

**UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA**

Magistrsko delo

**ELEMENTI TEHNIČNE PODPORE UPORABNIKOM PREKO
INTERNETA**

V Ljubljani, september 2003

Marjan Schaubach

IZJAVA

Študent Marjan Schaubach izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Andreja Kovačiča in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne: _____

Marjan Schaubach

VSEBINA

| | | |
|-----------|--|-----------|
| 1. | Uvod..... | 1 |
| 1.1. | Izhodišča naloge..... | 1 |
| 1.2. | Problematika - področje preučevanja..... | 2 |
| 1.3. | Namen raziskave, teze in omejitve..... | 4 |
| 1.4. | Cilji raziskave..... | 5 |
| 2. | Metodološke osnove načrtovanje informacijskih sistemov..... | 6 |
| 2.1. | Vloga modeliranja pri načrtovanju IS..... | 6 |
| 2.2. | Linearni pristop..... | 7 |
| 2.3. | Prototipni pristop..... | 8 |
| 2.4. | Objektni pristop..... | 9 |
| 2.5. | Modularno programiranje..... | 9 |
| 2.5.1. | Porazdeljene aplikacije..... | 11 |
| 2.6. | Vloga strežnikov..... | 13 |
| 2.6.1. | Osnovni razlogi za implementacijo aplikacijskih strežnikov..... | 13 |
| 2.6.2. | Delovanje aplikacijskega strežnika..... | 16 |
| 2.6.3. | Microsoftov transakcijski strežnik..... | 17 |
| 2.6.4. | Povzetek..... | 17 |
| 2.7. | Standardizacija..... | 18 |
| 2.7.1. | Sistem kakovosti..... | 18 |
| 2.7.2. | Standardi skupine ISO 9000:2000(E)..... | 18 |
| 3. | Portal..... | 21 |
| 3.1. | Komponente poslovnih portalov..... | 21 |
| 3.1.1. | Prednosti implementacije in uporabe poslovnih portalov..... | 25 |
| 3.2. | Storitve tretje stranke v poslovanju..... | 26 |
| 3.3. | Virtualne skupnosti..... | 26 |
| 3.4. | Ponudniki storitev v vrednostni verigi..... | 27 |
| 4. | Zaščita in varovanje podatkov..... | 30 |
| 4.1. | Temeljne zahteve varnosti..... | 31 |
| 4.1.1. | Varnost na internetu..... | 32 |
| 4.1.2. | Okolje..... | 32 |
| 4.2. | Vrste napadov..... | 33 |
| 4.2.1. | Prisluškovanje komunikacijskemu kanalu..... | 34 |
| 4.2.2. | Spreminjanje..... | 34 |
| 4.2.3. | Nepooblaščen uporaba virov..... | 34 |
| 4.2.4. | Nepooblaščen razkritje informacij..... | 34 |
| 4.2.5. | Analiza prometa..... | 34 |
| 4.2.6. | Bankomati..... | 34 |
| 4.2.7. | Varnost strežnika..... | 35 |
| 4.2.8. | Človeški dejavnik..... | 35 |
| 4.2.9. | Zanesljivost programske opreme..... | 35 |
| 4.3. | Varnostne storitve..... | 35 |
| 4.4. | Kriptografski mehanizmi..... | 36 |
| 4.4.1. | Šifriranje..... | 36 |
| | Varnost šifrirnih algoritmov..... | 38 |
| 4.4.2. | Elektronski podpis..... | 38 |
| 4.4.3. | Digitalni certifikati..... | 39 |

| | | |
|-----------|--|-----------|
| 4.5. | Zakonodaja in pravni okvir | 41 |
| 5. | Podatkovno rudarjenje za splet | 42 |
| 5.1. | Rudarjenje za ugotavljanje uporabe spleta | 43 |
| 5.1.1. | Modeliranje uporabnikov | 43 |
| 5.2. | Iskanje informacij in iskanje podatkov | 45 |
| 5.2.1. | Iskanje vsebine spletnih strani | 45 |
| 5.2.2. | Načini iskanja informacij | 47 |
| | Iskanje po celotni vsebini | 48 |
| | Iskanje po delu vsebine | 48 |
| 5.2.3. | Medjezično iskanje | 49 |
| 5.3. | Digitalne knjižnice in vzpostavljanje povezav do informacij | 53 |
| 5.4. | Boolejeva metoda | 53 |
| 5.5. | Indeksiranje z LSA | 54 |
| 5.5.1. | Model vektorskega prostora | 55 |
| 5.5.2. | Latentna semantična analiza (LSA) in razčlemba izrazov (SVD) | 56 |
| 5.6. | Iskalni stroji | 58 |
| 5.6.1. | Razvoj iskalnih strojev | 58 |
| 5.6.2. | Delovanje iskalnih strojev | 59 |
| 5.6.3. | Meta iskalni stroji | 62 |
| 5.6.4. | Knjižnice | 63 |
| 5.7. | Nevronske mreže | 64 |
| 5.7.1. | Pomen nevronske mreže | 65 |
| 5.7.2. | Tržne rešitve | 65 |
| 5.7.3. | Varnostne rešitve | 66 |
| 6. | Informatika v KDD | 67 |
| 6.1. | Poslanstvo družbe | 67 |
| 6.1.1. | Zagotavljanje storitev KDD | 67 |
| 6.1.2. | Uporabniki trga vrednostnih papirjev | 67 |
| | Člani KDD | 69 |
| | Izdajatelji VP | 69 |
| | Uporabniki informacijske tehnologije KDD | 70 |
| 6.1.3. | Uporabljene tehnologije v CRVP | 71 |
| 6.2. | Analiza obstoječega stanja | 72 |
| 6.2.1. | Portal KDD | 72 |
| 6.2.2. | Navodila | 72 |
| | Izdajatelji VP | 72 |
| | Člani - intranet | 73 |
| 6.3. | Predlog sprememb | 74 |
| 6.3.1. | Dostop do navodil | 74 |
| 6.3.2. | Obveščanje neplačnikov | 74 |
| 6.3.3. | Avtomatski prenosi – brez uporabe spletnega brskalnika | 74 |
| 6.3.4. | Pogosto zastavljena vprašanja | 74 |
| | Certifikat | 74 |
| | Dostop do datotek | 75 |
| | Program »Knjiga imetnikov« | 75 |
| 6.4. | Programski paket ReactPro | 75 |
| 6.4.1. | Namen uporabe | 75 |
| 6.4.2. | Končni cilji | 76 |

| | | |
|--------|--|-----------|
| 6.4.3. | Baza podatkov | 76 |
| | Partnerji..... | 76 |
| | Kontaktne osebe | 77 |
| | Problemi..... | 77 |
| | Zbiranje problemov | 78 |
| | Vnos problema..... | 79 |
| | Razporejanje problemov | 80 |
| | Reševanje | 80 |
| | Vključevanje in iskanje problemov na intranet-u | 80 |
| | Ustvarjanje baze znanja | 80 |
| 6.4.4. | Arhiviranje | 80 |
| 6.4.5. | Poročanje nadrejenim | 81 |
| 6.5. | Konstrukcija in prikaz modela pomoči uporabnikom | 81 |
| 6.6. | Ugotovitve ob prikazanem modelu..... | 83 |
| 6.7. | Analiza predlaganega modela | 83 |
| 7. | Sklepne ugotovitve | 85 |
| 8. | LITERATURA..... | 87 |

Kazalo slik

| | | |
|-----------|--|----|
| Slika 1: | Etape življenjskega cikla | 7 |
| Slika 2: | Značilne razvojne faze IS v okviru sodobnejših metodoloških pristopov..... | 8 |
| Slika 3: | Primer starega programiranja | 10 |
| Slika 4: | Primer današnjega programiranja osnovanega na komponentah..... | 10 |
| Slika 5: | Programska arhitektura Windows NT | 11 |
| Slika 6: | Tradicionalna arhitektura odjemalec strežnik (dvoslojna) | 12 |
| Slika 7: | Troslojna arhitektura odjemalec strežnik..... | 12 |
| Slika 8: | Delovanje programa pri uporabi terminala | 13 |
| Slika 9: | Delovanje sistema odjemalec – strežnik | 14 |
| Slika 10: | Delovanje sistema odjemalec – strežnik v internet okolju | 15 |
| Slika 11: | Zgradba aplikacijskega strežnika | 16 |
| Slika 12: | Model sistema vodenja kakovosti, osnovan na procesih | 19 |
| Slika 13: | Osnovne komponente poslovnih portalov | 22 |
| Slika 14: | Udeleženci v ASP vrednostni verigi | 27 |
| Slika 15: | Primerjava med tradicionalno in elektronsko vrednostno verigo | 28 |
| Slika 16: | Vrednostna veriga ASP-jev | 29 |
| Slika 17: | Trend povečevanja števila kodnih vrstic OS | 30 |
| Slika 18: | Elementi v globalni strategiji zaščite | 31 |
| Slika 19: | Poenostavljen model povezave preko interneta. | 32 |
| Slika 20: | Simetrično šifriranje | 36 |
| Slika 21: | Tabela algoritmov | 37 |
| Slika 22: | Asimetrično šifriranje..... | 38 |
| Slika 23: | Generiranje digitalnega podpisa in preverjanje | 39 |
| Slika 24: | Hierarhija certificiranja | 40 |
| Slika 25: | Podatkovno rudarjenje za splet..... | 42 |
| Slika 26: | Razlika med iskanjem podatkov in informacij | 45 |

| | | |
|-----------|--|----|
| Slika 27: | Problemi jezikovnih analiz tekstualnih informacij | 46 |
| Slika 28: | Klasifikacija sistemov za iskanje informacij..... | 47 |
| Slika 29: | Primer opisa »Lastnosti dokumenta - Properties« v Word2000 | 48 |
| Slika 30: | Struktura jezikoslovnih procesorjev..... | 50 |
| Slika 31: | Shema inteligentnega stroja za pridobivanje informacij | 51 |
| Slika 32: | Primerjava tehnologij za IR..... | 52 |
| Slika 33: | Funkcionalni pogled na IR | 53 |
| Slika 34: | Princip Boolejeve metode | 54 |
| Slika 35: | Predstavitev dokumentov v vektorskem prostoru..... | 55 |
| Slika 36: | Skupine dokumentov v vektorskem prostoru | 55 |
| Slika 37: | Shematski prikaz razčlenbe vrednosti matrike $t \times d$ – izrazi po dokumentih | 57 |
| Slika 38: | Shematski prikaz skržene matrike X_S | 57 |
| Slika 39: | Trosmerna učinkovitost iskalnega stroja | 59 |
| Slika 40: | Shematski prikaz delovanja iskalnega stroja | 60 |
| Slika 41: | Delovanje spletnega pajka..... | 61 |
| Slika 42: | Razmerje uporabe iskalnikov v obdobju januar 2003 v ZDA..... | 62 |
| Slika 43: | Primer povezave iskalnikov | 64 |
| Slika 44: | Povezave zunanjih uporabnikov s KDD | 68 |
| Slika 45: | Pregled načina prejema DK..... | 70 |
| Slika 46: | Osnovna spletna stran za člane KDD | 73 |
| Slika 47: | Pregled izdelanih certifikatov po mesecih | 78 |
| Slika 48: | Model delovanja HD v okviru IS KDD | 82 |

Priloge

| | | |
|------------|---|---|
| Priloga 1: | Primeri iskanja z Boolejevo metodo..... | 1 |
| Priloga 2: | Primer uporabe LSA | 2 |
| Priloga 3: | Pomen kratic | 7 |
| Priloga 4: | Razlaga nekaterih kratic | 9 |

1. Uvod

1.1. Izhodišča naloge

Od izdelave prvega splošnega računalnika imenovanega ENIAC leta 1946 do danes je razvoj na področju informacijske tehnologije (IT) in telekomunikacij (TK) napredoval v obsegu, ki ga težko dojamemo. Pred rojstvom internet-a v začetku sedemdesetih let (v obdobju velikih računalnikov – Mainframe) so priznani računalniški strokovnjaki napovedovali, da bo leta 2000 na svetu le nekaj velikih računalnikov, ki bodo pokrivali potrebe po informacijah celotnega svetovnega prebivalstva. Na srečo ali žalost se njihova napoved ni uresničila.

S koncentracijo podatkov na le nekaj računalnikih bi bili ti iz strateškega in varnostnega vidika veliko bolj ranljivi in občutljivi. Vsebinsko bi bilo možno kontrolirati in cenzurirati, zato bi bilo te podatkovne baze bistveno manj obsežne, iskanje določenih podatkov in informacije pa veliko lažje.

Danes je na svetu več sto milijonov najrazličnejših računalnikov samostojnih ali povezanih v računalniška omrežja. Internet pa omogoča dostop do spletnih strani kateregakoli računalnika, ki je povezan v to svetovno omrežje.

Informatika in sodobne komunikacijske rešitve so tudi na področju poslovanja z vrednostnimi papirji povzročile bistvene spremembe. Organizirano poslovanje z vrednostnimi papirji poteka v nematerializirani obliki, kar v praksi pomeni zamenjavo listin v pisni obliki z zapisi v elektronski (računalniški) obliki.

V skladu z uredbo vlade in zakonom, se zaključuje proces privatizacije in podjetja (v nadaljevanju izdajatelji) so izdala delnice v nematerializirani obliki v centralnem registru Klirinško depotne družbe d.d. (v nadaljevanju KDD). Slovenija je tako ena prvih držav, ki je v fazi tranzicije uspela s primerno organizacijo trga postaviti dematerializirano in informatizirano okolje poslovanja z vrednostnimi papirji.

Elektronsko poslovanje (e-poslovanje) je z vidika države, ki se pripravlja na vstop v EU in s tem širitvijo blagovne, kot tudi informacijske menjave, zelo pomembno tudi za KDD. Varno in zanesljivo elektronsko poslovanje zahteva:

- strateško načrtovanje razvoja informacijskih sistemov (IS),
- zagotavljanje enotnih metodologij in standardov,
- razvoj, prenova in integracija aplikativnih rešitev,
- planiranje in izvajanje nabav, zamenjava in vzdrževanje opreme,
- kontinuiran nadzor in implementacija rešitev,
- zagotavljanje pravnih in organizacijskih pogojev za implementacijo,
- uvajanje in pomoč uporabnikom,
- zagotavljanje kakovosti izvedenih postopkov in rešitev,
- zagotavljanje zaščite in varovanja podatkov.

Prenova informacijskega sistema mora izkoristiti vse možnosti, ki jih nudi hiter razvoj računalništva in komunikacij. S sistemsko analizo informacijskih potreb in

ovrednotenjem dosežkov in smeri razvoja informacijske tehnologije, je potrebno najti rešitev, ki bo zagotavljala optimalno življenjsko dobo, z minimalnimi stroški pri uporabi novih dosežkov.

1.2. Problematika - področje preučevanja

Čeprav je postavitve informacijskega sistema v KDD sorazmerno nova, je potrebno nenehno širjenje in posodabljanje, tako strojne kot programske opreme. Zelo pomembne so povezave s člani in Ljubljansko borzo s katero si KDD deli komunikacijsko infrastrukturo. Zanimariti pa se ne sme izdajateljev vrednostnih papirjev, ki najmanj enkrat mesečno dobivajo podatke o imetnikih vrednostnih papirjev, kakor tudi ne občanov, ki želijo informacije pri prodaji, nakupu ali o stanju svojih vrednostnih papirjev.

Namen poslovanja KDD ter sistema centralnega registra nematerializiranih vrednostnih papirjev je povečanje učinkovitosti poslovanja na trgu vrednostnih papirjev, in sicer:

- varno, enostavno in razumljivo poslovanje z vrednostnimi papirji (iz tehničnega in operativnega vidika) na celotnem trgu vrednostnih papirjev,
- »sočasno« izpolnjevanje denarnih obveznosti in obveznosti prenosov vrednostnih papirjev na podlagi poslov, sklenjenih na organiziranem trgu (borza),
- dosledna in natančna pravila celotnega poslovanja z vrednostnimi papirji preko KDD,
- sodobna in zanesljiva tehnična oziroma informacijska podpora poslovanja z vrednostnimi papirji,
- podrobno opredeljeni operativni postopki vseh področij poslovanja z vrednostnimi papirji prek KDD,
- manjši neposredni in posredni stroški poslovanja z vrednostnimi papirji, tako za imetnike vrednostnih papirjev kot za člane KDD in izdajatelje,
- učinkovita tehnična in operativna podpora zagotavljanja funkcije nadzora na trgu vrednostnih papirjev,
- uskladitev poslovanja z vrednostnimi papirji z mednarodnimi standardi.

Eden od ciljev KDD je uporaba moderne in učinkovite informacijske tehnologije pri zagotavljanju sistema poslovanja z vrednostnimi papirji ter vodenju centralnega registra nematerializiranih vrednostnih papirjev. Fizično izdane (tiskane) vrednostne papirje so z začetkom poslovanja KDD nadomestili nematerializirani vrednostni papirji. Lastništvo vrednostnih papirjev je torej vezano na vknjižbe in preknjižbe na računih vrednostnih papirjev imetnikov. Tehnologija, ki jo uporablja KDD, zagotavlja enostaven in zanesljiv dostop do podatkov, tudi imetnikom vrednostnih papirjev; člani KDD namreč v imenu in za račun imetnikov vodijo njihove račune in opravljajo preknjižbe.

KDD si prizadeva spremljati tehnološki razvoj in upoštevati najvišje tehnološke standarde pri vzpostavljanju in izpopolnjevanju informacijskega sistema poslovanja z

vrednostnimi papirji, ter vodenja centralnega registra nematerializiranih vrednostnih papirjev.

V KDD se je vodstvo odločilo, da svojim partnerjem (Borza vrednostnih papirjev, Člani, Izdajatelji VP) in drugim omogoči dostop do podatkov preko intraneta oziroma interneta. Svojo spletno stran in ponudbo nekaterih storitev na internetu je KDD objavila junija 1999.

Poleg splošnih podatkov, ki so dosegljivi vsem, imajo člani KDD možnost dostopa do svojih podatkov preko Intraneta in izdajatelji vrednostnih papirjev do podatkov njihove delniške knjige preko interneta. Internet naj bi v prihodnosti v celoti nadomestil posredovanje podatkov izdajateljem na disketi, vendar sedanje stanje pri izdajateljih tega v celoti ne dopušča, saj tehnično niso vsi dovolj opremljeni (nimajo dostopa do interneta) in nekateri zaradi bojazni (niso dovolj usposobljeni) ali odpora do novih tehnologij.

IZPOLNJEVANJE PRIPOROČIL G30

Postopek trgovanja z vrednostnimi papirji in s tem postopek izpolnitve obveznosti, je bistven element vsakega učinkovito organiziranega trga vrednostnih papirjev. Mednarodni standardi predstavljajo enotna načela, ki naj bi pripomogla k zagotovitvi učinkovitega, varnega in stabilnega trga vrednostnih papirjev. Skupina 30 najbolj razvitih držav (G 30) je zato oblikovala devet specifičnih in konkretnih priporočil o delovanju sistemov izpolnjevanja obveznosti, ki naj bi jih upoštevali na vsakem razvitem trgu vrednostnih papirjev. Na slovenskem trgu vrednostnih papirjev je osem od devetih priporočil v celoti upoštevanih, večina z delovanjem sistema izpolnjevanja obveznosti prek KDD.

Priporočilo št.1: Vse "primerjave" poslov na organiziranem trgu vrednostnih papirjev med neposrednimi udeleženci trga (člani borze) naj bi bile izvršene najpozneje dan po sklenitvi poslov (T + 1).

Priporočilo št.2: Posredni udeleženci organiziranega trga vrednostnih papirjev (kot so institucionalni investitorji ali drugi investitorji, ki niso borzni posredniki) naj bi bili člani sistema primerjave, ki omogoča enostransko potrditev pogojev posla.

Priporočilo št.3: Vsaka država naj bi imela učinkovit in popolno razvit centralni depo vrednostnih papirjev, ki naj bi bil organiziran tako, da spodbuja čim širši krog neposrednih udeležencev na trgu vrednostnih papirjev.

Priporočilo št.4: Vsaka država naj bi na podlagi obsega poslov in števila udeležencev trga preučila, ali bi vpeljava "neto" sistema izpolnjevanja obveznosti pomenila učinkovitejši in manj tvegan način izpolnjevanja obveznosti iz sklenjenih poslov z vrednostnimi papirji.

