

Informatika 2

Neslužbena skripta



SADRŽAJ

1. POJAM INFORMACIJSKOG SUSTAVA	4
1.1. Definicija informacijskog sustava	4
1.2. Razlozi izgradnje IS-a	4
1.2.1. Poslovni sustav	4
1.2.2. Sustavski pristup	5
1.3. Pojmovi vezani uz informacijski sustav	5
1.3.1. Podatak	5
1.3.2. Algoritam	6
1.3.3. Informacija	6
1.4. Funkcije informacijskog sustava u poslovnom sustavu	6
1.5. Ciljevi informacijskog sustava	7
1.6. Elementi informacijskog sustava	8
1.6.1. Hardware	8
1.6.2. Software	8
1.6.3. Liveware	8
1.6.4. Orgware	9
1.6.5. Netware	10
1.6.6. Dataware	10
2. INFORMACIJSKI SUSTAVI	12
2.1. Životni ciklus IS-a	12
2.2. Metode izgradnje IS-a	12
2.2.1. Vodopadna metoda	13
2.2.2. Metoda prototipiranja	13
2.2.3. Evolucijska metoda	14
2.2.4. Spiralna metoda	14
2.3. Dijelovi IS-a	14
2.3.1. Sustav za obradu transakcija	15
2.3.2. Upravljački izvještajni sustav	16
2.3.3. Sustav za podršku odlučivanju	16
2.3.4. Sustav uredskog poslovanja	17
2.4. Vrste IS-a	17
2.5. Elektroničko poslovanje	18
2.5.1. Vrste elektroničkog poslovanja	19
2.5.2. Sigurnosni problemi elektroničkog poslovanja	19
2.5.2.1. Kriptiranje sadržaja i kriptosustavi	19
2.5.2.2. Digitalni potpis i digitalni certifikati	20
2.5.3. Elektronička razmjena podataka	21
2.5.4. Elektronički marketing	21
2.5.5. Elektronička tržišta	22
2.5.6. Elektronički sustav plaćanja	23
2.5.6.1. Mikro plaćanje	23
2.5.6.2. Elektronička gotovina	23
2.5.6.3. Elektronički čekovi	24
2.5.6.4. Online transakcije s kreditnim karticama	24
2.6. Poslovno odlučivanje	24
2.6.1. Linearna optimizacija	24
2.6.2. Simulacije	25
2.6.3. Sustavi za potporu odlučivanju	26
2.6.4. Ekspertni sustavi	27
3. NAČINI PRIKAZA REZULTATA OBRADE	29
3.1. Tehnike prikaza podataka	29
3.1.1. Znakovni podaci	29
3.1.2. Slikovni podaci	29
3.1.3. Zvukovni podaci	30
3.1.4. Kompresija podataka	30
3.1.5. Kriptiranje podataka	31
3.1.6. Multimedija	31
3.1.7. Prividna stvarnost	32
3.1.8. Područja primjene multimedije	32
4. RAČUNALNE MREŽE I INTERNET	34
4.1. Pojam i vrste računalnih mreža	34
4.2. Elementi računalnih mreža	34
4.3. Topologija mreže	37
4.4. Serijski prijenos podataka	38
4.4.1. Sinkroni i asinkroni serijski prijenos	39
4.5. Paralelni prijenos podataka	39
4.6. Internet	40
4.6.1. Građa Interneta	41
4.6.2. Internetski servisi	41
4.6.3. Načini pretraživanja Interneta	43
4.6.3.1. Tražilice	43
4.6.3.2. Metatražilice	45
4.6.3.3. Tematski katalozi	46
4.6.3.4. Inteligentni agenti	46
4.6.4. Vrednovanje informacija pronađenih na Internetu	47
5. SIGURNOST I ZAŠTITA IS-a	48
5.1. Sigurnost IS-a	48
5.2.1. Pojam sigurnosti i zaštite IS-a	48

5.2.2. Izvori i oblici prijetnji sigurnosti IS-a	48
5.2.3. Mjere zaštite podatkovnog sadržaja	49
5.2.3.1. Fizičke i tehničke mjere zaštite	49
5.2.3.2. Programske mjere zaštite	49
5.2.3.3. Organizacijske mjere zaštite	50
5.2.3.4. Mjere zaštite iz oblasti prava	50
5.2.4. Kriptografija i sigurnosni mehanizmi	51

1. POJAM INFORMACIJSKOG SUSTAVA

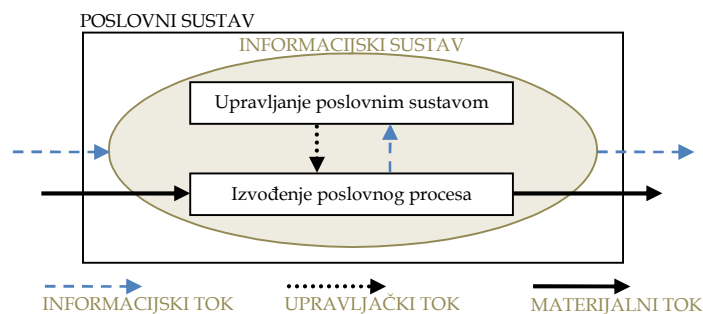
1.1. Definicija informacijskog sustava

- Efikasno obavljanje gotovo svih poslova, u bilo kojem poslovnom sustavu, popraćeno je informacijama i podacima. Nezavisno o vrsti poslovnih procesa koje podržava ili veličini organizacije u kojoj funkcionira, informacijski sustav (IS) se pojavljuje i primjenjuje kao ključni element poslovanja. Njegova je povećana uloga i važnost popraćena i rastućom primjenom informacijske tehnologije (IT).
- **Cilj je informacijskog sustava pribaviti informacije potrebne pri izvođenju poslovnog procesa i upravljanju poslovnim sustavom. Uobičajeni su dijelovi informacijskog sustava sustav za obradu transakcija, upravljački izvještajni sustav, sustav za potporu odlučivanju i sustav uredskog poslovanja.**
- Djelovanje IS-a upotpunjuje se primjenom IT-a i s njima povezanim programima, procedurama, uputama, algoritmima i znanjem kojima se IT pokreću zbog izvršenja poslovnih zadataka i ciljeva.
- Informacijski sustav (IS) je prema tome sprega i sustav materijalnih i nematerijalnih elemenata kojima se opisuje poslovna stvarnost, rješavaju poslovni zadaci i ispunjavaju poslovni ciljevi. Kao dio IS-a, čovjek/pojedinac formalizira poslovno okruženje u podatke, procedure, algoritme, informacije i znanja te usklađujući primjenu IT-a i programsku podršku, ispunjava poslovne funkcije i zadatke (dostavljanje i čuvanje podatka neophodnih za odlučivanje, održanje procesa te razvoj i neprekidnost poslovanja).
- Kao model poslovnog sustava, IS opisuje poslovni sustav, on je njegov informacijski model. Elementi poslovnog sustava (podaci, aktivnosti, funkcije, zadaci, izvršitelji, postupci itd), preslikavaju se na model informacijskog sustava gdje ih dijelimo na:
 - **model podataka** – definira podatke koji nastaju ili se koriste u poslovnom sustavu.
 - **model procesa** – definira procese ili funkcije koje se odvijaju u poslovnom sustavu.
 - **model izvršitelja** – definira one elemente koji obavljaju funkciju u poslovnom sustavu (software, hardware, liveware, orgware).

1.2. Razlozi izgradnje IS-a

1.2.1. Poslovni sustav

- Informacijski sustav djeluje unutar nekog poslovnog sustava, omogućavajući mu da komunicira unutar sebe i sa svojom okolinom. Slika prikazuje djelovanje informacijskog sustava unutar poslovnog sustava.



SLIKA 1.1 INFORMACIJSKI SUSTAV KAO DIO POSLOVNOG SUSTAVA

- U poslovni sustav ulaze i izlaze materijalni (materijal, sirovina, energija) i informacijski tokovi. Dvije su temeljne aktivnosti svakog poslovnog sustava:
 - **Izvršavanje poslovnih procesa**
 - Kad govorimo o poslovnom procesu, mislimo na osnovnu djelatnost promatranog poslovnog sustava odnosno na poslove koji se u njemu obavljaju.
 - U proizvodnom poduzeću poslovni proces sastoji se npr. od poslova proizvodnje, nabave potrebnih sirovina i energije, plasmana proizvedenih proizvoda itd.

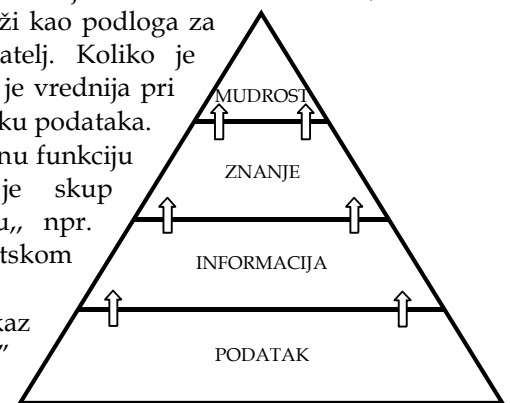
- U bankama poslovni proces obuhvaća poslove obavljanja finansijskih transakcija, kreditiranja, štednje itd.
- **Upravljanje poslovnim sustavom**
 - Svaki poslovni odnosno stvarni sustav (npr. poduzeće, ustanova, privreda, društvo) nastoji izgraditi svoj informacijski sustav koji će dati podlogu za brzo i kvalitetno odlučivanje, dakle za **transformaciju informacija u odluke**.
- Informacijska se tehnologija u mnogim poslovnim procesima koristi jer znatno podiže efikasnost odvijanja poslovnog procesa, npr. rezervacijski sustavi zrakoplovnih kompanija, poslovanje banaka...

1.2.2. Sustavski pristup

- Sustav je cjelina koja se ne može rastaviti na svoje dijelove a da se pri tome ne izgube njena osnovna svojstva.
- Sustavnim se pristupom **istražuju pojave i rješavaju problemi u njihovoj cjelokupnosti** i složenosti, obuhvaćajući sve bitne veze i odnose između dijelova sustava i između sustava i okoline. Pojave i probleme razmatraju s više gledišta stručnjaci različitih znanstvenih područja.
- Sustavni pristup ne označava spajanje samo dosad odvojenih predmeta znanstvenog proučavanja, nego i razdvojenih područja ljudskih aktivnosti. Sustav je sređena cjelina koju čine njegovi elementi povezani na određeni način, a njihovim međusobnim djelovanjem postižu se određeni ciljevi funkcioniranja sustava. Da bismo opisali neki sustav, potrebno je поближе odrediti:
 - koji *elementi* pripadaju sustavu,
 - koje *veze* postoje između elemenata unutar sustava i između elemenata sustava i okoline i
 - kakvo je *ponašanje* (funkcioniranje) sustava
- Realni sustav sačinjen je od elemenata koji su dio konkretnog realnog objekta, a koji se opisuju kao sustav (mehanički, fizički, biološki, društveni).

1.3. Pojmovi vezani uz informacijski sustav

- Iako se često pojmovi *informacija* i *podatak* smatraju sinonimima, njihovo značenje se razlikuje: informacija odnosno obavijest proizlazi iz podataka – zapisa na nekom mediju.
- **Informacija** odnosno obavijest jest činjenica s određenim značenjem. Ona donosi novost, obavještava o nečemu, te otklanja neizvjesnost i općenito služi kao podloga za odlučivanje. Vrijednost informacije određuje sam primatelj. Koliko je upotrebljena informacija relevantnija, točnija i svježija, toliko je vrednija pri odlučivanju. Informaciju ćemo sačuvati ako je zapišemo u obliku podataka.
- **Podatak** je pojam kojim opisujemo i kvantificiramo elementarnu funkciju realnog sustava u određenom trenutku. Podatak je skup prepoznatljivih znakova zapisanih na određenom mediju,, npr. papiru (knjiga, notes), filmu (fotografija, filmski zapis), magnetskom mediju (datoteka na disku u računalu)...
- Informatički gledano, **elementarni podatak** simbolički je prikaz jednog obilježja promatranog objekta. Npr. podatak "Marko" prikazuje nam ime promatrane osobe.
- **Znanje** je uređen skup informacija nekog područja. Njime se opisuje stanje stvari, koje je ustanovljeno po nekom prihvaćenom kriteriju. Svako područje organizira u danom vremenskom trenutku svoje znanje utvrđivanjem prikladnih kategorija koncepata (elemenata znanja), njihovih međusobnih odnosa i ograničenja. Postoje različiti načini prikaza znanja. Najpoznatiji prikaz znanja je u obliku pravila (npr. u matematici aksioma, teorema itd.).



SLIKA 1.2: PODATAK, INFORMACIJA, ZNANJE I MUDROST

1.3.1. Podatak

- **Podatak je skup prepoznatljivih znakova zapisanih na određenom mediju.** Elementarni podatak je simbolički prikaz jednog obilježja promatranog objekta.

- Osim tradicionalnih strukturiranih podataka u obliku datoteka i baza podataka sve se više koriste i slabo strukturirani podaci kao što su različite vrste dokumenata te multimedijški podaci kao što su grafika, fotografije, zvuk i video.
- Danas se podaci intenzivno distribuiraju na korporacijskim mrežama i na internetu. Također se intenzivno razvijaju skladišta podataka u koja se pohranjuju podaci iz više različitih izvora podataka.

1.3.2. Algoritam

- **Algoritam je postupak ili pravilo za sustavno rješavanje određene vrste problema.** To je bilo koje dobro rješenje bilo kojeg problema. Sastoji se od opisa konačnog skupa koraka. Svaki od njih sadrži jednu ili više izjava, a svaka izjava jednu ili više operacija.
- Algoritmima su u prvo vrijeme nazivana samo pravila računanja s brojevima zapisanim u dekadnom sustavu, da bi se kasnije taj naziv počeo koristiti za pravila obavljanja raznovrsnih zadataka.
- S praktičnog gledišta, algoritmi su jasno definirani postupci za izvršavanje određenog problema. Algoritmi, raščlanjeni na uzastopne korake, prevode neki skup početnih (ulaznih) vrijednosti u skup završnih (izlaznih) vrijednosti. Početne i završne vrijednosti te eventualni međurezultati pohranjuju se u prikladne strukture podataka.
- Algoritmi se koriste za jasno utvrđivanje pravila dostizanja nekog postavljenog cilja. Uz svaki algoritam moraju biti jasno definirana početna stanja objekta na kojima se obavljaju operacije.
- Algoritam mora biti sastavljen od konačnog broja koraka koji utvrđuju slijed operacija koje treba obaviti nad objektima kako bi se dobila završna stanja objekata ili rezultati. Svaki korak opisuje se instrukcijom. Obavljanje algoritma naziva se algoritamskim procesom.
- Vrste algoritma:
 - **Specijalizirani** – mogu se primjeniti samo na pojedina početna stanja objekata.
 - **Općeniti** – mogu djelovati uz različita početna stanja objekata. Kod njih se definira klasa objekata i početnih stanja koja su dopuštena.

1.3.3. Informacija

- Poslovne informacije se dijele na dizajn proizvoda, tehničke podatke, upute menadžmenta, operativne baze podataka, operativne procese, tehničke baze podataka, znanje zaposlenih i računalni softver, a nalazimo i podjelu na poslovne ugovore, radne upute, poslovne rezultate i izvješća, baze podataka, sistemsku dokumentaciju, korisničke priručnike, operativne procedure, planove, aplikacijski i sistemski softver, razvojne i pomoćne alate itd.
- U poslovnim sustavima one predstavljaju ključni izvor poslovanja, jednu od najvećih poslovnih vrijednosti, osnovni izvor za stjecanje dohotka i pokretačku snagu za stvaranje nove vrijednosti. Informacija su bitne u svim oblicima poslovanja, a posebno su važne pri donošenju odluka, poboljšanju performansa sustava, postizanju tržišnog uspjeha i u podršci radnim procesima. Naglašena je i komunikacijska uloga informacije. U svakom slučaju, **informacije su nosioci poslovnih promjena**, instrument formaliziranja poslovne okoline i upravljanja okolišem.
- Općenito govoreći, informacije nastaju kad se niz uređenih i prepoznatljivih, ali značenjem nezanimljivih znakova kojima se predstavlja obilježje nekog objekta ili stvarnosti sredi i organizira u smislen oblik koji ima značenje, a za primatelja je novost. U poslovnim organizacijama poslovnom informacijom postaje onaj sadržaj koji je u funkciji ostvarenja poslovnih ciljeva. Poslovne informacije najčešće služe kao temelj odlučivanja, ali se koriste i za održavanje i podršku poslovnim procesima, međusobnu komunikaciju zaposlenika itd., a mogu biti i osobito zanimljive ako se moraju čuvati ili pak predstavljaju neposrednu financijsku vrijednost.

1.4. Funkcije informacijskog sustava u poslovnom sustavu

- Informacijski sustav djeluje unutar nekog poslovnog sustava omogućavajući mu da komunicira unutar sebe i sa okolinom.
- Cilj informacijskog sustava je opskrbiti poslovni sustav sa svim potrebnim informacijama, potrebnim pri izvođenju poslovnog procesa i upravljanju poslovnim sustavom.
- Mnogobrojni pozitivni rezultati nastaju primjenom IS-a. Između ostalog ističu se uloge IS-a kao: pokretača poslovanja, osnovnog sredstva privređivanja, sredstva za stjecanje prednosti i razlikovanje, sredstva za unapređenje poslovanja, osnovnog podsustava organizacije itd.

- IS-om čovjek/pojedinac formalizira poslovno okružje u podatke, procedure, algoritme, informacije i znanja te usklađujući primjenu IT-a i programsku podršku, ispunjava poslovne funkcije i zadatke (dostavljanje i čuvanje podatka neophodnih za odlučivanje, održanje procesa te razvoj i neprekidnost poslovanja).
- Pritom se IS u velikoj mjeri oslanja na ICT (informacijsko-komunikacijsku tehnologiju) te njihovom primjenom obrađuje, prenosi, pohranjuje, dohvaća i objavljuje informacije i podatke kojima se opisuje tijek, stanja i procesi poslovnog sustava.

1.5. Ciljevi informacijskog sustava

- Informacijski sustav djeluje unutar nekog poslovnog sustava, omogućavajući mu da komunicira unutar sebe i sa svojom okolinom. Slika 1.1 prikazuje djelovanje informacijskog sustava unutar poslovnog sustava. U poslovni sustav ulaze i izlaze materijalni (materijal, sirovina, energija) i informacijski tokovi. Informacijski sustav preuzima informacije, obrađuje ih i prerađene prezentira poslovnom sustavu ili okolini. Informacijski je sustav, dakle, podsustav poslovnog sustava.
- Poslovni sustav dobiva informacije iz raznih izvora, vanjskih ili unutarnjih, a informacijski sustav ih obrađuje u nove i korisne informacije.
- Cilj je informacijskog sustava opskrbiti poslovni sustav svim njemu potrebnim informacijama, potrebnim pri:
 - **izvođenju poslovnog procesa**
 - **upravljanju poslovnim sustavom.**

IZVOĐENJE POSLOVNOG PROCESA:

- Kad govorimo o poslovnom procesu, mislimo na osnovnu djelatnost promatranog poslovnog sustava odnosno na poslove koji se u njemu obavljaju. U proizvodnom poduzeću poslovni proces sastoji se npr. od poslova proizvodnje, nabave potrebnih sirovina i energije, plasmana proizvedenih proizvoda itd. U bankama poslovni proces obuhvaća poslove obavljanja financijskih transakcija, kreditiranja, štednje itd.
- Informacijska se tehnologija u mnogim poslovnim procesima koristi jer znatno podiže efikasnost odvijanja poslovnog procesa. U nekim poslovnim procesima nemoguće je konkretno obavljati posao bez primjene informacijske tehnologije, npr. rezervacijski sustavi zrakoplovnih kompanija, poslovanje banaka itd. Upotrebom informacijske tehnologije može se izvođenje poslovnog procesa "automatizirati".
- **Automatizacija** poslovnog procesa jedan je od važnijih zadataka primjene informacijske tehnologije odnosno izgradnje informacijskog sustava temeljenog na informacijskoj tehnologiji.

UPRAVLJANJE POSLOVNIM SUSTAVOM I ODLUČIVANJE:

- Drugi zadatak informacijskog sustava jest osigurati informacije za efikasno upravljanje poslovnim sustavom. Informacija, bilo unutarnjeg ili vanjskog karaktera, predstavlja podlogu za donošenje određene poslovne odluke. Odluka je pak u funkciji ostvarivanja svrhe i cilja postojanja sustava. Pomoću odluka svjesno se upravlja sustavom (na Slici 1.1 to su upravljački tokovi).
- Prema tome, svaki poslovni, odnosno stvarni sustav (npr. poduzeće, ustanova, privreda, društvo) nastoji izgraditi svoj informacijski sustav koji će dati podlogu za brzo i kvalitetno odlučivanje, dakle za transformaciju informacija u odluke. Valja naglasiti da je odlučivanje proces koji ne traje samo u trenutku donošenja. Proces odlučivanja sastoji se od ovih koraka (Stallings i dr, 1988):
 - Prepoznavanje problema
 - Pronalaženje i ocjenjivanje opcija
 - Odabir opcije
 - Provedba
 - Ocjena
- Razmotrimo sada funkciju informacijskog sustava u pojedinim poslovnim područjima. Najvažnija poslovna područja primjene informacijskog sustava jednog poduzeća s primjerima primjene informacijske tehnologije su: proizvodnja, financije/računovodstvo, marketing, istraživanje i razvoj te ljudski resursi. Valja napomenuti da neki informacijski resursi, a to su

prvenstveno podaci, pripadaju čitavom poduzeću, a ne samo poslovnom području u kojem se obrađuju.

1.6. Elementi informacijskog sustava

1.6.1. Hardware

- Materijalna osnovica koju čine informacijske tehnologije, npr. računala, radne stanice, modemi, fizičke linije za komunikaciju itd.
- Hardver je najniža razina računalnog sustava. Čine je svi dijelovi od koje je načinjen računalni sustav:
 - svi mehanički dijelovi
 - magnetski, električni i elektronički sastavni dijelovi
 - naprave i uređaji (kućište, pogonski motor diska, magnetska vrpca, disk, poluvodička memorija, izvori električnog napajanja, integrirani sklopovi)
- Hardver je osnovica računalnog sustava u koju spadaju
 - **CPU** - sastavljena od elektroničkih komponenti i nema mehaničkih dijelova
 - **glavna memorija** kao osnovni uređaj za pohranu podataka koja se također sastoji od el. komponenti i ne sadrži mehaničke dijelove
 - **ulazno-izlazni uređaji** (tipkovnica, zaslon, pisači, veze, sabirnice...) i obično se sastoje od el. komponenti i različitih mehaničkih dijelova
 - **vanjska memorija** koja se također sastoji od el. dijelova i različitih mehaničkih komponenti
 - **komunikacijski uređaji**.

1.6.2. Software

- U software spada sva programska podrška koja se koristi pri radu tog sustava, to je skup svih programa koji se koriste u IS-u. Možemo ga definirati i kao onaj dio sustava koji postoji ali ne u fizičkom obliku nego u obliku informacija pohranjenih na računalu.
- Sistemski software čine programi koji promatrano zajedno predstavljaju skup programa koji služe za kontrolu i rad strojne podrške pri računalnoj obradi podataka.
- Software dijelimo na:
 - **Aplikativni** (korisnički programi) - skup korisničkih programa potrebnih za rješavanje raznih problemskih situacija koji proizlaze iz domene zadataka inf. Sustava.
 - **Sistemski** (sustavski programi) – skup strojno orijentiranih programa s funkcijom upravljanja i kontrole strojnog sustava u cilju sinhronizacije rada s aplikativnom podrškom.



