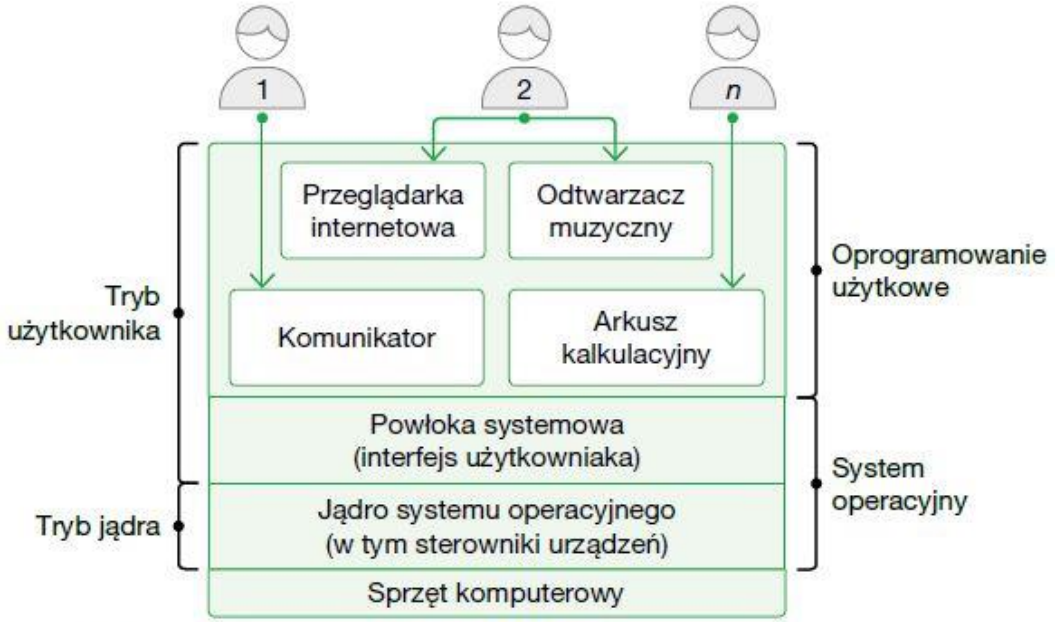
- **powłoka systemowa** (ang. shell) - umożliwia użytkownikowi komunikację z systemem operacyjnym. Dla jednego systemu operacyjnego może istnieć wiele powłok o różnym sposobie działania i różnym przeznaczeniu. Na przykład dla systemu Windows są to **Eksplorator Windows**, **Windows PowerShell** oraz **Wiersz polecenia** (cmd.exe).
- **jądro systemu operacyjnego** (ang. kernel) - to podstawowa część systemu operacyjnego, która odpowiada za realizację zadań. W tradycyjnych systemach jednym z elementów jądra są **sterowniki urządzeń**, które pozwalają na komunikację systemu operacyjnego ze sprzętem
- **system plików** (ang. file system) – określa sposób przechowywania plików oraz zarządzania nimi tak, by dostęp do danych był łatwy dla użytkownika. Dzięki systemowi plików, aby znaleźć plik zawierający interesującą nas informację nie musimy wiedzieć, w jaki sposób i gdzie fizycznie na nośniku jest on zapisany. Pozwala również precyzyjnie określić miejsce przechowywania pliku lub katalogu za pomocą **ścieżki dostępu**
  Np.: *C:/Users/Adam/Dokumenty/Prezentacje/sieci_komputerowe.pptx*

---

* Informatyka na czasie 1. Podręcznik dla liceum i technikum, zakres podstawowy. Janusz Mazur, Paweł Perekietka, Zbigniew Talaga, Janusz S. Wierzbicki. Nowa Era

Zadania systemu operacyjnego

Rys. 1.3. Zadania systemu operacyjnego



Rys. 1.4. Szczegółowy model systemu komputerowego

Zanim załaduje się system operacyjny

Współczesny komputer osobisty może działać pod kontrolą różnych systemów operacyjnych, a użytkownik może je swobodnie zmieniać. System ładowany jest z określonego nośnika, np. płyty CD/DVD lub karty pamięci. Komputer musi jednak wiedzieć, w jaki sposób system załadować.