Priporočilo št.5: Kot način izpolnjevanja obveznosti iz sklenjenih poslov z vrednostnimi papirji naj bi bil vpeljan sistem "izročitev proti plačilu" (delivery versus payment).

Priporočilo št.6: Izpolnitev obveznosti plačila iz sklenjenih poslov z vrednostnimi papirji naj bi bila izvršena po načelu "denar istega dne" (ang. same day funds).

Priporočilo št.7: Na vseh trgih vrednostnih papirjev naj bi bil vpeljan sistem "krožne izpolnitve obveznosti" (ang. rolling settlement). Dan izpolnitve obveznosti naj bi bil tri delovne dni po sklenitvi posla (T + 3).

Priporočilo št.8: Države naj bi spodbudile posojanje vrednostnih papirjev kot način izboljšanja sistema izpolnjevanja obveznosti iz sklenjenih poslov. Morebitne regulativne in davčne omejitve, ki otežujejo prakso posojanja vrednostnih papirjev, naj bi bile ukinjene.

Priporočilo št.9: Vsaka država naj bi uveljavila mednarodne ISO (International Standardization Organization) standarde, ki se nanašajo na sporočila v zvezi z vrednostnimi papirji.

1.3. Namen raziskave, teze in omejitve

Namen raziskave je sistematsko prikazati teoretične in praktične ugotovitve s področij:

- načrtovanja informacijskih sistemov,
- modularnega programiranja,
- standardizacije,
- izgradnje poslovnih portalov,
- zaščita in varovanje podatkov,
- podatkovnega rudarjenja za splet,
- iskanja informacij na spletu.

Posebno poglavje je posvečeno področju zaščite in varovanja podatkov, ki je pri poslovanju z vrednostnimi papirji primarnega pomena. Pri tem je potrebno upoštevati omejitve, da se nebi zapletali v podrobnosti in razkrivali varnostne politike KDD.

Postavitev spletne strani, brez ugotavljanja in merjenja odziva uporabnikov na objavljeno vsebino ali storitev na spletu, ni dovolj. Potrebna je jasna in natančna informacija o tem, kateri uporabniki dostopajo do naših internet strani, kako pogosto se vračajo na strani, katere informacije jih zanimajo, kako dolgo brskajo po podstraneh, od kod prihajajo in še bi lahko našteval. Investicija v izdelavo spletne strani ne sme biti le strošek, ne da bi vedeli kakšen je učinek.

Pri reševanju problemov je pogosto potrebno iskati podatke in informacije na spletu. Poznavanje načinov pridobivanja informacij oziroma podatkov in delovanja iskalnih sistemov, lahko bistveno skrajšajo čase reševanja problemov.

Z vstopom Slovenije v EU in prilagoditvijo zakonodaje, ki bo prekinila monopolni položaj, se bo tudi KDD soočila s konkurenco tujih klirinško depotnih družb. Zato mora za dobre odnose in zadovoljstvo strank poskrbeti že danes.

1.4. Cilji raziskave

V nalogi želim sistematično prikazati vpliv sodobne tehnologije na tehnično podporo uporabnikom informacijskih storitev v KDD. V teoretskem delu bom poskušal pojasniti problematiko pri načrtovanju informacijskega sistema ter vlogo in pomen aplikacijskih strežnikov, ki so sestavni del spletno orientiranih informacijskih sistemov.

Predstavljal bom komponente poslovnih portalov, ki predstavljajo vstopno točko do informacijskih virov na internetu, ter storitve tretjih strank, ki omogočajo uporabnikom dostop in uporabo interneta .

Zaščita in varovanje podatkov sta v svetu, ki postaja vedno bolj povezan in globaliziran ključnega pomena. Opremo in podatke lahko ustrezno zaščitimo in varujemo le, če poznamo nevarnosti, ki nas pri delu ogrožajo in načine za doseganje varnega poslovanja.

Pri iskanju informacij na svetovnem spletu si lahko pomagamo z različnimi iskaniki in orodji, ki lahko pri tehnični podpori uporabnikom skrajšajo odzivne čase. Med cilje raziskave zato sodi tudi področje iskanja informacij na spletu.

Na podlagi pridobljenega znanja in izkušenj zgraditi model primerne tehnične podpore in vzdrževanje aplikacij preko interneta, ki bo za KDD predstavljal:

- evidenco in pregled podpore,
- zbiranje, pregled in obravnavanje pripomb oziroma napak,
- nadgradnja programske opreme preko intraneta oziroma interneta,
- zmanjšanje stroškov vzdrževanja programske opreme,
- skrajšanje odzivnih časov pri podpori uporabnikom.

2. Metodološke osnove načrtovanje informacijskih sistemov

Pri načrtovanju razvoja informatike mora podjetje zagotoviti enotno in celovito bazo podatkov in povezavo z okoljem tako, da se izogne zmedi, ki je posledica uporabe novih, sodobnih informacijskih tehnologij. Končni cilj načrtovanja je uspešnost celotnega podjetja. V zadnjih letih podjetja vlagajo ogromna sredstva v informatiko.

Raziskave kažejo, da večina projektov kasni, stroški razvoja pa močno presežejo planirana sredstva. Čeprav se strojna oprema relativno ceni, rastejo naložbe za uvajanje novih tehnoloških orodij, ki omogočajo odpravo problemov vzdrževanja in dograjevanja obstoječega stanja.

Prva faza načrtovanja je ugotavljanje informacijskih potreb podjetja, ki se deli na naslednje aktivnosti:

- Zbiranje informacijskih potreb
- Opredelitev potreb
- Analiza potreb

Informacijske potrebe podjetja morajo biti dokumentirane v natančni in urejeni obliki, ki omogoča analizo s katero se ovrednoti njena celovitost, konsistenca in vrednost teh dokumentov [Kovačič 1998, stran 66].

2.1. Vloga modeliranja pri načrtovanju IS

Pri raziskovanju in reševanju problemov na najrazličnejših področjih uporabljamo modeliranje. Model je vedno le preslikava naših videnj in predstav in ne stvarnega stanja, kar povečuje možnosti za odstopanje med originalom in modelom. Med njima obstaja analogija in podobnost, kar se odraža v enaki strukturi, funkciji obnašanja ali v vseh treh lastnostih. Model ima nalogo da:

- omogoči boljšo predstavitev, opredelitev in s tem razumevanje problema,
- omogoča možnost predvidevanja.

Postopek zasnove in gradnje IS temelji na modeliranju posameznih razvojnih faz ne glede na izbrane tehnologije. Za sodobne metodologije zasnove in gradnje IS je značilno, da vsaka razvojna faza IS praviloma temelji na opredelitvi ustreznega modela. Razvojne faze (*slika 1*) si v praksi pogosto ne sledijo tako linearno, kot je mogoče iz slike sklepati.

Slika 1: Etape življenjskega cikla



Vir: Kovačič, 1994, stran 44

2.2. Linearni pristop

Na linearnem pristopu so temeljile vse tradicionalne metodologije projektiranja IS. Zanj je značilno, da si faze sledijo v zaporedju (slika 2, str.7) in se nobena ne more začeti, dokler ni v popolnosti dokončana predhodna faza. Po vsaki fazi se izdelava poročilo, ki je osnova za začetek naslednje faze.

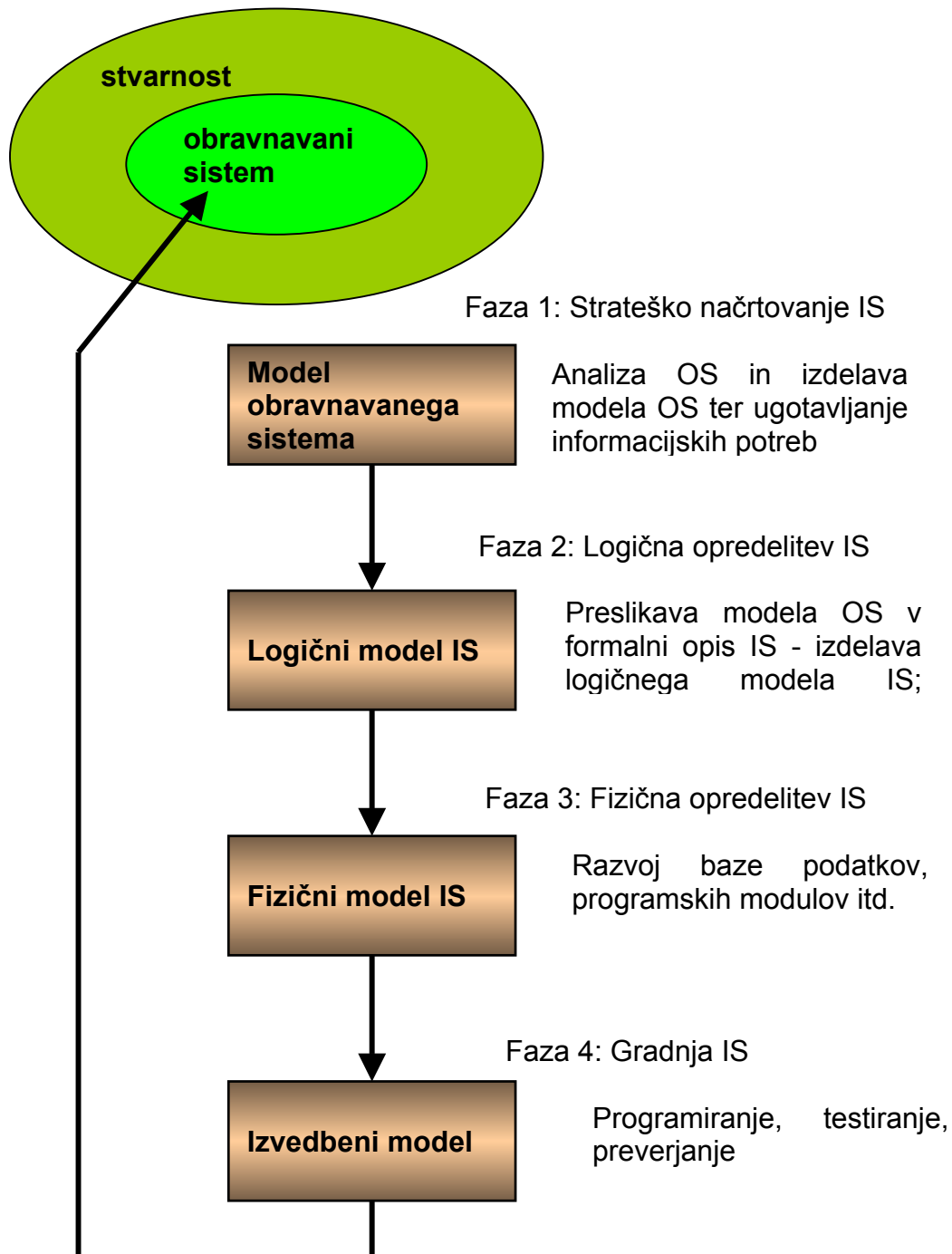
Značilnosti linearnega pristopa so naslednje (Kovačič, 1994, stran 45):

- razvoj IS poteka po "kaskadnem principu" skozi natančno določene faze, ki si sledijo sukcesivno,
- vsaka razvojna faza je natančno definirana in podrobno dokumentirana,
- modelni mehanizmi so, če lahko o njih sploh govorimo, preprosti in temeljijo na analitičnih in dokumentacijskih tehnikah ter večinoma verbalnih opisih obravnavanega problema,
- iz začetne analitične faze obravnavanega problema se praviloma izvrši neposreden prehod v izdelavo izvedbenega modela IS. Analitična faza je praviloma nenatančna, neformalizirana in zato vir mnogih napak.

Slabosti (Kovačič, 1994, stran 47):

- predolgi razvojni cikli,
- visoki razvojni stroški,
- napake in pomanjkljivosti se odkrijejo šele na koncu,
- sodelovanje uporabnikov je oteženo ali nemogoče.

Slika 2: Značilne razvojne faze IS v okviru sodobnejših metodoloških pristopov



Vir: Kovačič, 1994, stran 54

2.3. Prototipni pristop

Prototipni pristop lahko zasledimo pri linearnem načinu izgradnje IS. Namen prototipa je na preprostem primeru naročniku ali končnemu uporabniku predstaviti osnovne

funkcije sistema. Prototip je lahko izdelan z orodji ali celo programskim jezikom, ki se za izdelavo končnega izdelka ne uporabi. Z njim se skuša (Kovačič, 1994, stran 48):

- skrajšati čas, ki je potreben da pridemo do prvih rezultatov projekta,
- omogočiti sodelovanje uporabnikov skozi celotno razvojno obdobje projekta,
- zagotoviti, da se morebitne napake in pomanjkljivosti v projektu pokažejo v zgodnjih fazah, ko jih je možno relativno enostavno odpraviti.

2.4. Objektni pristop

Za razliko od predhodnih modelov ne obravnava ločeno statične (podatki) in dinamične (postopki) aspekte sistema. Ideja objektnega sistema je povezana z željo, da bi programsko opremo lahko razvijali podobno kot strojno iz množice standardiziranih sestavnih delov.

Ideje objektnega pristopa so pravzaprav že stare in so se pojavile z nastankom nekaterih programskih jezikov kot so SIMULA (1967), Smalltalk in C++. V začetku osemdesetih let so nastale osnovne ideje objektnega pristopa, med katerimi velja omeniti JSD (Jackson System Design) iz leta 1983.

Objektni pristop temelji na (Kovačič, 1994. stran 49):

- Objektih, ki vsebujejo podatkovne strukture in pripadajoče postopke na teh strukturah. Objekti nastopajo v realnem svetu kot produkti, komitenti (kupci in dobavitelji), občani, organizacijske enote itd. in jih pri konvencionalnem pristopu obravnavamo kot entitete.
- Sporočilih, to je sredstvu, s pomočjo katerega objekti komunicirajo med seboj pri izvajanju poslovnih postopkov.
- Tipih objektov, ki omogočajo realizacijo konceptov abstrakcije, ki jih poznamo iz podatkovnih modelov, kot so klasifikacija in generalizacija.

Objektni pristop predstavlja naslednje prednosti (Kovačič, 1994, stran 50):

- Večkratno uporabo istih objektov (reusability), kar skrajša čas za razvoj novih rešitev in s tem zmanjšuje stroške.
- S sestavljanjem rešitev iz že izdelanih in preizkušenih blokov (objektov) se poveča zanesljivost in kakovost rešitev.
- Individualni objekti kot zaključene celote se lahko spreminjajo, ne da bi to vplivalo na spremembe drugih objektov, kar poenostavi vzdrževanje programskih rešitev.

2.5. Modularno programiranje

V sedemdesetih letih so bili programi veliki, pisani dokaj okorno, največji problem pa je predstavljalo vzdrževanje. Z razdelitvijo programov na več manjših, so postali bolj pregledni in razumljivi. Objektno orientirani programski jeziki (C++, MS Visual Basic, MS Visual Studio, ...) omogočajo modularne programe, ki se izvajajo zaporedno.

Slika 3: Primer starega programiranja

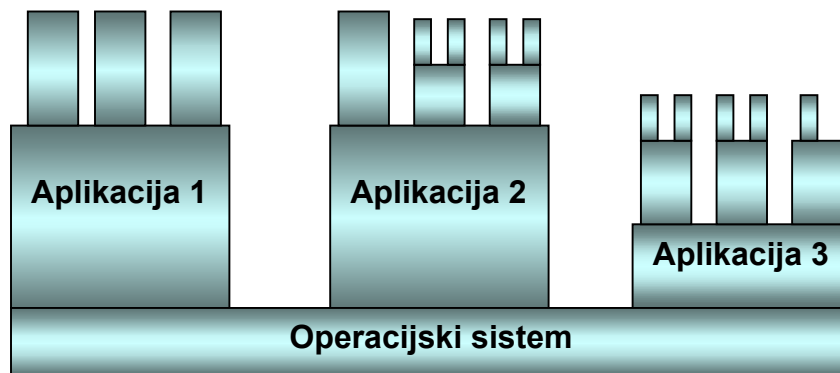


Vir: prirejeno po Schneier, 2000, str.160

Slika 3 simbolično prikazuje izvajanje velikih aplikacij na majhnem operacijskem sistemu.

Na sliki 4 je simbolično prikazana aplikacija 1 s komponentami, aplikacija 2 prikazuje komponente s komponentami. Komponenta je na primer Java navidezni stroj (ang. Java Virtual Machine) na katerem tečejo komponente (ang. applets). Urejevalniki tekstov ali tabel in brkljalniki se prodajajo kot samostojni programi, ki vsebujejo množico komponent (MS Word 97 preko 1.000). V praksi se torej najpogosteje srečamo s primerom aplikacije 3.

Slika 4: Primer današnjega programiranja osnovanega na komponentah

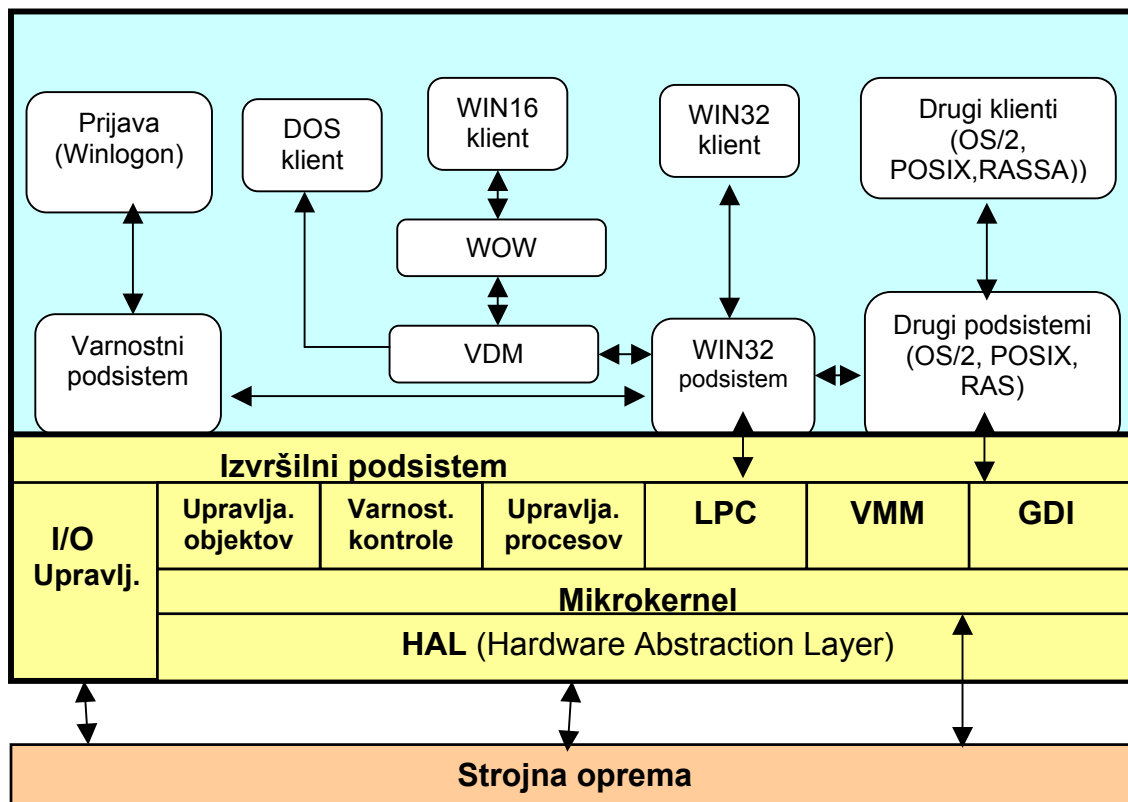


Vir: prirejeno po Schneier, 2000, str.160

Pri klasičnem programiranju je bilo potrebno posamezne dele programa združiti z "linkanjem" ter jih pred uporabo testirati in se prepričati, da vse pravilno deluje. Današnje komponente se najpogosteje dinamično združujejo, ko se zažene aplikacija. Takšna komponenta se v Windows okolju imenujejo DLL (Dinamic Linked Libraries). Iz vidika varnosti ni zagotovila, da so moduli popolnoma varni, lahko so odveč ali celo škodljivi. Ni nujno da moduli delujejo brezhibno v vseh možnih konfiguracijah. Dobra lastnost modulov je, da se lahko testirajo posamezno.

Pri klasičnem programiranju je različne programske dele povezoval operacijski sistem, ki je preprečil morebitno okvare programa zaradi napačnega delovanja drugega programa. Sodobni računalniki komunicirajo med seboj direktno in ne preko operacijskega sistema, zato tega varovala nimajo.