SLIKA 1.3: PODJELA SOFTWARE-A

1.6.3. Liveware

- U liveware ubrajamo "živu" komponentu IS-a.
- Odnosi se na zaposlenike individualce, timove, njihovo znanje i sve osobe uključen u djelovanje IS-a
- Čovjek je osnovna komponenta IS-a jer kao njegov dio čovjek/pojedinac formalizira poslovno okružje u podatke, procedure, algoritme, informacije i znanja te usklađujući primjenu IT-a i programsku podršku, ispunjava poslovne funkcije i zadatke (dostavljanje i čuvanje podataka neophodnih za odlučivanje, održanje procesa te razvoj i neprekidnost poslovanja).
- Zaposlenici IS-a koji ulaze u liveware definiciju su npr. *korisnici* - od IS-a primaju informacije, *sistem analitičari* - veza između korisnika i IS-a, *programeri* - stvaraju programe, *program*

analitičari - spoj poslova programera i program-analitičarima u manjim tvrtkama, operatori na računalu, operatori unosa podataka, analitičari baze podataka, administratori, menadžeri...

1.6.4. Orgware

- Pod pojmom "orgware" se podrazumijeva organizacija tehničke opreme IS-a (hardware), programske opreme IS-a (software) i ljudi-izvršitelja poslova u IS-u u skladnu cjelinu.
- Definira koncepciju i organizaciju rada informacijskog sustava.
- Razlikujemo više oblika organizacije IS-a radi čim boljeg upravljanja istim:
 - **Odjel za informacijski sustav**
 - **Korisničko računalstvo**
 - **Informacijski centar**
 - **Unajmljivanje informacijskih usluga (Outsourcing)**

ODJEL ZA INFORMACIJSKI SUSTAV:

- Centralizirani oblik upravljanja IS-om.
- Na čelu je glavni informacijski menadžer sa zadacima:
 - Planiranje strategije IS-a
 - Efikasno vođenje odjela za IS
 - Briga o sigurnosti IS-a
 - Praćenje tehnoloških trendova



SLIKA 1.4: INFORMACIJSKI SUSTAV PODUZE A

KORISNIČKO RAČUNALSTVO:

- Decentralizirani oblik upravljanja IS-om.
- Glavni razlog zbog kojeg se korisničko računalstvo razvilo je nemogućnost profesionalnih informatičara da odgovore na silne zahtjeve korisnika za novim programima.
- Stoga se potiče korisnika da sam pomoću neke već napravljene aplikacije konstruira program koji bi zadovoljio njegove specifične potrebe.

INFORMACIJSKI CENTAR:

- Informacijski centar (engl. Information Center), organizacijska je jedinica proizašla iz potrebe da se korisnicima na organiziran način pomogne u njihovim individualnim potrebama u vezi s obradama podataka.
- Najznačajniji zadaci informacijskog centra:
 - Izobrazba za informacijsku pismenost,
 - pomoć pri korištenju osobnih računala,

- izobrazba za korištenje pojedinih programa ili aplikacija te konzultiranje pri njihovom korištenju,
- održavanje služba pomoći korisnicima,
- ocjenjivanje, instaliranje i provjera novih programa ili aplikacija odnosno drugih proizvoda informacijske tehnologije,
- praćenje i poticanje upotrebe normi informacijske tehnologije,
- osiguranje sigurnosti sustava i podataka,
- izrada programa za povezivanje aplikacija,
- administriranje podacima,
- vođenje projekata uvođenja korisničkih aplikacija,
- osiguranje kvalitete korisničkih aplikacija,
- marketing programa ili aplikacija itd.

UNAJMLJIVANJE INFORMACIJSKIH USLUGA:

- Unajmljivanje informacijskih poslova izvan poduzeća počelo je početkom šezdesetih godina.
- Unajmljivanje ima pozitivne ali i negativne posljedice.
- Posljednjih godina mnoga poduzeća gledaju kako će informacijski servis iznajmiti izvana.
- Funkcije koje se mogu pribaviti izvan vlastitog poduzeća mogu biti vrlo jednostavne, npr. poslovi masovnog unosa podataka, ali i vrlo zahtjevne, kao što je razvoj i izgradnja kompletnog informacijskog sustava.
- Ima više razloga zašto je u posljednje vrijeme unajmljivanje informacijskih usluga u porastu:
 - osnovni razlog je u tome što se poduzeće želi u potpunosti posvetiti svom osnovnom poslu i u njemu biti vrhunsko
 - ponekad je razlog i nedostatak informacijskih stručnjaka

1.6.5. Netware

- Netware je mrežna komponenta IS-a, tj. komunikacijska infrastruktura bazirana na informacijskim tehnologijama. Jedan od primjera su računalne mreže.
- **Računalne mreže** su sustavi povezanih računala.
- U mrežnom okruženju računala razmjenjuju podatke, dijele vlastite izvore, omogućavaju komunikaciju, paralelni rad, kreiranje virtualne organizacije itd.
- Za ostvarenje računalne mreže potrebna je odgovarajuća softverska i hardverska podrška, a nazivamo je netware ili podrška za mrežu.
- Razlikuju se pojmovi:
 - arhitektura ili topologija mreže
 - organizacija mreže
 - mrežni protokoli
 - mrežna spojišta
 - LAN mreže
 - WAN mreže
 - prijenosni mediji koji su opisani kroz druge lekcije pa se ovdje neće detaljnije pojašnjavati

1.6.6. Dataware

- Dataware su svi sadržaji u informacijskom sustavu kojima se opisuju činjenice iz realnog svijeta i poslovnog sustava na koji se odnose a organizirani i oblikovani tako da budu razumljivi i da se mogu koristiti u poslovanju za donošenje odluka i ostvarivanje ciljeva i zadataka.
- Osnovno, dataware IS-a sadržan je u podacima, informacijama i znanju:
 - podatak je skup prepoznatljivih znakova zapisanih ne nekom mediju; podatak je simbolički prikaz jednog obilježja promatranog objekta.
 - informacije nastaju kad se niz uređenih i prepoznatljivih, ali značenjem nezanimljivih znakova kojima se predstavlja obilježje nekog objekta ili stvarnosti sredi i organizira u smislen oblik koji ima značenje a za primatelja je novost.
 - Za povezivanje činjenica iz stvarnog svijeta u podatke iz kojih nastaju informacije potrebno je znanje. **Znanje** je svijest i razumijevanje informacija i mogućnost njihova povezivanja u smislu podrške i obavljanja zadataka.

- U dataware IS-a ubrajaju se dizajn proizvoda, tehničke podaci, upute menadžmenta, operativne baze podataka, operativni procesi, tehničke baze podataka, znanje zaposlenih i računalni softver, poslovni ugovori, radne upute, poslovni rezultati i izvješća, baze podataka, sistemska dokumentacija, korisnički priručnici, operativne procedure, planovi, aplikacijski i sistemski softver, razvojni i pomoćni alati itd.

2. INFORMACIJSKI SUSTAVI

2.1. Životni ciklus IS-a

- Na životni ciklus IS-a možemo gledati slično kao i na životni vijek čovjeka – čovjek se rađa, razvija i na kraju umire. IS prolazi kroz slične faze.
- Životni ciklus IS-a započinje spoznajom o potrebi za izgradnjom IS-a unutar poslovnog sustava, a zatim slijedi razvojni ciklus IS-a.
- Životni ciklus nekog IS-a završava kad on biva zamijenjen drugim IS-om (novijim, boljim), tj. prestankom njegovog korištenja.
- Dakle, životni ciklus IS-a je vremenski period trenutka spoznaje za potrebom izgradnje novog IS-a, pa sve do trenutka kad se dotični IS prestaje koristiti ili zamjenjuje novim IS-om.
- **Životni ciklus IS-a ne treba miješati sa razvojnim ciklusom IS-a!**
 - Životni ciklus obuhvaća razvojni ciklus (razvojni ciklus je podskup (interval) životnog ciklusa). Razvojni ciklus se odnosi na faze projektiranja, razvoja, oblikovanja i uvođenja u rad IS-a

2.2. Metode izgradnje IS-a

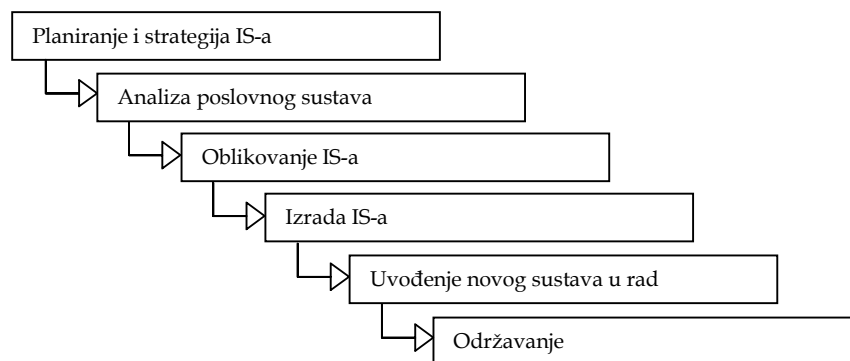
- Pri samom početku razvojnog ciklusa novog IS potrebno je definirati očekivanja i ciljeve. Potrebno je predvidjeti i budućnost te izraditi projekciju razvoja IS-a, razvoj poduzeća u okviru IS-a i bez njega. Odabir oblika razvoja dio je poslovne strategije i odnosi se na duži period. Oblik razvoja odabire se nakon prepoznavanja potreba ili problema u organizaciji, analize problema ili zahtjeva, spoznaje o mogućnostima, projekcije i planova o budućem poslovanju. Važnost oblika razvoja IS-a proističe iz toga što će odluka o obliku razvoja imati dugoročne posljedice na buduću uspjeh i organizaciju poslovanja. O njoj će možda ovisiti i preustroj poduzeća.
- Izgradnja informacijskog sustava je opsežan i vrlo složen proces, kojeg treba planirati, detaljno analizirati potrebe za izgradnju tog sustava, oblikovati, izraditi i uvesti u red sustav, a kasnije održavati tijek rada sustava.
- Metode izgradnje IS-a su:
 - **vodopadni ili linearni razvoj** - odvija se po fazama gdje se u svakoj fazi proizvedu određeni rezultati koji predstavljaju ulaz za sljedeću fazu (otuda poredba 'vodopadni'). To znači da se nakon svake faze mogu provjeriti rezultati prethodne te odlučiti o daljnjem nastavku projekta.
 - **evolucijski razvoj** - temelji se na modernim informacijskim sredstvima kojima se brže razvija sustav te se može korisnicima dati prije na provjeru a nakon toga se postepeno poboljšava i dograđuje dok se ne dobije zadovoljavajući IS.
 - **spiralni razvoj** - je oblik evolucijskog razvoja kod kojeg se cijeli razvojni ciklus odvija u nizu koraka koji se ponavljaju kao u spirali do konačnog rješenja (otuda i naziv). Svaki korak sastoji se od četiri aktivnosti koje se ponavljaju sa napredovanjem projekta, a svaki put se približava cilju.

Pristup razvoju	Osobine	Prednosti	Nedostaci
Linearni model	Sekvencijalni formalni proces Pisane specifikacije i odobrenja Limitirana uloga korisnika	Neophodno za velike sustave i projekte	Sporo i skupo Ne ohrabruje promjene Masivan posao papirologije
Prototipiranje	Zahtjevi se dinamički razvijaju s experimentiranjem na sustavu Proces je neformalan, brz i iterativan Korisnici su u neprekidnoj interakciji s prototipom	Brz i jeftin Dobar kod nejasnih zahtjeva i koda je važno sučelje s end-userima Promivira sudjelovanje korisnika	Neprijemeren za velike i složene sustave Može uzrokovati manjkavostima u analizi, dokumentaciji i testiranju
Razvoj softvera u paketima	Komercijalni softver eleinira potrebe za internim razvojem	Troškovi održavanja, programiranja, instalacije su reducirani Smanjena je potreba za internim resursima	Možda neće zadovoljiti jedinstvene potrebe poduzeća i sve funkcije korektno Prilagodba podiže razvojne troškove

End-User razvoj	Sustav kreiran od krajnjih korisnika korištenjem alata posljednje generacije Brz i neformalan Minimalna uloga IS stručnjaka i troškova	Korisnici kontroliraju izgradnju sustava skraćuje s vrijeme razvoja i troškovi	Može dovesti do nekontroliranog razvoja Sustav ne zadovoljava uvijek zahtjeve i standarde
Outsourcing	Sustav je izgrađen i većinom održavan od vanjskog partnera	Može smanjiti ili kontrolirati troškove. Osigurava uspjeh koji zbog unutarnjih ograničenja nije zajamčen	Ovisnost o smjernicama dobavljača sustav i njegovom razvoju

2.2.1. Vodopadna metoda

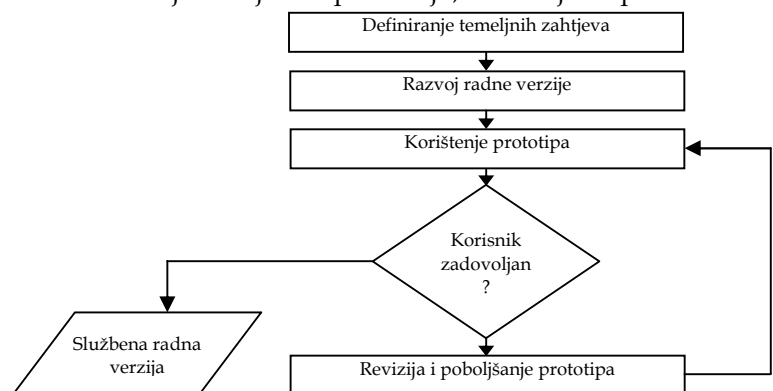
- Linearni pristup razvoju IS-a je oblik koji se ponajviše koristi pri razvoju velikih i složenih projekta. Svaka faza razvoja zahtijeva pažljivu analizu i pripremu, a prelazak na sljedeću fazu započinje kad prethodna završi. Najizraženiji nedostatak linearnog pristupa je u njegovoj nefleksibilnosti u promjenama sustava, duljini trajanja projekta i velikim troškovima.
- Općenito je to vrlo formalni pristup razvoju koji nije primjeren manjim organizacijama. Karakterizira ga izrazito slaba interakcija projektanta sustava s korisnicima te zahtjevi za uključivanjem značajnih ljudskih i materijalnih resursa. U prednosti linearnog pristupa se ubrajaju dobra analiza i definicija zahtjeva, dobra dokumentiranost i kvalitetne komponente gotovog sustava.



SLIKA 2.1: VODOPADNA METODA

2.2.2. Metoda prototipiranja

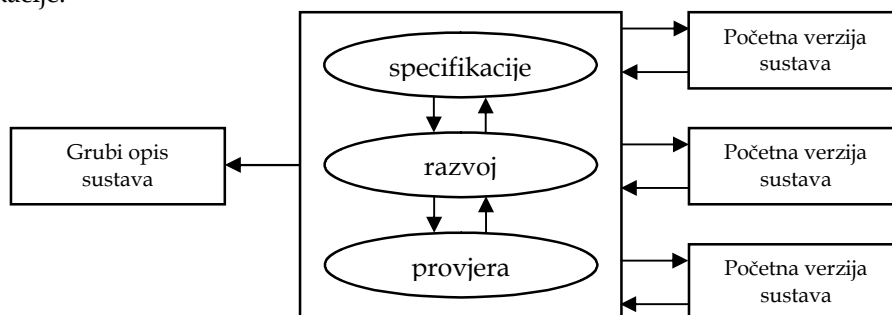
- Prototipiranje je pristup razvoju IS-a koji se temelji na razvijanju početne, radne verzije programa koja se zatim postepeno provjerava i dograđuje idejama i potrebama korisnika. Tim se pristupom IS relativno brzo razvija, a radi manjih zahtjeva u u fazi analize i dokumentiranja ne iziskuje velike troškove.
- Prednost pristupa je u dobroj interakciji korisnika s projektantima čime je osigurano obostrano zadovoljstvo. Radne se verzije nastale na temelju zahtjeva isprobavaju, rafiniraju i ponovo razrađuju. Proces se izvodi iteracijama do konačne verzije. Nedostaci prototipiranja su u tome što ne ispunjava zahtjeve za ažurnom dokumentacijom koja je nužna kod velikih projekta. Radi toga je teže održavanje, a ima i slučajeva kad prototip nikada ne bude konačno završen. Iako su početna ulaganja u ovaj oblik razvoja mala, s vremenom mogu i narasti.



SLIKA 2.2: METODA PROTOTIPIRANJA

2.2.3. Evolucijska metoda

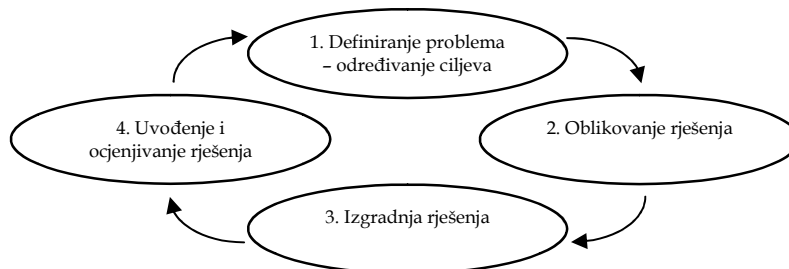
- Evolucijski pristup se temelji na modernim informacijskim sredstvima kojima se:
 - brže razvija početna verzija sustava,
 - IS se korisnicima može odmah dati na provjeru i korištenje,
 - IS se postepeno poboljšava i dograđuje dok se ne dobije zadovoljavajući IS
- U početku se dijelovi sustava razvijaju bez odgovarajućih preciznih specifikacija, pa se obično na taj način izrađuju manji dijelovi pojedinih informacijskih sustava – npr. pojedinačne aplikacije.



SLIKA 2.3: EVOLUCIJSKA METODA

2.2.4. Spiralna metoda

- Spiralni razvoj odvija se tako da se postupci vezuju u spiralu sve do konačnog rješenja. Spirala se sastoji od četiri aktivnosti:
 - definiranje problema i postavljanje cilja, utvrđivanje alternative, ocjena rizika
 - oblikovanje rješenja
 - izgradnja rješenja
 - uvođenje i ocjenjivanje rješenja.



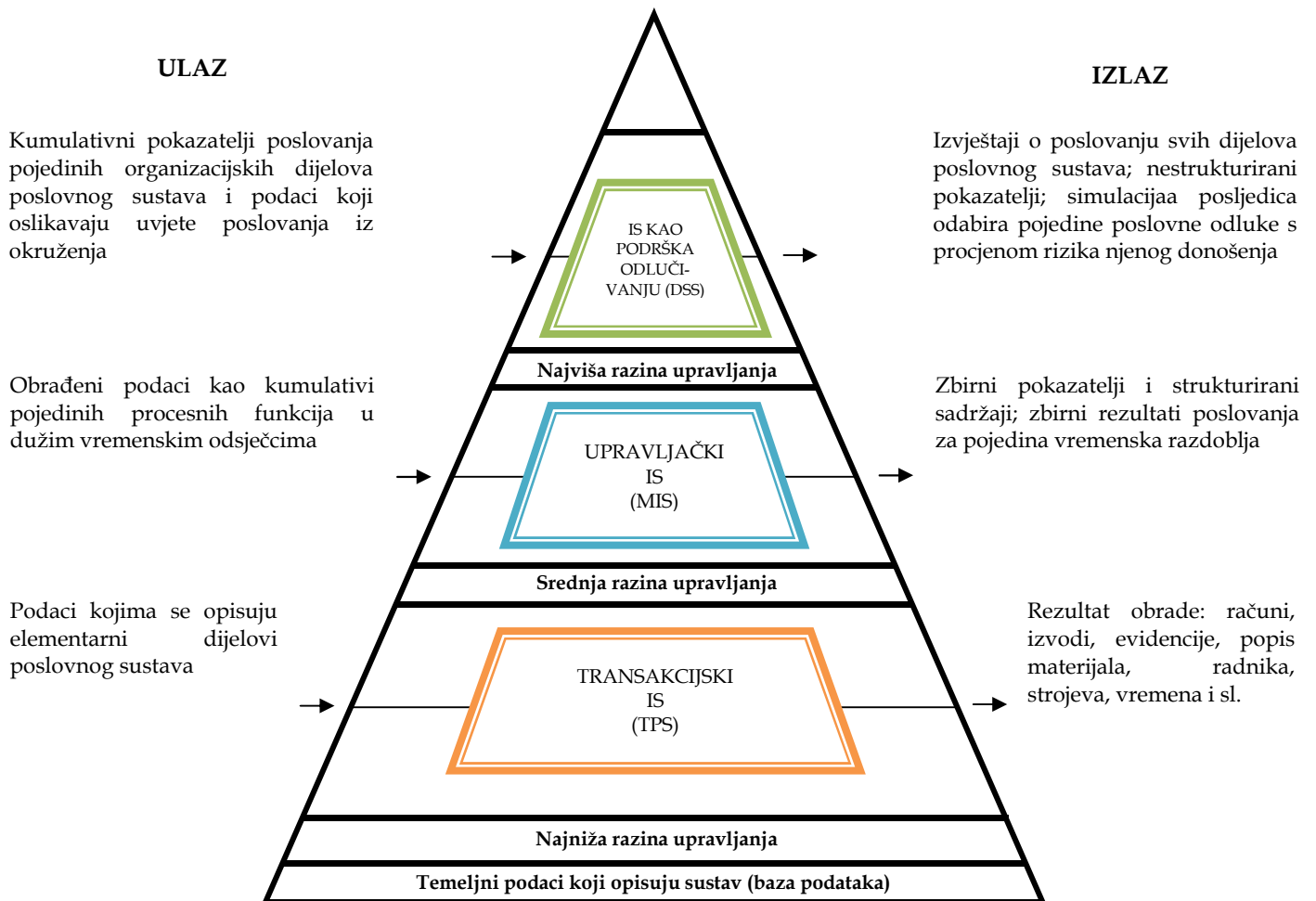
SLIKA 2.4: SPIRALNA METODA

- Nastao je na temelju evolucijskog modela i jedan je od novijih pristupa, a temelji se na izradi početne verzije nekog sustava i kasnijem usavršavanju te početne verzije gdje nastaje određeni broj inačica sustava.
- Usavršavanje se nastavlja sve dok se ne razvije verzija koja u potpunosti zadovoljava potrebe i zahtjeve korisnika. Dijelovi sustava u početku se razvijaju bez preciznih specifikacija pa se tako mogu izgraditi manji podsustavi odnosno pojedine aplikacije (npr. evidencija radne snage, izdavanje računa...). Iz grubog opisa sustava istovremeno se obavljaju specifikacije, razvoj i provjera sustava što rezultira početnom verzijom.
- Spiralni razvoj se najčešće koristi kod izgradnje **sustava za potporu u odlučivanju**, zbog toga što nije moguće unaprijed predvidjeti koje će sve informacije biti potrebne pri odlučivanju. Korisnik pronalazi i istražuje svoje zahtjeve u interakciji s podacima koje koristi, pa ih unaprijed nije moguće potanko precizirati.

2.3. Dijelovi IS-a

- **TIS** - sustav za obradu transakcija
- **MIS** - upravljački izvještajni sustav
- **DSS** - sustav za podršku odlučivanju
- **OIS** - sustav uredskog poslovanja

- Dijelovi informacijskog sustava mogu biti:
 - **Klasični (transakcijski)** informacijski sustav (TPS) koji evidentira promjenu u objektivnoj stvarnosti i posprema taj podatkovni sadržaj. Na osnovu tog praćenja možemo dobiti trendove, tj. možemo dobiti **Upravljački** informacijski sustav (MIS) i (razina više), Sustav za **potporu odlučivanju** (DSS). Kao najviši nivo dolazi na kraju **Ekspertni** sustav.



