**Informačné systémy (IS)**: IS sú určené na zhromažďovanie, uchovávanie, spracovanie a distribúciu informácií. Tieto systémy sa skladajú z hardvérových, softvérových, dátových, procedurálnych a ľudských komponentov, ktoré spolupracujú s cieľom zabezpečiť efektívne a presné spracovanie informácií. Životný cyklus vývoja IS zahŕňa tieto fázy:

* Analýza: identifikácia potrieb používateľov, špecifikácia požiadaviek, tvorba špecifikácií
* Návrh: podrobný plán implementácie systému, návrh databázy a používateľského rozhrania
* Implementácia: vývoj a programovanie systému
* Testovanie: overenie funkčnosti a výkonnosti, odhalenie a oprava chýb
* Nasadenie: inštalácia a uvedenie systému do prevádzky
* Údržba: pravidelné aktualizácie, opravy a optimalizácia systému

Analýza IS zahŕňa štúdium skutočných procesov a požiadaviek používateľov, ktoré vedie k vytvoreniu dokumentácie, ako sú diagramy procesov, dátové modely a špecifikácie funkčnosti.

Druhy údržby softwaru:

* Opravná údržba: oprava chýb a nedostatkov v systéme
* Adaptívna údržba: úpravy systému s cieľom prispôsobiť sa zmenám v prostredí
* Zdokonaľujúca údržba: zlepšovanie efektívnosti a výkonnosti systému
* Preventívna údržba: predchádzanie budúcim problémom a optimalizácia systému

**Server**: Servery sú počítačové systémy, ktoré poskytujú služby iným počítačom (klientom) v sieti. Typy serverov podľa ich účelu:

* Webové servery: hostiteľské webové stránky a aplikácie
* Databázové servery: spravujú databázy a poskytujú prístup k nim, napríklad MySQL, Oracle
* Aplikačné servery: spúšťajú podnikové aplikácie, napríklad servery Java EE
* Súborové servery: ukladajú a spravujú súbory na zdieľanie medzi používateľmi, napríklad servery NAS
* Poštové servery: spravujú a distribuujú elektronickú poštu, napríklad Microsoft Exchange

Komunikácia server-klient:

* Tenký klient: Vykonáva minimum operácií, väčšinu z nich zabezpečuje server. Vhodný pre prostredia s obmedzenými zdrojmi.
* Hrubý klient: Spracováva viac operácií na strane klienta, čo znižuje zaťaženie servera a môže zlepšiť výkon a odozvu aplikácie.

**Nemocničný informačný systém (NIS)**: NIS je komplexný systém na riadenie nemocničných procesov a zdravotníckych záznamov. Hlavné časti/komponenty NIS sú:

* Klinický informačný systém (CIS): Správa údajov o pacientoch, záznamy o liečbe, prepojenie s inými oddeleniami, ako je ambulantná a nemocničná starostlivosť.
* Laboratórny informačný systém (LIS): Spracovanie laboratórnych vzoriek, výsledkov, štatistík a fakturácie vykonaných postupov.
* Rádiologický informačný systém (RIS): Správa rádiologických snímok, ich popis a prepojenie s PACS a inými systémami
* PACS (Picture Archiving and Communication System): Technológia na správu, ukladanie, archiváciu a zobrazovanie obrazovej dokumentácie, ako sú röntgenové snímky, snímky MRI a CT.
* DICOM (Digital Imaging and Communications in Medicine): Medzinárodná norma na správu a prenos obrazových údajov v medicíne, ktorá umožňuje interoperabilitu medzi rôznymi zobrazovacími zariadeniami a systémami PACS.

**Pripojenie zdravotníckych zariadení do NIS**: Možnosti pripojenia zdravotníckych pomôcok k NIS zahŕňajú používanie štandardizovaných formátov údajov a protokolov, ako napr:

* HL7 (Health Level Seven): medzinárodný štandard na výmenu klinických a administratívnych údajov medzi zdravotníckymi informačnými systémami. Používa sa napríklad na prenos údajov o pacientoch, laboratórnych výsledkov a iných zdravotných informácií.
* DICOM (Digital Imaging and Communications in Medicine): štandard na správu a prenos obrazových informácií, ktorý umožňuje interoperabilitu medzi rôznymi zobrazovacími zariadeniami a systémami PACS. Umožňuje pripojenie zariadení, ako sú CT, MRI a ultrazvukové prístroje, k NIS.

**Dátové formáty a národné zdravotné registre**: Dátové formáty pre komunikáciu medzi zdravotníckymi zariadeniami a Ministerstvom zdravotníctva Českej republiky zahŕňajú:

* DaSta (dátový štandard): štandard pre výmenu zdravotných údajov v rámci Českej republiky, ktorý poskytuje jednotný formát údajov pre lepšiu interoperabilitu a zdieľanie informácií.
* HL7: medzinárodný štandard pre výmenu klinických a administratívnych údajov.