Slika 5: Programska arhitektura Windows NT



Vir: prirejeno po Schneier, 2000, str.161

Slika 5, prikazuje programsko arhitekturo operacijskega sistema Windows NT zgrajenega na principu modularnega programiranja.

2.5.1. Porazdeljene aplikacije

Porazdeljena aplikacija uporablja sredstva različnih računalnikov tako, da se deli proces aplikacije in funkcionalnosti na več prilagodljivih delov (particij), ki so razvite v različnih konfiguracijah. Razbitje aplikacije na dele prinaša prednosti kot so:

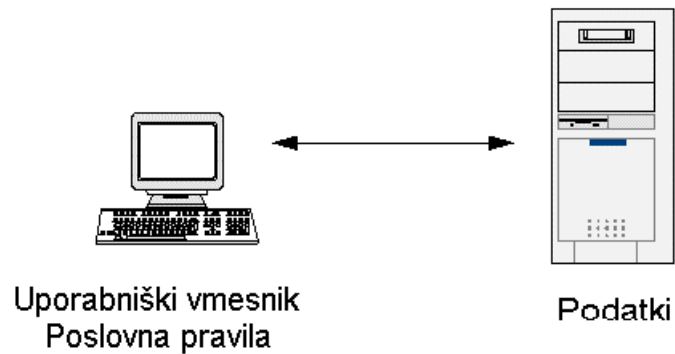
- večkratna uporabnost,
- nadgradljivost,
- prilagodljivost (manageability).

Glavni vzrok za potrebo po porazdeljenih aplikacijah je zelo hitra rast internet-a. Internetne aplikacije so lahko na voljo uporabnikom ne da bi jih pakirali in razpošiljali brez dodatnih zahtev po spremembah.

Porazdeljeno aplikacijo sestavljajo (Bortniker, 1999, str.11):

- porazdeljene komponente,
- porazdeljeni podatki,
- porazdeljeni uporabniki.

Slika 6: Tradicionalna arhitektura odjemalec strežnik (dvoslojna)



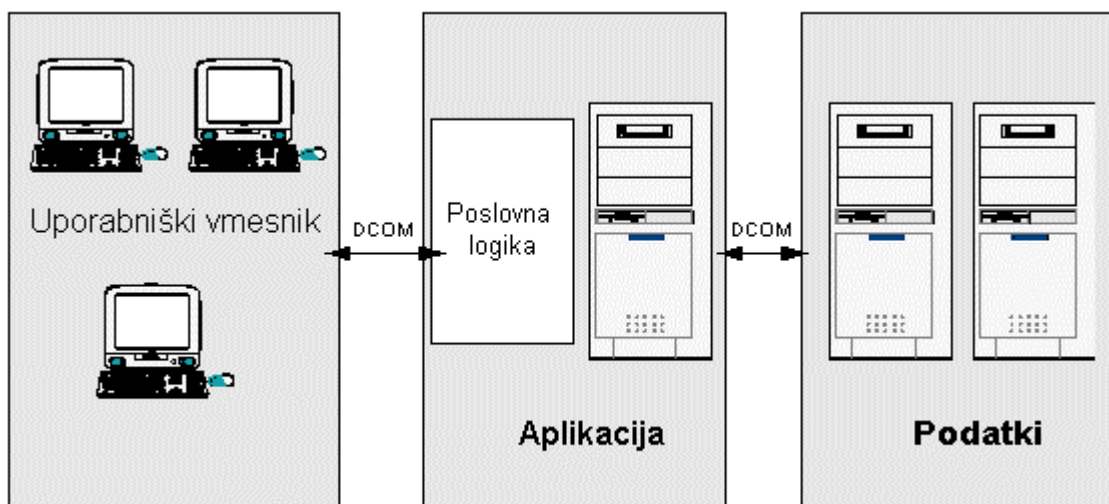
Vir: Bortniker, 1999, stran 15

Poleg dvoslojne (slika 6), obstaja tri ali večslojna arhitektura (slika 7), pri kateri so porazdeljene aplikacije na tri ali več logičnih nivojev ali sekcij. Komponente vsakega nivoja vsebujejo specifične tipe procesiranja. Delijo se na :

- uporabniški nivo (User Services),
- poslovni nivo (Business Services),
- podatkovni nivo (Data Services).

Večslojna arhitektura pomeni, da so razdeljeni in med seboj ločeni nivoji za odjemalca, aplikativne funkcije in podatke. Torej ni nujno, da se uporablja več različnih strežnikov, kot je prikazano na sliki 7. Seveda pa več strežnikov omogoča porazdeljeno programiranje.

Slika 7: Troslojna arhitektura odjemalec strežnik.



Vir: Bortniker, 1999, stran 15

Porazdeljene komponente objektnega modela (ang. Distributed Component Object Model - DCOM) služijo za koordinacijo in povezujejo posamezne nivoje v celovito aplikacijo. Predstavitveni nivo se nanaša na uporabniška opravila s katerimi komunicira uporabnik.

2.6. Vloga strežnikov

Strežniki omogočajo združevanje različnih tehnologij in arhitektur, ki so bila razvita v zadnjih desetletjih in so rezultat tehnologij, ki se danes uporabljajo v spletu (ang. Web). Strežniki niso zavezani enemu programskemu jeziku, podatkovni bazi ali modelu. Uporabljajo se kombinacije spletnih strežnikov (ang. Web Servers) kot so Apache ali Microsoft Internet Information server, ki upravljajo povezavo med uporabniki v internetu, ter aplikacijskimi (ang. Application Servers), oziroma transakcijskimi (ang. Transaction) strežniki, ki omogočajo posredovanje izoblikovanih informacij do uporabnika. Aplikacijski strežnik je lociran blizu spletnega strežnika ali pogosto celo na istem računalniku.

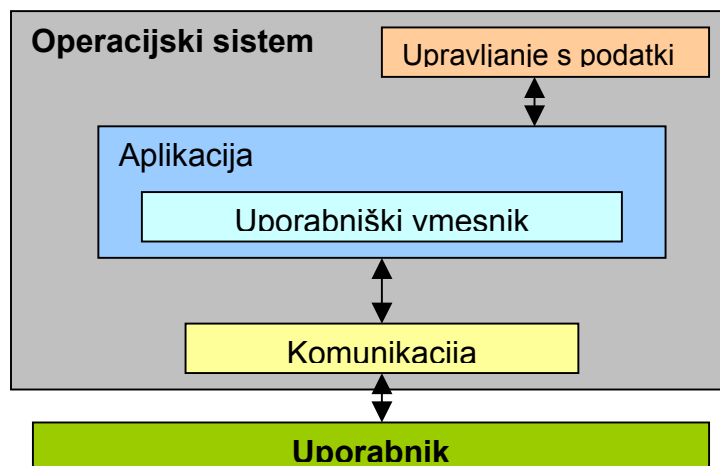
2.6.1. Osnovni razlogi za implementacijo aplikacijskih strežnikov

Za lažje razumevanje uporabnosti in pomena aplikacijskih strežnikov navajam šest osnovnih razlogov (Feiler, 2000, str. 34 do 45) za implementacijo aplikacijskih strežnikov, čeprav v dejanskih projektih večinoma srečujemo kombinacije teh razlogov.

Povezovanje starejših računalniških sistemov in podatkovnih baz

Marsikatero večje podjetje (ali ustanova kot so banke, zavarovalnice) je vložilo ogromna sredstva v računalniško strojno in programsko opremo ter pripadajočo podatkovno bazo. Računalniški sistemi za katere ni nujno da so zastareli, predstavljajo ogrodje informacijske infrastrukture, ki je nastajalo skozi leta. Zastarele terminale so zamenjali osebni računalniki, podatkovna baza pa je ostala na prvotnih sistemih. Terminali so predstavljali vmesnik med sistemom in uporabnikom, kjer je komunikacija potekala v preprosti tekstovni obliki (*slika 8*).

Slika 8: Delovanje programa pri uporabi terminala

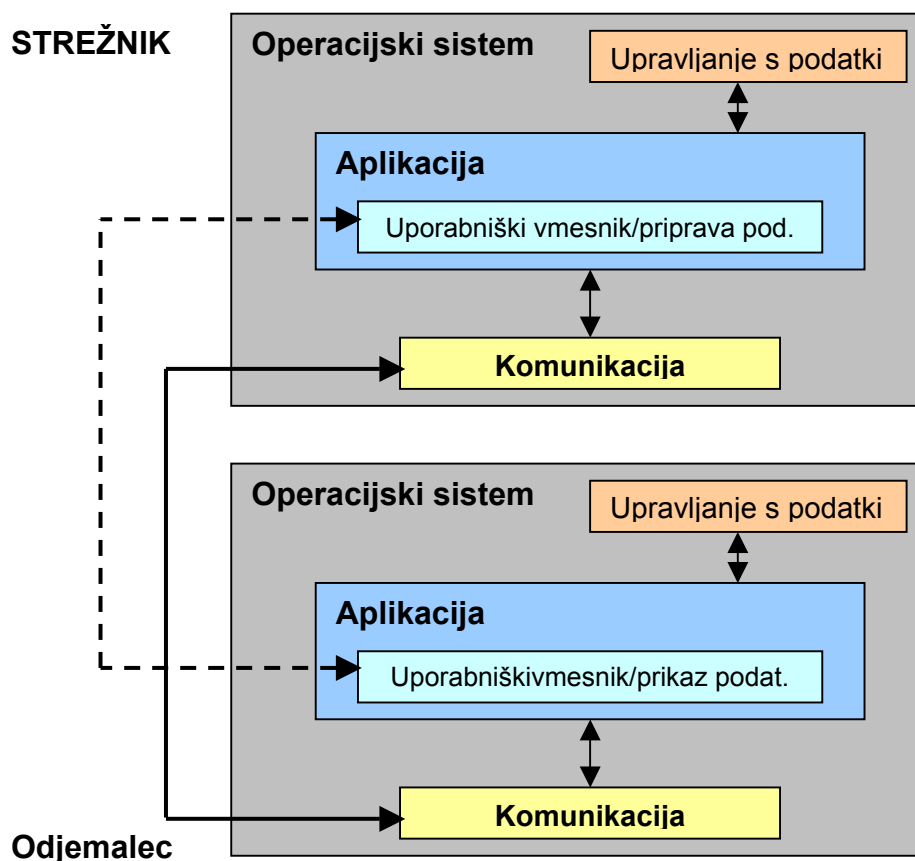


Vir: prirejeno po Feiler, 2000, str. 20

Uporaba osebnih računalnikov

Z naraščanjem uporabe omrežij osebnih računalnikov koncem devetdesetih in operacijskih sistemov (Windows95, Windows98, Macintosh) je nastal problem, kako

Slika 9: Delovanje sistema odjemalec – strežnik



Vir: prirejeno po Feiler, 2000, str. 21

povezati desetine, stotine ali tisočine omrežnih vozlišč. Novejši operacijski sistemi kot so WindowsNT, Windows2000, WindowsXP, Mac OS X in različne izpeljanke sistema Unix, so bolj robustni in podpirajo osnovne zahteve distribucijskih sistemov. Aplikacijski strežniki združujejo znanje in izkušnje iz področja varnosti, nadzora in delovanja sistemov iz preteklih desetletij. Namesto programiranja se z nastavljanjem parametrov definira varnostno politiko in strategijo uporabe resursov.

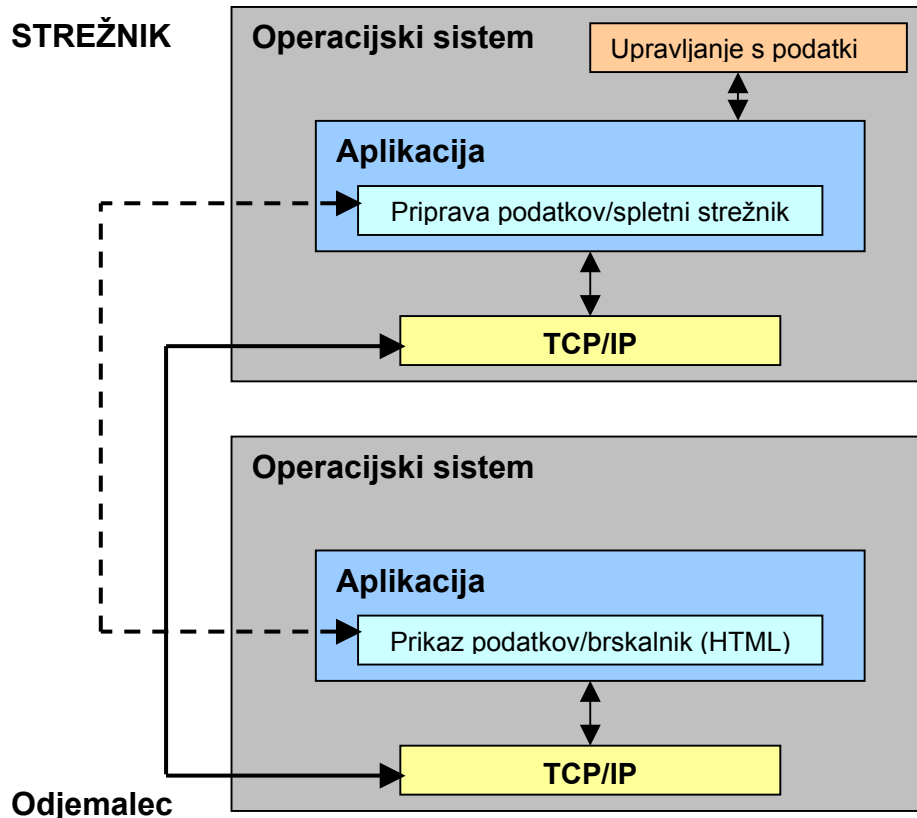
Osebnim računalnik - odjemalec (*slika 9*) je povezan s strežnikom preko komunikacijskega programa, ki teče na obeh sistemih. Uporabniški vmesnik omogoča pripravo podatkov na strežniku in prikaz podatkov odjemalcu.

Podpora spletnim stranem

Posamezniki in podjetja si danes postavljajo svoje spletne strani, ki predstavljajo normalni del poslovanja v današnjem načinu življenja. Razvoj in vzdrževanje spletnih strani pa predstavlja velik izziv. Uporabniški strežniki se uporabljajo za izdelavo dinamičnih spletnih strani, ki se oblikujejo avtomatsko po potrebi. V naprej se lahko

pripravi vzorčne strani (šablone) s pripravljenimi prostori za vpis podatkov, ki se dobivajo iz podatkovne baze, pripravljene na zahtevo. Ko so šablone izdelane nadaljnjo kodiranje v HTML ni potrebno.

Slika 10: Delovanje sistema odjemalec – strežnik v internet okolju



Vir: prirejeno po Feiler, 2000, str. 22

TCP/IP (Transmission Control Protocol/ Internet Protokol) komunikacijska programska oprema na sistemu odjemalca in strežnika (*slika 10*), omogoča povezavo med njima. Večina že obstoječe standardne programske opreme ostane uporabna, zato je implementacija takšnega sistema relativno enostavna, saj je potrebno v aplikaciji napisati le kodo, ki jo zahteva nova logika.

Razvoj integriranih spletnih sistemov

Izgradnja integriranih spletnih sistemov zahteva od razvijalcev in uporabnikov poznavanje in razumevanje poslovne logike, oblikovanje sistema in vmesnikov ter tehnologij za podatkovne baze in splet. Arhitektura aplikacijskega strežnika zagotavlja enostaven in strukturiran razvoj sistema. Vmesniki so jasno definirani (Hypertext Markup Language v nadaljevanju HTML – programski, Structured Query Language v nadaljevanju SQL-podatkovni), zato lahko razvoj poteka na podprojekti z minimalno potrebno koordinacijo. Drugi pristop pri načrtovanju spletnih integriranih sistemov je uporaba XML jezika.

Elektronsko poslovanje (E-Business)

Elektronsko poslovanje se uporablja tako v malih kot velikih podjetjih. Dostop do elektronskega trga je razmeroma preprost in poceni. Vzpostavitev E-poslovanja zahteva hitro odzivanje in reagiranje na spremembe. Aplikacijski strežniki so pogosto srce E-poslovanja, ki se ga postavi v obstoječe računalniško okolje, poveže z podatkovno bazo in že narejenimi HTML stranmi.

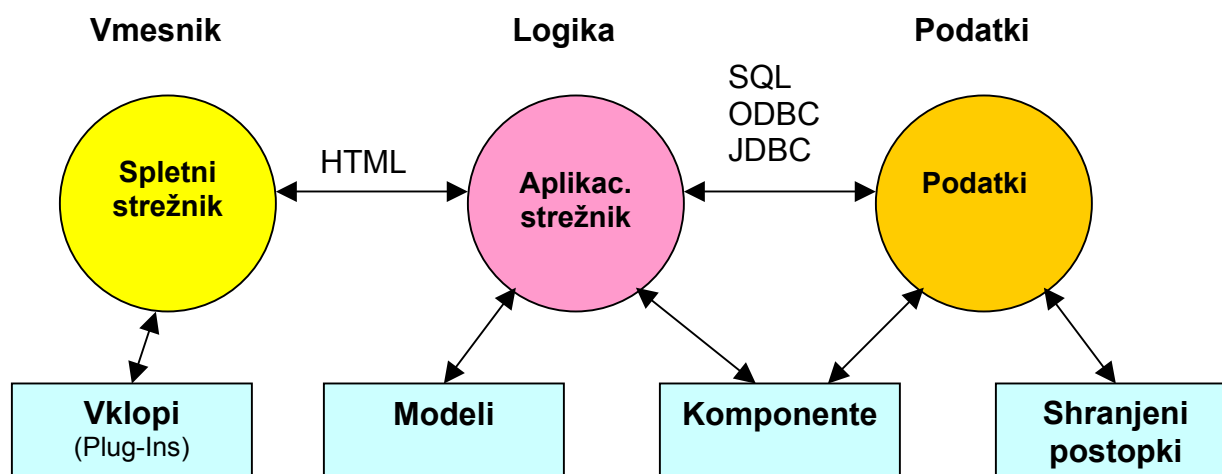
Učinkovito upravljanje

Za razliko od osebnega računalnika, ki ga povežemo na internet, za prikazovanje spletne strani pri večjih aplikacijah potrebujemo več različnih strežnikov in usklajeno medsebojno delovanje. Upravljanje velikih spletno usmerjenih sistemov je zahtevno delo, ki ni nikoli končano. Z uporabo modelov in orodij za upravljanje se lahko zagotovi dobro skrbništvo, ki vključuje tudi upravljanje z omrežjem in sistemske vire. Proizvajalci oziroma ponudniki podatkovnih in spletnih strežnikov ponujajo različna orodja za usklajevanje in povečevanje učinkovitosti proizvodov.

2.6.2. Delovanje aplikacijskega strežnika

Aplikacijski strežnik posreduje spletnemu strežniku HTML strani, katere pogosto vsebujejo podatke iz podatkovne baze. Spletni strežnik komunicira z uporabniki (odjemalci) preko standardnega HTTP (Hypertext Transfer Protocol) internet protokola in pošilja HTML strani uporabnikom. Tako spletni kot aplikacijski strežnik uporabljata HTML za medsebojno komuniciranje.

Slika 11: Zgradba aplikacijskega strežnika



Vir: prirejeno po Feiler,2000, str.48

Aplikacijski strežnik (*slika 11*) komunicira z podatkovno bazo preko standardnih mehanizmov kot so SQL, ODBC¹ (Open Database Connectivity) ali JDBC² (Java Database Connectivity). Ta arhitektura omogoča transformirati podatke v HTML brez kakršnegakoli kodiranja. Prav tako spletni strežnik dostopa do podatkov v SQL ali

¹ Vmesnik med aplikacijo in podatkovno bazo, ki bazira na SQL standardu.

² Vmesnik med aplikacijo in podatkovno bazo v Java okolju.

preko ODBC v katerokoli drugo bazo brez kodiranja. Odprta arhitektura in standardi omogočajo povezovanje sistemov različnih tehnologij, proizvajalcev in različnih podatkovnih baz.

2.6.3. Microsoftov transakcijski strežnik

Microsoftov transakcijski strežnik (MTS - Microsoft Transaction Server) je model, ki bazira na komponentah za relativno enostavno izgradnjo in razvoj varnih nadgradljivih aplikacij z visokimi zmogljivostmi. MTS predstavlja razširitev komponentnega objektnega modela COM (Component Object Model) v večplastno okolje. To razvijalcem omogoča, da se bolje posvetijo implementaciji poslovnih pravil kot kompleksnosti programiranja in pravil v distribuiranem, več uporabniškem okolju.