SLIKA 2.5: DIJELOVI INFORMACIJSKOG SUSTAVA

- Odnos upravljanja, korisnika, vrsta informacija i dijela informacijskog sustava:

Upravljanje	Korisnici	Vrsta informacija	Dio informacijskog sustava
operativno upravljanje	Menadžeri na Operativnoj razini	analitičke, dnevne	sustav za obradu transakcija
taktičko upravljanje	Menadžeri na taktičkoj Razini	Dijelomično sintetizirane, Periodičke	upravljački izvještajni sustav
strateško upravljanje	Menadžeri na Strateškoj razini	jako sintetizirane (agregirane), ad hoc	sustav za potporu odlučivanju

2.3.1. Sustav za obradu transakcija

- Sustav za obradu transakcija ili transakcijski sustav pruža potporu tekućem odvijanju poslovnog procesa. On dakle pripada operativnoj razini poslovnih aktivnosti. Sustav za obradu transakcija npr. prodajnog poduzeća prihvaća svaku kupovinu kupca kao jednu transakciju, koju na prikladan način obrađuje.

- Sustav za obradu transakcija jednog poduzeća može biti povezan sa sustavima za obradu transakcija drugih poduzeća.
- Sustavi za obradu transakcija imaju 3 opće funkcije:
 - vođenje evidencije
 - izdvajanje
 - izvještavanje.

2.3.2. Upravljački izvještajni sustav

- MIS (Management Information System) je računarski sustav za opskrbljivanje informacijama pri donošenju odluka, tj. Upravljački informacijski sustav.
- To je integrirani, korisničko-strojni sustav za osiguravanje informacija u podržavanju operacija, upravljanja, analize i funkcija donošenja odluka u organizaciji.
- Sustav upravlja informacijama, poslužuje računarski hardver i softver, razne procedure, modele za analize, planiranje, kontrolu i donošenje odluka, i baze podataka.
- Karakteristike MIS-a:
 - osiguravanje informacijama
 - MIS osigurava informacije koje pomažu menadžerima na različitim razinama u organizaciji
 - MIS je sastavljen od većeg broja komponenti, uključujući hardver, softver, ručne procedure i baze podataka
 - MIS je sustav korisnika i strojeva; korisnici su važni za sustav MIS kao i sami strojevi.

2.3.3. Sustav za podršku odlučivanju

- Sustav za potporu odlučivanju (engl. Decision Support System – DSS) obrađuje postojeće informacije dobivene iz različitih unutarnjih i vanjskih izvora, da bi stvorio informacije potrebne za odlučivanje.
- DSS pomaže menadžerima u rješavanju nestrukturiranih ili slabostrukturiranih problema, za razliku od programiranog sustava za odlučivanje (engl. Programmed Decision System) koji može zamijeniti čovjeka u rutinskom odnosu pri strukturiranom odlučivanju.
- Strukturnom se odlukom naziva takva odluka, koju je, za poznate ulaze, lako donijeti koristeći se određenim pravilima. Takve je odluke lako programirati. Taj sustav mora podržavati **nestrukturirano ili slabo strukturirano odlučivanje**, mora biti dovoljno fleksibilan da može prihvatiti i odgovoriti na promjenu postupka odlučivanja te mora biti jednostavan za korištenje.
- Pod vrstama DSS navodi se podjela za koju se može reći da rangira sustave prema vrsti odluka koje se donose, odnosno može se primjetiti podjela na hijerarhijske razine. Tu podjelu iznosi Čerić [Čerić 1998] te razlikuje:
 - **korporativni sustavi za planiranje** - namijenjeni su visokom menadžmentu i sadrže informacije relevantne za planiranje na razini cijele tvrtke
 - **funkcijski sustavi za potporu odlučivanju** - služe srednjem menadžmentu za donošenje odluka s kraćim vremenskim horizontom koje se odnose na neku od funkcija
 - **informacijski sustavi za izvršne menadžere** - koriste se za široki spektar kratkoročnih odluka visokog menadžmenta
 - **lokalni sustavi za potporu odlučivanju** - koristi ga niži menadžment za ad hoc informacije o nekom ograničenom aspektu funkcija poduzeća.
- Po Laudonu K. DSS sustavi se klasificiraju kao :
 - **orijentirani na model** - obično su razvijeni od krajnjih korisnika neovisno o informacijskom sustavu poduzeća. Jako se oslanjaju na postojeće metode analize i koriste se kod relativno dobro strukturiranih informacija
 - **orijentirani na podatke** - namijenjeni su organiziranju i analizi velikih količina podataka i obično su dio zajedničkog informacijskog sustava. Takvi sustavi prikupljaju podatke iz različitih izvora i vrše analize složenijih odluka.
 - **sustavi za rudarenje podacima** - namijenjeni su odlučivanju koje se ne temelji na jasnim i pristupačnim podacima. Koriste se za nestrukturirana i prognostička

odlučivanja, a podršku temelje na korištenju modela neuronskih mreža, fuzzy logike, genetičkih algoritama i umjetne inteligencije.

EKSPERTNI SUSTAVI:

- Ekspertni sustavi su računalni programi iz područja umjetne inteligencije temeljeni na znanju iz nekog specijalističkog područja. Ti sustavi rasuđuju na temelju prikaza ljudskog znanja u simboličkom obliku. mogu naći približno rješenje problema čak i kad su podaci o problemu nepotpuni te mogu objasniti način na koji su došli do rješenja. Za razliku od tradicionalnih računalnih programa ekspertni sustavi rasuđuju korištenjem prikaza ljudskog znanja u simboličkom obliku, mogu naći približno rješenje problema, čak i kada podaci o problemu nisu potpuni te mogu objasniti način na koji su došli do predloženog rješenja.
- Oni rade na sličan način kao i eksperti te koriste njihovo znanje i rasuđivanje kod rješavanja problema.
- Njihovo funkcioniranje počiva na sljedećim elementima: **bazi znanja, bazi činjenica, mehanizmu zaključivanja, korisničkom sučelju.**
- Ekspertni sustavi su iznimno korisna pomagala stručnjacima s raznih područja. Nastali spregom moderne tehnologije, znanja i rasuđivanja, pronalaze rješenja na razini eksperata za razne probleme.
- Struktura Ekspertnih sustava:
 - **baza znanja** - predstavlja izvor znanja, stabilne su tokom dužeg vremena, znanje je prikupljeno od eksperata
 - **baza činjenica** - sadrži činjenice o stanju specifičnog problema , mijenja se tokom vremena
 - **mehanizam zaključivanja** - predstavlja mehanizam za traženje rješenja problema, ispituje činjenice iz baze činjenica i znanje iz baze znanja
 - **korisničko sučelje** - omogućuje jednostavnu komunikaciju korisnika s ES ze posjeduje mehanizam za objašnjavanje rješenja.
- Ekspertiza o području interesa sastoji se od znanja o tom području te razumijevanja problema i sposobnosti njihova rješavanja. U rješavanju problema, ekspertni sustavi ponajviše se oslanjaju na znanje, a manje na metode rasuđivanja. Razlog tome je što značajan dio stvarnih problema nema rješenje u obliku algoritma, tj. preciznog i jednoznačnog postupka rješavanja problema te spoznaja da su eksperti efikasni u rješavanju problema zbog svog akumuliranog znanja

2.3.4. Sustav uredskog poslovanja

- Ured je mjesto u kojem menadžeri, stručni suradnici, tajnice ili uredsko osoblje obavljaju upravljačke ili administrativne poslove. Zato su funkcije ureda:
 - odlučivanje
 - manipulacija podacima
 - manipulacija dokumentima
 - komunikacija
 - arhiviranje.
- Temeljne mogućnosti informatizacije su:
 - obrada dokumenata
 - komunikacija
 - telekonferiranje
 - pomoćni sustavi.

2.4. Vrste IS-a

- **Financijski** informacijski sustav bavi se praćenjem izvora podataka (priljeva i odljeva novca), pretežno iz transakcijskog dijela informacijskog sustava. Nadalje se bavi financijskim planiranjem na temelju kojeg se izrađuje financijski plan poduzeća uzimajući u obzir sva zakonska pravila, strateški plan poduzeća i druge zadane uvjete.

- **Računovodstveni** informacijski sustav usko je povezan sa financijskim sustavom. Njegovi dijelovi su: glavna knjiga, obrada ulaznih i izlaznih računa, obrada narudžbi, nabavno i skladišno poslovanje te obrada plaća.
- **Marketinški** informacijski sustav obrađuje aspekte bitne za marketing kao poslovno područje odgovorno za utvrđivanje identiteta proizvoda i usluga koje poduzeće nudi. Da bi marketing dobio potrebne informacije, takav IS mu isporučuje obrađene informacije iz transakcijskog IS-a, istraživanja tržišta, sustava za potporu odlučivanju, raznih izvora o konkurenciji, vanjskih čimbenika i sl.
- **Proizvodni** informacijski sustav je vrlo važan dio svakog poslovnog sustava pošto proizvodnja predstavlja srž samog poduzeća. Danas se sve više uvodi upravljanje kvalitetom, te različite norme poput ISO 9000 i drugih certifikata. Informacijska se tehnologija upotrebljava u proizvodnji kroz upravljanje podržano računalom (CAD, Computer Aided Design), proizvodnju podržanu računalom (CAM, Computer Aided Manufacturing), te računalno integriranje proizvodnje (CIM, Computer Aided Manufacturing). Isto tako se koristi i JIT (Just In Time) koncept proizvodnje koji smanjuje zalihe i skladišta. Uvodi se i planiranje proizvodnje poznato pod nazivom MRP II (Manufacturing Resources Planning), te koncept fleksibilnih proizvodnih sustava (FMS, Flexible Manufacturing System).

2.5. Elektroničko poslovanje

- Nastalo je zbog umrežavanja organizacija i javne administracije, te razvoja Interneta što je zahtijevalo prelazak na radikalno drugačiji način poslovanja.
- Elektroničko poslovanje je opći koncept koji obuhvaća sve oblike poslovnih transakcija ili razmjene informacija koje se izvode korištenjem informacijske i komunikacijske tehnologije.
- Rane vrste elektroničkog poslovanja postavile su značajne temelje današnjem poslovanju poput:
 - elektroničkog prijenosa gotovine (EFT) - prvobitno razvijen za potrebe razmjene sredstava između banaka, a danas se koristi i pri plaćanju kreditnim karticama
 - elektroničke razmjene podataka (EDI) i elektroničke pošte – znatno su pridonijele smanjenju količine papira po uredima.
- Prednosti elektroničkog poslovanja:
 - smanjenje troškova poslovanja
 - unutrašnja i vanjska integracija tvrtki
 - grešaka kod elektroničkih transakcija
 - bolja potpora i usluga za vrijeme i nakon kupovanja (koje može biti i putem Interneta)
 - mogućnost digitalizacije i prijenosa različitih sadržaja (tekst, slika, zvuk, video).
- Nedostaci elektroničkog poslovanja:
 - sigurnost na Internetu
 - zaštita kreditnih kartica
 - propusnost mreže
 - ljudski faktor (usvajanje novih tehnologija itd.).
- Tehnološke pretpostavke za razvoj elektroničkog poslovanja:
 - informacijsko – komunikacijska infrastruktura zadovoljavajućeg kapaciteta
 - uređaji i alati za stvaranje, publiciranje i distribuciju multimedijских sadržaja
 - programe za stvaranje multimedijских dokumenata
 - mogućnost sigurnog prijenosa podataka kod izvođenja poslovnih transakcija i online plaćanja
 - standardizacija svih sudionika (materijalnih i ljudskih) elektroničkog plaćanja u svrhu postizanja potpune kompatibilnosti u takvom sustavu.
- Zakonske pretpostavke za razvoj elektroničkog poslovanja:
 - stvaranje sustava zaštite autorskih prava
 - sigurnost korisnika

- politika određivanja cijena pristupa mreži i informacijama.

2.5.1. Vrste elektroničkog poslovanja

- **Poslovanje unutar tvrtke**
 - primjenjuje se pri komunikaciji pojedinaca ili skupina u obliku videokonferencije ili elektroničke pošte
 - pri elektroničkoj objavi dokumenata kako bi tvrtka brzo i jeftino objavila dokumente od interesa za osoblje
 - ostvaruje se bolji protok informacija o vlastitim i konkurentskim proizvodima i uslugama unutar različitih dijelova tvrtke.
- **Poslovanje među tvrtkama**
 - elektronička izmjena podataka (EDI) je najčešće korištena u ovakvoj vrsti poslovanja i ona donosi niže nabavne cijene, smanjenje zaliha, skraćene proizvodne cikluse itd.
 - koriste se CAD i CAM tehnologije kako bi se omogućilo brže i lakše oblikovanje proizvoda i proizvodnog ciklusa što skraćuje sam proizvodni ciklus.
- **Poslovanje između tvrtke i potrošača**
 - takav oblik omogućuje oglašavanje i marketing proizvoda koristeći Internet i druge mrežne servise
 - oglašavanje preko Web-a je jeftino i ima globalni doseg, proizvodi koji se mogu pretvoriti u digitalni oblik se isporučuju putem Interneta ili pošte (CD mediji i sl.)
 - Web mjesto služi kao centar za pomoć (FAQ stranice)
 - sadržaj za učenje na daljinu.

2.5.2. Sigurnosni problemi elektroničkog poslovanja

- Jedna od najvećih prepreka bržem razvoju elektroničkog poslovanja je problem njegove sigurnosti, naročito u slučaju elektroničkog poslovanja putem Interneta.
- Postoje dva temeljna aspekta sigurnosti elektroničkog poslovanja:
 - **Autorizacija** – resursima smiju pristupati samo korisnici i programi koji za to imaju eksplicitna odobrenja
 - **Sigurnost podataka i transakcija** – podrazumijeva osiguravanje sljedećih aspekata poslovnih transakcija i podataka:
 - *Privatnost* – zaštita prenošenih podataka od neovlaštenog čitanja
 - *Autentifikacija (identifikacija)* – zaštita od krivog predstavljanja korisnika
 - *Integritet* – sadržaj poruke ostaje neizmijenjen tijekom prijenosa mrežnom infrastrukturom
 - *Povjerljivost* – sadržaj povjerljivih podataka mora ostati tajan, tj. ne smije biti neovlašteno objavljen
 - *Neporecivost* – pošiljatelj poruke ne može poreći (osporiti) da je baš on poslao poruku.
- Mehanizmi koji jamče sigurnost transakcija i podataka su:
 - **kriptiranje sadržaja i**
 - **digitalni potpisi i certifikati**

2.5.2.1. Kriptiranje sadržaja i kriptosustavi

- **Kriptiranje (šifriranje)** = postupak izmjene originalnog podatkovnog sadržaja u oblik koji može pročitati samo osoba koja ima ključ za dekriptiranje (dešifriranje). Ključ je obično dugačak binarni broj.
- Postoje dva temeljna kriptosustava:
 - **Kriptiranje s tajnim ključem (simetrično kriptiranje)** - jedan te isti tajni ključ (odatle pojam simetrično kriptiranje) koristi se i za kriptiranje i za dekriptiranje podatkovnog sadržaja.
 - **Kriptiranje s javnim ključem (asimetrično kriptiranje)** – jedan ključ se koristi za kriptiranje, a drugi za dekriptiranje poruke (odatle pojam asimetrično kriptiranje).

- Osobine asimetričnih ključeva
 - ključ za kriptiranje i ključ za dekriptiranje čine par i matematički su povezani
 - poruka koja je kriptirana jednim od njih može biti dekriptirana samo onim drugim ključem iz para
 - usprkos matematičkoj vezi među njima, na temelju jednog ključa iz para nije moguće izračunati drugog.
- Vrste asimetričnih ključeva
 - jedan od ključeva iz para zove se javni ključ i smije biti javno objavljen svima
 - drugi ključ iz para zove se tajni ključ i on ne smije biti poznat nikome drugome osim vlasniku para ključeva
- Infrastruktura javnog ključa (engl. Public Key Infrastructure - PKI)
 - Sigurnost podataka i informacija zaštićenih asimetričnim kriptiranjem ovisi o zaštiti samih ključeva. Zato je uspostavljena tzv. infrastruktura javnog ključa, koju čine mehanizmi, procedure i protokoli za:
 - zaštitu ključeva od modifikacija,
 - generiranje ključeva,
 - distribuciju ključeva,
 - pohranu ključeva i pristup do njih, te
 - korištenje, arhiviranje i uništavanje (opoziv) ključeva.

2.5.2.2. Digitalni potpis i digitalni certifikati

DIGITALNI POTPIS:

- Uloga digitalnog potpisa je dvojaka. Njime se dokazuje:
 - da je elektronički dokument zaista poslala osoba koja tvrdi da ga je poslala (provjera identiteta pošiljatelja)
 - da elektronički dokument nije bio promijenjen na putu od pošiljatelja do primatelja (provjera integriteta poruke).
- Temelji se na Infrastrukturi javnih ključeva (engl. Public Key Infrastructure – PKI) i asimetričnoj kriptografiji
- Svaki pojedinac koji želi digitalno potpisati elektronički dokument mora imati svoj par asimetričnih ključeva:
 - **tajni ključ** (poznat jedino svom vlasniku) i
 - **javni ključ** (može i mora biti objavljen svima).
- Princip digitalnog potpisivanja dokumenta:
 - Odgovarajući algoritam djeluje nad elektroničkim dokumentom kojeg treba digitalno potpisati. Rezultat rada tog algoritma je sažetak (engl. message digest) polaznog dokumenta. Obilježja tog sažetka su sljedeća:
 - bez obzira na duljinu polaznog dokumenta, duljina sažetka je uvijek jednaka
 - sažetak je jednosmjerno kriptiran – nikakvim matematičkim transformacijama nije moguće iz njega rekonstruirati originalni dokument (važno obilježje tzv. jednosmjernih hash funkcija koje se koriste u algoritmima za izračunavanje sažetka)
 - statistička vjerojatnost da se iz dva različita dokumenta može dobiti isti sažetak je zanemariva.
- Taj se sažetak kriptira tajnim ključem pošiljatelja i time dobivamo digitalni potpis polaznog dokumenta.
- Tako kriptirani sažetak (tj. digitalni potpis) pridodaje se izvornom elektroničkom dokumentu i zajedno se šalju do primatelja.
- Primatelj mora provjeriti ispravnost priloženog digitalnog potpisa.
- Primatelj mora na neki način (korištenjem nekih od servisa iz infrastrukture javnih ključeva) pribaviti javni ključ pošiljatelja koji korespondira s njegovim tajnim ključem (kojim je dokument digitalno potpisan).
- Odgovarajući softver će zatim izvršiti provjeru ispravnosti digitalnog potpisa na sljedeći način:

- korištenjem javnog ključa pošiljatelja dekriptirat će priloženi digitalni potpis, čime se dobiva originalni sažetak
 - primljenog originalnog dokumenta će istim algoritmom kao i kod pošiljatelja izračunati sažetak primljenog dokumenta
 - uspoređuju se dekriptirani i izračunati sažeci iz koraka 1. i 2.
- U slučaju bilo kakve razlike među njima (makar i u jednom jedinom bitu) potpis je neispravan. To može značiti da:
 - autor nije osoba koja se predstavlja autorom, i/ili
 - da je dokument bio na neki izmijenjen nakon digitalnog potpisivanja (greška u prijenosu, namjerna modifikacija, itd.)
 - autentičnost i cjelovitost sadržaja i/ili autora je upitna.
 - Ako razlike među njima nema, potpis je valjan, te se i dokument i autor smatraju autentičnima

DIGITALNI CERTIFIKATI:

- Digitalni certifikati služe za provjeru činjenice da određeni ključ pripada upravo onoj osobi koja bi ga trebala posjedovati, a ne nekoj drugoj osobi koja se lažno predstavlja.
- Postoji realan problem povjerenja u svima dostupne javne ključeve korištene za digitalno potpisivanje.
- Radi većeg povjerenja u digitalni potpis dokumenta, za točnost i istinitost para javni/tajni ključ jamči neovisna treća strana (tzv. certifikacijska organizacija – engl. Certification Authority - CA) izdavanjem digitalnog certifikata, kojim se digitalno potpisuje sam javni ključ. Za jamca (certifikacijsku organizaciju) jamči jedino njegova reputacija.
- Problem povjerenja u identitet web poslužitelja prilikom provođenja online transakcija:
 - Jedno od rješenja je digitalni certifikat, koji bi trebao biti izdan od strane javnog certifikacijskog tijela od povjerenja.
 - Izdaje se tzv. **poslužiteljski certifikat**, koji jamči da poslužiteljev par javnog/tajnog ključa zaista pripada tom poslužitelju.
- Problem povjerenja u identitet pojedinca koji sudjeluje u online transakciji općenito (dakle, ne samo kod digitalnog potpisivanja):
 - Jedno od mogućih rješenja je opet digitalni certifikat izdan od strane javnog certifikacijskog tijela od povjerenja.
 - U ovom slučaju izdaje se tzv. **osobni certifikat**.

2.5.3. Elektronička razmjena podataka

- Elektroničku razmjenu podataka nazivamo EDI (Electronic Data Interchange), a obuhvaća razmjenu dokumenata unutar i između organizacija u standardiziranom elektroničkom obliku i to direktno između računarskih aplikacija.
- Dva najčešće korištena standarda su X12 i EDI-FACT
- Jedino ograničenje prilikom uvođenja elektroničke razmjene podataka je cijena te usluge koja je još uvijek visoka jer zahtijeva ne samo široki komunikacijski kanal, već i sigurnosne standarde, te informatičku i programsku opremu
- U posljednje vrijeme raste tendencija razmjene podataka putem Interneta (Internet EDI, otvoreni EDI) s ciljem smanjenja cijene usluge i povećanja broja tvrtki s kojima je moguće podatke razmijeniti
- Isto tako je u porastu broj VPN, odnosno privatnih mreža kojima se kompanije koje su geografski dislocirane povezuju koristeći strukturu Interneta.

2.5.4. Elektronički marketing

- Razvojem Web-a tvrtkama je omogućeno vrlo jeftino reklamiranje, promidžba i marketing putem vlastitih Web mjesta. To je vrlo privlačno za sve posjetitelje koji sadržaju mogu pristupiti bez izlaženja iz kuće, čekanja u redu itd.

- Elektronički marketing je pogodan za:
 - oni vrlo često koriste računala, Internet, pa elektronički marketing pogoduje nuđenju proizvoda i usluga preko Web-a
 - proizvode i usluge – marketing pogoduje ponudama intelektualnog vlasništva, računalne opreme i ostalih visokih tehnologija
 - cijene – pogodni su proizvodi i usluge u srednjem rangu cijena, te oni čija se cijena brzo mijenja
 - promociju – Web mjesto tvrtke se može promovirati preko televizije, novina itd.
 - ostalo.
- Internet je vrlo pogodno mjesto za istraživanje tržišta i to za:
 - primarno istraživanje – pretraživanje Web-a i diskusijskih skupina, objava upitnika na vlastitim Web stranicama
 - sekundarno istraživanje – pronalazak rezultata istraživanja koja su provela neke druge organizacije.
- Neki od popularnih modela Web marketinga su:
 - **elektronički oglasnik** – pruža informacije o proizvodima i uslugama koje tvrtka nudi uz interaktivnost
 - **elektronička brošura** – prošireni oblik elektroničkog oglasnika s detaljnijim informacijama o proizvodima i uslugama
 - **elektronički katalog** – omogućuje povezivanje informacija o proizvodima i uslugama s naručivanjem
 - **izvrnuti elektronički katalog** – oblik elektroničkog kataloga u kojem se informacije i proizvodi ne nude izravno.
- Prilikom izrade Web-a potrebno je voditi računa i o marketinškim aspektima Web mjesta:
 - analiza interesa potencijalnih posjetitelja
 - bogatstvo Web mjesta u smislu informacija i odgovora na često postavljena pitanja
 - privlačenje posjetitelja da ponovno posjete Web stranice
 - omogućavanje komunikacije s tvrtkom, itd.

