# Operační systémy stanic

- Základní program, který **„oživuje“** technické díly počítače
- **Řídí využití** procesory, paměti a disků, síťovou komunikaci a tisk, ovládá všechen ostatní hardware
- **Zobrazuje** výstupy a čte vstupy z klávesnice, myši…
- **Umožňuje instalaci a spouštění** ostatních programů
- **Poskytuje zobrazení oken a programy**
- Zajišťuje **zabezpečení počítače**

Problémem je, že aplikace vytvořená pro Windows nefunguje na MacOS nebo Linuxu.

### Příklady:

- Linux – bezplatná varianta systému Unix, **jedná se o open source software**.
  Použití: od superpočítačů až po chytré hodinky
- BSD – varianta systému Unix pro webové servery
- MacOS – **grafický OS** od firmy Apple
- Microsoft Windows – OS od firmy Microsoft, nejnovější verze je Windows 11.
  Existuje i verze pro servery

### Start operačního systému

- Po zapnutí nebo resetu počítače je HW nastaven dle konfigurace BIOSu
- Jako první se načte instrukce BIOSu a spustí se základní test = test přítomnosti a funkčnosti HW
- Jádro OS je zavedeno do paměti a předává se mu řízení počítače

### Dělení operačního systému podle počtu úloh

1. Jednoúlohový (single task)
   - Jednoduchý, rychlý, levný
   - Vývoj ukončen, má stabilní vlastnosti
2. Víceúlohový (multi task)
   - Umožňuje paralelní zpracování úloh
   - Má efektivní využití kapacity hardwaru
   - Nevýhody: obtížné programování, možnost zahlcení a problém s bezpečností
   - Vývoj probíhá, objevují se proto nové vlastnosti OS, ale také nové chyby

# Nadstavby

- Jedná se o rozhraní, které výrobci přidávají na základní operační systém k přizpůsobení vzhledu, uživatelských rozhraní a specifických funkcí.
- Další funkce: odstraňování nepotřebných souborů, historie programů, systémových informací, správce procesů.

**Příklady:**

- PC Tools – nadstavba DOS
- XTree – nadstavba DOS
- Diskový manažer – OS nemůže číst a zapisovat data do nenaformátovaného nebo cizího disku. Umožňuje dělit a formátovat disky, Windows využívá NTFS.
- Správce procesů – poskytuje přehled o spuštěných procesorech (jméno souboru, cesta, obsazení paměti, využití procesoru, přidělení priority).

# Struktura

- **Jádro (kernel)** – zajišťuje spuštění programů, přístup k HW
- Spuštění programu – poskytuje rozhraní mezi uživatelským programem a HW
- **Ovladače** – SW, který umožňuje interakci s HW zařízeními
- **Bezpečnost** – zadání uživatelského jména a hesla, OS zabezpečen pomocí antivirů a firewallu.
- **Správa paměti**

# Konfigurační soubory config.sys, win.ini, autoexec.bat

## config.sys

- Konfigurační soubor pro DOS i Windows
- Textový soubor, obsahuje instrukce pro zavádění systému do operační paměti

## win.ini

- Textový konfigurační soubor, který se u Windows používal k uložení základního nastavení při bootování

## autoexec.bat

- Textový dávkový soubor (dávkový = spouští příkazy ze souboru, každý příkaz je na samostatném řádku)
- Nachází se v kořenovém adresáři diskového oddílu, ze kterého je zaváděn DOS i Windows

# Alokační strategie

1. **first fit**
   - Výběr prvního dostatečně velkého bloku
   - Správce paměti hledá dostatečně velký blok s požadovanou velikostí, následně ho alokuje a zbytek ponechá volný pro další alokaci.
2. **best fit**
   - Výběr bloku, jehož velikost nejlépe odpovídá požadované velikosti
   - správce paměti projde všechny volné bloky a z těch, které jsou dostatečně velké, vyhledá nejmenší

## Správci procesů **// kliknutí na nadpis umožní přesměrování na odpověď**

# Dědění práv

Proces, kdy například daný uživatel dědí přístupová práva k dané složce či souborům.

## Certifikáty **// kliknutí na nadpis umožní přesměrování na odpověď**

# Multitasking

- Umožňuje chod více aplikací současně
- Rozděluje výpočetní čas procesoru
- Rozlišujeme: 1) Preemptivní multitasking – OS rozhoduje o odebírání procesoru
  2) Nepreemptivní (kooperativní) – Úlohy mají aktivní spoluúčast – samy se po čase vzdají procesoru

# Popiš způsoby a důvody zabezpečení

### Způsoby

1. Antivirové programy: detekce a odstranění malwaru a virů
2. Zálohování: pravidelné zálohování dat pro ochranu před ztrátou
3. Firewall: filtrace síťového provozu, blokování neautorizovaného přístupu
4. Autentizace: ověření identity uživatele (heslo, biometrie, tokeny)

### Důvody

- Ochrana citlivých dat: prevence před krádeží nebo zneužitím osobních dat
- Prevence útoků: ochrana před hackery, malwarem a jinými kyberhrozbami
- Zajištění dostupnosti: prevence před ztrátou přístupu k důležitým informacím

# Zabezpečení u OS Windows, certifikáty, Kerberos

## Autentizace v OS Windows

1. Interaktivní přihlášení – CTRL + ALT + DELETE – při startu počítače
2. Neinteraktivní přihlášení – uživatel požádá o přístup ke vzdáleným zdrojům

## Certifikáty

- Obsahují veřejný klíč, jméno a další údaje
- Vydány certifikačními autoritami (CA), kterým ostatní důvěřují
- Veřejný klíč = slouží k zašifrování zpráv, ale nelze pomocí něj zprávy přečíst. Je volně dostupný, tudíž každý může poslat zašifrovanou zprávu, ale nemůže nic číst. Odšifrovat zprávu může jen ten, který má soukromý klíč.

**Asymetrická kryptografie** – metoda s odlišnými klíči pro šifrování a odšifrování komunikace.

**Kerberos** – autentizační protokol pro klient-server, který zajišťuje vzájemnou identifikaci a brání odposlechu – klient i server si ověří identitu své protistrany. (protokol, který brání odposlechu)

# Praktické úkoly

## Změň bootovací priority v BIOSu

## Vytvoř podsložku složky test s názvem test1 a u ní zruš dědění práv a změň je