MTS podpira (Bortniker, 1999, str.10):

- izvajanje transakcij (Transactions),
- usklajeno obdelovanje poslov (Static load balancing),
- povezovanje različnih komponent in usklajevanje delovanja (Multi-threading and resource pooling),
- odpravljanje napak (Fault-tolerance),
- koordiniranje več hkratnih uporabnikov (Multi-user concurrency),
- osnovno varnost (Role-based security).

Za MTS je značilno, da združuje naslednja produkta(Bortniker, 1999, str.10):

- **Object Request Broker (ORB)**. MTS upravlja z zahtevami in servisi objektov komponent ki jih sestavlja v delavno okolje.
- **Transaction Processor**. MTS uporablja MS DTC (Microsoft Distributed Transaction Coordinator), ki skrbi za koordinacijo transakcij skozi več različnih tipov podatkovnih virov.

MTS zagotavlja lastno programsko infrastrukturo z implementacijo dinamično povezanih knjižnic (DLL). Dinamično povezane knjižnice so obravnavane izven procesa odjemalca.

2.6.4. Povzetek

Tehnologija aplikacijskih strežnikov omogoča implementacijo dinamičnih spletnih strani na osnovi obstoječega okolja, ki lahko zajema starejše računalniške sisteme in različne podatkovne baze. Tako predstavlja relativno preprosto možnost povezave med preteklostjo in prihodnostjo, kar omogočajo standardni vmesniki in protokoli. Stare podatkovne baze (na primer 20 let) se lahko na dokaj preprost način nadomestijo z novimi ob uporabi ODBC ali JDBC standardov.

Arhitektura aplikacijskega strežnika omogoča različne načine implementacije od samostojnega osebnega računalnika do velikega sistema. Prehod na arhitekturo uporabniških strežnikov pomeni predvsem zaupanje v arhitekturo in ne v določeno strojno in programsko opremo.

2.7. Standardizacija

Slovenske nacionalne standarde je do leta 2001 pripravljala, sprejemala in izdajala Urad Republike Slovenije za standardizacijo in meroslovje in za tem Urad RS za meroslovje. Po reorganizaciji urada v letu 2001 pa je za to pristojen Slovenski inštitut za standardizacijo. Vloga inštituta kot nacionalnega organa za standarde v Sloveniji je poleg navedenega še sodelovanje, zastopanje in predstavljanje Republike Slovenije v mednarodnih in evropskih organizacijah za standardizacijo v skladu s potrebami in na nacionalni ravni dogovorjenimi interesi zainteresiranih.

2.7.1. Sistem kakovosti

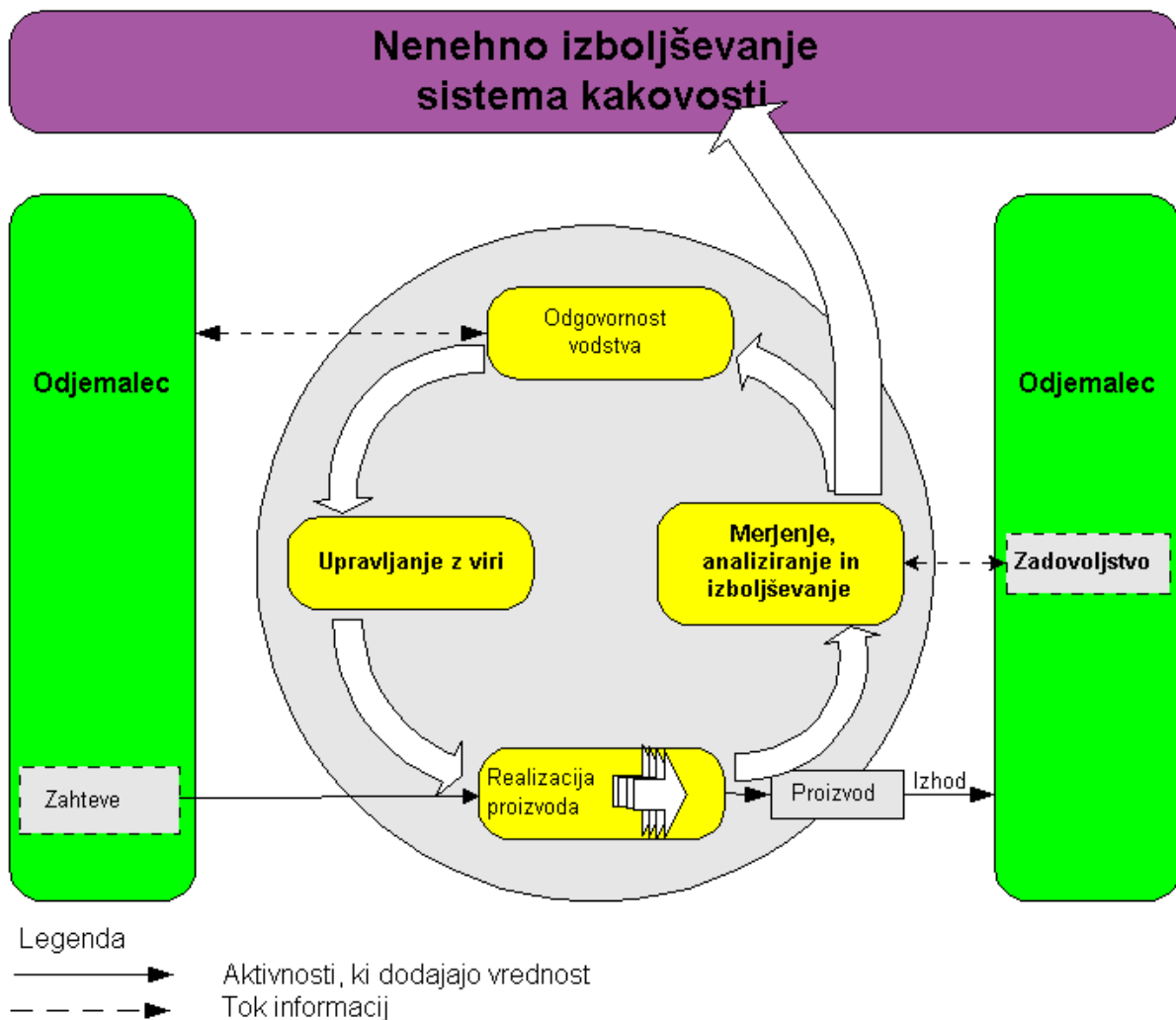
Nove razmere na trgu so zaradi preusmeritve slovenskega gospodarstva na zahtevne evropske oziroma svetovne trge marsikatero slovensko podjetje prisilile k drugačnemu načinu razmišljanja in pristopa k poslovanju. Zavedajo se, da brez kakovosti ne bo možno zdržati zahtevne tekme konkurenčnosti, ki se nam obeta v naslednjih letih. Kakovost največkrat povezujemo z znižanjem stroškov poslovanja, povečanjem dobička in celovito prenovo podjetja (reinženiring). Seveda je samoumevna želja, da se kakovost v podjetju tudi verificira. To storimo z implementacijo zahtev, ki jih predpisujejo standardi kakovosti. Standard ISO 9001, je najkompleksnejši iz družine standardov ISO 9000 in pomeni obvladovanje kakovosti delovanja podjetja na vseh njegovih področjih, kot so: vodenje podjetja, proizvodnja, razvoj, trženje, izobraževanje, projektni sistem, kontrola, dokumentacija, reklamacije.

Za učinkovito in uspešno poslovanje je potrebno neprestano meriti, ugotavljati, izboljševati in zagotavljati kakovost na vseh področjih poslovanja. Danes se uporablja sistem kakovosti kot učinkovito konkurenčno orožje tako v proizvodnem kot storitvenem področju poslovanja. Pri tem je najpomembnejše zadovoljevanje želja in zahtev kupca, saj nam le ta zagotavlja dohodek. Takšna filozofija zagotavlja konkurenčne prednosti dolgoročnega značaja, kot so trajna prisotnost in rast na tržišču. Za kakovost ni odgovorna le posebna služba, ki se s področjem kakovosti ukvarja, temveč vsi zaposleni. Ugotovitve presoje kakovosti so vodstvu organizacije v pomoč pri upravljanju. Zahteve po občasni presoji, analiziranju in primerjanju rezultatov ter primernem ukrepanju so trajna naloga vodstva organizacije. Zunanji razlogi za izvedbo presoje so zahteve tržišča in poslovnih partnerjev.

2.7.2. Standardi skupine ISO 9000:2000(E)

Mednarodna organizacija za standardizacijo (ISO - International Standard Organization) je svetovna zveza nacionalnih organov za standarde, ki so člani ISO. Člani delujejo na določenem področju, za katerega je bil ustanovljen tehnični odbor in imajo pravico biti zastopani v tem odboru. Pri delu sodelujejo mednarodne vladne in nevladne organizacije, povezane v ISO. V ISO je predvidena redna revizija standardov vsakih 5 let. Revizija temelji na podrobni raziskavi celotnega spektra uporabnikov standardov. Med uporabnike spadajo tako organizacije, ki uvajajo oziroma vzdržujejo lasten sistem kakovosti, podjetja za izdajo certifikatov, svetovalci in izobraževalne organizacije za področje standardizacije. V novi izdaji standardov, ki so izšli konec leta 2000 oziroma začetku leta 2001 je nastala vrsta sprememb, ki vplivajo predvsem na lažje razumevanje in lažjo interpretacijo zahtev v standardih ter enakovredno uporabo za vse tipe organizacij.

Slika 12: Model sistema vodenja kakovosti, osnovan na procesih



Nova izdaja družine standardov ISO 9000:2000(E) temelji na naslednjih principih:

1. Orientacija na kupca (odjemalca)

Organizacije so odvisne od svojih kupcev (odjemalcev) in morajo razumeti njihove trenutne zahteve kakor tudi zahteve in potrebe, ki se bodo pojavile v prihodnosti in se prizadevati izpolniti kupčeva pričakovanja.

2. Vodenje

Vodstvo mora vzpostaviti enotne smernice in cilje v organizaciji. Ustvariti in vzdrževati okolje v katerem bodo vsi zaposleni vključeni v doseganje ciljev organizacije.

3. Vključevanje zaposlenih

Zaposleni na vseh nivojih v organizaciji od najvišjega do najnižjega in njihova popolna vključitev omogoča, da so njihove zmožnosti in sposobnost uporabljene za doprinos in koristi podjetja.

4. Procesni pristop

Želeni rezultati so boljši (učinkovitost je večja), če se vključeni viri in aktivnosti vodijo kot proces.

5. Sistemski pristop k vodenju

Odkrivanje, razumevanje in vodenje sistema medsebojnih procesov poveča učinkovitost in uspešnost pri doseganju ciljev organizacije.

6. Neprestano izboljševanje

Neprestano izboljševanje vseh storitev mora biti stalen cilj organizacije.

7. Odločanje na osnovi dejstev

Učinkovite odločitve temeljijo na analizi podatkov in informacij.

8. Vzajemno koristni odnosi s partnerji

Organizacija in njeni dobavitelji so medsebojno odvisni in vzajemno koristen odnos povečuje zmožnosti obeh za ustvarjanje dodane vrednosti.

Skupina standardov ISO 9000:2000(E)

- **ISO 9000:** Opisuje osnove sistema vodenja kakovosti in specificira izraze,
- **ISO 9001:** specificira zahteve za vodenje kakovosti, ki omogočajo organizaciji izdelati produkt, ki bo zadovoljil stranko v vseh njenih zahtevah in ciljih.
- **ISO 9004:** smernice za doseg učinkovitosti in uspešnosti sistema kakovosti
- **ISO 19011:** smernice za presojo sistema vodenja

Standarda ISO9002 in ISO9003 po novem ne obstajata več. Novi standard ISO9001 je edini po katerem se lahko pridobi certifikat, zato bodo morale organizacije, ki so že certificirane po teh dveh standardih, po določenem prehodnem obdobju svoje sisteme prilagoditi zahtevam standarda ISO9001.

3. Portal

Portal predstavlja prvo stran, oziroma vstopno točko preko katere se vstopa do informacijskih virov na internetu. Vmesnik ponavadi integrira vse potrebne elemente portalov v celoto, ki omogočajo uporabnikom želene informacije. Vmesnik mora vsebovati bogato vsebino, da je lahko sploh uporaben. Uporabniki lahko z uporabo brskalnika dostopijo do vseh informacijskih objektov, tako strukturiranih kot tudi nestrukturiranih, ne da bi poznali njihovo lokacijo ali celo format.

Poslovni portali povezujejo različne koncepte, različne informacijske tehnologije, in sicer od najnovejših, še ne preskušanih, do tehnologij, ki so že dalj časa znane na področju informatike. Portal sestavlja niz tehnologij, ki informacije povezujejo v celoto. Tako izza portalov najdemo predstavitveno tehnologijo uporabniških vmesnikov, sisteme varnosti, tehnologijo personalizacije, ki predstavlja specifične informacije posameznim skupinam uporabnikov, skupinsko delo, formate za distribucijo dokumentov, iskalne in poizvedovalne funkcije ter tehnologijo integracije različnih virov podatkov.

3.1. Komponente poslovnih portalov

Slika 13 na strani 22 prikazuje osnovne komponente poslovnih portalov, ki so:

Nadgradljivost

Poslovni portal je običajno sestavljen iz večnitnih aplikacijskih storitev, ki so lahko porazdeljene na različnih strežnikih. Portal mora obvladovati veliko število diskretnih informacijskih objektov, ne da bi se to poznalo na odzivnosti oziroma njihovi dosegljivosti. Poslovni portal bo verjetno podpiral tisoč in več uporabnikov z veliko frekvenco potreb po informacijah. Tako mora portal minimalno podpirati tri ali n-nivojsko arhitekturo, kjer se večina procesiranja dogaja na vmesnem aplikacijskem strežniku. Portal mora podpirati aplikacije, ki se izvajajo na različnih računalniških platformah.

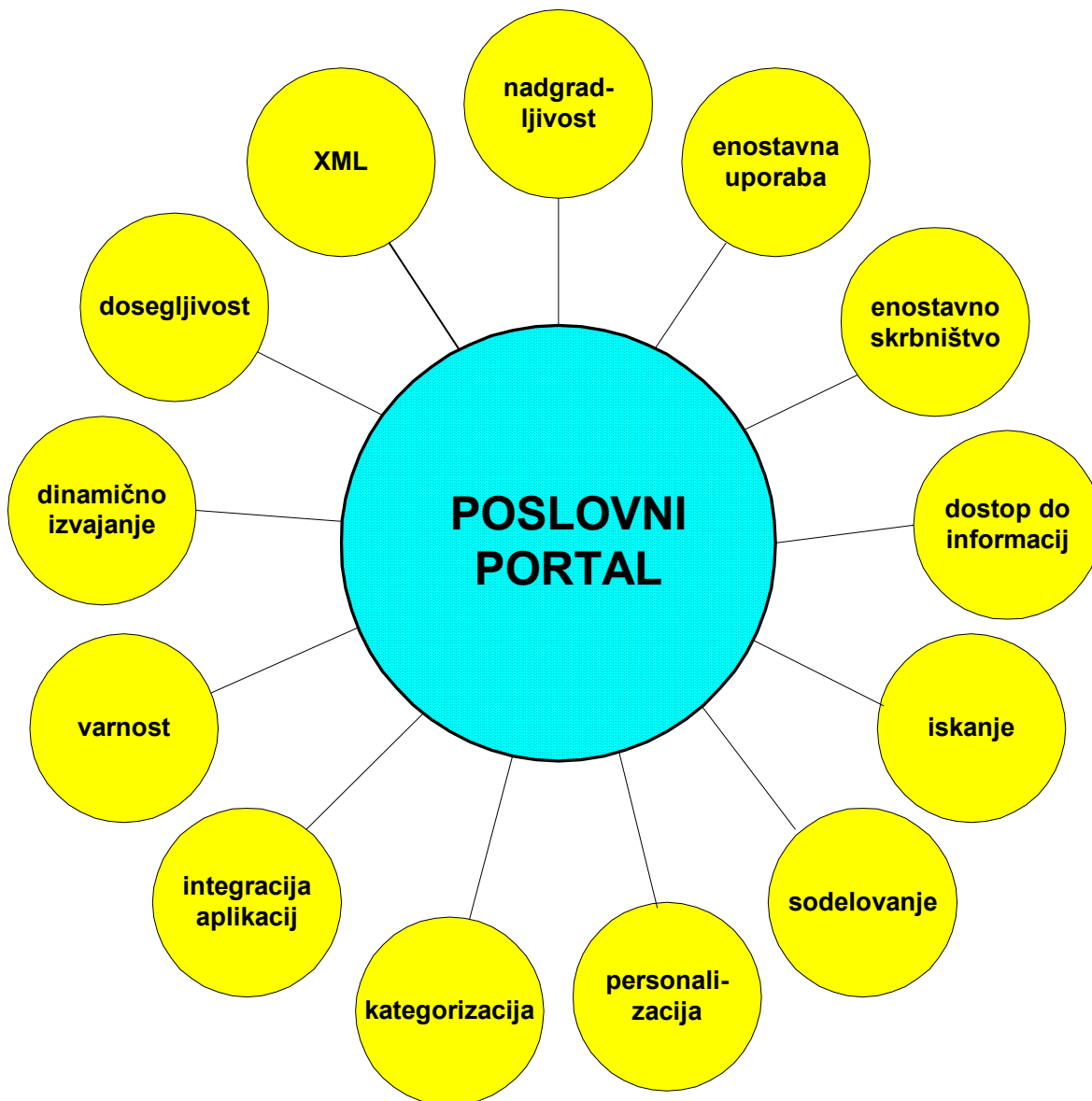
Poslovni portal zagotavlja arhitekturo lahkega odjemalca ('thin-client'), da se izogne odvečni distribuciji in vzdrževanju programske opreme pri tisočih delovnih postajah uporabnikov. To pomeni tudi enostavnejšo instalacijo, konfiguracijo in vzdrževanje.

Enostavna uporaba

Poslovni portali so primarno postavljeni za zadostitev informacijskih potreb uporabnikom, ki želijo hiter in enostaven dostop do informacij. Njihova uporaba mora biti enostavna s čim manjšimi potrebami po učenju uporabe. Zato so brskalniki primerno orodje za hiter, enostaven dostop in uporabo poslovnih portalov.

Verjetno največja korist uporabe poslovnih portalov je njihova zmožnost posredovati potrebne informacije uporabnikom, ki niso najbolj veščji rabe računalnikov. Portali uporabljajo tehnologijo brskalnikov, ki je poznana vsem uporabnikom, ki so že uporabljali internet, kar tudi zmanjša potrebo po učenju njihove uporabe. Učinkovit portal novim uporabnikom ponuja enostavno uporabo, bolj izkušenim pa tudi razna dodatna orodja (npr. analitična orodja).

Slika 13: Osnovne komponente poslovnih portalov



Vir: prirejeno po Ixtlan

Enostavno skrbništvo

Enostavnost uporabe moramo razširiti tudi na področje skrbništva portalov. Skrbniki pa tudi zahtevnejši uporabniki morajo imeti na voljo enostavna orodja za npr. kreiranje novih poročil, za shranjevanje in indeksiranje informacijskih objektov v repozitorij, za upravljanje repozitorija,...

Učinkovit portal mora uporabljati obstoječo poslovno logiko ter obstoječe podatke v obstoječih podatkovnih bazah in ne zahtevati razne predelave kot to zahteva npr. tehnologija podatkovnih skladišč. Skrbniki morajo imeti možnost definirati pravice za posameznike, skupine uporabnikov znotraj podjetja. Pravica opredeljuje kategorije do

katerih lahko posamezen uporabnik dostopa, funkcionalnost, ki jo lahko uporablja, podatke, ki jih lahko vidi.

Univerzalni dostop do informacijskih virov

Poslovni portal mora biti povezan z velikim številom heterogenih podatkovnih skladišč, kar vključuje relacijske in objektno podatkovne baze, multidimenzionalne podatkovne baze, sisteme za upravljanje z dokumenti, sisteme elektronske pošte, spletne strežnike, in različne datotečne sisteme ter ostale strežnike. Omogočati mora dostop do vseh teh informacij, da lahko zadosti potrebi uporabnikov po vseh potrebnih informacijah za učinkovito opravljanje njihovega dela.

