**5. Operační systémy v mobilních zařízeních**

* základní charakteristika a popis rozhraní OS Android a iOS,
* nejběžnější funkce mobilních zařízení,
* možnosti zabezpečení mobilních zařízení.

**Základní charakteristika a popis rozhraní OS Android a iOS**

**Open Source vs Closed Source**

* stejně jako stolní počítače a notebooky potřebují i mobilní zařízení pro spuštění SW operační systém.
* Open Source -> pokud se vývojář softwaru rozhodne poskytnout zdrojový kód programu
* Closed Source -> pokud není zdrojový kód softwaru k dispozici

U iOS -> aplikace pro mobilní zařízení s operačním systémem Apple iOS se získávají z internetového obchodu App Store, kde jsou buď zdarma, nebo za poplatek.

* Firma Apple používá pro aplikaci model „walled garden“ -> předtím, než je aplikace uvolněna pro uživatele, musí být schválena firmou Apple

U Androidu -> aplikace jsou dostupné buď z internetového obchodu Google Play, nebo z webů poskytovatelů třetí strany -> App Store od firmy Amazon

* Aplikace běží v izolovaném prostředí (sandboxu) a mají pouze ta oprávnění, která jim přiřadí uživatel
* Programy třetích stran, popřípadě vlastní programy se instalují prostřednictvím souborů APK -> umožňuje uživatelům přímou instalaci aplikací bez nutnosti používat internetový obchod -> sideloading.

**Android:**

* **Otevřený systém:** Postavený na Linuxovém jádru, Android je open-source platforma, která umožňuje výrobcům i vývojářům vysokou míru přizpůsobení.
* **Uživatelské rozhraní:** Moderní a flexibilní s podporou widgetů, dynamických launcherů a různých přizpůsobitelných ozdob. Nabízí intuitivní navigaci pomocí gest a notifikačního centra.
* **Ekosystém a obchod:** Google Play Store poskytuje široký výběr aplikací, her a služeb. Android úzce spolupracuje s Google službami jako Gmail, Google Maps nebo YouTube.
* **Rozmanitost zařízení:** Operační systém je implementován na různých typech hardwaru od mnoha výrobců, což umožňuje nabídku zařízení v různých cenových relacích a konfiguracích.

**iOS:**

* **Uzavřený systém:** Vyvinutý společností Apple, iOS je proprietární platforma, která běží výhradně na zařízeních Apple.
* **Konzistentní a intuitivní uživatelské rozhraní:** iOS se vyznačuje jednoduchým a jednotným designem, který je navržen pro snadnou navigaci a vysokou použitelnost.
* **App Store a bezpečnost:** Apple přísně kontroluje aplikace v App Store, což přispívá k vyšší bezpečnosti a stabilitě platformy.
* **Integrace v ekosystému Apple:** Silná synchronizace s dalšími zařízeními Apple (Mac, Apple Watch) a službami (iCloud, Apple Music), což umožňuje plynulé propojení napříč celým ekosystémem.

**Nejběžnější funkce mobilních zařízení**

Mobilní zařízení dnes poskytují komplexní funkce, které zahrnují:

* **Komunikace:** Telefonování, SMS, e-mail, videohovory a instant messaging.
* **Přístup k internetu:** Prohlížení webu, sociální sítě, streamování videa a hudby.
* **Multimédia:** Kvalitní fotoaparáty a kamery, přehrávače hudby a videa, editory fotografií a videí.
* **Navigační služby:** Vestavěné GPS, mapové aplikace a lokalizační služby.
* **Produktivita:** Kancelářské aplikace, kalendáře, poznámkové bloky, cloudové úložiště a synchronizace dat.
* **Senzory a biometrie:** Akcelerometry, gyroskopy, snímače otisků prstů či rozpoznávání obličeje, které slouží k usnadnění interakce a zabezpečení zařízení.
* **Bezdrátová konektivita:** Wi-Fi, Bluetooth, NFC a mobilní data (3G, 4G, 5G) pro široké možnosti připojení k síti.
* **Bezkontaktní možnost platby:** NFC, vzdálený přístup k bankovnímu účtu.

**Možnosti zabezpečení mobilních zařízení:**

Zabezpečení mobilních zařízení je zásadní pro ochranu osobních i firemních dat. Klíčové metody zahrnují:

* **Aktualizace systému:** Pravidelná instalace aktualizací operačního systému a aplikací, které opravují bezpečnostní chyby a zranitelnosti.
* **Biometrická autentizace:** Použití otisku prstu, rozpoznávání obličeje či jiných biometrických metod pro odemykání zařízení a ověřování uživatele.
* **Silné přístupové kódy:** Nastavení složitých PIN kódů, hesel nebo grafických vzorů, které brání neautorizovanému přístupu.
* **Šifrování dat:** Šifrování interních úložišť a komunikace (např. pomocí VPN) k ochraně dat při přenosu i v případě ztráty či krádeže zařízení.
* **Správa aplikací:** Instalace aplikací výhradně z oficiálních obchodů (Google Play, App Store) a pravidelné monitorování oprávnění, která aplikace požadují.
* **Mobilní Device Management (MDM):** Centrální správa a konfigurace bezpečnostních politik pro firemní zařízení, která umožňuje vzdálené vymazání dat a sledování zařízení.
* **Bezpečnostní školení:** Edukace uživatelů o potenciálních hrozbách, jako jsou phishingové útoky nebo škodlivé aplikace, a o správných bezpečnostních postupech.

Zajímavost:

**Rooting a Jailbreaking**

Operační systémy pro mobilní zaířzení jsou obvykle chráněny pomocí řady softwarových omezení.

* Autorizovaný kód aplikace může spustit pouze nezměněná kopie OS iOS. Uživatel má navíc jen velmi omezený přístup k souborovému systému.

Omezení a ochranu přidanou do operačních systémů pro mobilní zařízení lze odstranit pomocí operací označovaných jako Rooting nebo Jailbreaking.

* Pojem Rooting se používá na zařízeních s OS Android. Umožňuje získat privilegovaný přístup nebo přístup pod uživatelem root. Díky tomu lze upravovat zdrojový kód nebo instalovat software, který nebyl pro toto zařízení určen.
* Pojem Jailbreaking se typicky používá u mobilních zařízení s OS iOS, kde takto dochází l odstranění omezení nastavených výrobcem a umožňuje na zařízení spustit libovolný kód, získat úplný přístup k souborovému systému a k modulům jádra operačního systému.

Pomocí operací rooting nebo jailbreaking je možné zásadně proměnit i rozhraní GUI. Dále je možné provést takové úpravy v operačním systému, které vedou ke zrychlení a zvýšení reakce na povely zadané uživatelem. Rovněž je možné instalovat aplikace z alternativních nebo nepodporovaných zdrojů.

**Shrnutí**

* **Android a iOS** jsou nejrozšířenější mobilní operační systémy, přičemž Android nabízí otevřenost a přizpůsobitelnost, zatímco iOS se vyznačuje konzistentním, uzavřeným ekosystémem a vysokou bezpečností.
* Mobilní zařízení dnes kombinují funkce komunikace, multimédií, navigace, produktivity a mnoho dalších díky široké škále senzorů a připojovacích možností.
* **Zabezpečení mobilních zařízení** je klíčové a zahrnuje pravidelné aktualizace, biometrickou a heslovou ochranu, šifrování dat, správu aplikací, využití VPN a MDM, stejně jako vzdělávání uživatelů v oblasti bezpečnosti.