Národné zdravotné registre sa používajú na centralizáciu a správu zdravotných údajov. Príkladom sú registre na sledovanie epidemiologických údajov, onkologické registre a registre na sledovanie špecifických zdravotných stavov a postupov.

**Systémy klasifikácie diagnóz a postupov**:

* MKCH10 (Medzinárodná klasifikácia chorôb, 10. revízia): Systém klasifikácie diagnóz, ktorý používajú zdravotnícki pracovníci na kódovanie chorôb a zdravotných stavov. Obsahuje tisíce kódov pre rôzne diagnózy a je štandardom pre lekárske záznamy na celom svete.
* SNOMED (Systematized Nomenclature of Medicine): Podrobný lexikón na kódovanie lekárskych termínov, ktorý umožňuje presné a konzistentné záznamy o lekárskych stavoch a postupoch. SNOMED CT pokrýva širokú škálu lekárskych termínov a používa sa na interoperabilitu medzi zdravotníckymi informačnými systémami.

**Dátové štandardy**: sú kľúčom k zabezpečeniu interoperability medzi rôznymi systémami v zdravotníckych zariadeniach. Medzi hlavné štandardy patria:

* DaSta: Štandard pre výmenu zdravotných údajov v Českej republike.
* HL7: Medzinárodný štandard pre výmenu klinických a administratívnych údajov, ktorý umožňuje jednotnú komunikáciu medzi rôznymi systémami zdravotnej starostlivosti.
* DICOM: Štandard na správu a prenos lekárskych obrazových informácií, ktorý zabezpečuje kompatibilitu medzi zobrazovacími zariadeniami a PACS.
* PACS a ePACS: Systémy na správu, archiváciu a distribúciu obrazových údajov. PACS umožňuje centralizované ukladanie obrazových údajov a ich jednoduché zdieľanie medzi zdravotníckymi pracovníkmi.

**Zdravotná dokumentácia**: Právne predpisy o zdravotnej dokumentácii zahŕňajú pravidlá o správe a uchovávaní zdravotnej dokumentácie s cieľom zabezpečiť jej dôvernosť a integritu. V rámci NIS je dôležitá bezpečnosť prístupu k týmto záznamom a úlohy používateľov musia byť jasne definované. Medzi kľúčové aspekty patria:

* Bezpečnosť: ochrana údajov pred neoprávneným prístupom pomocou overovania, šifrovania a prístupových práv.
* Používateľské roly: definovanie oprávnení a zodpovedností jednotlivých používateľov systému, čím sa zabezpečí, že k citlivým informáciám majú prístup len oprávnení pracovníci.

**Elektronické zdravotné záznamy (EHR, EMR, EPR)**: Elektronické zdravotné záznamy (EHR, EMR, EPR) umožňujú centralizovanú správu údajov o pacientoch, čo zlepšuje koordináciu starostlivosti a znižuje riziko chýb. Rozdiely medzi nimi:

* EHR (elektronický zdravotný záznam): súhrnný záznam pacienta, ktorý sa môže zdieľať medzi rôznymi zdravotníckymi zariadeniami a obsahuje všetky relevantné zdravotné informácie o pacientovi.
* EMR (elektronický medicínsky záznam): elektronický záznam špecifický pre jedno zdravotnícke zariadenie, ktorý obsahuje informácie o pacientoch liečených v tomto zariadení.
* EPR (elektronický záznam pacienta): širší pojem, ktorý zahŕňa EHR aj EMR a poskytuje úplný prehľad o zdravotnom stave pacienta v rôznych zdravotníckych zariadeniach.

**eHealth v ČR**: Elektronizácia zdravotníctva v Českej republike zahŕňa rôzne iniciatívy:

* eRecept: elektronická správa receptov, ktorá umožňuje lekárom vystavovať recepty elektronicky a pacientom ich vyzdvihnúť v ktorejkoľvek lekárni.
* eNeschopenka: elektronická správa práceneschopnosti, ktorá zjednodušuje proces hlásenia a správy práceneschopnosti pre pacientov, lekárov a zamestnávateľov.