Iskanje

Uporabnik želi le enkrat postaviti vprašanje ter nato dobiti vse relevantne informacije povezane s vprašanjem. Izvor informacij ga ne zanima, te informacije lahko izhajajo iz elektronske pošte, se sklicujejo na določen telefaks, ali je to kopija pogodbe ali pa so rezultat podrobne OLAP (On-Line Analytical Processing) analize.

Hiter dostop do informacij je ena od osnovnih lastnosti portalov; hiter dostop do virov informacij tako znotraj kot tudi zunaj podjetja. To pa ni tako enostavno kot zveni, ker se informacije nahajajo v različnih oblikah. Zato mora portal zagotoviti tehnologijo, ki podpira enoten ter integriran dostop do vseh vrst virov informacij in bo uporabniku sposobna posredovati informacije po katerih poizveduje.

Ne samo, da se informacije nahajajo v različnih sistemih, tudi shranjene so na različne načine. Portal mora zagotoviti dostop do informacij v vseh oblikah, ne glede na to ali so shranjene v relacijskih podatkovnih bazah, spletnih dokumentih, tekstovnih datotekah, slikah, ali pa avdio-video formatu. Ponavadi je v okviru portala združenih več različnih poizvedovalnih-iskalnih orodij, vsako optimizirano in prilagojeno svojemu namenu, vsa skupaj pa opravljajo integrirano multi-iskalno funkcijo. Nekaj osnovnih značilnosti iskalnih orodij:

- iskanje v različnih podatkovnih virih,
- iskanja dokumentov v različnih jezikih,
- iskanja shranjenih objektov, ki vsebujejo tako parametrizirane podatke, kot tudi navaden tekst,
- zmožnost iskanja s pomočjo boolejeve algebre,
- razvrščanje rezultatov glede na njihovo relevantnost,
- grafični prikaz iskanje (image search),
- podpora XML in HTML jeziku.

Sodelovanje

Uporabniki morajo biti med seboj povezani. Pridobljene informacije med seboj izmenjujejo in na njihovi podlagi sprožajo nadaljnje aktivnosti. To jim lahko omogoči ustrezen portal, ki mora podpirati tudi skupinsko delo (ang. 'groupware').

Portal mora podpirati sodelovanje med uporabniki v realnem času tako, da le-ti enostavno poiščejo sodelavce, partnerje, kupce, dobavitelje in z njimi komunicirajo ne glede na to kje se nahaja njihovo delovno mesto. Ta storitev omogoča uporabnikom obveščanje ali so njihovi sodelavci, partnerji dosegljivi ter omogoča izmenjavo dokumentov in aplikacij med njimi.

Portal postaja osrednja točka preko katere lahko uporabnik komunicira, izmenjuje informacije, jih ureja in organizira, se dogovarja za sestanke, je torej točka s pomočjo katere lahko opravlja in organizira svoje vsakodnevno delo.

Personalizacija

Produktivnost uporabnikov je lahko bolj učinkovita in se poveča, če je sistem prilagojen njihovim osebnim potrebam. Personalizacija predstavlja prilagajanje osebnim potrebam uporabnika z namenom enostavne in učinkovite uporabe. Personalizacija predstavlja zmožnost oskrbovanja uporabnika s pravimi, potrebnimi informacijami tako s strani samega uporabnika kot tudi s strani podjetja, ki je postavilo določen portal.

Personalizacijo je možno doseči na več načinov:

- Uporabnik po lastni izbiri določi sklop informacij do katerih bo dostopal preko portala (ang. '**profile based**').
- Definirane so skupine uporabnikov z enakimi ali podobnimi zahtevami po informacijah (ang. '**collaborative filtering**').
- Pristop, ki deluje avtomatsko z rangiranjem uporabnikov glede na skupne potrebe po informacijah. Na podlagi shranjenih informacij se izdelajo vzorci, ki avtomatsko razvrstijo uporabnika v določeno skupino (ang. '**real-time recommendations**')
- Na osnovi ključnih besed ugotavlja primernost posameznega dokumenta za uporabnika (ang. '**content-based filtering**'). Način je primeren, ko izbrani dokumenti ustrezajo vsem uporabnikom (ni subjektivne izbire).
- Avtomatsko izločaje meta podatkov iz različnih virov ali **kategorizacija**, pomeni filtriranje informacij iz notranjih virov podjetja, kot tudi interneta ter njihovo sortiranje in razvrščanje v različne kategorije. Kategorizacija in personalizacija tvorita osnovo za pridobivanje relevantnih informacij uporabniku portala.
- **Integracija** aplikacij uporabniku omogoča, da iz ene izhodiščne točke dostopa do vseh informacij, ki jih potrebuje pri svojem delu in s pomočjo portala poganja poslovne aplikacije.

Varnost portala

Informacije morajo biti zavarovane pred nepooblaščenim dostopom, hkrati pa morajo omogočati enostaven in hiter dostop. Portal mora biti integriran z vsemi obstoječimi varnostnimi shemami. S strani uporabnika mora biti omogočena le ena prijava v sistem, pri tem pa mora sistem upravljanja dostopa do informacij zagotoviti dostop do vseh relevantnih virov do katerih ima pooblastilo.

Dinamično izvajanje

Portal mora uporabniku dostaviti informacije v realnem času. Te informacije morajo biti pripravljene iz najnovejših (ang. 'up-to-date') podatkov.

Dosegljivost portala

Osnovna značilnost poslovnih portalov je tudi možnost njihove uporabe z obeh strani požarne pregrade (ang. 'firewall') podjetja. To omogoča dostop do informacijskih objektov podjetja s strani zaposlenih, ki se lahko nahajajo zunaj podjetja, kupcev, distributerjev, dobaviteljev, raznih podružnic in ostalih partnerjev. Velja tudi obratno - podjetje lahko preko portala dostopa tudi do informacij svojih poslovnih partnerjev. Takšen dostop do poslovnih informacij je lahko tudi ključni element elektronskega poslovanja podjetja.

Večina podjetij že ima razvitih veliko uporabniških knjižnic (ang. 'directory'), repozitorijev in raznih storitev v okviru intraneta. Podjetniški portal mora omogočati vmesnike tudi za dostop to teh virov. Poslovni portal morajo biti dosegljivi iz drugih aplikacij preko raznih API funkcij.

Jezik XML ('eXtensible Markup Language')

XML je samoopisni jezik, ena najbolj uporabljenih novih tehnologij v svetu interneta, ki jo podpirajo vsa najmočnejša svetovna računalniška podjetja (IBM, Microsoft, Netscape, SUN, Oracle). Na nivoju poslovnih portalov XML igra ključno vlogo kot zelo fleksibilen izvor podatkov, visoko zmogljiv način izmenjave informacij in univerzalen format izmenjave podatkov.

Za razliko od jezika HTML, kjer so vsebina in podatki za prikaz le-te med seboj združeni, XML poenostavlja izmenjavo podatkov med različnimi računalniškimi sistemi in omogoča jasno ločitev vsebine od prikaza. Jezik je razširljiv, prav tako pa so razširljive tudi sheme, ki temeljijo na tem jeziku.

3.1.1. Prednosti implementacije in uporabe poslovnih portalov

Večja donosnost naložb v informacijske projekte (ang. Return of Investment – ROI)

Poslovni portali omogočajo uporabnikom boljše izkoriščanje že implementiranih podatkovnih skladišč (ang. 'data warehouse'), podatkovnih trgov (ang. 'data mart') in raznih poslovnih aplikacij, kar pripomore k boljšim poslovnim odločitvam in s tem maksimalne koristi teh projektov. Vložena sredstva v investicijo se torej hitreje povrnejo.

Večja učinkovitost poslovanja

Uporabniki porabijo manj časa za iskanje informacij ter več časa za njihovo uporabo in analizo. Prav tako skrbniki porabijo manj časa za pomoč uporabnikom. Vse to lahko pomeni večjo učinkovitost samega poslovanja.

Večja produktivnost

Boljše informacije vodijo k boljšim in hitrejšim odločitvam. To lahko pomeni tudi hitrejšo izkoriščanje poslovnih priložnosti, ki jih ponujajo nove tehnologije.

Zmanjševanje stroškov

Poslovni portal, ki omogoča uporabnikom, da si sami kreirajo razna poročila, pomeni tudi zniževanje stroškov informacijskih oddelkov, ki so v preteklosti posvetili veliko časa prav pripravi raznih poročil končnim uporabnikom.

Boljša usposobljenost končnih uporabnikov

Boljša usposobljenost končnih uporabnikov ima nekatere stranske učinke kot so nižji stroški uporabe informacijske tehnologije, boljše odločanje, itd. Ima pa tudi pozitiven vpliv na uporabnike same - lahko se poveča njihova samozavest in neodvisnost ter reducirajo razne frustracije, ki izhajajo iz neznanja uporabe računalniških aplikacij.

Elektronsko poslovanje

Zmožnost učinkovitega in varnega dostopa do informacij tudi zunanjim partnerjem povečuje učinkovitost v celotni oskrbovalni verigi (ang. 'supply chain') od dobaviteljev, distributerjev do končnih kupcev. Takšen dostop do poslovnih informacij podjetja je lahko tudi ključni element njegovega elektronskega poslovanja.

3.2. Storitve tretje stranke v poslovanju

Storitve tretje stranke v poslovanju je prevod angleškega izraza »3rd party marketplace« in predstavlja poslovni model, ki je primeren za podjetja, ki prepustijo spletni marketing zunanjemu izvajalcu. Zunanji izvajalec nudi skupen uporabniški vmesnik za kataloge svojih strank, ki so dobavitelji izdelkov. Poleg zagotavljanja varnih transakcij omogočajo trženje blagovne znamke, storitve elektronskega plačilnega sistema in logistiko. Zaradi zagotavljanja varnosti pri elektronskem načinu plačevanja je model privlačen za banke in ponudnike dostopa do omrežja (ang. Internet Service Provider - ISP), ki razpolagajo z ustreznim tehnološkim znanjem in zahtevno opremo. Izvajalci teh storitev se financirajo z plačili za enkratno storitev in plačili za posamezno opravljeno transakcijo. Pri nas je najbolj znano podjetje EON d.o.o.¹

3.3. Virtualne skupnosti

So mreže posameznikov in podjetij, ki funkcionirajo na spletu tako, da prispevajo informacije (strank ali partnerjev) o posameznem izdelku, vrsti izdelkov, uslug in podobno. Vir dohodka podjetjem, ki uporabljajo tak poslovni model so članarine in oglaševanje. Namen virtualne skupnosti je na enem mestu predstaviti poslovne in finančne informacije, ki so urejene in pripravljene tako, da predstavljajo najbolj učinkovit vir informacij za poslovne stranke. Sistem običajno zagotavlja učinkovito iskanje informacij ter spreminjanje in izdelovanje agregiranih poročil na enoten in učinkovit način. Informacije se oblikovane v različne pakete, ki so na voljo strankam glede na

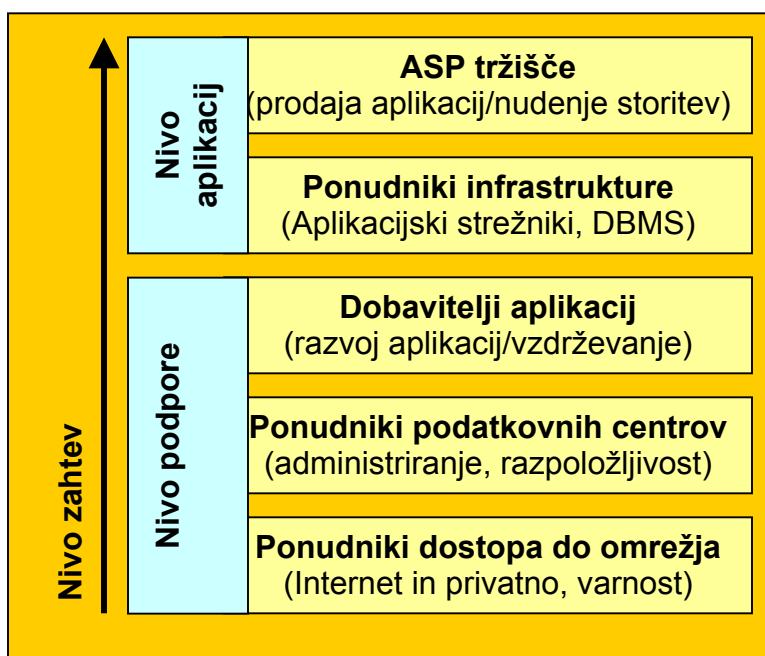
¹ <http://www.eon.si>

njihov interes. Takšne skupnosti predstavljajo Factmerchanta², ki združuje vodilne informacijske hiše Evrope in Azije ali ZapaNet³, ki združuje preko 400 podjetij iz industrije usnjenih izdelkov iz vsega sveta.

3.4. Ponudniki storitev v vrednostni verigi

Elektronsko poslovanje ne pomeni samo uporabo novih tehnologij, temveč tudi novih pogojev na tržišču programske opreme in posredno tudi na celotnem tržišču informacijske in telekomunikacijske tehnologije. Nove možnosti poslovanja in dobave izdelkov in storitev so povzročile oblikovanje novih poslovnih modelov, ki jih imenujemo ponudniki poslovnih aplikacij in storitev (Application Service Provider - ASP).

Slika 14: Udeleženci v ASP vrednostni verigi



Vir: prirejeno po Cimetiere (TechMetric Research)

Današnja podjetja so pod nenehnim pritiskom, saj morajo pri svojem poslovanju obvladovati vse kritične parametre kot so stroški, kvaliteta in čas, ob tem pa se prilagajati spremembam, ki jih narekuje trg. Obvladovanje sprememb je ena ključnih nalog tudi pri elektronskem poslovanju, saj bodo le podjetja, ki so dovolj fleksibilna preživela na vse bolj surovem svetovnem trgu.

Informacijska tehnologija in njena vloga v poslovanju se je v zadnjem desetletju bistveno spremenila. Od prejšnje vloge, ko je bila informacijska tehnologija in informatika le sredstvo, ki je omogočalo razvoj novih poslovnih modelov in način poslovanja, je njena današnja vloga veliko večja, saj dobesedno sili podjetja v uporabo in s tem prestrukturiranje dosedanjih poslovnih procesov in modelov. Poslovni model pomeni, kako podjetje opravlja in odvija svoje poslovanje in definira, kako podjetje ustvarja dohodke za opravljanje svojega poslanstva. Porter definira vrednostno verigo v

² <http://www.factmerchant.com>

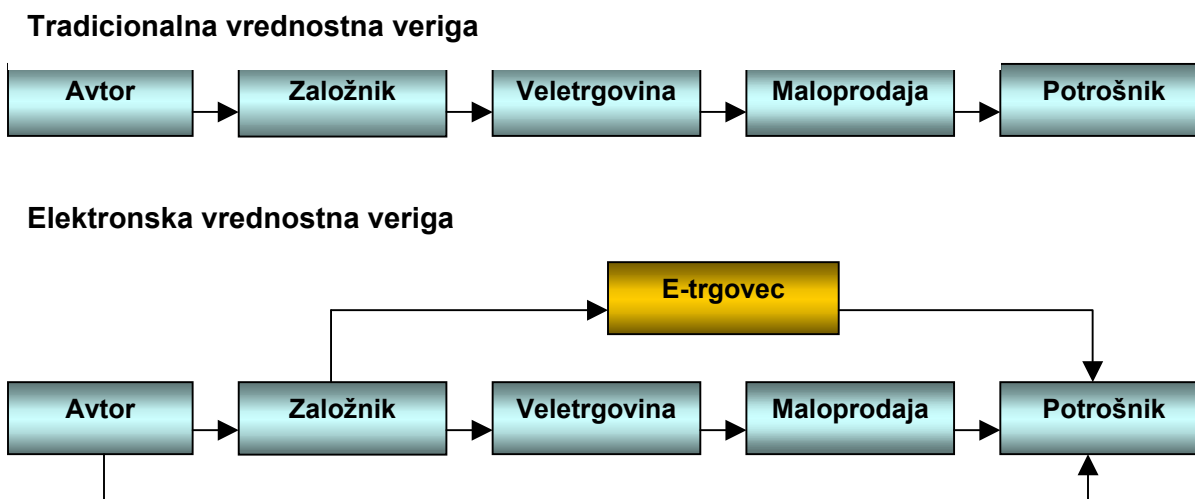
³ <http://www.zapanet.com>

podjetju kot skupek aktivnosti, ki jih podjetje opravlja za doseganje operativnega dobička. Celotna vrednostna veriga dejavnosti se v klasičnem gospodarstvu deli na:

- dobavitelje,
- proizvajalce,
- distributerje,
- prodajalce,
- končne kupce in uporabnike.

Z uporabo spletnih tehnologij so se razmere na tržišču spremenile, saj ponujajo majhnim podjetjem, ki šele vstopajo na tržišče, da z uporabo informacijske tehnologije konkurirajo večjim že uveljavljenim podjetjem. Za že uveljavljena podjetja pa to pomeni spremenjene razmere na tržišču in s tem potrebo po spremembi že utečenih poslovnih procesov, s katerimi so ustvarjala dobiček v preteklosti in potrebo po novem pozicioniranju na tržišču, kakor tudi v vrednostni verigi dejavnosti.

Slika 15: Primerjava med tradicionalno in elektronsko vrednostno verigo



V založništvu poteka tradicionalna vrednostna veriga od avtorja, založnika, distributerja in prodajalca do končnega kupca (*slika 15*). Z uporabo informacijske tehnologije pa se odprejo nove možnosti tako za trgovce, založnike in avtorje. Na področju založništva je najbolj znana spletna knjigarna Amazon⁴, katere poslovni model temelji na kvaliteti storitev. Z elektronskim založništvom, se lahko avtorji izognejo vsem posrednikom v verigi in omogočijo, da njihovo delo prispe do končnega potrošnika.

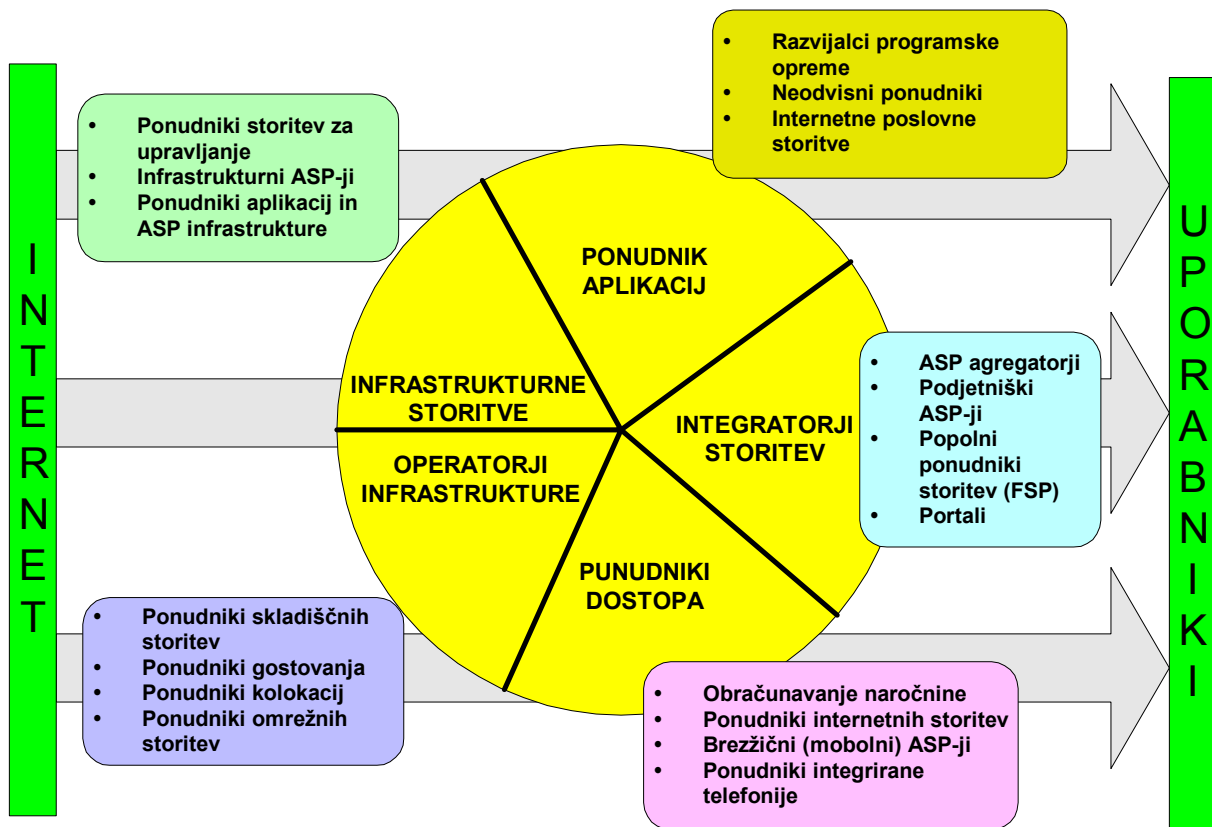
Tako kot so se razvijale zahteve in potrebe uporabnikov informacijske tehnologije, so se spreminjali tudi poslovni modeli podjetij, ki se ukvarjajo z informacijsko tehnologijo. Veliko število specializiranih ponudnikov informacijskih rešitev je v mnogih podjetjih povzročilo kopičenje slabih ali nekompatibilnih informacijskih rešitev. S spletnimi tehnologijami in s široko uporabo interneta imajo informacijska podjetja možnost

⁴ <http://www.amazon.com>

ponuditi storitve, ki kupcem omogočajo, da imajo informacijsko podporo načrtovano in pod stalno kontrolo, kar posledično zmanjšuje stroške.