2.5.5. Elektronička tržišta

- Ne postoji jedinstvena definicija.
- Jedni autori smatraju da je elektroničko tržište takav elektronički sustav koji podržava makar jednu od funkcija klasičnog tržišta. Drugi pak autori smatraju da je za stvaranje elektroničkog tržišta potrebno i susretanje kupaca i prodavača, te pregovaranje o uvjetima kupnje.

POSLOVNI MODELI ELEKTRONIČKIH TRŽIŠTA

- U širem smislu, odnosno oni koji ostvaruju samo neke funkcije tržišta:
 - **elektronička prodavaonica** (engl. e-shop) – isprva je to bilo Web mjesto za oglašavanje proizvoda i usluga tvrtke, a danas već omogućuje naručivanje i plaćanje proizvoda
 - **elektronički nabavni centar** (engl. e-procurement) – odnosi se na velike tvrtke, a omogućuje nuđenje i kupovanje većih dobara i usluga čime se postiže veći izbor nabavljača, niže nabavne cijene i viša kvaliteta
 - **elektronički prodajni centar** (engl. e-mall) – kolekcija elektroničkih prodavaonica koja omogućuje standardizaciju nekih transakcija poput plaćanja.
- U užem smislu, odnosno oni koji ostvaruju veći broj funkcija tržišta:
 - **elektronički sajam** (engl. e-bazaar) – omogućuje svojim članovima da komuniciraju i trguju
 - **elektronička dražba** (engl. e-auction) – zasniva se na elektroničkom obliku ponude koja može koristiti multimedijску prezentaciju dobara, a često se proširuje i na ugovaranje, plaćanje i isporuku dobara
 - **elektroničko posredništvo** (engl. e-brokerage) – posredništvo između potrošača (postavljaju svoje zahtjeve) i dobavljača (nude proizvode i usluge)

- Elektronička tržišta se još koriste i za digitalnu isporuku dobara i usluga čime se omogućuje zatvaranje prodajnog ciklusa na elektroničkom mediju
- Razvijaju se i modeli ponašanja kupaca kako bi se stvorio sustav potpore odlučivanju korisnicima

2.5.6. Elektronički sustav plaćanja

- Kao i kod klasičnog trgovanja, u elektroničkom sustavu poslovanja postoji potreba za financijskom razmjenom između kupaca i prodavača. Ta se razmjena ne provodi u klasičnom obliku, već se koriste instrumenti digitalnog plaćanja:
 - **elektronička gotovina**
 - **elektronički čekovi**, te
 - **online transakcije s kreditnim karticama.**
- Problem je što ne postoje univerzalne metode plaćanja koje su prihvaćene i od trgovaca i od banaka
 - tvrtke razvijaju vlastita rješenja
 - (ne)kompatibilnost različitih rješenja
 - (ne)kvaliteta različitih rješenja (naročito sa stanovišta sigurnosti).
- Elektroničko plaćanje u stvarnom vremenu
 - Ovakav oblik plaćanja putem Interneta zahtijeva sljedeće korake:
 - Kupac putem web preglednika šalje zahtjev za plaćanjem
 - Trgovac prosljeđuje zahtjev instituciji koja pruža servis elektroničkog plaćanja
 - Institucija provjerava autentičnost kupca i prebacuje zadani iznos novca s računa kupca na račun prodavača.
- U odnosu na klasični sustav plaćanja uočljive su 2 razlike:
 - Kupac i prodavač se ne susreću fizički
 - Brzina izvođenja procesa plaćanja ne ostavlja mnogo vremena za otkrivanje krađa i prijevara

2.5.6.1. Mikro plaćanje

- Odnosi se na mogućnost plaćanja malih novčanih iznosa (manjih od osnovne monetarne jedinice – npr. iznos od nekoliko centi, lipa i sl.)
- Brojne informacije koje se prodaju putem Interneta nude se u tzv. modularnom obliku (npr. samo pojedino poglavlje knjige ili pojedine stranice, i sl.)
- Obrada takve transakcije kroz tradicionalne metode plaćanja je neisplativo, jer trošak njene obrade veći od samog iznosa transakcije.
- Mikro plaćanje poduprto je tzv. elektroničkim žetonima koje priznaju brojne banke i financijske ustanove. Postoje dva oblika elektroničkih žetona:
 - **Žetoni u stvarnom vremenu** - kupac unaprijed plaća novčanu protuvrijednost robe – elektroničkom gotovinom, debitnim karticama i sl.
 - **Žetoni koji se naknadno naplaćuju** - vrijednost robe se ne naplaćuje odmah – upotrebom elektroničkih čekova, kreditne kartice i sl.

2.5.6.2. Elektronička gotovina

- Svojstva:
 - ima monetarnu vrijednost (pokriće u stvarnom novcu u banci)
 - razmjenjiva je za gotovinu i druge oblike financijskih dobara
 - mora biti pohranjiva u banke i pretraživa
 - mora biti sigurna (zaštićena od kopiranja, falsificiranja, dvostrukog obračunavanja i sl.)
 - temelji se na kriptografiji javnog ključa i digitalnom potpisu.
- Princip dobavljanja elektroničke gotovine:
 - Korisnik kupuje el. gotovinu od banaka ili sličnih ustanova (otvara račun u instituciji i osigurava financijsko pokriće za kupovinu el. gotovine)

- Banka dostavlja klijentu softver kojim korisnik traži kupovinu el. Gotovine
- generira se zahtjev, zahtjev se kriptira i šalje se banci putem mreže
- Banka svojim privatnim ključem potpisuje zahtjev i vraća ga korisniku, skidajući pri tome odgovarajući iznos novca s njegovog računa
- korisnik time dobiva elektroničku novčanicu odgovarajuće vrijednosti i serijskog broja, digitalno potpisanu od strane banke
- Korisnik javnim ključem banke provjerava ispravnost novčanice.

2.5.6.3. Elektronički čekovi

- Napravljeni su po uzoru na klasične čekove, uz sljedeće razlike:
 - u elektroničkom su obliku
 - u svrhu potpisivanja čeka i za odobravanje čeka koriste digitalni potpisi
 - zahtijeva se korištenje digitalnih certifikata u svrhu dokazivanja autentičnosti
 - kupca,
 - njegove banke, te
 - bankovnog računa.
- Primjeri implementacije:
 - NetCheck
 - Secure Pay...

2.5.6.4. Online transakcije s kreditnim karticama

- Dva su osnovna oblika:
 - **Plaćanje s kriptiranim podacima o kreditnoj kartici**
 - kupac sigurnim kanalom dostavlja trgovcu svoj potpis i broj kartice
 - trgovac prosljeđuje podatke o opterećenju kartice i dig. potpis instituciji koja se bavi online kartičarstvom
 - ova institucija šalje te informacije banci kupca na autorizaciju
 - banka vraća trgovcu podatke o kreditnoj kartici i njenom opterećenju.
 - **Plaćanje uz pomoć treće strane**
 - servisi koji osiguravaju da se broj kreditne kartice nikada ne šalje Internetom – riješen je jedan od glavnih sigurnosnih problema kod ovakvih transakcija.

2.6. Poslovno odlučivanje

- Donošenje odluka predstavlja važan aspekt poslovanja koji se odvija svakodnevno na svim razinama odlučivanja i područjima poslovanja, te u svim vrstama poslovnih organizacija
- Kvaliteta odluka se temelji na adekvatnosti informacija, kvaliteti i broju opcija između kojih se može birati
- Odluke se mogu donositi na tri razine – **strateškoj, taktičkoj i operativnoj**
- S obzirom na stupanj strukturiranosti, razlikujemo sljedeće odluke:
 - **visoko strukturirane** – one koje su se već često donosile i s njima menadžeri već imaju iskustva. Nazivamo ih i programiranim odlukama
 - **polustrukturirane** – znanje o nekim aspektima odlučivanja je dobro poznato, a o nekima nije, pa je potrebno sakupiti odgovarajuće znanje da sa može kvalitetno odlučiti
 - **nestrukturirane** odluke – donose se u izvanrednim situacijama i to u pravilu samo jednom.

2.6.1. Linearna optimizacija

- Brojni poslovni problemi mogu se opisati formalno, korištenjem matematičke notacije.
- Rješenja takvih problema najčešće nisu trivijalna, jer uključuju velik broj ograničenja o kojima treba voditi računa, a često u problemu postoji i veći broj nepoznanica (nepoznatih varijabli).
- U kontekstu poslovnog odlučivanja, brojne odluke se donose baš u takvim situacijama, kada su problemi formalne prirode i kad ih je moguće matematički riješiti.
- Razvijeni su brojni postupci i metode koje rješavaju formalizirane probleme. Očita je potreba za uključivanjem potpore za rješavanje takvih problema u informacijske sustave poslovnih sustava.

- Linearna optimizacija je skup matematičkih metoda koje omogućavaju pronalaženje najpovoljnijih rješenja različitih praktičnih problema, koji se matematički mogu opisati pomoću linearnih jednadžbi (funkcija).
- Tipični problemi koji se rješavaju metodama linearne optimizacije su:
 - pronalaženje optimalne dobiti ili minimalnog utroška resursa u procesu proizvodnje
 - transportni problemi – traženje takve strukture (ruta) transporta robe da troškovi dostave budu minimalni, a potrebna potražnja za robom zadovoljena
 - problemi dodjeljivanja (raspoređivanja) zadataka – kako n zadataka optimalno raspodijeliti na n radnih mjesta, tako da cjelokupni posao obavi uz minimalne troškove ili u što kraćem vremenu.
- Najčešće korištene metode iz domene linearne optimizacije su:
 - **linearno programiranje** - jednom linearnom jednadžbom opisuje se funkcija cilja. Funkciju cilja treba:
 - minimalizirati – u slučaju da se traži što manji utrošak resursa (tj. što manji troškovi) u postizanju cilja ILI
 - maksimalizirati – u slučaju da se traži što veća dobit
 - s jednom ili više linearnih jednadžbi zadaju se ograničenja, koja su specifična za konkretni problem koji treba riješiti
 - rezultat često nije jedinstven, već je moguć veći broj rješenja, koja uz zadana ograničenja minimaliziraju troškove ili maksimaliziraju dobit
 - **cjelobrojno linearno programiranje** – poseban slučaj linearnog programiranja, kod kojeg su dopuštena isključivo cjelobrojna rješenja
 - **višekriterijsko programiranje** – koristi se u situacijama kad postoji više ciljeva koje treba ispuniti (linearno programiranje se koristi kod problema sa samo jednim ciljem, tj. funkcijom cilja)
 - **ciljno programiranje** – kod problema gdje nije moguće/potrebno izračunati točna rješenja, već je dovoljno približiti se željenoj ciljnoj vrijednosti.

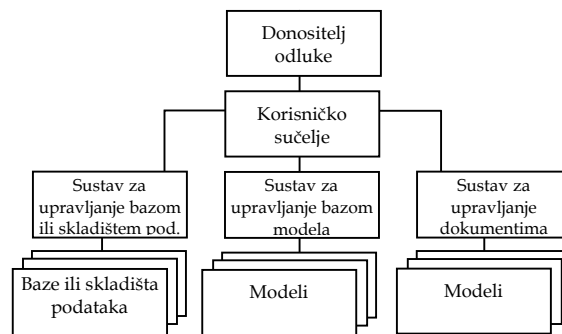
2.6.2. Simulacije

- Postoje brojni realni sustavi s velikim brojem elemenata koji su međusobno povezani različitim oblicima veza. Veze ne moraju nužno biti linearne prirode. Sustav ne mora biti statičan, već se različito ponaša kroz vrijeme. Moguće je da u sustavu postoje varijable slučajne prirode.
- Takve sustave nije moguće modelirati ni analizirati klasičnim matematičkim metodama.
- Razvijene su nove metode koje omogućavaju simulaciju ponašanja takvog sustava na temelju pretpostavljenog modela sustava.
- Brojne poslovne odluke svejedno treba donijeti i u takvim okolnostima, pa je često potrebno uključiti simulacijske algoritme u informacijske sustave poslovnih sustava.
- Dvije su generalne simulacijske metode:
 - **diskretna simulacija**
 - prvenstveno se koristi za simulacije sustava s redovima čekanja (npr. blagajne, šalteri, organizacija procesorskog vremena, i sl.)
 - modeli detaljno opisuju strukturu i elemente sustava
 - modeli oponašaju stvarne sustave – dakle, objekti u modelu predstavljaju objekte iz stvarnih sustava koji se modeliraju
 - tipične primjene:
 - simulacija proizvodnje, simulacija uslužnih djelatnosti, simulacija poslovnih procesa, simulacija transporta...
 - sistemska dinamika
 - prvenstveno se koristi za modeliranje sustava s povratnom vezom (spregom) i za analizu upravljanja radom kod takvih sustava
 - istražuje se dinamika razvoja različitih društvenih, tehničkih i bioloških sustavi
 - sistemska dinamika je metoda kontinuirane simulacije s povratnom spregom

- **kontinuirana simulacija**
 - pojedinačni događaji se združuju i prikazuju u (kvazi)kontinuiranom obliku
 - povratna sprega je zatvoreni krug uzroka i posljedica koji dovodi do toga da neki element sustava utječe sam na sebe
 - **pozitivna povratna sprega**
 - uzrok utječe sam na sebe tako da pojačava vlastite promjene
 - dobivamo stalan porast ili stalno smanjenje dotičnog uzroka
 - **negativna povratna sprega**
 - uzrok utječe sam na sebe tako da dovodi do promjene smjera vlastitog djelovanja
 - ako uzrok poraste iznad razine ravnotežnog stanja, negativna povratna sprega će ga smanjiti, i obrnuto
 - negativna povratna sprega je iznimno važan mehanizam u stabilizaciji ponašanja nekog sustava, tj. kod uravnoteženja njegovog rada
 - tipične primjene
 - simulacija zapošljavanja, simulacija rasta poduzeća, simulacija proizvodnje, simulacija zaliha...

2.6.3. Sustavi za potporu odlučivanju

- Sustav za potporu odlučivanju (DSS) je računalni sustav koji podupire proces odlučivanja tako što pomaže menadžerima u organizaciji informacija, identifikaciji i dohvatit informacija potrebnih za donošenje odluka, analizi i transformaciji tih informacija, izboru odgovarajućih modela potrebnih za rješavanje problema odlučivanja, izvođenju tih modela te analizi dobivenih rezultata za potrebe donositelja odluke.
- Takvi se sustavi najčešće koriste za potporu slabo strukturiranih problema odlučivanja
- Najkorisniji su u situacijama u kojima nije očito koje su informacije potrebne za odluku, koje bi modele trebalo koristiti, te koje bi kriterije trebalo upotrijebiti



SLIKA 2.6: GRAFA SUSTAVA ZA POTPORU ODLUČIVANJU

PODACI

- osnovni izvori podataka jesu:
 - **unutarnji podaci** – sadrže zapise o podacima i transakcijama koje se odvijaju unutar tvrtke
 - **vanjski podaci** – podaci o činiteljima izvan tvrtke (preferencije kupaca, regionalna potražnja itd.)
 - **javni podaci** – podaci koji se mogu dobiti iz javnih izvora
 - **privatni podaci** – sakupljaju se tijekom vremena i mogu biti korisni prilikom odlučivanja.
- ovdje je važno spomenuti i sustave za upravljanje bazom ili skladištem podataka koji omogućuju pristup strukturiranim podacima, te softverske agente koji samostalno izvode neke radne za koje ih je ovlastio njihov vlasnik
- rudarenje podataka obuhvaća različite metode ispitivanja podataka kako bi se ispitala povezanost među podacima, tražili trendovi u vremenu, predviđale buduće vrijednosti podataka i sl.

MODELI

- sustav za upravljanje bazom modela omogućuje jednostavno korištenje modela koji su potrebni za analizu opcija
- u sustav za potporu odlučivanju moguće je uključiti različite vrste modela kako po metodama na kojima se modeli temelje, tako i po vrstama problema koje rješavaju i razinama upravljanja na kojima se koriste
- prema razini na kojoj se modeli koriste mogu biti strategijski (za visoki menadžment), taktički (za srednji menadžment), te operacijski (za donošenje kratkoročnih odluka).

DOKUMENTI

- predstavljaju noviju komponentu sustava za potporu odlučivanju koja omogućuje da sustav koristi različite vrste nestrukturiranih podataka
- dokumenti se pretežno sastoje od teksta, grafičkih prikaza, poruka, ugovora itd.
- važan izvor dokumenata jesu elektroničke poruke
- sve važniji izvor predstavljaju i online baze podataka.

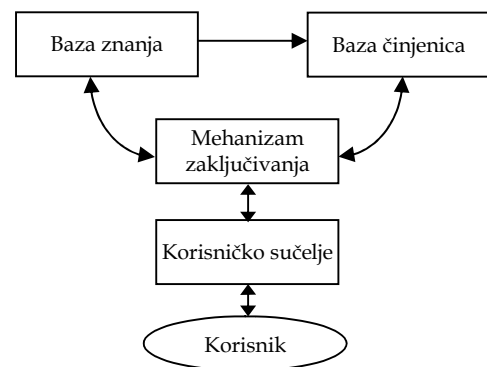
KORISNIČKO SUČELJE

- obuhvaća mehanizme potrebne za unos podataka u sustav, izvođenje modela, te izlaz podataka
- vrlo je važno oblikovanje tog sučelja koje mora biti kvalitetno izvedeno, te je u taj proces potrebno uključiti potencijalne korisnike tog sučelja, standardne poslovne termine, laganu navigaciju kroz sustav, te što je više moguće smanjiti vrijeme odaziva sustava.
- Sa stajališta organizacije razlikujemo četiri vrste sustava za potporu odlučivanju:
 - **korporativni sustavi za planiranje** – namijenjeni visokom menadžmentu i sadrže informacije relevantne za planiranje na razini cijele tvrtke
 - **funkcijski sustavi za potporu odlučivanju** – služe srednjem menadžmentu za donošenje odluka s kraćim vremenskim hodom
 - **informacijski sustav za izvršne menadžere** – koristi se za široki spektar kratkoročnih odluka visokog menadžmenta (posebno za tzv. ad hoc odluke)
 - **lokalne sustave za potporu odlučivanju** – koristi ih niži menadžment za ad hoc informacije o nekom ograničenom aspektu funkcija poduzeća.

2.6.4. Ekspertni sustavi

- Ekspertni sustavi su računalni programi temeljeni na znanju iz nekog specijalističkog područja.
- Takvi sustavi koriste znanje eksperata u simboličkom obliku, te su u mogućnosti objasniti način na koji su došli do rješenja problema.
- Imaju više poželjnih osobina poput povećane dostupnosti, smanjene cijene, povećane pouzdanosti, brzine reakcije i tumačenja rezultata.

- Sustav se sastoji od sljedećih dijelova:
 - **baze znanja** – izvor znanja o području, prikupljeno od eksperata
 - **baze činjenica** – sadrži činjenice o stanju specifičnog problema koji se upravo rješava
 - **mehanizma zaključivanja** – mehanizam za traženje rješenja problema
 - **korisničkog sučelja** – omogućuje komunikaciju korisnika i ekspertnog sustava.



SLIKA 2.7: STRUKTURA EKSPERTNOG SUSTAVA

- **znanje** je informacija o svijetu koja ekspertu omogućuje donošenje odluke
- **činjenice** su elementarne sastavnice znanja koje prikazuju objekte, njihove atribute i veze među objektima

- **pravila** su za čovjeka prirodan način prikazivanja znanja čiji redosljed nije potrebno odrediti unaprijed, a možemo ih prikazati na dva načina:
 - u obliku prema naprijed – zaključak slijedi pretpostavku na akcijski orijentiran način
 - u obliku prema natrag – traže se uvjeti u kojima pojedini zaključci postaju točni
- isto tako, pravila mogu biti i nesigurna što se prikazuje faktorom pouzdanosti (FP), te mogu biti specifična (odnose se na određene situacije i objekte) i opća (odnosi se na cijelu klasu situacija ili objekata).
- Proces zaključivanja:
 - mehanizam zaključivanja korištenjem činjenica i pravila izvodi niz akcija pomoću kojih pokušava dokazati neki unaprijed zadani cilj
 - dva osnovna tipa zaključivanja su:
 - **ULANČAVANJE PREMA NATRAG**
 - proces rasuđivanja izvodi se od zadanog cilja pretraživanja prema činjenicama
 - cilj je hipoteza koja se mora dokazati na način da se dokažu pretpostavke jednog ili više pravila koja u zaključku imaju zadani cilj
 - pretpostavke postaju podciljevi koji se dokazuju na isti način kao i zadani cilj
 - **ULANČAVANJE PREMA NAPRIJED**
 - polazi od dostupnih činjenica i ide prema cilju pretraživanja
 - pretražuju se pravila tako dugo dok se ne nađe pravilo čija se pretpostavka podudara s činjenicom
 - takvo se pravilo smatra dokazanim i njegov se zaključak dodaje bazi činjenica
 - postupak zaključivanja završava kada se stvori činjenica koja je identična cilju pretraživanja ili kada ES ne može stvoriti nove činjenice
 - algoritam ulančavanja prema naprijed ima sljedeće faze:
 - *podudaranje*
 - *razrješavanje konflikata*, koje sadrži sljedeće strategije:
 - izaberi samo prvo pravilo čije se pretpostavke podudaraju s činjenicama iz baze činjenica
 - izaberi najspecifičnije pravilo čije se pretpostavke podudaraju s činjenicama
 - izaberi pravilo čije se pretpostavke podudaraju s činjenicama koje su najsvježije dodane bazi činjenica
 - *izvođenje*.
- Izgradnja ekspertnih sustava
 - postoji nekoliko faktora o kojima ovisi izgradnja ekspertnih sustava poput nedostatka eksperata u danom području, nedostatka algoritma rješavanja nekog problema, nesigurnost znanja i ne postojanje procedura rješavanja problema itd.
 - osnovni problem prilikom izgradnje takvog sustava leži u prikupljanju znanja eksperata koje može biti izvedeno kao intervju, zatim preko učenja s interakcijom, učenja s edukacijom itd.
 - potrebno je napraviti i izbor područja za koje će se razvijati ekspertni sustavi, te graditi više manjih sustava pošto je to financijski isplativije.

3. NAČINI PRIKAZA REZULTATA OBRADE

3.1. Tehnike prikaza podataka

- Tehnike prikaza podataka bave se načinima bilježenja raznovrsnih podataka na računalnom mediju. Prema medijskoj vrsti podaci mogu biti: znakovni, zvučni i slikovni, a moguće su i njihove međusobne kombinacije.
- Pri tom je osnovni korištni pojam kodiranje. Kako računalo može neposredno razumijeti samo jezik binarnih brojeva, neophodno je sve podatke s kojima on radi prevesti u takav oblik. Isto tako, unutar računala različite komponente zahtijevaju određeni format i oblik zapisivanja u binarnom zapisu korištenjem određenih formata strojnih riječi.