BIOS

Komputery są wyposażone w podstawowy system wejścia i wyjścia, czyli **BIOS** (ang. Basic Input/ Output System), który jest zapisany jako zestaw podstawowych procedur w pamięci urządzenia. **BIOS wczytuje się jako pierwszy pierwszy program po uruchomieniu komputera.** Zawiera procedury testujące poprawność pracy elementów systemu komputerowego (np. pamięci, podłączonego dysku). Zajmuje się wstępną obsługą urządzeń wejścia i wyjścia, kontroluje transfer danych między komponentami takimi jak dysk lub procesor oraz dostarcza procedury pozwalające wczytać właściwy system operacyjny.

Użytkownik za pomocą wbudowanego w BIOS interfejsu, tzw. **BIOS Setup może zmieniać ustawienia, np. parametry podłączonych urządzeń lub zachowanie komputera po uruchomieniu.** Można również ustalić kolejność urządzeń, na których BIOS będzie poszukiwał systemu operacyjnego, np. najpierw napęd CD, potem twardy dysk.

UEFI - następca BIOS

Nowocześniejsze rozwiązanie — **UEFI** (ang. Unified Extensible Firmware Interface). Pozwala na pracę z dyskami o pojemności większej niż 2 TB oraz oferuje dużo nowocześniejszy interfej.

Do ustawień konfiguracyjnych BIOS lub UEFI można się dostać, przytrzymując odpowiedni klawisz podczas uruchamiania komputera. Najczęściej jest to **DEL, F2** lub **F10**. Dla konkretnego urządzenia zawsze można to sprawdzić w dokumentacji komputera albo płyty głównej.

Praca w środowisku sieciowym

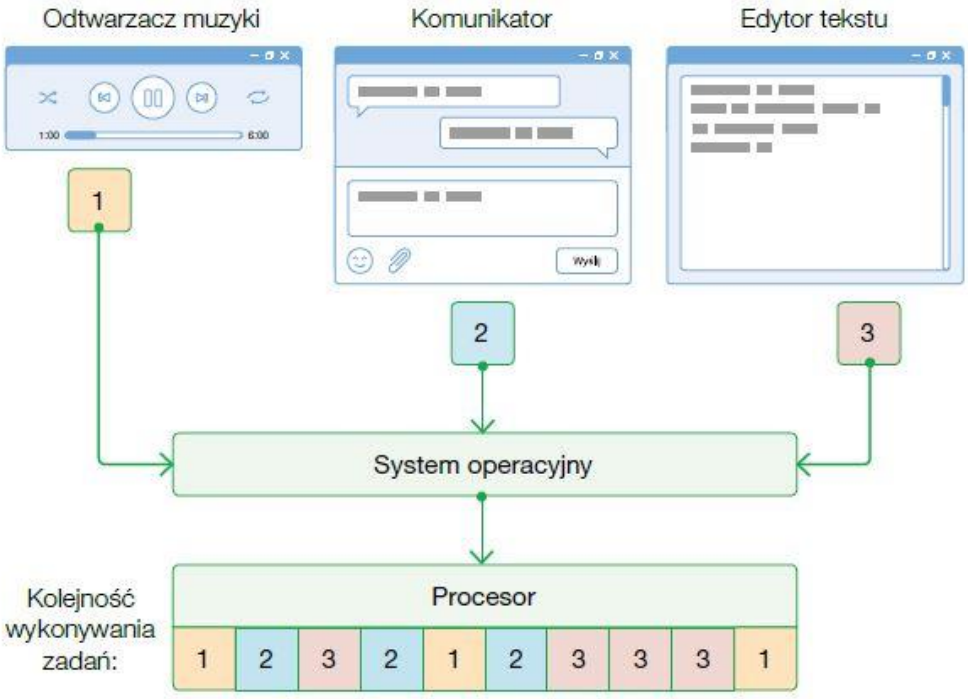
Większość urządzeń, których dzisiaj używamy, jest podłączona do sieci telekomunikacyjnej lub komputerowej. Pozwala to na korzystanie z zasobów lokalnej sieci komputerowej (LAN) i internetu. W sieciach lokalnych często wykorzystuje się **drukarki sieciowe** oraz **bazy danych** oraz **serwery plików**, umożliwiające użytkownikom dzielenie się dokumentami i wspólną pracę nad nimi.