Slika 16 prikazuje udeležence v vrednostni verigi, ki uporabniku omogočajo dostop, uporabo in storitve internet-a. Podjetja na področju žičnih in brezžičnih (mobilnih) telefonskih komunikacij zagotavljajo ustrezno komunikacijsko infrastrukturo, naslednji člen so podjetja, ki ponujajo ustrezno platformo za gostovanje aplikacij različnih proizvajalcev programske opreme. Podjetja, ki omogočajo dostop do interneta (ang. »Internet Service Providers«), razvijalci aplikacij, ko dejansko kreirajo vsebino rešitev in kot zadnji člen so podjetja, ki imajo stik s končnim uporabnikom aplikacij. To so podjetja, ki vzdržujejo različne poslovne portale in jih imenujemo agregatorji poslovnih storitev in rešitev.

Slika 16: Vrednostna veriga ASP-jev



Vir: prirejeno po Wainwright, 2001,

4. Zaščita in varovanje podatkov

Že pred uporabo interneta, ko so bili računalniški sistemi med seboj povezani le preko modemske povezave, so nepridipravi poskušali vdirati v računalniške sisteme tako, da bi se izognili avtorizaciji. Izredna rast novih omrežij, ki jih omogočajo novejša telekomunikacijske tehnologije so povzročile naraščanje števila in oblik kriminalnih dejanj.

Internet je verjetno najbolj kompleksen sistem, ki je bil do sedaj razvit. Povezuje preko 400 milijonov računalnikov v nepredstavljivo kompleksno fizično omrežje. Na vsakem računalniku deluje na stotine programov, od katerih nekateri vplivajo na delo drugih programov na istem ali kateremkoli drugem računalniku v mreži. Digitalni sistemi so zapleteni, saj že preprost program vsebuje na stotine kodnih vrstic.

Slika 17: Trend povečevanja števila kodnih vrstic OS

| Operacijski sistem | Leto | Število kodnih vrstic |
|--------------------|------|-----------------------|
| Windows 3.1 | 1992 | 3×10^6 |
| Windows NT | 1992 | 4×10^6 |
| Windows 95 | 1995 | 15×10^6 |
| Windows NT 4.0 | 1996 | $16,5 \times 10^6$ |
| Windows 98 | 1998 | 18×10^6 |
| Windows 2000 | 2000 | $35 - 60 \times 10^6$ |

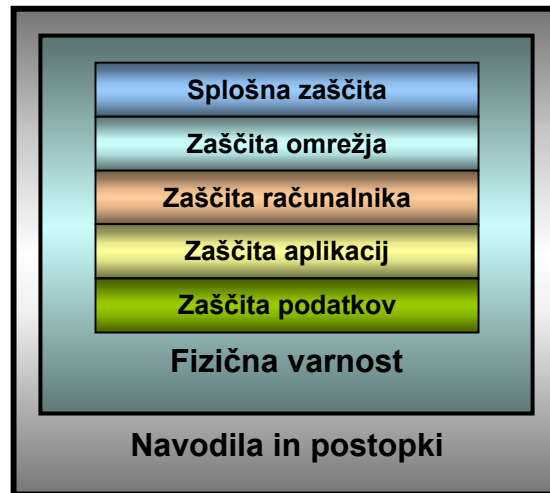
Vir: prirejeno po Schneier, 2000, str. 357

Sistemi povezani med seboj se formirajo v večje sisteme. Med njimi so lahko tudi takšni, ki vsebujejo skrite napake in počnejo nepredvidljive stvari, ki so neodvisne od uporabnikov. Takšne napake računalniških sistemov imenujemo hrošči (ang. Bug) in pomenijo nenaden pojav, ko se sistem v posebnih primerih nepričakovano in nepredvidljivo obnaša.

V teoriji deluje sistem dobro in varno le v idealnih razmerah in laboratorijskih pogojih, ki jih v praksi ne moremo pričakovati. Pri načrtovanju želimo graditi idealne sisteme in aplikacije, ki bodo omogočale najvišjo možno stopnjo varnosti, vendar je popolno 100% varnost, v realnih razmerah nemogoče doseči.

Na sliki 18 so prikazani elementi globalne strategije zaščite, ki so v poglavju 4.1. podrobneje opisani.

Slika 18: Elementi v globalni strategiji zaščite



Vir: prirejeno po Microsoft 2002, str.22

4.1. Temeljne zahteve varnosti

Celovitost (vir: KDD – interna dokumentacija)

- zavarovanje stavbe, vhodov, prostorov z računalniško in TK opremo,
- analizo stanja in poslovnih procesov podjetja, identificiranje kritičnih faktorjev poslovanja,
- notranje in zunanje okolje podjetja,
- usposabljanje ljudi,
- nadzor dostopa do informacijskih in TK sistemov,
- upravljanje s pravicami uporabnikov,
- zaščita pred virusi, črvi in logičnimi bombami,
- zaupnost podatkov pri prenosu preko omrežij,
- varnost podatkovnih baz.

Dokumentiranost

- podrobno napisana pravila,
- postopkov in načinov za uporabo sredstev za varovanje,
- predpisani varnostni ukrepi,
- identifikacija pomembnosti oziroma vrednosti podatkov,
- identifikacija posledic.

Preventiva, odkrivanje in ukrepanje

- preventiva na področju celotne varnostne politike,
- pravočasno odkrivanje in obveščanje o poskusih kršitve varnosti (sporočanje preko SMS, elektronske pošte službi za varovanje,..)

Nenehno izboljševanje in nadgrajevanje

- uporaba zadnjih proti virusnih programov,
- popravki operacijskega sistema. (Večina vdorov, ki so jih Crackerji izkoriščali je bilo znanih več let, preden jih je Microsoft odpravil s popravki.)

Plan ukrepov in zaščite v primeru izjemnih nesreč oziroma nepredvidenih dogodkov

- Kako bi vdor v sistem vplival na delo organizacije kot celote?
- Kako dolgo lahko organizacija vzdrži brez informacijskega sistema?
- Kakšni so stroški odprave posledic?
- Kako bodo reagirali partnerji?

Zavarovanje

Odškodninsko zavarovanje informacijskih sistemov (CIDS - Computer Information and Data Security Insurance) ponuja zavarovalnica Lloyds in sicer do 50 milijonov USA\$ odškodnine za:

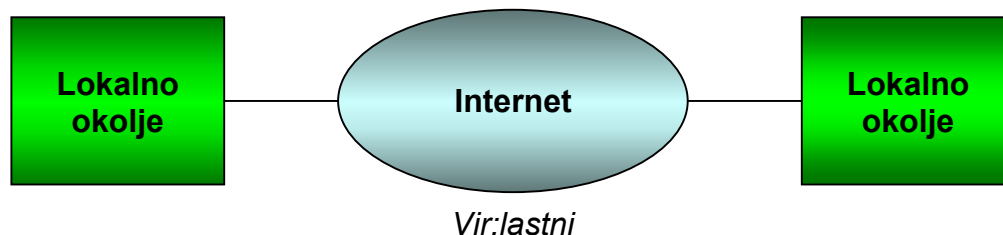
- zlonamerno dejanje zaposlenih ali tretjih oseb,
- izgubo računalniških sistemov in programov,
- izgubo elektromagnetnih podatkov in medijev,
- napade računalniških virusov,
- vdore v informacijske sisteme,
- prekinitvev poslovanja

4.1.1. Varnost na internetu

Internet ima dve pomembni karakteristiki:

- porazdeljen pretok
- odprte komunikacije

Slika 19: Poenostavljen model povezave preko interneta.



Lokalno okolje (*slika 19*) lahko predstavlja samostojni osebni računalnik (PC) ali večje število različnih delovnih postaj povezanih v lokalno omrežje (LAN - Local Area Network). Delovanje posameznih nalog je lahko porazdeljeno med lokalnimi okolji povezanimi preko interneta. Internet je odprt sistem zato nezaščiteni podatki lahko pridejo v roke tretjim osebam, ki lahko podatke zlorabijo ali spremenijo in spremenjene pošljejo pravemu naslovniku.

4.1.2. Okolje

Pogosto prodajalci v svojih oglasih zatrjujejo, da je njihov sistem ali program varen ali pa zagotavljajo popolno varnost njihovega poslovanja (trgovanja) na spletu. Zastavlja se vprašanje: "Varen pred kom?" in "Varen pred čim?"

Različne varnostne tehnologije imajo pomembno vlogo pri celotni varnostni zaščiti. Sistem je lahko varen pred povprečnimi uporabniki, organiziranimi kriminalci, industrijskimi vohuni ali državnimi varnostnimi službami z izkušnjami in najsodobnejšimi

pripomočki, dokler se ne zgodi določena matematična odvisnost, poteče določen čas, ali pred določenimi načini vdora.

Potencialne sovražnike lahko kategoriziramo glede na:

- Namen; povzročiti materialno škodo, kraja informacij, finančna kraja, itd.. Ta kategorizacija je prvi korak pri postavitvi protiukrepov.
- Dostopnost; notranji sovražnik (zaposleni, svetovalci, pogodbeni izvajalci, ...) ima lažje delo kot zunanji, saj je že znotraj sistema in pozna organizacijo in notranjo strukturo. Med zunanje sodi "Hacker", ki s svojimi dejanji ni pridobitno usmerjen in "Cracker", ki deluje s slabimi nameni. Za oba velja da dobro obvladata računalniške sisteme in omrežja.
- Dostop do pripomočkov in virov. Nekateri imajo na voljo le skromna sredstva, drugi pa najmodernejšo strojno in programsko opremo.
- Znanje. Nekateri nimajo praktično nikakršnega znanja drugi so šolani in izkušeni.
- Tveganje, ki so ga pripravljene sprejeti. Teroristi so pripravljene umreti za svojo stvar, medtem ko kriminalci tvegajo le zaporno kazen.

4.2. Vrste napadov

Napadi so lahko različni in jih lahko razdelimo na (Schneier, 2000, str.23 do 41) :

- Prezare in zvižace kot so razne piramidne in več nivojske trgovalne sheme.
- Uničevalne napade (ang. 'Denial of Service – DOS'), ki imajo namen fizično poškodovati eno ali več komponent računalnika, uničiti ali poškodovati podatke ali obremeniti nek sistem do te mere, da ga ni mogoče normalno uporabljati. V začetku leta 2000, je bil izvršen tak napad, ki je povzročil prenehanje delovanja Yahoo, Amazon, CNN in še nekaterih strežnikov.
- Krajo intelektualne lastnine. Elektronska verzija knjig, revij in časopisov, digitalna glasba, filmi, programska oprema, zasebne podatkovne zbirke se lahko preko elektronskih medijev hitro razmnožujejo brez avtorjeve vednosti in privolitve. Za leto 1997 je BSA³ objavil podatek, da so podjetja, ki se ukvarjajo s programsko opremo izgubila 28.900 \$ na minuto ali 15 milijard \$ v celem letu zaradi piratstva.
- Krajo identitete. Pridobiti osebne podatke nekoga preko informacijskih povezav je manj tvegano in lažje kot vlom v njegovo hišo.
- Krajo zaščitne znamke. Pri elektronskem trgovanju, ko ima vsakdo lahko svojo spletno stran, uporabniki težko ločijo katera stran je vredna ogleda, kje je varno naročiti izdelke in kupovati in s katerimi se je varno povezovati. Vsakdo se lahko na svoji spletni strani baha z znanimi imeni svetovnih proizvajalcev in ponuja proizvode svetovnih znamk z namenom čim boljše prodaje svojih izdelkov.
- Kršitve zasebnosti niso vedno kriminalno dejanje, lahko pa so. Ljudje danes niso več lastniki svojih osebnih podatkov, ampak se ti nahajajo v najrazličnejših računalniških sistemih. Zdravstveni podatki, premoženjsko stanje, nakupovalne

³ BSA - Business Software Alliance

navade, itd. so predmet najrazličnejših tržnih raziskav, ki veliko stanejo, zato je mnogokrat hitreje in ceneje priti do nelegalnih podatkov.

- Nadzor. Banke, menjalnice, trgovine in mnoge druge javne površine so opremljene z video nadzorom. V veselju je na stotine satelitov, ki služijo za prenos radijskih in televizijskih signalov, za meteorološke, navigacijske in znanstvene namene poleg tega pa služijo vojaškim ter protiobveščevalnim službam in drugim. Sam nadzor ni sporen, ne sme pa se tako zbrane podatke zlorabljati v nepoštene namene.

4.2.1. Prisluškovanje komunikacijskemu kanalu

Sporočila med odjemalcem in strežnikom tečejo v digitalni obliki po javnih telefonskih linijah, katerim ni težko prisluškovati. Sporočila se lahko prestreže in čeprav so kodirana je možno ugotoviti pravi - originalni pomen sporočila. Od načina kodiranja je odvisno v kakšnem času bodo dekodirana.

4.2.2. Spreminjanje

Prestrežena sporočila in zlonamerno spremenjena lahko vplivajo na obnašanje odjemalca, strežnika ali celo prekine povezavo med njima in s tem onemogoči delo na spletu. Prestrežena elektronska pošta se lahko spremeni in spremenjena vsebina pošlje prejemniku kateremu je bila namenjena.

4.2.3. Nepooblaščen uporaba virov

Zdravstveni podatki so ključnega pomena za zdravnika pri pregledu pacienta, so pa tudi dragocen podatek zavarovalnicam pri politiki sklepanja življenjskih zavarovanj.

4.2.4. Nepooblaščen razkritje informacij

Novinarji pogosto prihajajo do različnih informacij na bolj ali manj legalen način. Z objavo le teh pa poskušajo pritegniti medijsko pozornost (povečanje naklade časopisa ali gledanosti TV kanala).

4.2.5. Analiza prometa

Analiza prometa predstavlja študijo komunikacijskih vzorcev. V tem primeru ni pomembna vsebina medsebojnih sporočil ampak njihova karakteristika. Kdo komunicira in s kom? Kdaj? Kako dolga so sporočila? Kako hitro so posredovani odgovori in kako dolgi so? Kakšni so odzivi na posamezna sporočila? Odgovori na ta sporočila lahko dajo veliko informacij. V resnici se ne zavedamo kako zelo ranljiva je naša komunikacija (še posebno preko interneta) za takšne analize.

4.2.6. Bankomati

Avtomatske blagajne - bankomati (ang. Automatic Teller Machines - ATM) dokazujejo, da so varnostni modeli bolj zapleteni kot si lahko predstavljamo. ATM zbira podatke, ki jih pridobiva iz magnetne kartice uporabnika. To so lahko zaupni podatki kot so identifikacijska številka (ang. Personal Identification Number - PIN), uporabniško ime in tip uporabnika, ki jih pošilja na centralni strežnik, ki nato vrne sporočilo na podlagi katerega se odobri ali zavrne postopek izplačila denarja, zadrži ali vrne magnetno kartico in podobno.

ATM mora biti zaščiten pred fizičnim vdorom do denarja in pred krajo celega avtomata. Prvi avtomati so delovali v prostorih bank ali v dobro varovanih okoljih. S povečanjem števila in razširitvijo ponudbe avtomatov se je njihova velikost zmanjšala. Locirani so praktično na vseh mestih kjer človek potrebuje gotovino; večjih trgovinah, blagovnih centrih, bencinskih servisih, poštah itd.

4.2.7. Varnost strežnika

Strežnik ali gostitelj računalnik je lahko predmet vdora z namenom pridobiti pomembne podatke kot so na primer številke kreditnih kartic, številke bančnih računov s stanji itd.

Strežnike ločimo glede na uporabo:

- Javna uporaba – podatki na strežniku so namenjeni javnosti in dostop do podatkov ni omejen.
- Notranja uporaba – informacije so internega značaja, namenjene zaprti skupini ljudi in njihovo javno razkritje lahko povzroči organizaciji škodo.
- Zaupna uporaba – razkritje informacij lahko povzroči resno škodo in pomeni grožnjo celotni organizaciji. Informacije so zaupne narave in izmenjava poteka samo med poznanimi subjekti. Po priporočilih Microsoft-a morajo biti informacije zavarovane z vsaj dvema požarnima zidovoma pred internet okoljem.

4.2.8. Človeški dejavnik

Popolno varnost v računalništvu je težko morda celo nemogoče doseči, vendar si je potrebno vedno prizadevati, da bi jo dosegli. Uporabo šifriranja zaupnih dokumentov, varnih protokolov, zanesljive in varne strojne in programske opreme na žalost niso dovolj. Najšibkejši člen v varnostni verigi je človek.

Za poprečnega uporabnika je pomembno, da mu računalnik služi pri njegovem delu in ga podrobno o delovanju računalnika in varnost ne zanima, zato so ljudje najšibkejši člen v varnostni verigi. Gledano z uporabniške strani računalniki delajo tako malo napak, da takrat ko se napaka zgodi ne verjamejo, da se je zgodila in ne vedo kako v takem primeru ukrepati.

4.2.9. Zanesljivost programske opreme

Programska oprema je vedno bolj kompleksna. V implementaciji varnostnih funkcij in sistemov se skrivajo napake. Kljub temu, da se vlaga velika sredstva v razvoj novih verzij operacijskih sistemov in programskih orodij se v programih pojavljajo napake, ki lahko usodno vplivajo na varnost. Proizvajalci programske opreme po odkritju napake izdelajo popravke, ki jih moramo ažurno spremljati in naložiti na svoj sistem.

4.3. Varnostne storitve

Varno elektronsko poslovanje zagotavljajo naslednji pojmi (Jerman Blažič, 2001, str.101):

- **overjanje** identitete subjektov s katerimi se komunicira in izvor podatkov,
- **zaupnost** določenih informacij, ki ne smejo biti razkrite tretjim osebam,

- **neokrnjenost** podatkov, ki morajo biti zaščiteni pred nepooblaščenim spreminjanjem. Če je do spremembe prišlo jo moramo biti sposobni odkriti,
- **nadzor** dostopa do sredstev nepooblaščenim osebam ali uporabe sredstev v namene za katere niso predvidena,
- **preprečevanje zanikanja** subjektov sodelujočih v določeni aktivnosti elektronskega poslovanja, ki so v tej aktivnosti dejansko sodelovala,
- **razpoložljivost** storitev elektronskega poslovanja mora biti stalno na voljo.

4.4. Kriptografski mehanizmi

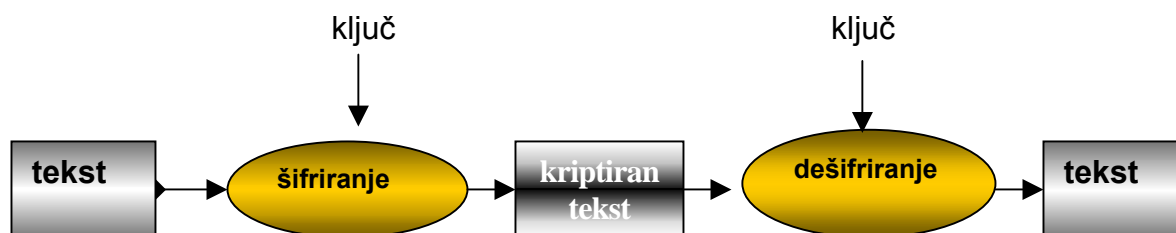
Kriptografija (beseda izhaja iz grške besede "kryptos logos", ki pomeni skriti tekst) je veda o zakrivanju sporočil, ki se je skozi zgodovino ukvarjala s problemom, kako skriti pomembne informacije ali zaupne podatke pri komunikaciji. Temelji na matematičnih problemih, ki so težko rešljivi. V preteklosti se je kriptografija uporabljala predvsem v vojaške namene, z razvojem računalniških omrežij pa je postala nujna v vsakdanjem življenju. Kriptografija je podlaga za šifriranje sporočil, elektronsko podpisovanje, postopek za preverjanje identitete, nadzor dostopa, zagotavljanje neokrnjenosti ter beleženje in nadzor.