3.1.1. Znakovni podaci

- Znakovnim podacima prikazani su podaci mnogih obilježja koje promatramo, kao što su ime, iznos računa, datum rođenja itd. Znakovni su podaci prikazani u obliku teksta ili brojaka. Neki od uobičajenih formata zapisa jesu ASCII, EBCDIC i RTF.
- Pri tome se koriste odgovarajući kodovi za svaku vrstu podataka. Pod te kodove uvrštavam nekoliko simboličkih kodova koji odgovaraju određenim potrebama i to su:
 - tetradni kodovi
 - BCD
 - Aiken
 - Excess-3
 - Gray
 - ASCII
 - EBCDI
- Važno je da sustav kodiranja mora zadovoljiti načelo **jednoznačnosti i ekonomičnosti**. Jednoznačan je onaj kod u kojem su sve riječi različite. Ekonomičan je onaj kod koji ima najmanju redundanciju.
- **ASCII** kod (engl. American Standard Code for Information Interchange) je kod propisan američkim standardom, a propisuje dodjeljivanje 8 bitnog binarnog broja brojevima, slovima i nekim specijalnim znakovima. Kod je sastavio 1968.g. Amerikanac Robert W. Bemer. 1977. kod je postao i službeni ANSI i ISO (ISO 646) standard. Sedam bitova binarnog broja ASCII koda namijenjeno je kodiranju, a osmi bit je bit pariteta koji služi za provjeru ispravnosti podatka. Predviđen je za kodiranje velikog broja znakova (ukupno 127). U širokoj je uporabi za razmjenu podataka kod računala i komunikacijske opreme.
- **UNICODE**: Unicode standard je pokušaj objedinjavanja potrebnih znakova praktički svih pisama unutar jednog koda. On svakom znaku pridružuje 16 bitni binarni broj, pa je na raspolaganju 65536 znakova! Još uvijek je u razvoju. Nedostatak-veličina (povećana memorija, duže vrijeme obrade podataka, nekompatibilnost s postojećim programima i opremom).
- **OSTALI KODOVI**: **Exces-3** kod (njegove tetrade su u odnosu na BCD pomaknute za tri mjesta); Aiken kod (simetričan je što olakšava računanje-komplementarnost); **Gray** kod...

3.1.2. Slikovni podaci

- Slikovni podaci sadrže:
 - nepokretne slike (fotografije)
 - pokretne slike (videosekvence)
- Slika je objekt koji se vizualno percipira i koji je, u mnogim primjenama, sadržajno bogatiji od teksta tj. riječi. Za slikovne podatke je važno da su količinski znatno obimniji od znakovnih jer slika u boji sadrži toliku količinu podataka, mjerenu u bitovima, koliko čitava knjiga samog teksta.
- Podaci slikovnih objekata bilježe se u različitim formatima zapisa. To su: GIF, JPEG, BMP, WMF i PCX.
- Pokretne slike odnosno video daju iluziju pokreta. Video se sastoji od serije statičkih slika koji se pred ljudskim okom smjenjuju najmanje 24 puta u sekundi te daju iluziju pokreta.

- Slika se u računalu prikazuje na dva načina:
 - **rasterski**
 - **vektorski**.
- Kod **rasterskog prikaza** svaka slika se prikazuje kao polje točaka (piksela). Boja i svjetlina svake takve točke je jednolična. Svjetlosne karakteristike svakog piksela prikazuju se u računalu u različitim oblicima: od 1,4,8,16 ili 24 bita, pa čak i više. Što je veća razlučivost (veći broj piksela) i veći oblik binarnog broja za prikaz, to je kvaliteta slike bolja. Što je veća kvaliteta i dimenzija slike veće je i zauzeće memorije.
- **Vektorski prikaz** slike stvara sliku uporabom odsječaka pravaca i zaobljenih linija te jednolično obojenih ploha, oneđenim tim linijama. Vektorski prikaz je pogodan za prikaz crteža. Princip postizanja vizualnog dojma može se kod rasterskog prikaza slike usporediti sa slikanjem, dok je vektorski prikaz usporediv sa crtanjem.

3.1.3. Zvukovni podaci

- Zvukovnim podacima opisuje se glazba, ljudski glas i ostali zvuci. Zvučni su podaci često komprimirani jer su količinski dosta obimni. Često su isprepleteni, tj. zajednički kodirani, s odgovarajućim videozapisom te istovremeno i komprimirani.
- Tako MPEG pohranjuje isprepletenu više zvučnih zapisa i video zapisa.
- Ostali formati zapisa zvučnih podataka jesu: WAV, MID, AIFF, IBK, RMI i VOC.
- Zvuk se u računalu pretvara u digitalni oblik. Da bi se prikazao stereo zvuk kvalitete koncertne glazbe (CD kvaliteta) u trajanju od 60 sekundi te prikazom uzorka na 16 bitova, zauzet će se 10,6 MB memorijskog prostora.

3.1.4. Kompresija podataka

- Kompresiranje podataka je smanjivanje veličine zapisa podataka radi smanjenja memorijskog prostora, pri pohranjivanju podataka (naročito onih koji se rjeđe koriste) odnosno skraćanjem vremena prenošenja komunikacijskim putovima
- Postoje dva načina (tehnike) na koje je moguće izvršiti kompresiju - **s gubicima ili bez njih**. Najčešće je to označeno na engleskom, kao *lossy* (s gubicima) ili *normal* (što znači bez gubitaka).
- Iako naizgled besmislena, kompresija s gubicima ima smisla, jer iako gubimo podatke, što znači da podaci nakon dekompresije nisu identični podacima prije kompresije, u vrijeme samog postupka kompresije pokušavamo odbaciti ili izgubiti one podatke koji nam najmanje znače. Ta metoda nije primjenjiva npr. na dokumente jer kod njih nema nebitnih stvari, ali se vrlo često koristi kod spremanja slike ili zvuka, gdje možemo sačuvati osnovnu informaciju bez obzira na odbačene podatke.
- Tehnikom kompresije bez gubitka sadržaja smanjuje se ukupna količina podataka, a da se pritom ni najmanje ne gubi sadržaj podataka. Te se tehnike koriste pri komprimiranju sadržaja datoteke s poslovnim podacima.
- Kompresija i dekompresija podataka izvode se programski ili sklopovski. Današnji algoritmi sažimanja vrlo su složeni i računalno vrlo zahtijevni tako da je u primjeni zasad težište na sklopovskoj kompresiji i dekompresiji. Programsko sažimanje će u skoroj budućnosti biti također više prisutno zbog prilagođavanja arhitekture mikroprocesora računala i porasta njihove snage.
- **Mjera kompresije** je omjer koji nam govori koliko smo podataka spremili za svaki podatak zapisan na disku. Primjerice, ako na disk zapišemo 1000 bajtova podataka, uz kompresiju 2:1, to znači da je izvornih podataka bilo dva puta više, tj. 2000.
- Primjeri standarda za sažimanje/kompresiju podataka:

Skraćeni naziv standarda	Omjer sažimanja i primjena
JPEG	15:1, primjena kod mirnih slika s kontinuiranim nijansama (fotografije)
H.261 (px64)	100:1 do 200:1, telekomunikacijske audio-vizualne usluge (videotelefon)
MPEG	200:1, primjena kod videa s intezivnim pokretima na slici i kod audio zapisa (filmovi i glazba)

3.1.5. Kriptiranje podataka

- **Kriptiranje** je izmjena informacija (tekst, grafika ili video) u oblik koji može pročitati samo onaj tko ima ključ za dekriptiranje. Ono predstavlja pretvaranje informacije u nečitak oblik za sve osim za one koji imaju ključ za njeno dekriptiranje. Kriptiranje ili šifriranje je postupak kojim se razumljivi tekst prevodi u uljezu nerazumljivi kriptirani tekst. Dekriptiranje ili dešifriranje je obrnuti postupak prevođenja kriptiranog teksta u razumljivi tekst. Poslovima kriptiranja bavi se kriptografija.
- **Kriptografija** je drevna znanost koja graniči s umjetnošću, a u moderno je doba doživjela naglu ekspanziju postavši jednom od najatraktivnijih znanstvenih disciplina. Kriptoanaliza je postupak pronalaženja izvornog teksta bez poznavanja upotrijebljenog ključa. Kriptologija je znanstvena disciplina koja studira kriptografske metode.
- Poznati su mnogi postupci kriptiranja u kojima se pojedina slova ili skupine slova zamjenjuju drugim slovima ili skupinama slova uporabom jednostavnih operacija. Današnje gledanje na postupke kriptiranja svodi se na uporabu algoritama kriptiranja koji se u skraćenom obliku mogu napisati na sljedeći način: $C = E(P, KE)$, gdje je P razgovijetni tekst, KE ključ kriptiranja i C kriptirani tekst.
- **Dekriptiranje** se svodi na uporabu pripadne funkcije dekriptiranja D, koja uz uporabu ključa dekriptiranja KD, prevodi kriptirani tekst natrag u razgovijetni tekst, tj. možemo pisati da je $P = D(C, KD)$.
- Funkcije kriptiranja i dekriptiranja E i D sačinjavaju **kriptosustav**. Današnji kriptosustavi zasnivaju se na postupcima koji se efikasno mogu izvoditi na računalima, i to bilo sklopovski ili programski. Ti se postupci zasnivaju na algoritmima koji su u pravilu opće poznati, ali s ključevima koji imaju velik broj mogućih vrijednosti i time omogućuju vrlo velik broj raznih oblika kriptiranog teksta.
- Osnovni oblici kriptosustava:
 - **Simetrični kriptosustavi** (sustavi s tajnim ključevima)
 - **Asimetrični kriptosustavi** (sustavi s javnim ključevima).

3.1.6. Multimedija

- Pojam sastavljen od dvije latinske riječi:
 - *multus* = mnogo, više
 - *medium* = sredstvo komunikacije.
- Najčešće se koristi za opis načina prijenosa sadržaja od pošiljatelja do primatelja.
- Globalna područja primjene multimedije:
 - Računalno tehnološko područje
 - Komunikološko područje
 - Informatičko područje
- Multimedija u području računalne tehnologije:
 - podrazumijeva računalo sastavljeno od dijelova koji mogu prihvatiti više medija, te prihvatiti, digitalizirati i interpretirati zvuk, govor, sliku i sekvencu filma
 - takva računala moraju raspolagati velikom količinom memorijskih resursa (RAM memorija i diskovni resursi) kako bi se smjestio multimedijски sadržaj
 - potrebna je i velika procesorska moć kako bi se izvršavali razni algoritmi kompresije podataka u cilju smanjenja diskovnog prostora.
- Multimedija u komunikacijskom području
 - u ovom području se pojam multimedije izvorno primjenjuje
 - u tom smislu multimedijom se označava prenošenje poruke u komunikacijskom sustavu od pošiljatelja do primatelja
 - prilikom prijenosa sadržaja najviše se pažnje treba pridati multimedijском sredstvu za prijenos tog sadržaja
 - u početku su se rabila različita sredstva od gramofona za prijenos zvuka, diaprojektora za prijenos slike, grafoskopa za prijenos crteža, grafikona ili teksta, pa do kinoprojektora za prikaz filma

- da se smanji pogreška kao posljedica ljudske nepažnje, potrebna oprema za vizualizaciju se priključuje na računalo i pri tome se različiti sadržaji digitaliziraju kako bi za njihovo prezentiranje bilo dovoljno samo računalo, te eventualno projektor i zvučnici
 - digitalizacija sadržaja omogućuje lakše i jeftinije umnožavanje istog, te individualiziranu upotrebu
 - učestalom upotrebom digitaliziranog sadržaja javlja se potreba nelinearnog kretanja kroz isti, pa se stoga javljaju hipertekstualni i hipermedijalni dokumenti
 - **hipertekstualni dokument** izrađen je tako da se sadržaj povezuje poveznicama koje predstavljaju riječi koje reprezentiraju određeni pojam ili sadržaj koji je objašnjen i/ili obrađen na nekom drugom području
 - **hipermedijalni dokument** je dokument u kojem sadržaj teksta ilustriramo slikom, grafikonom, zvukom ili sekvencom filma, a svaki od tih objekata može predstavljati vezu na neku drugu lokaciju.
- **Multimedija u informatici**
 - podatak koji se rabi kao opis realnog sustava postaje nedovoljno jednoznačan zbog sve složenijih aplikacija poput prepoznavanja boje oka što je znatno lakše učiniti sa slikom negoli sa podatkom, zatim aplikacija za prepoznavanje glasa što je znatno lakše učiniti sa uzorkom zvuka (zvučnim zapisom) negoli sa skupom podataka
 - takav je razvoj opisa realnog sustava polučio razvoj cijele jedne grupe aplikacija koju nazivamo Prividna stvarnost (engl. Virtual Reality).

3.1.7. Prividna stvarnost

- temeljem odnosa realno – prividno, razlikujemo aplikacije prividne stvarnosti s:
 - izmišljenim objektima, izmišljenim prostorima i izmišljenim odnosima između objekata i prostora (primjer: računalne igre)
 - slikama realnih objekata u realnim ili izmišljenim prostorima i u realnim ili izmišljenim odnosima (primjer: virtualne trgovine)
 - reduciranim slikama realnih objekata u realnim prostorima i u realnim odnosima (primjer: upotreba u vojne svrhe, avijacija)

3.1.8. Područja primjene multimedije

- prezentacijsko – promotivne aplikacije
 - omogućuje upotrebu teksta, slike, zvuka, govora i video sekvence čime se osiguravaju veći efekti u percepciji izloženog sadržaja
 - poslovne aplikacije
 - pojedini sadržaji se opisuju upotrebom slike i zvuka kao npr. prilikom identifikacije osoba
 - medicina
 - prvobitno se multimedija upotrebljavala za pohranu medicinske dokumentacije
 - danas se upotrebljava i kod videokonferencija, dijagnostičkim metodama itd.
 - Turizam
 - prodaja turističkih proizvoda primjenom multimedijskog opisa destinacije i objekata na destinaciji
 - trgovina
 - upotreba multimedijskih aplikacija s mogućnošću hipermedijskog povezivanja sadržaja
 - web aplikacije, virtualni dućani itd.
 - Obrazovanje
 - multimedijom se služi u svim fazama obrazovnog procesa
 - sustavi za učenje da daljinu implementiraju multimediju kao osnovno sredstvo obrazovanja korisnika
 - zabava itd.
- Primjena multimedije kod prividne stvarnosti:
 - Kako bi se čovjek lakše snalazio u apstraktnim podacima, generiraju se trodimenzijski svjetovi na temelju tih apstraktnih podataka. Korištenjem trodimenzionalnog prikaza

podataka efikasno ćemo moći upotrijebiti vlastiti sustav percepcije za razumijevanje dobivene informacije. Za ostvarivanje prividne stvarnosti potrebno je :

- stvoriti prividni svijet
 - osigurati programsku podršku za upravljanje prividnim svijetom
 - osigurati materijalnu podršku
 - stvoriti sučelje prema čovjeku.
- Prvi korak u izgradnji objekata jest izgradnja geometrijskog modela. Geometrijski model može biti izrađen na tri načina:
 - Na osnovi zamišljenog objekta
 - Na temelju uzorkovanih podataka
 - Na temelju apstraktnih podataka.
 - Izgradnja geometrijskog modela na osnovi zamišljenog objekta. Model izgrađen na osnovi zamišljenog objekta izgrađujemo poput projektanta ili umjetnika. Zamislimo objekt koji želimo realizirati i izgradimo njegov model. Taj model predstavlja novi, nepostojeći objekt, koji želimo sagraditi u stvarnom svijetu, nad kojim možemo načiniti simulacije ili ga samo želimo prikazati. To može biti zgrada, interijer zgrade, planina ili stablo.
 - Izrada geometrijskog modela na temelju uzorkovanih podataka. Taj način izgradnje modela možemo prikazati na primjeru iz strojarstva. Promatrani objekt se uzorkuje u trodimenzijskom prostoru. Uobičajeni načini uzorkovanja objekta jesu računalna tomografija, magnetska rezonancija i ultrazvuk. Na ovaj način ostvarujemo niz poprečnih presjeka objekta, odnosno trodimenzijsko skalarno polje, na osnovi kojeg načinimo vizualizaciju unutrašnjosti objekta.
 - Izgradnja geometrijskog modela na temelju apstraktnih podataka. To je npr. Prikaz fraktalnog objekta. A fraktalni objekti su oni objekti koji pokazuju svojstvo samosličnosti. Kao ilustracija može poslužiti niz definiran iterativno formulom: $z_{n+1} = f(z_n) + c$, $z, c \in \mathbb{C}$
 - Za svaku točku c odabranog područja kompleksne ravnine, promatra se ponašanje dobivene sekvence brojeva. Ovisno o tome da li se apsolutna vrijednost brojeva smanjuje ili povećava i teži u beskonačnost, te kojom brzinom se to dešava, odabire se boja odnosno sivi ton u prikazu.
 - Kako u prividni svijet želimo ući, bit će potrebno ostvariti sučelje prema našim osjetilnim sustavima. Sučelje možemo načiniti prema sustavu vida, sustavu sluha, sustavu njuha, sustavu za osjet dodira. Interaktivno sudjelovanje zahtijeva da na svaku promjenu u sceni koju izazovemo dobijemo povratnu informaciju našim podražajnim sustavima.
 - Za sustav vida koristi se zasloni uređaj postavljen na oči odnosno glavu HMD (engl. Head Mounted Display). Osim proiciranja slike na zaslone ispred očiju HMD određuje i položaj, odnosno orijentaciju scene, što omogućuje kontrolu smjera gledanja, a u slučaju kašnjenja prikaza u odnosu na okretanje glave možemo izazvati "morsku bolest". Važan element okoliša u prividnom svijetu jest i akustičko okruženje. Uobičajeni zvukovi kada radimo na računalu jesu kliktanje tipkovnice ili miša, zujanje ventilatora i diska te poneka zvučna poruka upozorenja.

4. RAČUNALNE MREŽE I INTERNET

- Računalne mreže su složeni sustavi povezanih računala koji pružaju više pogodnosti kod raspodjele zajedničkih resursa, te povećavaju raspoloživost takvih resursa.

4.1. Pojam i vrste računalnih mreža

- Razvojem tehnologije došlo je do stapanja računalnog i telekomunikacijskog područja, čime su nastali složeni sustavi koje danas nazivamo računalnim mrežama.
- Uvođenjem računalnih mreža omogućen je odmak od stare prakse kod koje je sva računalna obrada bila izvršavana u računskom centru na (najčešće) jednom velikom računalu (mainframe) – mreže su omogućile raspodjelu obrade na veći broj odvojenih, ali međusobno komunikacijski povezanih računala.
- Računalna mreža ima nekoliko temeljnih funkcija:
 - **Funkcija suradnje** – povezivanje distribuiranih računalnih procesa u cjelinu prilikom izvršavanja raspodjeljenih zadataka
 - **Funkcija povezivanja** – komunikacijsko povezivanje udaljenih partnera
 - **Funkcija prijenosa podataka** – pouzdan prijenos podataka između udaljenih sustava.
- Jedan od najčešćih kriterija za klasifikaciju računalnih mreža je splet veličine, tehnologije prijenosa podataka i organizacije (topologije) mreže, a prema tom spletu kriterija se računalne mreže dijele na:
 - **Lokalne mreže (LAN – Local Area Network)** – mreže kratkog dosegaja koje tipično povezuju računala unutar jedne zgrade ili kompleksa zgrada
 - **Gradske mreže (MAN – Metropolitan Area Network)** – lokalne mreže srednjeg dosegaja koje se koriste za povezivanje pojedinačnih lokalnih mreža u veće cjeline na širim gradskim područjima
 - **Globalne mreže (WAN – Wide Area Network)** – mreže koje povezuju lokacije na velikim udaljenostima, a tipično su izgrađene nad već postojećom globalnom telekomunikacijskom infrastrukturom (telefonske parice, optička vlakna...).

4.2. Elementi računalnih mreža

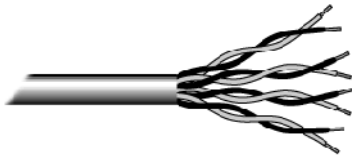
- Za ostvarenje komunikacije u računalnoj mreži potrebno je povezati u cjelinu nekolicinu hardverskih i softverskih komponenti – računala, mrežne adaptere, komunikacijske kanale, mrežne posrednike, mrežne protokole i sistemsku i aplikativnu softversku podršku.

RAČUNALA

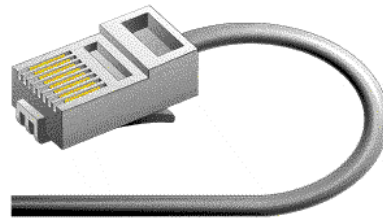
- Za realizaciju bilo kakve računalne mreže potrebno je imati barem dva računala

KOMUNIKACIJSKI KANALI

- Služe za prijenos podataka između udaljenih računala, tj. povezuju udaljena računala (čvorove računalne mreže)
- Veza između čvorova može se uspostaviti pomoću raznih vrsta fizičkih nosioca signala. Ti se nosioci obično nazivaju medijima za prenos signala/podataka. Osnovne (i najkorištenije) vrste medija su:
- **Opletena parica (twisted pair)** - sastoji se od dvije bakrene žice koje su međusobno "opletene" (zavijene jedna oko druge); takve parice nalazimo kod klasičnih lokalnih telefonskih veza. Najstariji i najuobičajeniji prijenosni medij je parica – par izoliranih bakrenih vodiča promjera oko 1 mm koji su helikoidalno raspoređeni radi smanjivanja električkog utjecaja na susjedne parove i obratno. U računalnim se mrežama, napose onim lokalnima, koriste dvije izvedbe:
 - **oklopljena** (shielded twisted pair, STP) i
 - **neoklopljena** (unshielded twisted pair, UTP). Neoklopljena izvedba je zbog velike raširenosti preuzeta za lokalne mreže tipa Ethernet.

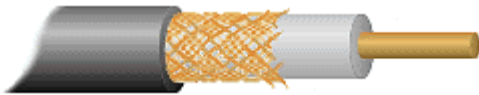


SLIKA 4.1: PARICA- TWISTED PAIR

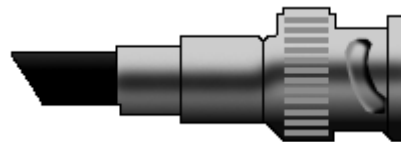


SLIKA 4.2: RJ-45 KONEKTOR – PREMA MREŽNOM ADAPTERU

- **Koaksijalni kabel** (coaxial cable) - sastoji se od središnjeg bakrenog vodiča, koji je omotan zaštitnim slojem izolacije (plastike), i vanjskog vodiča koji ima oblik bakrene mreže, i koji je prekriven dodatnim slojem izolacije; koaksijalni kabel daje se vidjeti npr. kod televizijskih antena. Zbog posebne izvedbe kod koje je drugi vodič plašt kojim je kabel oklopljen, koaksijalni kabel bolje je od parice zaštićen od djelovanja smetnji pa su i brzina prijenosa i dopuštena duljina veće. Koaksijalni kabel se koristi za digitalni i analogni prijenos, kako u globalnoj, tako i u lokalnoj domeni.

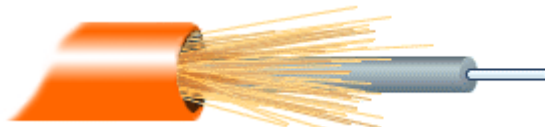


SLIKA 4.3: KOAKSIJALNI KABEL



SLIKA 4.4: BNC KONEKTOR – PREMA MREŽNOM ADAPTERU

- **Optička vlakna** (fiber) - sastoje se od središnje staklene niti (koja provodi optički signal), i od jednog ili više zaštitnih omotača; optička vlakna imaju veliku širinu pojasa (propusnost), i redovito se koriste za prenos podataka na velike udaljenosti (ali mogu se koristiti i za lokalne mreže).
- Optičko vlakno tanki je fleksibilni medij (od silike ili plastike promjera 2 do 125 μm) koji može voditi zrake svjetla. Izvor svjetla je svjetleća ili laserska dioda, a detektor fotodioda.
- Optička se vlakna izrađuju kao višenačinska (multimode) ili jednonačinska (single-mode).
 - *Višenačinska vlakna* imaju relativno velik promjer pa stoga i mnogo načina rasprostiranja svjetla (refleksijama od granice jezgra-omotač). Ova vrsta vlakana je jeftinija za proizvodnju te se dodatno mogu koristiti jeftinije svjetleće diode zbog većeg promjera jezgre što omogućuje utiskivanje veće snage u vlakno. Parametar propusnost x udaljenost iznosi 20 MHz x km.
 - *Jednonačinska vlakna* (single-mode) imaju promjer reduciran na veličinu sumjerljivu valnoj duljini prenošenih svjetlosnih signala, tako da se svjetlost rasprostire pravocrtno (bez refleksija od granice jezgra-omotač). Ta su vlakna skuplja, omogućavaju veće domete, ali nužno zahtijevaju efikasnije i skuplje laserske diode koje mogu generirati uže fokusirane svjetlosne impulse. Parametar propusnost x udaljenost iznosi tipično 1000 GHz x km.