Część systemów operacyjnych integruje się z usługami sieciowymi, co oznacza, że aby w pełni korzystać z ich możliwości, należy założyć konto w usługach sieciowych producenta systemu operacyjnego. Jedną z **ważniejszych zalet** takich usług jest to, że **automatycznie tworzą się na dysku wirtualnym kopie zapasowe wszystkich dokumentów**.

Bezpieczeństwo pracy w systemie operacyjnym

Wygoda, którą zapewnia system operacyjny, wynika nie tylko z intuicyjnego i szybkiego interfejsu użytkownika, lecz także z bezpieczeństwa i stabilności użytkowania. Naruszenie bezpieczeństwa systemu operacyjnego zwykle kojarzymy jedynie z zagrożeniami z zewnątrz, np. atakami z sieci lub wirusami (**cyberbezpieczeństwo**). W celu zwiększenia bezpieczeństwa stosuje się m.in. **oprogramowanie antywirusowe i zapory sieciowe**. To jednak nie wszystko — system operacyjny musi być wyposażony w mechanizmy zapobiegające nieprawidłowemu działaniu, np. zniszczeniu danych wskutek błędów programów.

System operacyjny odpowiada także za wydajne wykorzystanie zasobów sprzętowych. Oznacza to m.in. takie zarządzanie sprzętem, żeby bezpiecznie można było realizować **wiele zadań uruchomionych jednocześnie** przez użytkownika. System dba o to, aby wykonywanie jednego zadania nie powodowało nieprawidłowości w realizacji innego, czyli rozwiązuje konflikty między programami w dostępie do zasobów — np. kiedy próbujemy jednocześnie wydrukować na drukarce kilka dokumentów. Obsługa wielu zadań i użytkowników jednocześnie



Rys. 1.7. Podział czasu pracy procesora między wykonywane zadania

Rodzaje kont użytkowników

Z jednego systemu komputerowego może korzystać wiele różnych osób, dlatego większość systemów operacyjnych pozwala tworzyć oddzielne konta dla poszczególnych użytkowników. Konta mogą mieć różny poziom uprawnień. **Standardowe konto użytkownika** służy **do codziennej pracy**, pozwala na uruchamianie programów oraz konfigurowanie środowiska pracy. Z poziomu **konta administratora** można **zarządzać** systemem operacyjnym — zmieniać parametry wpływające na pracę wszystkich jego użytkowników, instalować oprogramowanie.

> **W codziennej pracy należy korzystać ze standardowego konta użytkownika, nawet na komputerze domowym. Konta administratora powinno się używać tylko wtedy, kiedy trzeba wykonać prace administracyjne.**

Niezwykle ważnym zagadnieniem jest ochrona danych użytkownika przed nieuprawnionymi osobami i programami, szczególnie gdy system operacyjny jest podłączony do sieci komputerowej. Podstawowym zabezpieczeniem dostępu do konta przed niepowołanymi użytkownikami jest **hasło**. Dzisiaj hasłem mogą być np. odcisk palca, twarz użytkownika lub wzór, który kreśli się na ekranie dotykowym. Jednak nadal w wielu systemach operacyjnych (a także w serwisach e-usług) posługujemy się ciągiem znaków. **Kiedy sami wymyślamy hasło, należy zadbać o to, by było trudne do złamania.**