4.4.1. Šifriranje

Šifriranje pomeni transformacijo podatkov v obliko, ki onemogoča njihovo razumevanje in tako zagotavlja tajnost. Obratni proces je dešifriranje.

Simetrično šifriranje (*slika 20*) pomeni, da je isti ključ namenjen tako šifriranju kot dešifriranju sporočil. Pošiljatelj sporočila uporablja enak ključ kot prejemnik, to pa predstavlja problem pri izmenjavi ključev. Pri večjem številu uporabnikov pa se pojavi velika količina ključev, saj vsak par uporablja svoj ključ.

Slika 20: Simetrično šifriranje



Vir: povzeto po Fegghi, 1999, str.33

Za šifriranje podatkov v elektronskem poslovanju so v uporabi različni matematični algoritmi. Med najbolj znanimi je simetrični algoritem DES (Data Encryption Standard), ki pa se zaradi prekratkih ključev opušča. Za naslednika je bil 2. 10.2000 izbran AES (Advanced Encryption Standard), katerega avtorja sta Joan Daemen in Vincent Rijmen. AES ponuja možnost uporabe treh dolžin ključev: 128, 192 in 256 bitov, prav take so

tudi možne dolžine blokov. Število zank je odvisno od kombinacije dolžin bloka in ključa:

| Število zank | | | |
|--------------|----------|----------|----------|
| | Blok=128 | blok=192 | Blok=256 |
| ključ=128 | 10 | 12 | 14 |
| ključ=192 | 12 | 12 | 14 |
| ključ=256 | 14 | 14 | 14 |

Iz ključa se na začetku izračunajo ključi za vsako zanko. V vsaki zanki se zvrstijo substitucije in premiki, nazadnje pa se prišteje ključ za zanko. Na začetku se bo večinoma uporabljali algoritem s 128-bitnim ključem nad 128-bitnimi bloki v desetih zankah. Avtorja zatrjujeta, da že šest zank dovolj razprši informacijo.

Pri simetričnem šifriranju se uporabljata dva načina šifriranja. Pri blokovnem načinu se tekst razdeli na bloke enake dolžine (običajno 64 bit). Na sliki 21 so opisani algoritmi nekaterih ključev.

Slika 21: Tabela algoritmov

| Algoritem | Način šifriranja | Dolžina ključa |
|------------|------------------|-----------------------|
| Blowfish | Blok | Spremenljiva do 448 |
| DES | Blok | 56 |
| IDEA | Blok | 128 |
| RC2 | Blok | Spremenljiva 1 – 2048 |
| RC4 | Niz | Spremenljiva 1 – 2048 |
| RC5 | Blok | Spremenljiva 1 – 2048 |
| Triple DES | Blok | 56, 112 |

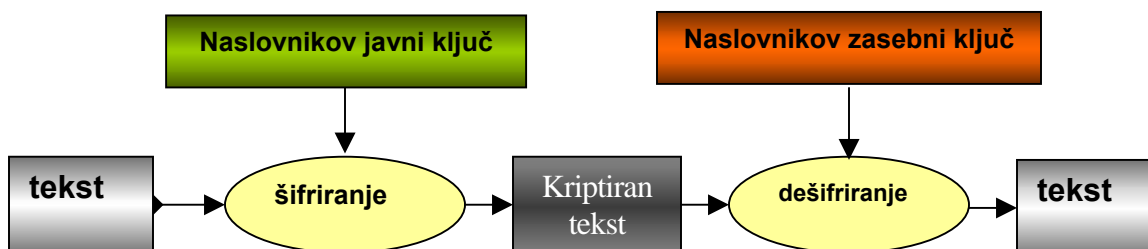
vir: Fegghi, 1999, str.34

Asimetrično šifriranje (slika 22) je v uporabi od leta 1976. Značilnost tega sistema je, da ključa za šifriranje in dešifriranje nista enaka. Ključi nastopajo v parih vendar iz enega ključa, brez poznavanja dodatnih informacij ni mogoče določiti drugega. En ključ lahko zato javno objavimo in se imenuje javni ključ, drugega pa zasebni ključ, ki ga mora lastnik varno shraniti. Zaupno sporočilo kodirano z javnim ključem lahko dešifrira le oseba z ustreznim zasebnim ključem.

Asimetrični kriptosistemi so veliko počasnejši od simetričnih, zato se le redko uporabljajo za daljša sporočila. Običajno se šifrirajo podatki s simetričnim kriptosalgoritmom, ključa za te algoritme pa z asimetričnimi.

Algoritem javnega ključa je spremenljiv (reverzibilen), če se lahko uporabi istočasno za kriptiranje in elektronski podpis. Nespremenljiv javni ključ se uporablja samo za digitalni podpis. Nespremenljiv algoritem javnega ključa lahko zakriptira besedilo, ne more pa dekriptirati šifriranega besedila.

Slika 22: Asimetrično šifriranje



Vir: povzeto po Fegghi, 1999, str.33

Najpogosteje uporabljen asimetrični kriptografski algoritem je RSA (avtorji: Rivest, Shamir, Adleman), katerega pomanjkljivost je predolga dolžina ključa in počasnost. Algoritmi, ki delujejo na osnovi eliptičnih krivulj zagotavljajo enako stopnjo varnosti pri krajši dolžini ključa in večji hitrosti, kar je velika prednost za uporabo pri pametnih karticah.

Varnost šifrirnih algoritmov

Predpostavlja se, da so najbolj znani in preizkušeni simetrični algoritmi varni in ne vsebujejo nikakršnih varnostnih lukenj. Dešifrirati jih je možno tako, da se preizkusi vse možne ključe, to pa zahteva določen čas, ki je odvisen od velikosti ključa in zmogljivosti opreme. Za varnost je zelo pomembno, da je velikost ključev in s tem tudi število ključev čim večje. Algoritmi s 40 bitnim ključem danes ne predstavljajo več varnega poslovanja. Pri ključu dolžine 56 bitov je vseh možnih ključev 2^{56} ali približno 10^{17} . Z dovolj zmogljivim računalnikom je možno vse kombinacije preizkusiti v enem dnevu.

Pri asimetričnih algoritmih poleg preizkušanja vseh možnih ključev obstajajo tudi druge metode za razkrivanje. Velikost ključev za simetrično in asimetrično šifriranje ne smemo slepo primerjati med seboj.

4.4.2. Elektronski podpis

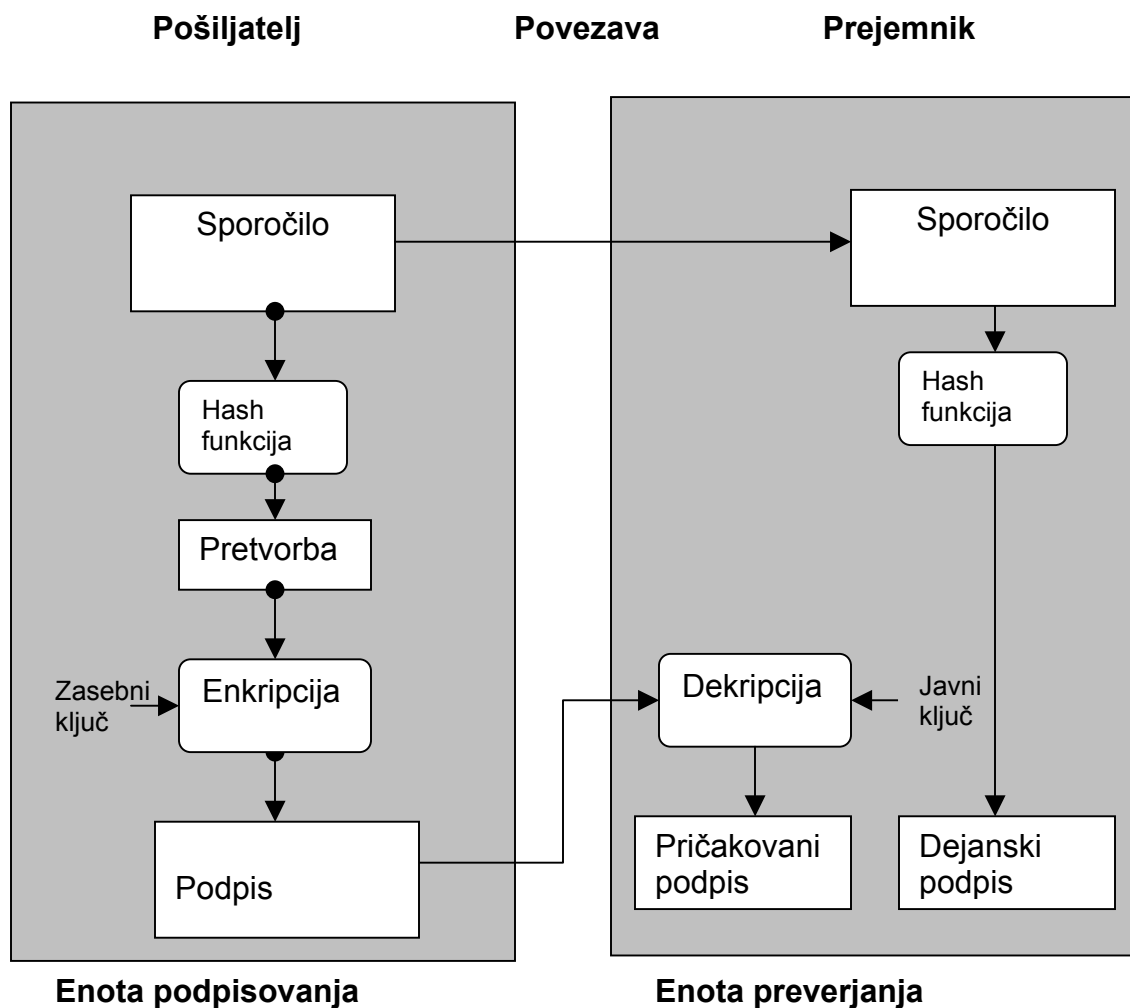
V elektronskem poslovanju se uporablja elektronski podpis namesto lastnoročnega podpisa. Za elektronsko podpisovanje obstaja več metod. Med bolj enostavne načine sodi vključitev slike lastnoročnega podpisa v dokument, podpis z elektronskim peresom in metode na podlagi simetričnih kriptografskih mehanizmov kot je MAC (Message Authentication Code). Enostavne metode ne zagotavljajo tako visoke varnosti kot digitalno podpisovanje, ki temelji na asimetrični kriptografiji. Neokrnjenost podpisanega dokumenta je pogoj za veljavnost podpisa. Digitalni podpis je odvisen od vsebine sporočila in postane neveljaven ob vsaki najmanjši spremembi v besedilu, zato ga ni možno kopirati in z njim podpisati druge dokumente. Identiteto podpisnika lahko vsakič preverimo, zanikanje podpisnika pa je skoraj nemogoče, saj je praktično nemogoče določiti zasebni ključ, ki je znan le njegovemu lastniku.

Od zahtev uporabnika in okolja je odvisno kakšno metodo in obliko podpisa se bo uporabilo. Najpogosteje se uporablja algoritem RSA v kombinaciji z enosmernimi zgoščevalnimi funkcijami in metoda DSS.

Pri RSA se uporablja dva ključa enako kot pri šifriranju z asimetričnim ključem. Zasebni ključ za podpisovanje mora poznati in ga lahko generira le lastnik, ki se z njim identificira. Pri šifriranju pa ključ omogoča dostop do šifriranih podatkov in ga lahko pozna več subjektov. Podpis dokumenta poteka v dveh korakih (*slika 23*). Podatke se najprej skrči z eno od zgoščevalnih (hash) funkcij, ki poljubno dolgo besedilo preslika v blok konstantne dolžine. Dobljeni blok, ki predstavlja »prstni odtis« besedila se nato šifrira z zasebnim ključem in tako dobimo digitalni podpis.

Preverjanje podpisa poteka tako, da se najprej dešifrira podpis z javnim ključem, nato pa se izračuna vrednost enosmerne zgoščevalne funkcije podpisanih podatkov. S primerjavo blokov, ki morata biti enaka, ugotovimo ali je podpis pravi.

Slika 23: Generiranje digitalnega podpisa in preverjanje



Vir: prirejeno po Fegghi, 1999, str.47

4.4.3. Digitalni certifikati

Pri uporabi javnih ključev se je potrebno prepričati, da ključ pripada pravi entiteti, ki jo lahko predstavlja oseba, strojna oprema (računalnik ali usmerjevalnik) ali programski

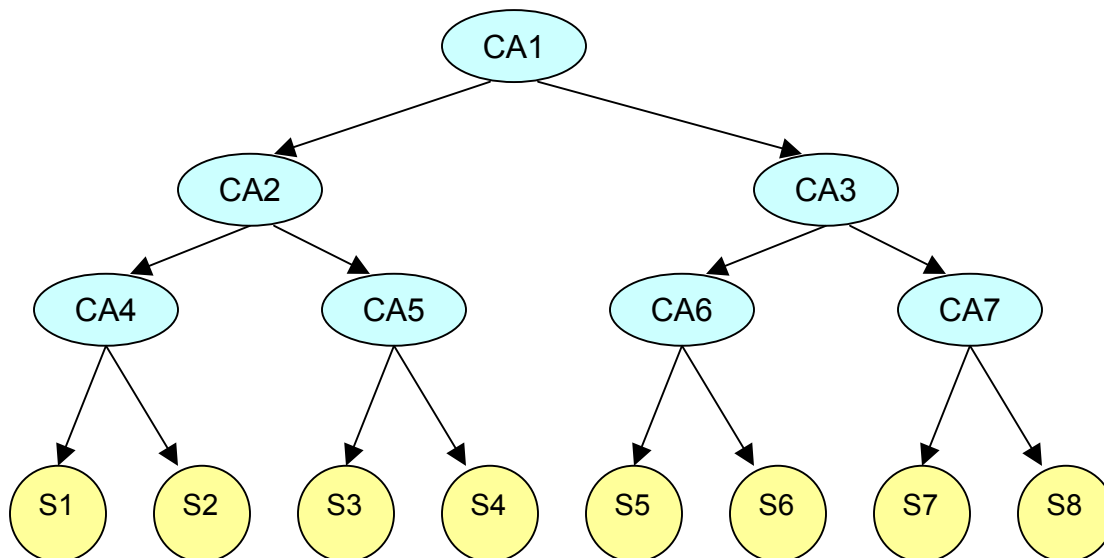
proces. Overjanje javnih ključev je temeljni pogoj za uporabo varnostnih mehanizmov, ki temeljijo na asimetrični kriptografiji. Overjanje omogočajo posebne ustanove oziroma agencije za certificiranje javnih ključev (ang. Certificate Authority - CA). Agencija izda lastniku javnega ključa digitalno podpisano potrdilo (certifikat), s katerim drugim uporabnikom zagotavlja avtentičnost ključa in s tem identiteto lastnika certifikata.

Certifikati se izdajajo za različne namene in v različnih okoljih; elektronskem bančništvu, državni upravi, akademskem ali vojaškem okolju, zato obstajajo tudi različne agencije za certificiranje javnih ključev, ki se lahko med seboj logično povezujejo. Večina je komercialnih agencij med katerimi je najbolj poznana Verisign. Ključi znanih AC so lahko vgrajeni v programsko opremo kot je spletni brskalnik, ali pa jih tja sami dodamo. Na certifikat moramo paziti in ga hraniti skoraj tako kot svoj zasebni ključ.

SI-CA (Slovenian Certification Authority) je bila prva agencija za overjanje v Sloveniji, ki je s svojim delom pričela že v letu 1995 v okviru evropskega projekta ICE-TEL. SI-CA spada danes pod okrilje Zavoda za varnostne tehnologije informacijske družbe in elektronsko poslovanje (SETCCE). SI-CA je namenjen vsem uporabnikom varnostnih tehnologij, zasnovanih na standardiziranih potrdilih X.509. S članstvom v panevropski mreži overiteljev EuroPKI, namenjeni akademski in izobraževalni sferi ter podpisuje javne ključe drugih slovenskih overiteljev, posameznikov in spletnih strežnikov organizacij.

Poleg SI-CA ima svojo agencijo tudi Center vlade za informatiko, Trade Point Slovenija ter nekatere komercialne organizacije. Za potrebe identifikacije svojih komitentov izdaja digitalne certifikate tudi NLB.

Slika 24: Hierarhija certificiranja



Vir: Fegghi, 1999, str. 85

Puščica na sliki 24 med agencijo za certificiranje CA in podpisnikom S pomeni, da je agencija certificirala podpisnikov javni ključ. Zaupanje med posameznimi izdajatelji pomeni, da si morajo med seboj zaupati tudi nadrejene CA.

4.5. Zakonodaja in pravni okviri

Kazensko pravni pregon je pri kršitvah preko omrežij problematičen, saj nastopijo problemi, ko nekdo iz svojega doma preko elektronskega omrežja izvrši kriminalno dejanje v drugi državi ali celo drugem kontinentu. V kateri državi in po katerih veljavnih zakonih se naj kršitev obravnava? Zaradi hitrega tehnološkega razvoja tudi zakonodaja v državah po svetu ne sledi vsem oblikam možnega kriminala. Nekatere države nimajo zakona za pregon internet kriminalcev. Zakoni in pravni okviri ne služijo le pregonu in zatiranju kriminala ampak tudi legalizaciji in zakonski uporabi najnovejših načinov in postopkov elektronskega poslovanja. Na mednarodni ravni je bil leta 1996 sprejet modelni zakon o elektronskem poslovanju pri komisiji Združenih narodov za mednarodno gospodarsko pravo UNCITRAL. V pripravah za vstop v Evropsko skupnost (ES) je za Slovenijo pomembna predvsem evropska zakonodaja. ES je konec leta 1999 sprejela direktivo z naslovom Okvir Unije za elektronske podpise (A Community framework for electronic signatures), ki so jih morale države članice sprovesti do postavljenega roka 19.7.2001. Direktiva obravnava vse vrste elektronskih podpisov in izpostavlja podpise, ki imajo enako pravno osnovo kot lastnoročni podpis pri dokumentih v papirni obliki.

V skladu z direktivo ES je bil junija 2000 v Sloveniji sprejet zakon o elektronskem poslovanju in elektronskem podpisu. Zakon razlikuje elektronski in varni elektronski podpis ter navadna in kvalificirana potrdila (digitalni certifikat), določa pogoje, ki jih morajo izpolnjevati ponudniki in uporabniki storitev v zvezi z overovljanjem javnih ključev in elektronskimi podpisi ter določa tehnične zahteve za varno elektronsko podpisovanje, obliko digitalnih potrdil in akreditacijsko shemo, ureja odgovornosti vpletenih subjektov in določa oblike nadzora ponudnikov storitev. Zardi hitrega tehnološkega napredka in sprememb v informacijski tehnologiji je zakon tehnološko nevtralen. Podrobnejše tehnične zahteve in merila bodo opredeljena v podzakonskih aktih.