SLIKA 4.5: OPTI KO VLAKNO

- **Prostor** (space) - prostor ćemo ovdje definirati kao "ono u čemu se uspješno šire radiovalovi", mikrovalovi, infracrveni valovi i brojne druge vrste valova pomoću kojih se bežično prenose podaci.
- Kao medij za bežični prijenos signala se koriste elektromagnetski valovi (i svjetlo je elektromagnetski val). Elektromagnetske valove dijelimo prema njihovim frekvencijama (koje se izražavaju u Hertzima - Hz).
- Frekvenciju možemo slikovito opisati kao "broj vrhova vala u sekundi"; npr. val frekvencije 300 Hz ima 300 "vrhova" u sekundi. Razdaljina između dva vrha vala (mjerena u metrima) naziva se valnom dužinom (wavelength).

- Valna dužina je kvocijent brzine širenja signala i njegove frekvencije.
- Prema vrsti korištenih elektromagnetskih valova razlikujemo:
 - Prijenos pomoću radio-valova
 - Mikrovalni prijenos – WiFi, Bluetooth, GSM...
 - Infracrveni prijenos
 - Laserski prijenos.

MREŽNI ADAPTERI

- Potrebni su kako bi prilagodili podatke pohranjene u računalu u oblik pogodan za prijenos određenim komunikacijskim kanalom.
- Ako računalo mora komunicirati sa ostalim računalima posredstvom lokalne mreže, tada je mrežni adapter realiziran u obliku mrežne kartice koja je smještena u računalu.
- Ako računalo treba izravno povezati na globalnu mrežu (npr. Internet), tada je mrežni adapter realiziran u obliku:
 - modema (pretvara digitalne signale iz računala u analogne signale koji se prenose telefonskom mrežom), ili
 - ISDN adaptera (bez analogno-digitalne pretvorbe – kod digitalne telefonske mreže), ili
 - Nekog oblika broadband (širokopojasnog) adaptera – DSL adapteri, kabelski "modemi"...

MREŽNI POSREDNICI

- Omogućavaju različite načine povezivanja čvorova u računalnoj mreži, a time i različite oblike organizacije računalnih mreža.
- **Repetitori ili prijenosnici (Repeaters)** – povezuju dijelove iste mreže. Pojačavaju signale koji prolaze kroz njih, omogućavajući time veći doseg signalima. Npr. ako je fizički limit difuzije signala u LAN mreži 100m, tada bi uz pomoć repetitora (smještenog u blizini 100-tog metra) bilo moguće poslati signal i na udaljenost do 200m.
- **Premosnici (Bridges)** – odvajaju veliku lokalnu mrežu na manje segmente. Svaki čvor unutar segmenta može slobodno komunicirati sa bilo kojim čvorom unutar istog segmenta mreže, a sa čvorovima iz drugih segmenata je moguća komunikacija jedino posredstvom premosnika.
- **Koncentratori (Hubs) i sklopke (Switches)** – omogućavaju podjelu lokalne mreže na manje segmente (domene), čime se povećava propusnost mreže između bliskih čvorova (koji čine jedan segment). Cjelovitost mreže je očuvana kroz mogućnost hijerarhijskog međusobnog povezivanja koncentrataora i sklopki.
- **Spojni pristupi (Gateways)** – povezuju različite mreže u cjelinu kroz konverzije mrežnih protokola koji se koriste u tim mrežama – bez sojnog pristupa se takve mreže "ne bi međusobno razumjele" – tj. svaka bi mreža "govorila" svojim jezikom (mrežnim protokolom).
- **Usmjernici (Routers)** – imaju sličnu ulogu u povezivanju različitih mreža kao i spojni pristupi, ali usmjernici taj posao obavljaju na nižoj razini (npr. samo na razini IP protokola) – usklađuju formate adresa pojedinih čvorova, duljine podatkovnih paketa itd., ali ne ulaze u cjelovitu konverziju protokola, kao što to rade spojni pristupnici.

MREŽNI PROTOKOLI

- **Mrežni protokol** je skup pravila po kojima se izvršava komunikacija unutar računalne mreža – pojednostavljeno rečeno, mrežni protokol je "govorni jezik" neke računalne mreže – da bi određeni čvor mogao sudjelovati u radu određene računalne mreže, dotični čvor mora "govoriti jezikom" te mreže, tj. poznavati mrežne protokole koji se u dotičnoj mreži koriste.
- Npr. Internet se temelji na skupu **TCP/IP** protokola – iz skraćenice se naziru samo dva protokola – TCP (Transmission Control Protocol) i IP (Internet Protocol), ali za funkcioniranje Interneta u obliku kakvog ga svi znamo je potreban još cijeli niz protokola (ICMP, IGMP, ARP, ...) koji zajedno čine tzv. TCP/IP stack.

SISTEMSKA SOFTVERSKA PODRŠKA

- Na čvoru računalne mreže se izvodi pogonski program (dio operacijskog sustava) koji upravlja radom mrežnog adaptera. Npr. driver (pogonski program) određuje iz kojeg se prostora u memoriji čvora treba uzeti sadržaj koji se upućuje u mrežu, odnosno u koji memorijski prostor treba pohraniti sadržaj koji iz mreže stiže na adapter... – kao i kod

računala općenito, bez potpore i upravljanja na razini sistemskog softvera računalna mreža bi bila samo nakupina beskorisnog hardvera.

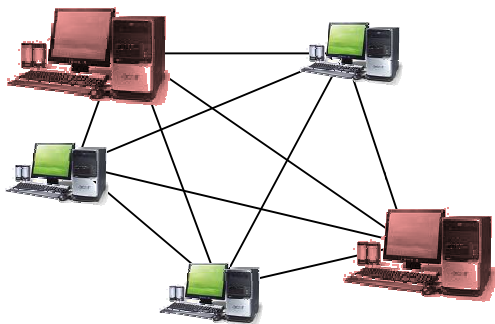
- U sistemsku softversku podršku uključujemo i mrežne protokole.

APLIKATIVNA SOFTVERSKA PODRŠKA

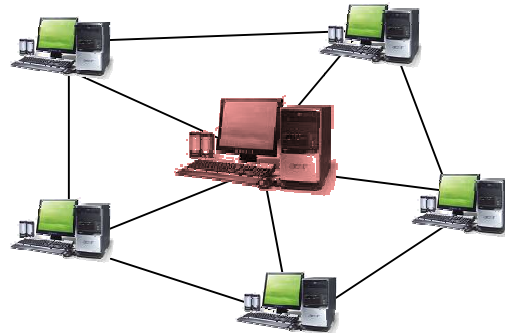
- Ovdje ubrajamo korisničke aplikacije koje za svoj rad zahtijevaju postojanje računalne mreže – zbog njih se izgrađuju računalne mreže.
- Preglednici Interneta, aplikacije za razmjenu elektroničke pošte, čitanje mrežnih novina, chat, razmjenu datoteka (FTP, P2P...), razne mrežne aplikacije specifičnih namjena (e-business, e-learning...).

4.3. Topologija mreže

- S razvojem telekomunikacija i brzih računalnih mreža omogućeno je povezivanje međusobno udaljenih računala. Pri tome geografska udaljenosti nije važna tako da se mogu povezivati i vrlo udaljena računala (međukontinentalno).
- Takvi računalni sustavi (koji djeluju na međusobno odvojenim lokacijama) povezani su mrežnom infrastrukturom (hardware, software, netware). Osobitost im je što podaci nastaju, koriste se i pohranjuju na različitim mjestima.
- Način korištenja podataka, hardwara i softwera može biti izveden kao:
 - **decentraliziran**, na pojedinačnim računalima (PC, radne stanice, osobne baze podataka) -što je pogodno za manje mreže (LAN - lokalne mreže)
 - **centraliziran**, (na velikim poslužiteljima, distribuiranim bazama podataka, višeprocorska računala velikih kapaciteta) što je pogodno za velike mreže (WAN - mreže širokog opsega).



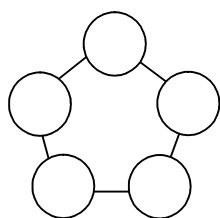
SLIKA 4.6: DECENTRALIZIRANA OBRADA



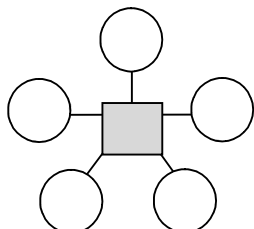
SLIKA 4.7: CENTRALIZIRANA OBRADA

- Kod povezivanja računala razlikuju se sljedeći oblici povezivanja (topologije):
 - **Zvjezdasto** oblikovana mreža – predstavlja oblik pogodan za centralizirani sustav distribuirane obrade podataka. Središnje računalo izvršava ključne i najsloženije obrade te povezuje slabija tzv. satelitska računala. Satelitska računala međusobno mogu komunicirati samo preko središnjeg. Karakterizira je velika ovisnost o središnjem računalu što je veliki nedostatak (u slučaju prekida rada središnjeg računala pada cijeli sustav). U stvarnim sustavima to se kompenzira uvođenjem paralelnog rezervnog poslužitelja.
 - **Prstenasto** oblikovana mreža – ne ovisi o središnjem računalu i otpornija je na greške u sustavu (ako jedno računalo ispadne ništa se neće dogoditi). Ako je mreža izvedena centralno, glavni poslužitelj se spaja na isti način kao i ostala računala. Računala međusobno komuniciraju koristeći zajednički prsten. Podaci putuju od računala do računala u jednom smjeru (npr. BNC mreža). Pogodno za vrlo male mreže (npr. povezani terminali).
 - **Sabirno** oblikovana mreža – računala komuniciraju koristeći jednu kablensku vezu u oba smjera. Nema potrebe za središnjim računalom i takav je oblik pogodan za lokalne mreže računala (LAN) – npr. Ethernet mreža.
 - **Hibridno** oblikovana mreža – je kombinacija prethodnih oblika povezivanja.

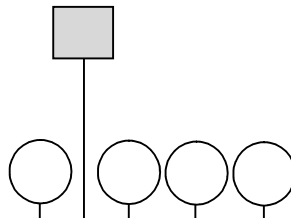
- **Puna mrežna struktura** – koristi se kod potpuno decentraliziranih mreža. Obuhvaća niz ravnopravnih specijaliziranih računala povezanih u jedinstvenu mrežu. Sva su računala izravno povezana sa svakim preostalim računalom i mogu izravno međusobno komunicirati (razmjenjivati podatke). Korisnik jednog računala ima izravan pristup na svako računalo i njegove periferne uređaje. Takav sustav obično obrađuje podatke u realnom vremenu.



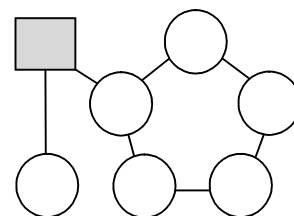
SLIKA 4.8: PRSTENASTA MREŽA



SLIKA 4.9: ZVJEZDASTA MREŽA



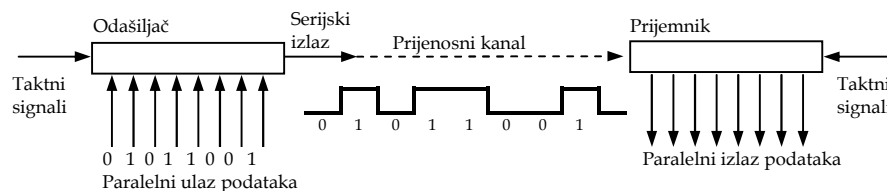
SLIKA 4.10: SABIRNA MREŽA



SLIKA 4.11: HIBRIDNA MREŽA

4.4. Serijski prijenos podataka

- Pristupni sklopovi mogu, s obzirom na “širinu” podataka koji se prenose, biti:
 - paralelni pristupni sklopovi
 - serijski pristupni sklopovi
- Serijski pristupni sklopovi dopuštaju prijenos jednog bita u jedinici vremena, tako da se n-bitna riječ prenosi u obliku “vlaka” od n bitova u slijedu.
- Obično se naponske razine koje odgovaraju vrijednostima bitova pojavljuju jedna za drugom u ritmu taktnog signala prijema (ili predaje).
- Serijski pristupni sklopovi, zbog manjeg broja linija (samo je jedna signalna linija, odnosno dvožični vod potreban za prijenos) upotrebljavaju se za prijenos podataka na veću daljinu. (npr. pomoću posebnih sklopova za moduliranje i demoduliranje signala (modem) omogućen je prijenos podataka na daljinu preko telefonskih linija)
- Serijski prijenos obično se koristi **za prijenos podataka na velike udaljenosti**.
- Na takav način podaci se prenose jednom linijom tako da s odašiljačkog registra prelaze jedan iza drugog na liniju a na prijemnom mjestu prihvaćaju ih uređaji koji ih zapisuju na prijemni registar jednog po jednog kako nailaze.
- Po jednoj podatkovnoj liniji se prenose podaci, kao niz bitova, jedan iza drugoga.
- Potreban je samo jedan kanal za prijenos, ali je zbog toga i sam prijenos sporiji.
- Ovaj način prijenosa podataka koristi se za prijenos manje količine podataka, ali na veće udaljenosti.
- Poseban slučaj je serijski prijenos podataka preko telefonskih linija (modem – digitalni podaci se pretvaraju u analogne zbog prijenosa na daljinu).
- Vršiti se na **sinkroni** (USRT – Universal Synchronous Receiver Transmitter) ili **asinkroni** (UART – Universal Asynchronous Receiver Transmitter) način.
- Sklopovi za serijski prijenos moraju imati:
 - odašiljački dio, i
 - prijemni dio.
- Za dvosmjernu komunikaciju moraju na oba kraja postojati i odašiljač i prijemnik.
- **Odašiljač:**
 - Podatke primljene na paralelan (npr. sa neke od sabirnica u računalu) način pretvara u niz bitova koji serijski, jedan iza drugoga putuju, po prijenosnom kanalu do prijemnika.
- **Prijemnik:**
 - Prihvaća niz nadolazećih serijskih podataka i od njih oblikuje riječ prikladnu za daljnji paralelni prijenos (npr. putem sabirnica).



SLIKA 4.12: SERIJSKI PRIJENOS PODATAKA

4.4.1. Sinkroni i asinkroni serijski prijenos

- Na velike udaljenosti koristi se serijski način prijenosa podataka.
- Na takav se način podaci prenose jednom linijom, tako da s odašiljačkog registra prelaze jedan iza drugog na liniju.
- Uređaji na prijemnom mjestu prihvaćaju bitove podataka jednog po jednog kako nailaze i zapisuju ih na prijemni registar.
- Pri takvom načinu prijenosa podataka, prijenos se može obavljati sinkrono ili asinkrono.

SINKRONI PRIJENOS PODATAKA

- Prenose se blokovi podataka sastavljeni od velikog niza znakova.
- Između pojedinih znakova nema »start-stop« impulsa, nego prijemnik prihvaća određeni broj bitova iz niza nailazećih bitova kao jedan znak.
- Sinkronizacijski signali šalju se povremeno kako bi predajnik i prijemnik bili sinkronizirani i pravilno obavljali prijenos.
- Dovoljno je da prijemnik svrsta samo jedan bit više ili manje u neki znak, pa da cijeli blok podataka, koji čini neku poruku, bude krivo prihvaćen.
- Zahtjevi za sinkronizaciju su pri sinkronom prijenosu vrlo oštri, ali je i brzina prijenosa veća.
- Takav način upotrebljava se tamo gdje se prenosi više podataka da bi se isplatilo ugrađivati složeniju opremu koja omogućuje takav prijenos, a i njegovu provjeru točnosti.
- Podaci koji nailaze obično se u odašiljaču pohranjuju u »buffer« memoriju, a kad se skupi dovoljan broj podataka, cijeli se blok podataka velikom brzinom sinkronim prijenosom prenese na odredište
- Na kraju prijenosa provjerava se na neki način ispravnost prijenosa. Ako se utvrdi greška, prijenos se ponovi.

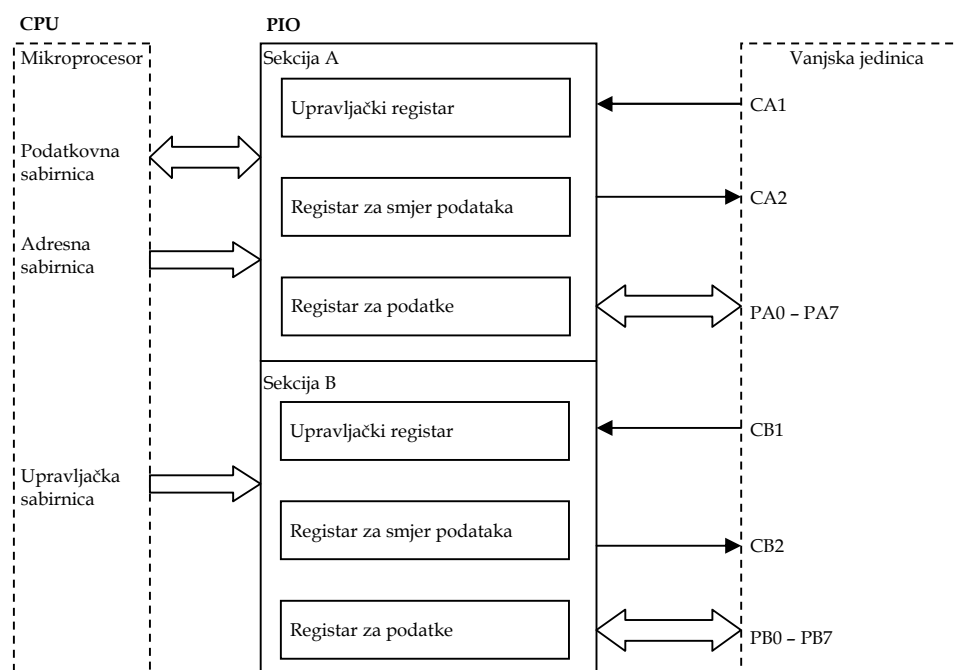
ASINKRONI PRIJENOS PODATAKA

- Kod asinkronog prijenosa (start-stop prijenos) prenosi se jedan podatak (znak, karakter) odjednom.
- Na početku prijenosa nalazi se startni bit kojim se prijemnik obavještava da će sljedećih nekoliko bitova sačinjavati podatak.
- Za vrijeme »start« bita prijemnik se pripremi na prijem podatka, te se izvrši sinkronizacija davatelja i primatelja.
- Nakon serijskog prijenosa ostalih bitova podatka, prenosi se znak »stop« koji označava kraj jednog podatka.
- Taj znak »stop« može trajati onoliko koliko obično traje 1 do 2 bita.
- Nakon toga linija miruje do odašiljanja sljedećeg znaka.
- Sljedeći znak se odašilje na isti način, »start« i »stop« impulsi, a između njih bitovi znaka koji se prenosi.

4.5. Paralelni prijenos podataka

- Pristupni sklopovi mogu, s obzirom na "širinu" podataka koji se prenose, biti:
 - paralelni pristupni sklopovi
 - serijski pristupni sklopovi.
- Kod paralelnih pristupnih sklopova su svi bitovi jedne strojne riječi koja se prenosi istodobno prisutni na njegovu ulazu (ili izlazu).
- Pri takvom prijenosu svaki bit podataka ima svoju liniju (vodič) za prijenos.

- Kod paralelnog načina prijenosa podataka svaki bit s odašiljačkog registra zahtijeva poseban prijenosni put (liniju, kanal) za povezivanje s odgovarajućim bitom prijemnog registra, pa treba onoliko broj linija od koliko se bitova sastoji podatak.
- Pošto se odjednom prenosi niz bitova, najčešće jedan bajt, za takav prijenos je potrebno najmanje osam linija za podatke.
- Sklopovi za paralelni prijenos zovu se PIO (eng. Parallel Input/Output) sklopovi.
- Računalo, prije početka U/I prijenosa pomoću određenog programa inicijalizacije programira PIO sklop i pripremi ga da bude sposoban obavljati funkciju koja se od njega zahtijeva.
- PIO sklop je spojen na sabirnicu podataka, te adresnu i upravljačku sabirnicu.
- Na izlazu iz PIO sklopa su linije za prijenos podataka i upravljačke linije koje povezuju PIO sklop s vanjskom jedinicom.
- PIO sklop, prikazan na slici dolje sastoji se od dvije potpuno jednake sekcije, A i B, a svaka se sekcija sastoji od tri 8-bitna registra, i osam linija za podatke, te dvije upravljačke linije.
- Zbog mnogo upotrijebljenih linija takav način prijenosa dolazi u obzir samo na kraćim udaljenostima npr. u kućama između računala i njegovih terminala.



SLIKA 4.13: PARALELNI PRIJENOS PODATAKA

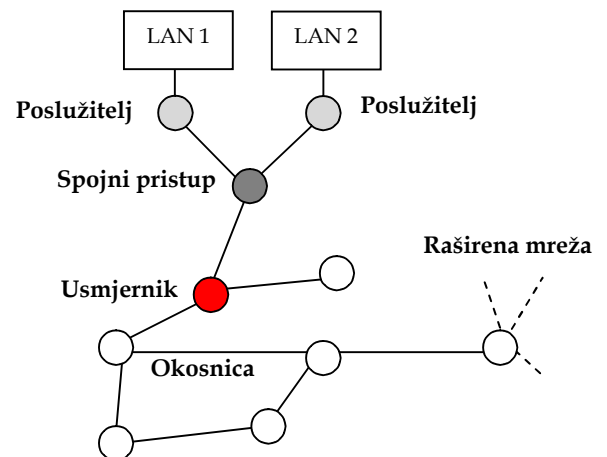
4.6. Internet

- Osnove računalnih mreža postavljene su u prvoj polovini šezdesetih godina u okviru nezavisnih znanstvenih istraživanja o računalima i komunikacijskim mrežama u dva američka i jednom britanskom istraživačkom centru. Godine 1965. u SAD-u je uspjelo prvo povezivanje dvaju računala, a 1969. godine proradila je u SAD-u ARPANET mreža u kojoj su bila uključena 4 superračunala. Tijekom sedamdesetih godina razvijeni su važni Internet servisi ako što su elektronička pošta, korištenje udaljenih računala, prijenos datoteka i sustav elektroničkih novosti, a objavljen je i TCP protokol.
- Internet danas čini nekoliko desetaka milijuna najrazličitijih računala povezanih u globalnu mrežu. Ta golema računalna mreža globalni je komunikacijski prostor u kojem svatko može komunicirati s bilo kime. Ona je također i globalni informacijski prostor u kojem svatko u bilo koje doba dana i noći može pretraživati sve raspoložive informacije bez obzira na kojem se mjestu globusa one nalazile. Informacije mogu biti različitog oblika: podaci, programi, tekstovi, grafika, zvuk ili video.
- Internet je i novi medij za publiciranje u kojem svaki pojedinac i organizacija može drugima staviti na raspolaganje svoje informacije, koje tako dobivaju globalni doseg. Internet je također veliki laboratorij u kojem se neprekidno ispituju nove ideje te novi softver i hardver; novi istraživački i obrazovni medij, a sve više i važan globalni medij za elektroničko poslovanje.