**Kvantitatívne rozhodovacie modely**: Kvantitatívne rozhodovacie modely v medicíne zahŕňajú hodnotenie diagnostických testov a liečby pomocou ukazovateľov, ako sú:

* Krivka ROC (Receiver Operating Characteristic): grafické znázornenie schopnosti diagnostického testu rozlišovať medzi pozitívnymi a negatívnymi prípadmi. Zobrazuje vzťah medzi citlivosťou (pravdepodobnosť správneho určenia pozitívneho prípadu) a špecificitou (pravdepodobnosť správneho určenia negatívneho prípadu) pri rôznych prahových hodnotách.
* Citlivosť a špecifickosť: metriky na hodnotenie výkonnosti diagnostických testov. Citlivosť meria schopnosť testu správne identifikovať pozitívne prípady (pravdepodobnosť správneho odhalenia chorého jedinca), špecifickosť meria schopnosť testu správne identifikovať negatívne prípady (pravdepodobnosť správneho odhalenia zdravého jedinca).

**Databáza a správa databáz**: Databázové systémy zabezpečujú efektívnu správu údajov.

* Dátové modely: Štruktúry na organizáciu údajov, napríklad relačný model, ktorý používa tabuľky na ukladanie údajov a vzťahov medzi nimi.
* Obmedzenia integrity: Pravidlá na zabezpečenie správnosti a konzistentnosti údajov, napríklad primárne a cudzie kľúče, jedinečnosť, nenulové hodnoty.
* Normalizácia údajov: Proces usporiadania údajov do tabuliek s cieľom minimalizovať redundanciu a zabezpečiť integritu údajov. Medzi stupne normalizácie patrí prvá normálna forma (1NF), druhá normálna forma (2NF), tretia normálna forma (3NF) a Boyceova-Coddova normálna forma (BCNF).
* Transakčné spracovanie: Zabezpečenie správneho a úplného vykonávania operácií s databázou, ktoré zahŕňa vlastnosti ACID (atomicita, konzistencia, izolácia, perzistencia).
* Obnova po poruche: Mechanizmy na obnovu databázy po poruche, ako je zálohovanie a obnova, protokolovanie transakcií.

**Bezpečnosť IT a kryptografické mechanizmy**: Bezpečnosť IT zahŕňa ochranu údajov a systémov pred neoprávneným prístupom a útokmi. Medzi kľúčové kryptografické mechanizmy patria:

* Šifrovanie: ochrana údajov pomocou kryptografických algoritmov, ako je symetrické (napr. AES) a asymetrické (napr. RSA) šifrovanie.
* Digitálny podpis: overovanie identity a integrity údajov pomocou kryptografických algoritmov. Digitálne podpisy zabezpečujú, že údaje neboli zmenené, a potvrdzujú totožnosť odosielateľa.
* Certifikáty a certifikačné autority: certifikáty sa používajú na overenie identity; certifikačné autority (CA) vydávajú a spravujú certifikáty, ako sú napríklad certifikáty SSL/TLS na bezpečnú komunikáciu cez internet.
* Hashovacie funkcie: kryptografické funkcie, ktoré zabezpečujú údaje pred neoprávnenými zmenami. Hashovacie funkcie, ako napríklad SHA-256, generujú jedinečný odtlačok údajov, ktorý sa môže použiť na overenie integrity.

**Identifikácia a autentifikácia**: Metódy identifikácie a autentifikácie zahŕňajú:

* Heslá: Tradičná metóda overovania, požiadavky na zložitosť, dĺžku a pravidelné zmeny zabezpečujú bezpečnosť. Silné heslá obsahujú kombináciu písmen, číslic a špeciálnych znakov.
* Biometria: Overovanie pomocou jedinečných fyzických charakteristík používateľa, ako sú odtlačky prstov, rozpoznávanie tváre a skenovanie dúhovky.
* Čipové karty a kryptografia: Používanie hardvérových tokenov, ako sú čipové karty, na bezpečné overovanie. Tieto karty môžu obsahovať kryptografické kľúče na šifrovanie a dešifrovanie údajov.

**Princípy antivírusových programov**: Antivírusové programy sú určené na detekciu a odstránenie škodlivého softvéru (malvéru). Medzi hlavné metódy patria:

* Skenovanie súborov: kontrola súborov podľa databázy známych vírusov, hľadanie známych vírusových signatúr.
* Heuristická analýza: zisťovanie nových a neznámych hrozieb analýzou správania programov, identifikácia podozrivých činností.
* Rezidentné štíty: ochrana v reálnom čase, kontrola volaní špecifických funkcií operačného systému a blokovanie škodlivých činností pred ich vykonaním.
* Pravidelné aktualizácie: aktualizácia vírusových databáz na ochranu pred novými hrozbami. Antivírusové programy sa musia pravidelne aktualizovať, aby boli účinné proti najnovším hrozbám.
* Zálohovanie údajov: pravidelné zálohovanie dôležitých údajov, aby bolo možné ich obnovenie po infekcii. Je dôležité uchovávať zálohy na bezpečnom mieste, oddelene od hlavného systému.