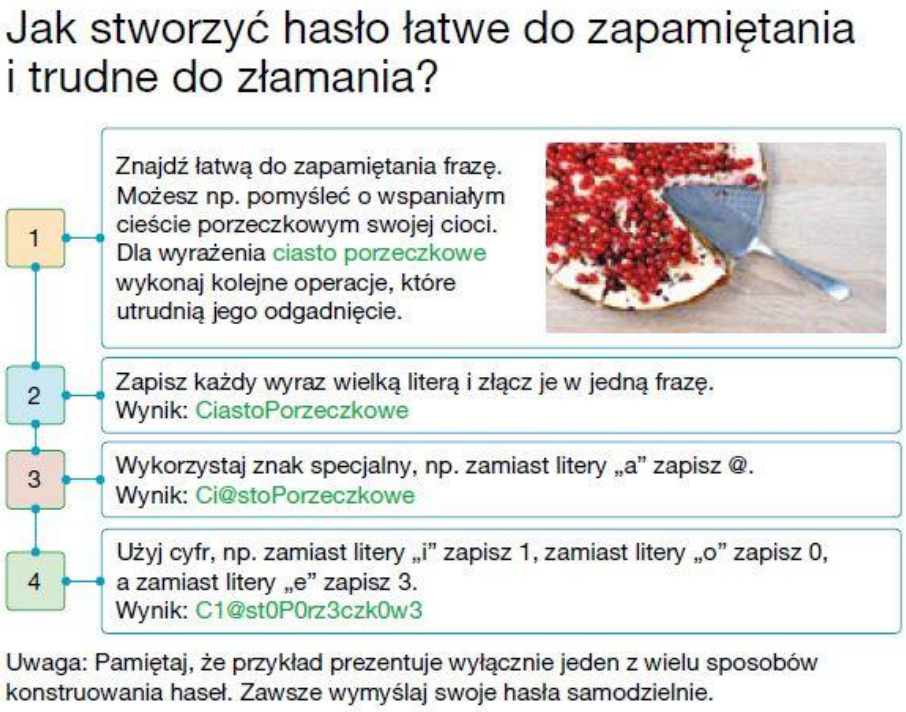
Hasło będące ciągiem znaków powinno być łatwe do zapamiętania dla nas, ale trudne do odgadnięcia przez inne osoby lub programy do tego służące. Dlatego **nie powinno** być związane

z powszechnie znanymi informacjami o nas — rokiem urodzenia, ulubionym zwierzęciem, idolem itp. **Hasło powinno się więc składać nie tylko z liter, lecz także z cyfr i znaków specjalnych.** Należy również pamiętać, że **im dłuższe hasło, tym trudniejsze do odgadnięcia**.

Pamiętaj — nigdy nie zapisuj swoich haseł w niezaszyfrowany sposób.

Oto najważniejsze zasady tworzenia i używania haseł.

- Twórz hasła łatwe do zapamiętania, ale trudne do odgadnięcia lub maszynowego złamania.
- W jednym haśle używaj co najmniej ośmiu znaków, w tym małych i wielkich liter, cyfr oraz znaków specjalnych.
- Unikaj ciągów takich samych znaków oraz zbyt częstego powtarzania tego samego znaku.
- Używaj różnych haseł w różnych serwisach oraz na różnych urządzeniach.
- Nie zapamiętuj haseł (np. w przeglądarkach internetowych) na urządzeniach wykorzystywanych przez wielu użytkowników.
- Zanim wprowadzisz hasło w przeglądarce, upewnij się, że łączysz się z właściwą stroną, a połączenie jest bezpieczne i szyfrowane.



Instalacja i aktualizacja oprogramowania

Ze względów bezpieczeństwa należy dbać o aktualizację oprogramowania, systemowego oraz używanych aplikacji. Aktualizacje nie tylko dostarczają nowych funkcji, ale przede wszystkim likwidują błędy, w tym luki bezpieczeństwa, które mogą wykorzystywać cyberprzestępcy. Zabezpieczenie kont użytkowników

Kopie zapasowe

Większość systemów operacyjnych pozwala tworzyć **kopie zapasowe**, i zwane również **kopiami bezpieczeństwa** (ang. backup). Mogą one zawierać informacje i pliki niezbędne do uruchomienia systemu w razie awarii oraz dane, programy i dokumenty jego użytkowników. Pełna kopia zapasowa umożliwiająca odtworzenie stanu komputera jest nazywana **obrazem systemu.** Użytkownik tworzący kopię zapasową i może zdecydować, co dokładnie ma ona zawierać.

Kopie zapasowe można wykonywać na różnych nośnikach, np. na dyskach zewnętrznych lub na innych komputerach (serwerach) w sieci lokalnej. Wiele systemów (szczególnie mobilnych) pozwala tworzyć i przechowywać kopie zapasowe w usługach działających w chmurze.

Szyfrowanie danych i dysków

Jedną z metod zabezpieczania danych jest ich **szyfrowanie**. Współczesne systemy operacyjne zazwyczaj mają wbudowane odpowiednie mechanizmy pozwalające zaszyfrować pojedyncze pliki lub całe dyski. Szyfrowanie danych chroni je przed nieuprawnionym dostępem np. w przypadku kradzieży komputera lub dysku.
Jeśli decydujemy się na zaszyfrowanie danych, koniecznie trzeba zachować w bezpiecznym miejscu klucz pozwalający je odszyfrować. W przeciwnym wypadku w sytuacji awaryjnej możemy nie odzyskać do nich dostępu.