- U svojoj tehničkoj osnovici Internet je spoj različitih mreža računala u jedinstvenu svijetsku računalnu mrežu koja nudi velik broj informacijskih i komunikacijskih usluga. Internet prerasta obično fizičko umrežavanje različitih računalnih mreža i postaje temeljno sredstvo komunikacije pojedinaca, grupa i poslovnih subjekata. S obzirom na sve veću brojnost osobnih računala i njihovo jednostavno priključivanje u Internet, stvara se novo područje privrednog i kulturnog djelovanja s novim profilom potrošača.
- Internet se danas razvija vrtoglavom brzinom a razvijat će se još brže. Broj korisnika Interneta raste iz dana u dan tako je 1984 na Internet bilo spojeno preko 1000 računala, 1987. godine 10 000 računala, 1989. godine 100 000 računala, 1992 milijun računala, 1996 10 milijuna računala. Možemo zaključiti da će se Internet još povećavati u budućnosti i da će biti prisutan u svakoj firmi i svakoj kući.
- Internet je bitno poboljšao i pojednostavio komunikaciju te omogućio jednostavno i globalno publiciranje dokumenata te pretraživanje ogromnog broja raznovrsnih informacija. Time je znatno ubrzan i prelazak na elektroničko poslovanje koje danas uključuje različite aspekte poslovanja kao što su marketing, bankarstvo i rad u skupini.

4.6.1. Građa Interneta

- Za Internet se ne može reći da ima jasno definiranu topologiju mreže. S obzirom na veličinu i razgranatost, u strukturi Interneta su zastupljeni svi oblici topologija mreža. Ipak, osnovni elementi u arhitekturi Interneta su jasno definirani i bit će ukratko opisani u ovoj lekciji.
- Okosnicu Interneta čini tzv. temeljna mreža (engl. Backbone) – mreža iznimno velikog kapaciteta koja omogućava vrlo brz protok velike količine podataka.
- Na okosnicu se putem usmjernika (engl. Routers) povezuju pojedinačne mreže koje čine dio Interneta. Zadatak routera je usmjeravanje podatkovnih paketa koji se razmjenjuju prema zadanim odredištima.
- Lokalne mreže i/ili pojedinačna računala ne komuniciraju izravno sa usmjernikom, nego posredno, preko spojnog pristupa šalju i primaju podatke. Spojni pristupi (engl. Gateway) pretvara raznorazne protokole pripadne lokalne mreže u protokole koji se koriste na Internetu (i koje usmjernik jedino razumije) i obratno.
- Unutar mreža koje se povezuju na Internet mogu postojati računala-poslužitelji (engl. Servers), koja poslužuju radne stanice (engl. Hosts) sa raznim aplikacijama, podacima pohranjenim u bazama podataka...



SLIKA 4.14: SKICA GRAĐE INTERNETA

4.6.2. Internetski servisi

- Putem Interneta su dostupne različite usluge, koje se realiziraju pomoću različitih vrsta internetskih servisa, npr:
 - **www** - World Wide Web
 - **ftp** - File Transfer Protocol (prenošenje datoteka)
 - **gopher** - gopher poslužitelj
 - **e-mail** - elektronička pošta
 - **telnet** - pristup udaljenom računalu
 - **news** - diskusijske skupine.

WWW

- Godine 1991 razvijen je multimedijски World Wide Web(WWW) servis kao i PGP sustav šifriranja poruka, što je pobudilo interes poslovnog svijeta i madija. 1994 godine na internetu se pojavljuju prve elektroničke (virtualne) prodavaonice te prva virtualna banka i radiostanica. Iste godine razvijeni su i prvi pretraživački servisi za Internet(Lycos i Altavista). 1995 nastali su jezik Java za dinamičko programiranje za WWW te jezik VRML za modeliranje virtualne stvarnosti. 1997 pojavljuju se servisi koji sami periodički šalju informacije korisnicima omogućujući dobivanje personalizirane informacije po svojoj želji.

- World Wide Web (WWW) je usluga koja omogućuje prijenos teksta, slike, zvuka i animacije, kroz najveću računalnu mrežu - Internet, kao i izvođenje aplikacija na udaljenim hostovima. Mogućnosti WWW-a su nemjerljive, a danas sve veću primjenu pronalazi u informatičkom marketingu, komunikacijama i općenito elektronskom poslovanju. Na taj način moguće je jeftino prezentirati Vaše proizvode i usluge svim korisnicima Interneta širom svijeta (kojih danas ima preko 50.000.000), kao i komunicirati sa vašim poslovnim partnerima u zemlji i inozemstvu.
- Adrese WWW lokacija mogu imati sljedeći izgled:
 - <http://www.foi.hr>
 - <http://www.carnet.hr>
 - <http://serverwin2k.prof.foi.hr>

ELEKTRONIČKA POŠTA

- E-mail je mogućnost razmjene poruka među udaljenim korisnicima preko računalne mreže. Osim razmjene jednostavnih i kratkih poruka, uključuje i razmjenu obimnih poslovnih podataka, programa, itd. Svaki korisnik posjeduje svoj vlastiti elektronski sandučić. Koristeći određene komande korisnik može pretražiti sadržaj poruka u poštanskom sandučiću i prikazati isti na ekranu, te odasliti poruku drugom korisniku. Da bi se poslala poruka nije nužno da primalac bude trenutno za računalom. Poruka se pohranjuje u poštanski sandučić računala sve dok se ne pročita.
- Neke od značajki E-maila su što je to asinkroni način komunikacije u kojem primatelj ne mora biti prisutan u trenutku slanja poruke, što je slanje i primanje krajnje jednostavno i jeftino (nema papira, olovki...) a poruke se mogu čitati kada to korisniku odgovara, poruke stižu u vrlo kratkom roku na bilo koji dio zemaljske kugle...

FTP (FILE TRANSFER PROTOCOL)

- FTP (File Transfer Protokol) je protokol i istovremeno naziv programa za prijenos datoteka između dva udaljena računala. Njegovo korištenje se odnosi na kopiranje podataka s Internet-poslužitelja. U Unix naredbenom prozoru FTP naredba se koristi za prijenos podataka između lokalnog i udaljenog računala koje radi kao ftp poslužitelj.

NEWS

- News grupe su servis koji omogućuje odvijanje rasprave skupinama ljudi s zajedničkim interesima. Ovaj je servis iznimno popularan te broji preko 10,000 news grupa u svim zamislivim područjima ljudskog interesa. Poruke se pretplatnicima šalju e-m@ilom, te se nalaze na "BBoardu" na kojem ih svatko može pročitati. Za čitanje poruka je potreban poseban software koji je danas uključen u sve bolje Web Browsers. Newsgrupe mogu biti moderirane i nemoderirane.
- Kod nemoderiranih skupina nema centralne kontrole poruka, dok se kod moderiranih skupina moderator odlučuje koja će poruka biti prosljeđena korisnicima, a koja ne. Najbolji izvor informacija o newsgrupama je www.dejanews.com na kojem su hijerarhijski prikazane najvažnije skupine s kratkim opisima tema kojima se bavi koja grupa, itd. Forum može napraviti svaki korisnik Interneta koji postavi neko pitanje ili pokrene diskusiju o određenoj temi.

MAILING LISTE

- Mailing liste predstavljaju servis u kojem članovi liste komuniciraju pomoću e-m@ila. Poruke poslone na listu automatski se dostavljaju svim pretplatnicima liste. Problem s mailing listama je u tome što ako postoji veći broj korisnika pojedine liste, u vrlo kratkom roku može doći do petrpavanja "mailboxa". Kao i newsgrupe, mogu biti moderirane i nemoderirane.

TELNET

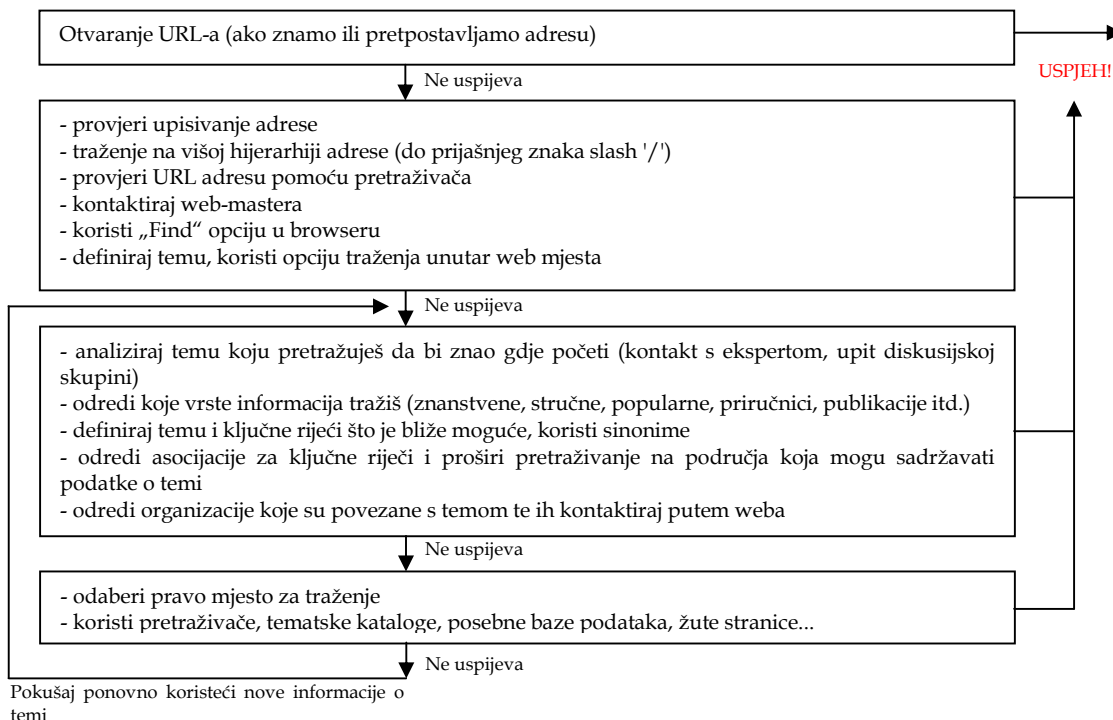
- TelNet je servis koji nam omogućuje spajanje na udaljena računala. Pravilnije govoreći, on korisniku dopušta da s dopuštenjem koristi resurse udaljenih računala baš kao da se nalazi za terminalom izravno povezanim s tim računalom. Npr. jedna od uporaba Telnet-a je izvođenje određenih programa na snažnijim računalima kojih nema u našoj blizini.

GOPHER

- Gopher je servis koji nam omogućava traženje internet resursa korištenjem lista i izbornika i to hijerarhijskom navigacijom kroz razine izbornika.
- Gopher je brzi tekstualni servis, a nijme se mogu pronaći datoteke smještene na različim dijelovima globusa. Pronađene datoteke mogu sadržavati bilo koji oblik informacija: tekstove, slike, zvučne zapise, itd. URL s korisnim popisom Gopher resursa je: [gopher://netlink.wlu.edu:1020/11/ty%20](http://netlink.wlu.edu:1020/11/ty%20)

4.6.3. Načini pretraživanja Interneta

- Mnoštvo podataka i informacija dostupnih na Internetu moguće je pretraživati na različite načine korištenjem brojnih dostupnih tehnologija za pretraživanje Interneta. Najčešće korištene tehnologije su sljedeće:
 - **Tražilice** (pretraživači),
 - **Metatražilice** (metapretraživači),
 - **Tematski katalozi**, te
 - **Inteligentni agenti**.
- Preporuča se započeti pretraživanje s definiranjem sadržaja koji želimo pronaći. Toga se korisnici često ne pridržavaju, jer sigurni u sebe, potaknuti brzinom i dostupnošću Interneta započinju pretraživanje s nerazrađenim ciljem i područjem pretraživanja želeći što prije pronaći potreban sadržaj. U praktičnom korištenju takav način ne daje uvijek pravovremene informacije.
- Na temelju razmišljanja većeg broja autora tijekom pretraživanja može se podijeliti u sljedeće faze:



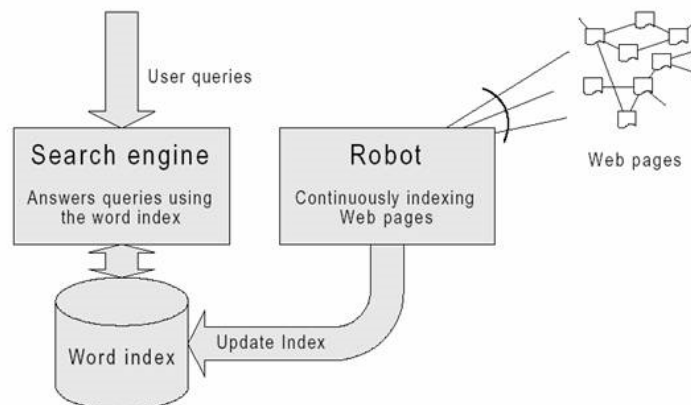
SLIKA 4.15: JEDAN OD MOGUĆIH NAČINA PRETRAŽIVANJA INTERNETA

- Općenito, nema najboljeg načina pretraživanja, a ni najboljeg Web-servisa za pretraživanje.
- U stvarnoj situaciji treba koristiti njihovu kombinaciju, odnosno više pristupa ne bi li se dobili što bolji rezultati.

4.6.3.1. Tražilice

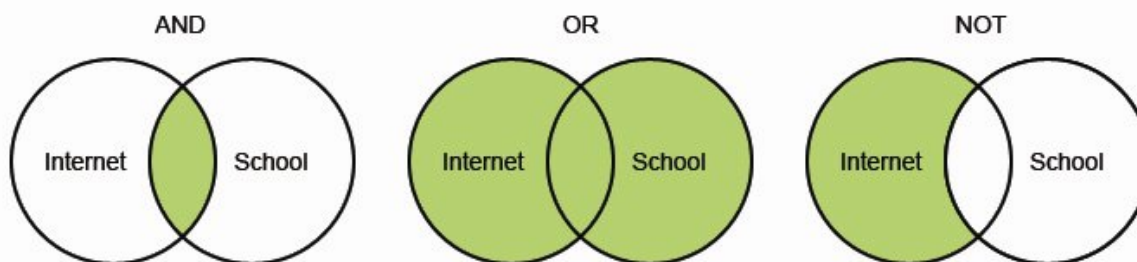
- Tražilice ili pretraživači (eng. Search Engines) predstavljaju automatizirani način traženja informacija na Webu. Svaka tražilica ima tri bitna dijela:
 - programe (tzv. robote ili pauke) koji neprekidno pretražuju Web stranice diljem Interneta i prenose te informacije u baze podataka pretraživača

- program (search engine) za pretraživanje baza podataka i prikaz pronađenih rezultata krajnjem korisniku
 - baze indeksiranih stranica.
- Shema tipičnog web-pretraživača



SLIKA 4.16: SHEMA TIPIČNOG WEB-PRETRAŽIVAČA

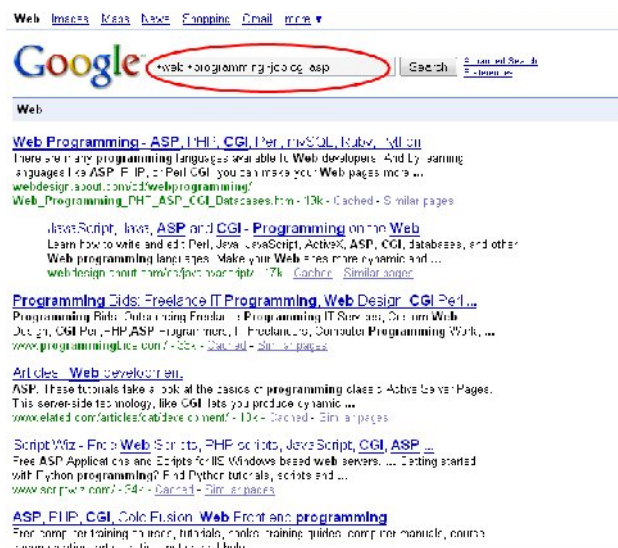
- Korisnici zadaju upite koje search engine pokušava pronaći u bazama podataka pretraživača. Upit se sastoji od ključnih riječi i operatora koje definira krajnji korisnik.
- **Jednostavni upiti**
 - Pretražuju se dokumenti koji sadrže:
 - sve riječi,
 - bilo koju riječ ili
 - frazu koju ste upisali.
- **Složeniji upiti**
 - koristi se Booleova logika za dobivanje preciznijih rezultata pretraživanja
 - AND - pronalazi samo dokumente koji sadrže sve tražene riječi ili fraze
 - OR - pronalazi dokumente koji sadrže barem jednu od traženih riječi ili fraza
 - NOT - ne uključuje dokumente koji sadrže navedenu riječ ili frazu.
- Primjeri Booleovih operatora kod složenijih upita:



SLIKA 4.17: OSNOVNI BOOLOVI OPERATORI

- Razne tražilice na razne načine koriste logičke operatore. Ovi bi se upiti realizirali pomoću Google tražilice (trenutno najbolje i najpoznatije) na sljedeći način:
 - AND primjer: +Internet +School
 - OR primjer: Internet School
 - NOT primjer: Internet -School
- Npr. želimo pronaći stranice o web programiranju ASP ili CGI tehnologije, ali ne želimo pri tome dobiti i stranice sa ponudama za posao. Google realizacija takvog upita bi bila sljedeća:

• +web +programming -job cgi asp

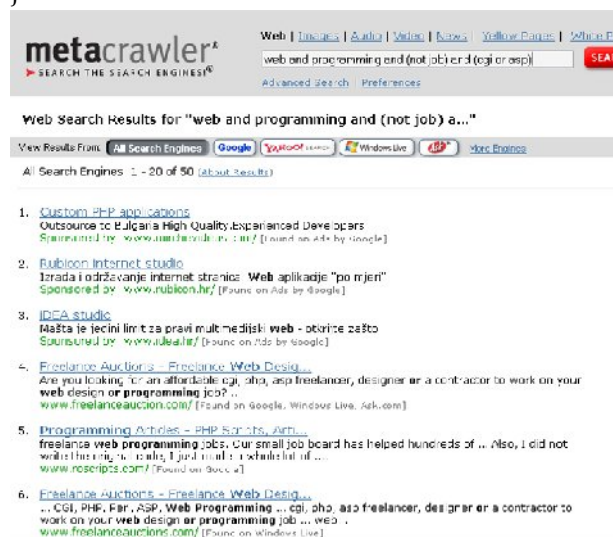


SLIKA 4.18: NAPREDNIJA PRETRAGA U GOOGLE-U

4.6.3.2. Metatražilice

- Po logici rada su slične tražilicama, ali se od njih razlikuju po sljedećem:
 - ne sadrže vlastitu pretraživu bazu indeksiranih web stranica niti vlastite programe-robote
 - na temelju zadanog upita simultano pretražuju baze podataka nekoliko individualnih pretraživača
 - metapretraživači omogućuju brzo i jednostavno pronalaženje najboljih rezultata većeg broja pojedinačnih tražilica.
- Kod postavljanja upita najčešće nisu na raspolaganju svi mogući operatori svih klasičnih tražilica s kojima metatražilica komunicira – skup operatora je ograničen na najmanji zajednički nazivnik svih korištenih tražilica.
- Prikaz rezultata
 - rezultati prikupljeni od većeg broja tražilica se najčešće dodatno grupiraju i/ili sortiraju po kriterijima koje zadaje krajnji korisnik.
 - **jednostruka lista** (eng. single list) - rezultati su kombinirani iz više tražilica i prikazani u jednoj listi, poredani su po relevantnosti i ne pojavljuju se duple web adrese.
 - **višestruka lista** (eng. multiple list) - prikazani su najbolji rezultati za svaku korištenu tražilicu, moguća su ponavljanja rezultata pretraživanja.

Npr. želimo ponoviti upit o web programiranju iz primjera s tražilicama. Koristit ćemo jedan od najpoznatijih metapretraživača – **Metacrawler**. Metacrawler koristi vlastita pravila za oblikovanje složenih upita pomoću logičkih operacija, koje onda prilagođava sintaksi svake pojedine tražilice kojoj upućuje upit. Upit bi glasio:

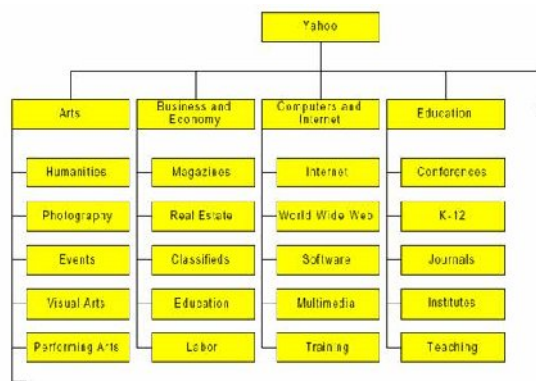


SLIKA 4.19: PRETRAŽIVANJE WEB TRAZILICA

- web and programming and (not job) and (cgi or asp)

4.6.3.3. Tematski katalogi

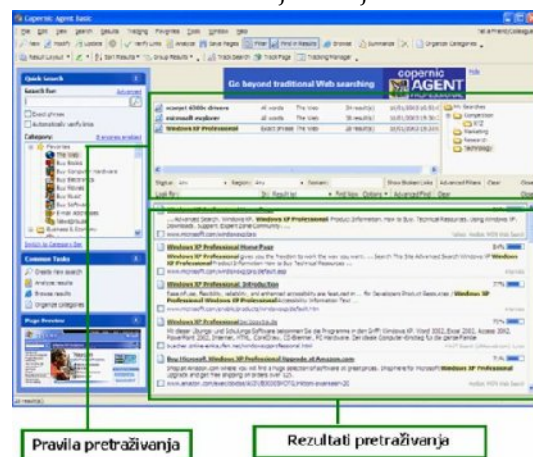
- Tematski katalogi (eng.subject trees) hijerarhijski su katalogi WWW stranica uređeni po temama.
- Karakteristike tematskih kataloga:
 - Svaka od tema u katalogu dijeli se u podteme, koje se onda mogu dalje dijeliti
 - Na najnižoj razini podtema nalaze se odabrane liste Web dokumenata posvećene toj temi
 - Dokumenti na listi najčešće su poredani abecednim redom
 - Da bi mogli uspješno pronaći željeni pojam u katalogu, moramo ga znati svrstati u odgovarajuće nadređene kategorije:
 - Počinjemo pretragu od prve razine tema i spuštamo se jednu razinu niže izborom odgovarajućeg tematskog područja
 - Ako na drugoj razini nismo pronašli ono što nas interesira, spuštamo se još jednu razinu niže izborom još užeg tematskog područja, itd. sve dok ne nađemo tražene informacije.
- Kako nastaju tematski katalogi?
 - Tematske kataloge rade ljudi koji analiziraju publikacije s Interneta, izabiru one koje se ističu svojom vrijednošću i katalogiziraju ih u temu kojoj pojedina publikacija najbolje odgovara.
 - Neke od kataloga razvijaju timovi administratora koji najčešće rade za neke tvrtke.
- Prednosti tematskih kataloga
 - Brzo i relativno lako se nalaze precizne informacije na Internetu
 - Prilično su rašireni na Internetu
 - Korak naprijed u indeksiranju mnoštva informacija na Internetu.
- Nedostaci tematskih kataloga
 - Iako pomoću njih lako možemo pronaći informacije o praktički svemu što nas zanima, obično su to svega 2-3 stranice, rijetko više
 - Stvaranje tematskih kataloga vremenski, a dakako i novčano iznimno je zahtjevan posao
 - Potreba za stalnim ručnim ažuriranjem.