Rozpoznawanie i rozwiązywanie problemów z komputerem

Podczas użytkowania komputera, tabletu lub smartfona zdarzają się awarie. Czasami urządzenie pracuje zbyt wolno, niekiedy przestaje działać jakaś aplikacja, rzadziej całe urządzenie. W takich przypadkach można skorzystać z dostarczonych wraz z systemem narzędzi diagnostycznych, służących do rozwiązywania problemów.

Niedziałająca aplikacja

Kiedy aplikacja przestaje działać, najczęściej wystarczy ją wyłączyć, a następnie uruchomić ponownie. Jeśli aplikacja nie odpowiada, najczęściej nie można jej również w standardowy sposób zamknąć. W takim przypadku pomocne może się okazać narzędzie do zarządzania uruchomionymi aplikacjami i procesami. W systemie Windows jest to **Menedżer zadań**. Po jego uruchomieniu możemy przeglądać i wszystkie działające procesy.

Menedżer zadań można uruchomić na kilka sposobów, ale w przypadku niedziałającej aplikacji w systemie Windows najlepiej wcisnąć jednocześnie klawisze **Ctrl+Alt+Del** i wybrać z wyświetlonego menu opcję Menedżer zadań.

Problem z uruchomieniem urządzenia

Systemy operacyjne dysponują procedurami awaryjnego uruchamiania. Zaliczamy do nich zarówno standardowe ponowne uruchomienie systemu, jak i uruchomienie tzw. **trybu awaryjnego** w celu naprawienia systemu, przywrócenia ustawień fabrycznych lub ustawień z kopii zapasowej.

Tryb awaryjny pozwala uruchomić system operacyjny z obsługą niezbędnych do tego urządzeń. Jeśli system przestał działać po podłączeniu nowego urządzenia, możemy w trybie awaryjnym odinstalować jego sterowniki i zainstalować na nowo. Tryb ten pozwala także zabezpieczyć dane zgromadzone na dysku — np. poprzez ich skopiowanie na nośnik wymienny.

Obciążenia pamięci lub procesora

Aktualne obciążenia pamięci i procesora w systemie Windows możemy sprawdzić w Menedżerze zadań. Po kliknięciu na tytule kolumny możemy posortować wszystkie zadania, np. w kolejności od tych, które najbardziej wykorzystują w danym momencie poszczególne komponenty systemu komputerowego. Wtedy jeśli zauważymy, że obciążenie generują aplikacje mało istotne z punktu widzenia systemu lub niepotrzebne, możemy je wyłączyć.

Brak miejsca na dysku.

Niezależnie od objętości dysku komputera lub urządzenia mobilnego prędzej czy później może zabraknąć na nim miejsca, w związku z czym system np. nie jest w stanie pobrać i zainstalować aktualizacji. W takich przypadkach pomóc mogą **narzędzia do oczyszczania dysku**. W systemie Windows 10 możemy skorzystać z narzędzia systemowego Oczyszczanie dysku.

PODSUMOWANIE

- System operacyjny zapewnia wygodne, bezpieczne i wydajne środowisko, w którym użytkownicy mogą uruchamiać programy.
- Zadania realizowane przez system operacyjny możemy podzielić na cztery główne grupy, związane z zarządzaniem: sprzętem, danymi, procesami i komunikacją z użytkownikami.
- System operacyjny korzysta z systemów plików, aby wykonywać zadania związane z gro- madzeniem danych i zarządzaniem nimi. Jeden system operacyjny może wykorzystywać wiele różnych systemów plików.
- Ochrona danych w systemie operacyjnym dotyczy m.in. tworzenia i ochrony silnych haseł użytkowników, tworzenia kopii zapasowych, szyfrowania danych, dbania o aktualizacje oprogramowania oraz ochronę przed wirusami i oprogramowaniem szpiegowskim.
- W razie awarii systemu komputerowego kopia zapasowa pozwala na odtworzenie danych użytkowników, a także programów oraz systemu operacyjnego — jeśli zostały w niej zapisane.