SLIKA 4.20: ORGANIZACIJA SADRŽAJA NA TEMATSKIM KATALOGIMA (PRIMJER YAHOO)

4.6.3.4. Inteligentni agenti

- Inteligentni agenti su programi koji samostalno izvode neki zadatak u ime korisnika – jedan od takvih zadataka može biti i pretraživanje Web.
- Oni pretražuju Web slično kao i metapretraživači, korištenjem većeg broja samostalnih tražilica, ali razlike u odnosu na metapretraživače su sljedeće:
 - inteligentni agent je program instaliran na korisničkom računalu
 - oni posjeduju određenu razinu inteligencije koja im omogućava da razumiju želje svog vlasnika i postavljaju upite u njegovo ime
 - inteligentne agente prvo treba uvježbati
 - vlasnik mora definirati područja svog interesa, pravila pretraživanja, vremenska ograničenja, itd.
 - nakon toga vlasnik periodički provjerava performanse pretraživanja, ispravlja eventualne pogreške i detaljnije uvježbava agenta
- Postoje brojni inteligentni agenti koji pretražuju Web – npr. WebCompass, Copernic Agent...



SLIKA 4.21: INTELIGENTNI AGENTI

4.6.4. Vrednovanje informacija pronađenih na Internetu

- Dokumenti koje nalazimo na Web-u najčešće nisu ni na koji način filtrirani (za razliku od knjiga, časopisa i drugih resursa koje nalazimo u knjižnicama).
- Lakoća stvaranja Web dokumenata i nedostatak standarda kojih bi se autori Web dokumenata morali pridržavati dovode do toga da se kvaliteta sadržaja pronađenih Web dokumenata kreće u najširem mogućem rasponu – od izvanrednih do potpuno bezvrijednih.
- Zbog toga je nužna provjera Web dokumenata kako bi se u njih mogli pouzdati. Postoji više kriterija po kojima je moguće procjenjivati vrijednost Web dokumenta, od kojih su najvažniji sljedeći:
 - Autorstvo dokumenta
 - Institucija koja objavljuje dokument
 - Recenziranost dokumenta
 - Ažurnost dokumenta
- **Autorstvo dokumenta**
 - bitno je provjeriti je li autor dokumenta uopće naveden u dokumentu i da li je on poznat na tom području (npr. citiran od drugih i sl.)
 - pouzdanost će porasti ako je dokument referenciran od nekog drugog Web dokumenta izrađenog od poznatog autora ili ako se može naći biografija autora na Internetu
 - također korisno je provjeriti da li je dokument na autorovoj osobnoj Web stranici ili se nalazi na službenom poslužitelju institucije u kojoj je autor možda zaposlen.
- **Institucija koja objavljuje dokument**
 - ukoliko je institucija autor dokumenta, treba provjeriti da li se radi o poznatoj instituciji i da li navedeno njeno ime u dokumentu
 - na početnoj stranici (home page) možemo provjeriti da je dokument koji koristimo iz područja djelovanje te institucije
 - korisno je provjeriti i identitet Web poslužitelja na kojem se dokument nalazi.
- **Recenziranost dokumenta**
 - treba provjeriti da li institucija koja je objavila dokumente recenzira dokumente
 - ako se radi npr. o elektroničkom časopisu, potrebno je provjeriti da li se negdje u dokumentu izričito navodi da je dokument recenziran.
- **Ažurnost dokumenta**
 - odnosi se na datum objavljivanja i ažuriranja informacija u dokumentu
 - zato je potrebno provjeriti da li se navodi datum kada su podaci ažurirani
 - ukoliko postoji potreba za redovitim ažuriranjem onda je potrebno provjeriti i da li se navodi frekvencija ažuriranja informacija.

5. SIGURNOST I ZAŠTITA IS-a

5.1. Sigurnost IS-a

- Sigurnost, kao sve važnija komponenta računalnih sustava, spada u područje koje je u fazi intenzivnog napretka.
- Sigurnosni zahtjevi ovise o vrsti informacijskog sustava koji želimo štititi.
- Opća koncepcija sigurnosti ima svoje moralne i pravne aspekte koji se reguliraju zakonodavstvom i odgovarajućim kaznenim mjerama.
- Sigurnosne mehanizme možemo podijeliti na:
 - Zaštitu od vanjskih utjecaja,
 - Zaštitu ostvarenu sučeljem prema korisniku,
 - Unutarnje zaštitne mehanizme, te
 - Komunikacijske zaštitne mehanizme.
- Sigurnost računalnih sustava ostvaruje se ispunjavanjem triju osnovnih sigurnosnih zahtjeva:
 - **Tajnost** (informacije smiju biti pristupačne samo ovlaštenim osobama),
 - **Raspoloživost** (informacije moraju uvijek biti na raspolaganju ovlaštenim korisnicima),
 - **Besprijekornost** (informacije mogu mijenjati samo ovlašteni korisnici).

5.2.1. Pojam sigurnosti i zaštite IS-a

- Sigurnost informacijskog sustava predstavlja niz mjera i postupaka koji se poduzimaju da bi se omogućila funkcionalnost informacijskog sustava i integritet njegovog sadržaja u svim uobičajenim oblicima njegovog djelovanja. To je garancija da će taj sustav omogućiti nesmetano obavljanje operacija, odvijanje poslovnog procesa, i ispuniti zahtjeve koje postavljamo. Stupanj sigurnosti određuje se kvantitativnim veličinama do kojih se dolazi matematičkim i statističkim metodama procjene rizika i otpornosti na rizične situacije.
- Zaštita informacijskog sustava je skup metoda, postupaka, materijalnih i nematerijalnih mjera koje se poduzimaju u cilju smanjivanja ugroženosti informacijskog sustava od pretpostavljenih oblika prijetnji.
- Da bismo mogli provesti adekvatnu zaštitu informacijskog sustava, moramo napraviti:
 - *Procjenu značaja podatkovnog sadržaja* – izrađuje se na osnovi analize odnosa države prema pojedinoj vrsti podataka i evidencija koje se vode u poslovnom sustavu, te na osnovi interesa rukovodne strukture poslovnog sustava.
 - *Procjenu izvora i oblika prijetnji podatkovnom sadržaju* – izrađuje se temeljem rezultata prethodne procjene.

5.2.2. Izvori i oblici prijetnji sigurnosti IS-a

- Prijetnje se mogu klasificirati prema više kriterija:
 - načinu djelovanja (korupcija ili promjena informacije, krađa ili gubitak, otkrivanje, prekid usluga ili servisa);
 - mjestu nastanka (unutarnje, vanjske);
 - mjestu djelovanja (ljudski izvori, nosioci informacija, uređaji i oprema);
 - karakteru namjere (namjerne, nenamjerne, slučajne);
 - izvoru itd.
- Izvori prijetnji informacijskom sadržaju mogu se podijeliti na:
 - **prirodne prijetnje** - vatra, poplava, ekološko zagađenje, potres, bolesti, erupcije vulkana, zračenje, vremenske nepogode (oluje, snijeg, vrućina, vlaga, kiša, hladnoća), potres, vlaga i vrućina itd.
 - **čovjek s atribucijom namjernosti** - fizička sabotaža, elektronička sabotaža, špijunaža, ratna razaranja, građanski nemiri, protestni skupovi, otkrivanje informacija, krađa, prijevara itd.
 - **čovjek s atribucijom nenamjernosti** - nepažnja, neznanje, nemar, (ne)zanimanje itd.
 - **tehnička greška** - nestanak energije, kvar uređaja, havarije strojeva i uređaja, tehničke nesreće, preopterećenje, loša kvaliteta, neprimjeren operativni sustav, statički elektricitet, prašina;

- Oblike prijetnja informacijskom sadržaju, s obzirom na posljedice njihova djelovanja dijelimo na:
 - **Neautorizirano korištenje sadržaja** informacijskog sustava – uposlenik prenosi podatke za koje je procijenjeno da predstavljaju tajnu ili korist iz svog poslovnog sustava; krađa podataka iz informacijskog sustava
 - **Neidentificiranu promjenu informacijskog sadržaja** – ostavlja najteže i najdalekosežnije posljedice za informacijski sustav. Ulazi se uštićeno područje informacijskog sustava, te se uz krađu ili mimo nje promijene podaci informacijskog sustava
 - **Uništenje sadržaja** informacijskog sustava – najradikalnija metoda koja se i najrjeđe koristi, jer se najlakše otkriva.

5.2.3. Mjere zaštite podatkovnog sadržaja

- S obzirom na elemente informacijskog sustava, određuju se mjere i oblici zaštite informacijskog sustava.
- Zaštita podatkovnog sadržaja kroz zaštitu materijalnih nositelja podataka:
 - Podaci opisuju realno stanje sustava u određenom trenutku, pa su oni kao takvi nenadoknadivi. Podatkovni sadržaj ne može se koristiti u vremenu i prostoru ukoliko nije materijaliziran na nekom od materijalnih nositelja.
 - Štititeći materijalne nositelje, štitimo i podatke koji su na njima zapisani.

5.2.3.1. Fizičke i tehničke mjere zaštite

- Fizička zaštita podatkovnog sadržaja obuhvaća zaštitu računalne opreme, programa i datoteka od uništenja, neovlaštenog mijenjanja sadržaja, požara, poplave, oluja i drugih prirodnih katastrofa.
- Mjere fizičke zaštite ostvaruju se mjerama tehničke zaštite.
- Za ostvarivanje mjera fizičke i tehničke zaštite služimo se bravama, sefovima, protuprovalnim vitrinama itd.
- Mjere fizičke i tehničke zaštite ostvaruju se primjenom slijedećih mjera ili uređaja:
 - **vanjske prepreke** – organiziraju se u tri sloja zaštite
 - **zaštita zgrada**
 - **unutarnji sloj fizičke zaštite**
 - uređaji za detekciju
 - uređaji za identifikaciju (priključuju se izravno na računalo)
 - zaštita od sabotaze (sabotaža je namjerno uništenje dijela informacijskog sustava)
 - čuvari i patrole
 - **protupožarna zaštita.**

5.2.3.2. Programske mjere zaštite

- Na razini operacijskog sustava:
 - jedнокorisnički, višekorisnički operacijski sustavi
 - zaštita korisničke okoline
 - zaporke.
- Mjere zaštite na razini korisničkih programa:
 - zaporke za pokretanje korisničkih programa i njegovih hijerarhijski ustrojenih dijelova
 - brisanje mape u koju su pohranjeni brisani podaci
 - upotreba DBMS sustava.
- Sigurnosno kopiranje promjenom materijalnog nositelja:
 - svrha: ponovno vraćanje podataka u sustav u slučaju gubitka podataka iz računalnog sustava
 - najpoznatije tehnike su:
 - **potpuno kopiranje** – pohranjuju se sve datoteke bez obira da li su označene za pohranu ili ne,

- **diferencijalno kopiranje** – pohranjuje nove datoteke i one datoteke koje su označene kao nearhivirane, i
 - **inkrementalno kopiranje** – pohranjuje one datoteke na kojima postoji atribut archive (archive).
- Kriptiranje kao mjera zaštite u mrežnoj komunikaciji
 - javlja se zbog dislociranosti pojedinih poslovnih jedinica
 - mora osigurati jednoznačnost prijenosa i onemogućiti neautorizirano korištenje ili promjenu sadržaja u prijenosu
 - utjecati se može na promjenu komunikacijskog sadržaja preko komunikacijskog kanala na različite načine:
 - prisluškivanje
 - prekid u komunikaciji
 - promjena komunikacijskog sadržaja
 - generiranje nepostojećeg sadržaja.
 - Zaštita od virusa
 - **računalni virus** je program posebne namjene koji je najčešće destruktivnog karaktera (uništenje podataka i programa na "zaraženom" računalu)
 - virusi mogu biti destruktivni i/ili bezopasni
 - razlikujemo više vrsta zlonamjerno napisanih programa:
 - **crv** – samostalan program koji se širi kroz mrežu samoumnožavanjem
 - **trojanski konj** – program koji služi za izvršavanje drugih operacija, a ne onih za koje je deklariran
 - **logička bomba** – nije cjelovit mehanizam, već je najčešće sastavni dio zlonamjerno napisanih programa
 - **zamka** – nedokumentirana funkcija programa koja se pokreće unaprijed definiranim načinom
 - **virus** – dio programskog koda sa sposobnošću samokopiranja (infekcije), te dodavanja vlastitog sadržaja u druge programe ili dijelove operacijskog sustava. Virus lako mogu izbjeći sve ostale mjere zaštite, pa se zato moraju poduzeti:
 - preventivne mjere (organizacijske, nadzorne i sanacijske)
 - mjere sanacije štete.
 - Zaštitni zid (Firewall)
 - to je inteligentni sustav programa koji se postavlja na odvojeno računalo (ili ulazno računalo u lokalnu mrežu), a zadaća mu je da onemogućava pristup u lokalnu mrežu neautoriziranim korisnicima ili sadržajima koji nisu u protokolu razmjene
 - nad razmjenom poruka izvodi se (a) autorizacijskim opslužiteljem i (b) selektiranjem, odabirom, te kontrolom ulaznog sadržaja.

5.2.3.3. Organizacijske mjere zaštite

- Organizacijske mjere poduzima poslovni sustav da bi se osigurala željena razina funkcionalnosti sustava i integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji.
- Tim mjerama ne degradira se rad sustava, već se doprinosi raspoloživosti i djelotvornosti čitavog sustava.
- Mjere se razlikuju ovisno o području rada i vrsti djelatnosti pojedinog poslovnog sustava.

5.2.3.4. Mjere zaštite iz oblasti prava

- Pravni aspekt zaštite informacijskog sustava odnosi se na poštivanje svih pravnih norma koje donosi država kao pravni okvir za ostvarivanje mjera zaštite.
- Potrebno je ugraditi sve pravne odredbe jedne države kako bi se osigurali integritet i raspoloživost podataka.
- Time se postiže jednaka razina zaštite jednake podatkovne strukture u svim sredinama bez obzira na državu u kojoj to bilo.

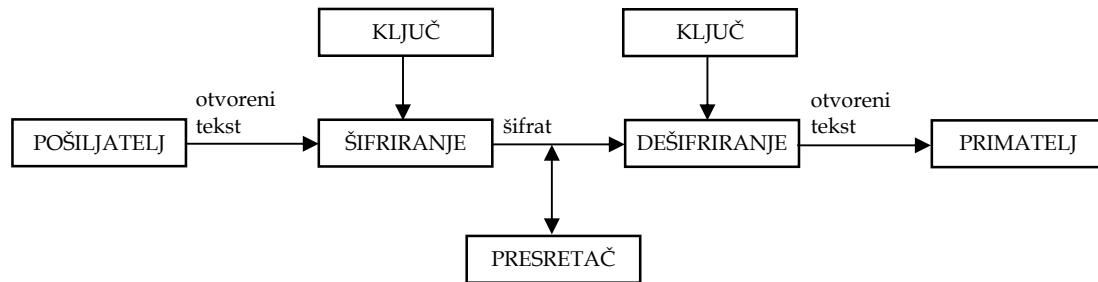
5.2.4. Kriptografija i sigurnosni mehanizmi

- **Kriptiranje** ili šifriranje postupak je kojim se razumljivi tekst prevodi u uljezu nerazumljivi kriptirani tekst. Obrnuti postupak prevođenja kriptiranog teksta u razumljivi tekst nazivamo dekriptiranjem ili dešifriranjem. Današnje gledanje na postupke kriptiranja svodi se na uporabu algoritama kriptiranja koji se u skraćenom obliku mogu zapisati:

$$C = E(P, Ke)$$

- gdje je P razgovjetni tekst, Ke ključ kriptiranja, E funkcija kriptiranja i C kriptirani tekst.
- **Dekriptiranje** se svodi na uporabu pripadne funkcije dekriptiranja D, koja uz uporabu ključa dekriptiranja Kd, pretvori kriptirani tekst natrag u razgovjetni tekst, tj. možemo pisati da je:

$$P = D(C, Kd)$$

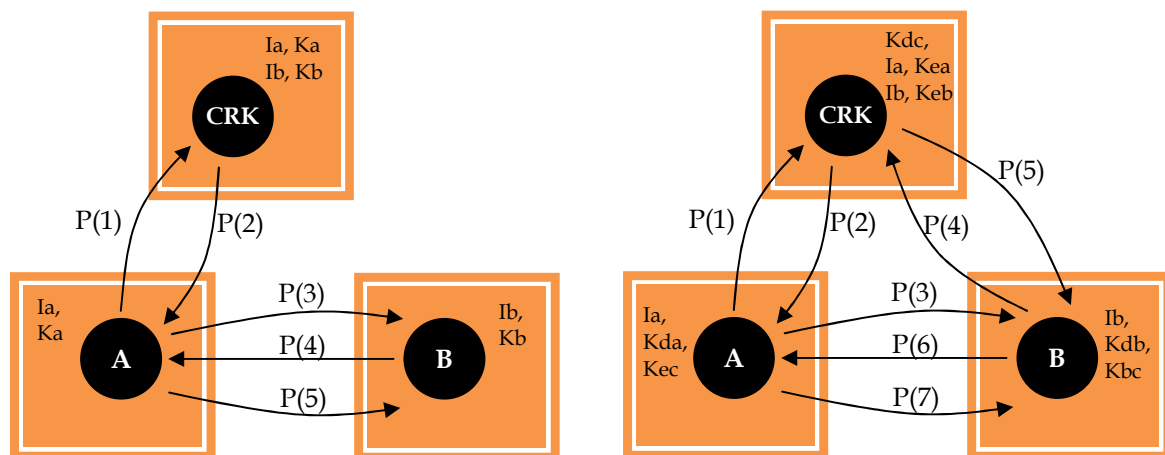


SLIKA 5.1: OSNOVE KRIPTIRANJA

SIMETRIČNI KRIPTOSUSTAV

- Najpoznatiji današnji simetrični kriptosustav (sustav s tajnim ključem) je poznat po svojoj kratici DES (od eng. Data Encryption Standard). On je izvorno razvijen u tvrtki IBM i kasnije prihvaćen kao standard u SAD-u godine 1977. Do danas nije objavljeno ni jedno razbijanje DES kriptiranja.
- DES se zasniva na logičkoj operaciji isključiva ILI. Označimo li dvije moguće vrijednosti logičke varijable s 0 i 1, operacija XOR dat će kao rezultat vrijednost jedan onda kada samo jedna od ulaznih vrijednost ima vrijednost jedan.

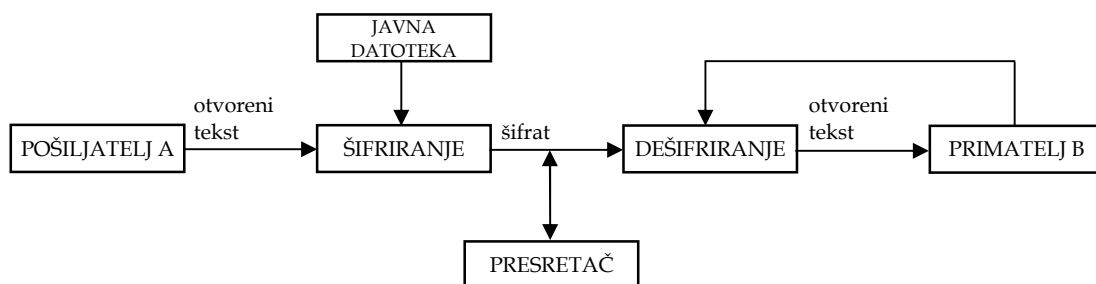
ASIMETRIČNI KRIPTOSUSTAV



PROCES DODJELE TAJNOG KLJU A	NADZOR JAVNIH KLJU EVA U ASIMETRI NOM SUSTAVU
CRK - centar za raspodjelu ključeva	Ia, Ib - identifikatori korisnika A i B
Ia, Ib - identifikatori korisnika A i B	Kec, Kdc - javni i tajni ključ centra
Ka, Kb - tajni ključevi korisnika A i B	Keb, Kdb - javni i tajni ključ sudionika a
	Kea, Kda - javni i tajni ključ sudionika b

SLIKA 5.2: DODJELA I NADZOR KLJU EVA

- Najpoznatiji današnji asimetrični kriptosustav razradili su Rivest, A. Shamir i L. Adleman i on je njihovim početnim slovima nazvan RSA sustavom. Taj se sustav zasniva na teoriji brojeva:
- Odabiru se dva velika prosta broja P i Q ($P > 10$ na 100, $Q > 10$ na 1000).
- Odredi se umnožak $N = P * Q$, te vrijednost $(P - 1) * (Q - 1)$ koju označujemo s $L(N)$.
- Odabire se broj d tako da bude $\max(P, Q) < d < L(N)$.
- Izračunava se broj e tako da bude $0 < e < L(N)$ i da je $(e * d) \bmod L(N) = 1$ što je isto kao da odredimo najmanji k za koji vrijedi $e * d = k * L(N) + 1$.
- Par (e, N) proglašava se javnim ključem.
- Samo vlasnik ključa poznaje broj d i može dekriptirati kriptirani broj, tako da par (d, N) predstavlja tajni ključ. Bit postupka sastoji se u tome da se samo poznavanjem brojeva e i N vrlo teško može odrediti d.
- Dodjela ključeva u simetričnom kriptosustavu
 - U raspodjeljenom sustavu svi sudionici imaju svoj identifikator i pohranjuju samo vlastiti tajni ključ. Centar za raspodjelu tajnih ključeva poznaje tajne ključeve svih korisnika. Kada korisnik A zaželi komunicirati s korisnikom B, onda on mora zatražiti od centra tajni ključ koji će vrijediti samo za tu komunikaciju. Protokol za dodjelu tog ključa koji su predložili R.M. Nedham i M.D. Schroeder, sastoji se od pet poruka P(1) do P(5), kako je ilustrirano na slici 1. (broj u zagradi označava redosljed poruka). Centar za raspodjelu ključeva sadrži tablicu svih tajnih ključeva tako da uz identifikatore Ia i Ib, koji su javno poznati, može pridružiti tajne ključeve Ka i Kb. Na traženje korisnika A koji želi komunicirati s korisnikom B centar će dodijeliti jednokratni tajni ključ Kab.
- Nadzor javnih ključeva u asimetričnom kriptosustavu
 - Korisnik A koji želi komunicirati s korisnikom B uporabom javnog ključa želi biti siguran da je objavljeni ključ pravi ključ korisnika B. Drugim riječima, protokol nadzora javnih ključeva u asimetričnom kriptosustavu ujedno je i protokol autentifikacije sudionika u komuniciranju. Svi sudionici u komuniciranju imaju svoj javni ključ Ke i svoj tajni ključ Kd. Oni moraju biti prijavljeni centru za nadzor javnih ključeva. U centru se oblikuje tablica javnih ključeva svih potencijalnih sudionika u komunikaciji, a tajni ključevi pohranjeni su samo u čvoru pojedinih korisnika. Centar nadzora također ima svoj par ključeva, a svi sudionici u komuniciranju znaju javni ključ centra. Slika 2. ilustrira dio sustava u kojem želimo uspostaviti pouzdani komunikacijski kanal između sudionika A i B (i to na zahtjev korisnika A). Centar sadrži tablicu javnih ključeva i poznaje svoj tajni ključ Kdc. Javni ključ centra Kec poznat je svim sudionicima koji su registrirani u centru. Protokol se izvodi slanjem sedam poruka od P(1) do P(7).



SLIKA 5.3: KRIPTOSUSTAV S JAVNIM KLJUČEM

KRAJ.