5. Podatkovno rudarjenje za splet

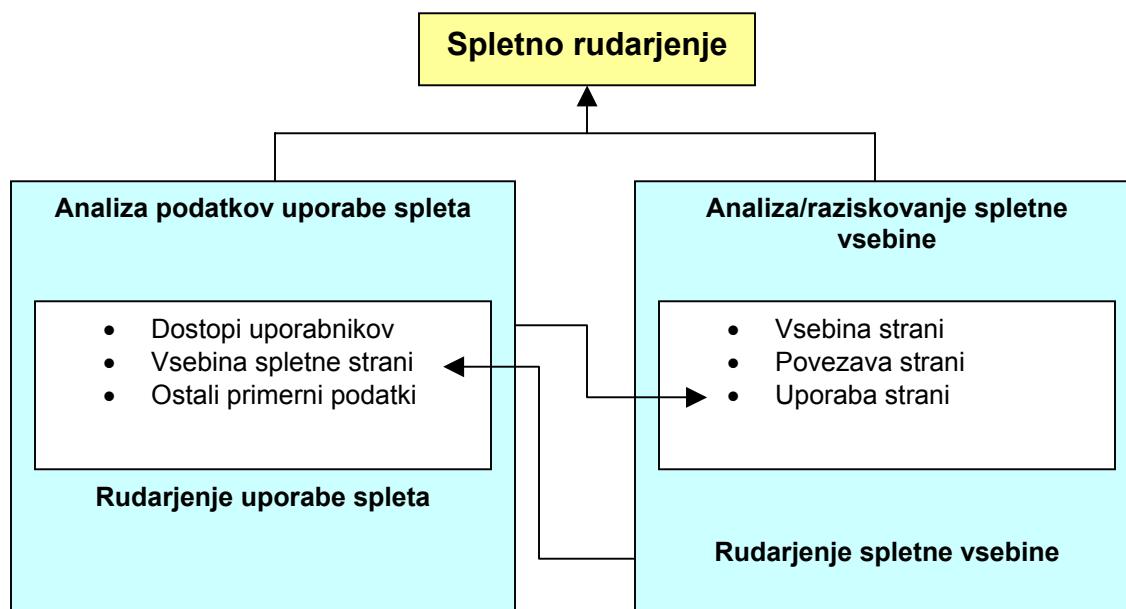
Splet je povzročil revolucionarne spremembe načina komuniciranja in medsebojnega sodelovanja. Ponuja nove načine poslovanja business-to-business (B2B) in business-to-customer (B2C), nove mehanizme za medsebojno komuniciranje person-to-person (P2P) in nove načine raziskovanja in uporabe informacij. Splet se lahko obravnava kot ničvredno močvirje ali zlata jama, saj lahko vsebuje izvrstne, dvomljive in nesprejemljive ali preprosto nepoznane informacije.

Uspehi pri uporabi podatkovnega rudarjenja konvencionalnih podatkov so spodbuda za tovrstna raziskovanja spletnih informacij. V odvisnosti od namena raziskovanja uporabe podatkov ločimo:

- rudarjenje spletne vsebine
- rudarjenje uporabe spleta

Rudarjenje spletne vsebine (*slika 25*) se koncentrira na raziskovanje uporabnih informacij na spletu in analizira, kategorizira in klasificira dokumente. Pri analizi dokumentov nas ne zanima samo vsebina dokumenta, ampak tudi medsebojne povezave na spletnih straneh in potencialni vpliv na semantiko povezav. Dostopi do strani lahko pokažejo, kako uporabniki dojemajo in razumejo vsebino in medsebojne vsebinske povezave.

Slika 25: Podatkovno rudarjenje za splet



Vir: Masand at al., 2000, str.1

5.1. Rudarjenje za ugotavljanje uporabe spleta

Internet uporablja množica uporabnikov, ki predstavljajo velik potencial za oglaševanje. Dandanes je postalo že običaj, da spletne strani vsebujejo oglase. Oglaševalci že od nekdaj želijo, da njihova sporočila dosežejo ljudi z določenimi demografskimi atributi, to pa pri anonimnih uporabnikih spleta povzroča problem.

Prvi način da se izognejo temu problemu je, da svoj oglas objavijo na spletni strani za katero se ve, da jo obiskujejo uporabniki, ki jim je oglas namenjen. Drugi način je, da se oglas objavi, glede na zbrane podatke o obnašanju uporabnika na spletu.

5.1.1. Modeliranje uporabnikov

Modeliranje uporabnikov pomeni pridobivanje informacij, ki jih program lahko zbere o uporabniku z namenom, da se zviša kvaliteta interakcije med človekom in računalnikom. Modeliranje uporabnikov se je že v preteklosti uporabljalo za raziskovanje na različnih področjih in v različne namene. V trgovski in servisni dejavnosti masovne proizvodnje je pomembno poznavanje individualnih zahtev in želja potencialnih porabnikov. Uporabniški modeli se danes uporabljajo na številnih področjih znanstvenega informiranja, pri katerem prihaja do uporabe metod umetne inteligence; inteligentni vmesniki do klasičnih podatkovnih zbirk, sistemi za računalniško poučevanje, inteligentni sistemi za odkrivanje in iskanje informacij na internetu.

Ugotavljanje profila uporabnika je pomembna naloga spletnih aplikacij. Zbiranje končnih informacij, kaj in kako uporabniki spleta obiskujejo na spletnih straneh lahko da zaključek, kako se uporabniki obnašajo. Murray in Durrel [Masand, 2000, str.3] sta preučevala kako vplivajo demografski atributi, kot sta spol in starost, na dostopanje do spletnih strani. Podatki so bili zbrani in preurejeni z uporabo modela latentne semantične analize vektorskega prostora in nato klasificirani z nevronskimi mrežami. Predhodno klasificirani podatki po demografskem pregledu so bili uporabljeni za vzpostavitev mreže, s katero se je lahko neznane uporabnike določilo po demografskih lastnostih, z dovolj veliko stopnjo verjetnosti.

Preden lahko uporabimo vmesnik za demografsko klasificiranje uporabnikov potrebujemo vhodne podatke. Čeprav so uporabniki spleta praviloma anonimni nam zagotavljajo določene informacije kot so:

- besede s katerimi iščejo informacije na spletu in
- spletne strani, ki jih obiskujejo.

Modele delimo po načinu zbiranja znanja o uporabnikih (povzeto po Rich, 1983) na:

Kanonični modeli

Analizirajo delo uporabnika z namenom, da se ugotovi, kako uporablja podatkovne zbirke poprečen uporabnik ali tipičen informacijski posrednik. Na osnovi zbranih podatkov se izdelava kanoničen model, ki je podlaga za izdelavo programske opreme. Prednost take programske opreme je velika začetna učinkovitost sistema, ki pa nima sposobnosti naknadnega dodatnega prilagajanja.

Individualni modeli

Sistem med delom zbira informacije o uporabniku, jih obdela in se jim prilagaja. Število individualnih lastnosti je omejeno, da se izognejo preveliki zapletenosti pri zbiranju in hranjenju informacij.

Eksplicitni in implicitni modeli

Modela lahko nastane tako, da programski sistem eksplicitno postavi vprašanja na katera mora uporabnik odgovoriti, da lahko sistem učinkovito deluje. Ta način je enostaven za implementacijo v programih a naporen za uporabnika.

Implicitni modeli zbirajo znanje o uporabniku prikrito brez njegovega sodelovanja. Sistem spremlja potek seans in iz njih ugotavlja značilnosti uporabnika. Prednost tega modela je v tem, da ne obremenjuje uporabnika z nevsebinskimi vidiki seanse in omogoča zbiranje informacij, ki presegajo razumevanje postopkov delovanja podatkovnih zbirk večine uporabnikov.

Trajanje modela

Modelu, pri katerem sistem hrani podatke samo za tekočo seanso, pravimo, da je kratkotrajen. To so običajno eksplicitni enostavni modeli. Primer kratkotrajnega implicitnega modela je program za računalniško poučevanje, kjer se sistem sproti prilagaja stopnji znanja uporabnika, ocenjevanje nivoja znanja pa opravi avtomatsko.

Pri dolgotrajnih modelih, se podatki zbirajo in dograjujejo med zaporednimi seansami in so vezani na konkretnega uporabnika ali najmanj tip uporabnika. Potek dela se zapisuje v posebne datoteke (log files). Z avtomatsko obdelavo teh datotek se poišče zakonitosti, ki dopolnjujejo uporabniški model.

Oblikovanje znanja o uporabnikih

Zaradi velikega števila uporabnikov, kot tudi njihovih lastnosti, ki jih želimo zbirati je praktično nemogoče uporabnike modelirati povsem individualno. Navadno uporabnike ločimo glede na njihove specifične lastnosti v razrede. Zbir lastnosti vsakega razreda imenujemo stereotip razreda. S pravilno izbiro lastnosti uporabnika in grupiranjem v razred, lahko razred dovolj natančno predstavlja uporabnika, s tem pa se olajša izvedljivost modeliranja v programskem smislu.

Stereotipi so v sodobnih sistemih dolgotrajni in evolutivni modeli in se s časom dograjujejo in spreminjajo. Prav tako lahko uporabniki glede na spremenjene lastnosti prehajajo iz enega stereotipa v drugega.

Modeliranje uporabnikov naj bi prineslo izboljšanje delovanja sistemov za shranjevanje in iskanje informacij. Z znanjem, ki je shranjeno v uporabniških modelih lahko:

- Uporabniški vmesniki koristijo dodatne informacije, ki dopolnjujejo in nadgradijo uporabnikovo informacijsko potrebo. To so predvsem podatki, ki niso izraženi v iskalni zahtevi, a zahtevo na nek način dopolnjujejo (jezik, starost dokumentov,).
- Sistem komunicira z uporabnikom, zato se uporabnik lahko osredotoči na vsebino poizvedbe in pride do boljšega rezultata v krajšem času.
- Program uporabnika opozori o napačni ali nenatančni iskalni zahtevi in je sposoben samodejno odpravljati pogoste ponavljajoče napake uporabnika.

- Program samodejno opravi nekatere naloge namesto uporabnika (osnovni izbor zbirk dokumentov, nivo zahtevnosti ukaznega jezika, izbor formata prikaza rezultatov, ...).

5.2. Iskanje informacij in iskanje podatkov

Iskanje informacij (ang. information retrieval - IR) in podatkov se med seboj razlikujeta, zato je potrebno naprej definirati razliko. Pri iskanju podatkov (ang. data retrieval - DR) ponavadi želimo najti točno določen izraz in ugotavljamo ali se nahaja v preiskovanem zapisu. Pri IR pa običajno ni nujno da je v preiskovanem zapisu točno določen izraz ampak je lahko več podobnih, ki se vsebinsko ali pomensko ujemajo z iskanim izrazom. Rezultat DR temelji na deduktivni metodi (sklepanje iz splošnega na posamezen primer) medtem ko pri IR ugotavljamo stopnjo verjetnosti rezultata iskanja. Model iskanja podatkov je determinističen in je neodvisen od človekove volje in njegovega delovanja za razliko od modela IR, ki je probabilističen in zato le bolj ali manj verjeten.

Klasifikacija posameznih postavk v razredu, ki pripada posameznim objektom je pri DR definirana z atributi, ki vsebujejo potreben in zadosten pogoj za razvrstitev. Pri IR atributi predstavljajo le dimenzije oziroma meje v katerih se morajo postavke nahajati, da se razvrstijo v razrede.

Poizvedbeni jezik se pri DR tvori umetno z določeno sintakso in slovarjem ter običajno s popolno specifikacijo tega, kar se išče. Pri IR se priporoča naravni jezik, čeprav obstajajo tudi izjeme in nepopolna specifikacija zahtev iskanja.

DR je bolj občutljivo na napake pri vnosu poizvedbe, saj primerjava ne bo uspešna in sistem ne bo prikazal pravega rezultata, če je storjena napaka pri vnosu. Pri IR majhne napake v splošnem ne vplivajo bistveno na učinek primerjave.

Slika 26: Razlika med iskanjem podatkov in informacij

| | Iskanje podatkov | Iskanje informacij |
|------------------------|-------------------------|---------------------------|
| Primerjava | popolna | delna |
| Sklepanje | deduktivno | na podlagi primera |
| Model | determinističen | stohastičen |
| Klasifikacija | enotna | nedoločena |
| poizvedbeni jezik | umetno | naravno |
| specifikacija poizvedb | popolna | nepopolna |
| iskana postavka | enaka | ustrezna |
| občutljivost na napake | da | ne |

Vir: prirejeno po Rijsbergen, 1979

5.2.1. Iskanje vsebine spletnih strani

Z razvojem interneta se je močno razširilo spletno založništvo, kar je sprožilo razvoj spletnih iskalnikov. Opisovanje vsebine dokumentov v zbirkah teh iskalnikov temelji na ključnih besedah in besednih zvezah, ki se avtomatsko tvorijo iz samih dokumentov. V začetku so bili dokumenti večinoma v angleškem jeziku v zadnjih letih pa se povečuje

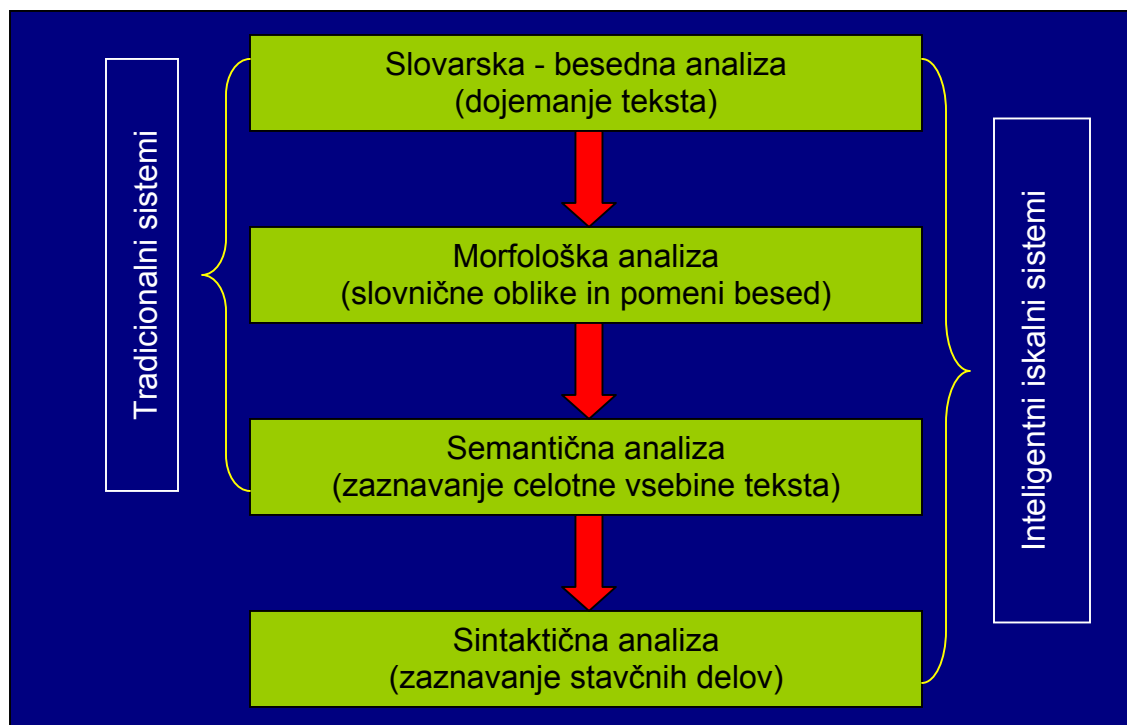
delež neangleških dokumentov na spletu, kot tudi v urejenih digitalnih knjižnicah. V zadnjih letih se je število angleških dokumentov letno povečevalo za približno polovico, medtem ko se je število neangleških povečevalo za 90% (Brascher, Schaeuble, 1998). Po podatkih OCLC (Online Computer Library Center) je bil v letu 2001 delež dokumentov v angleškem jeziku 73% medtem ko je bilo v enem od ostalih evropskih jezikov 21% dokumentov. Spletni dokumenti v različnih jezikih se odražajo tudi v jezikovni pestrosti zbirk spletnih iskalnikov.

Iskanje z iskalnimi zahtevami v enem jeziku pomeni primerjanje besed ali besednih zvez iz iskalne zahteve z besedami ali besednimi zvezami v dokumentih. Iskanje ne more dati rezultatov, če sta primerjalna iskalna zahteva in dokument v različnih jezikih, zato potrebujemo iskalnike, ki omogočajo večjezično oziroma medjezično iskanje. V svetu se veliko raziskuje in razvija na področju metodologij za medjezično iskanje (cross-language information retrieval – CLIR) na področju shranjevanja in iskanja informacij (information retrieval – IR).

Proces pridobivanja informacij iz teksta vključuje naslednje stopnje:

- Formalizacija uporabnikovih iskalnih zahtev.
- Predhodno izbiranje testnih dokumentov, ki formalno ustrezajo iskalnim zahtevam.
- Analize izbranih dokumentov (besedne, slovnične, sintaktične, semantične analize).
- Ocenjevanje skladnosti semantične vsebine najdenih informacij z zahtevami poizvedb.

Slika 27: Problemi jezikovnih analiz tekstualnih informacij



Vir: prirejeno po STOCONA

Slika 27 prikazuje implementacijo jezikovnih analiz tekstualnih informacij, ki bazira na rešitvah problemov, ki jih povzročajo naslednje analize:

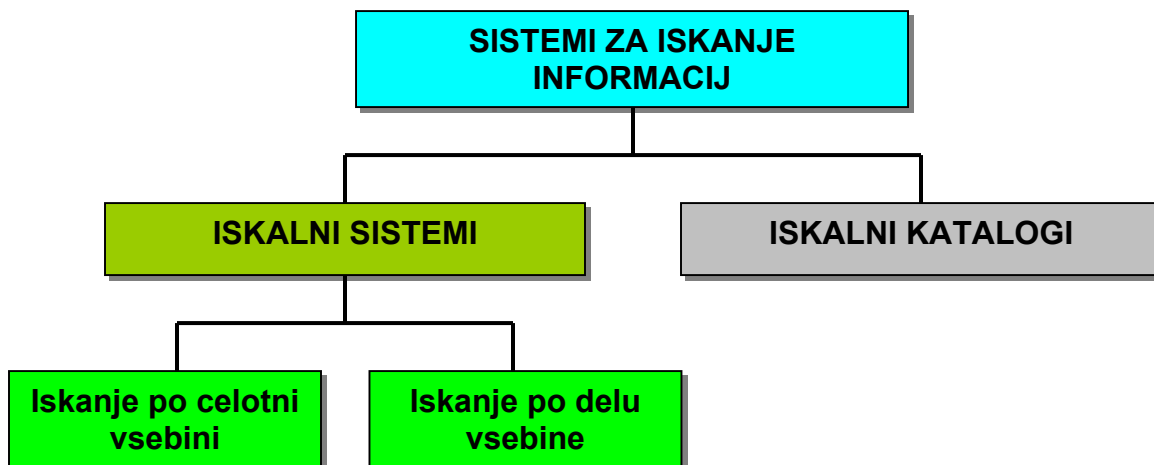
Slovarska - besedna analiza združuje analize tekstovnih informacij po posameznih odstavkih, stavkih in besedah, ki jih predstavljajo posamezni jeziki. To so predvsem razlike v besednem izražanju kot so uporaba narečja, slenga ali žargona, in neprimernih besed (žaljivke, psovke).

Morfološke analize omogočajo avtomatsko prepoznavanje besed z enakim pomenom v besedilu. Vsaka beseda se primerja in razporedi glede na slovničen in slovarski pomen. Slovnična opredelitev je narejena z avtomatskim izločanjem semantične vsebine stavka.

Semantične analize so narejene na osnovi definicije samo-opisnih tekstovnih informacij in izbranih podatkov, ki predstavljajo logično osnovo. Izdelava avtomatičnih semantičnih analiz omogoča iskanje in rangiranje semantične vsebine v tekstu. To predstavlja postopke, ki jih je težko formalizirati v skladu s potrebami strokovnjakov po stopnji kvalitete pridobljenih informacij.

Klasično iskanje dokumentov preko interneta, brez avtomatskega rangiranja je zamudno, saj je potrebno preverjanje ogromnega števila dokumentov. Vse nove specialne tehnologije, ki so danes dosegljive, še ne zagotavljajo učinkovitega avtomatičnega rangiranja vsebin za iskalne sisteme.

Slika 28: Klasifikacija sistemov za iskanje informacij



Vir: prirejeno po STOCONA

5.2.2. Načini iskanja informacij

Sistemi za pridobivanje informacij (slika 28) omogočajo avtomatsko indeksiranje velikega števila dokumentov. Preprosti sistemi imajo nizko stopnjo ustreznih rezultatov poizvedb za razliko od bolj kompleksnih, ki s pripomočki umetne inteligence omogočajo različne stopnje jezikovne analize, ki vključuje vrednotenje besedne, morfološke, sintaktične in semantične vsebine informacij.

Načine iskanja informacij lahko razdelimo na naslednje kategorije (Stocona) :

| | |
|-------------------------|--|
| s ključnimi besedami | metoda multipleksiranja besed (Boolejeva metoda) |
| po razporeditvi besed | s pomočjo presledkov med besedami |
| s primerjanjem | semantično (pomen besed) |
| po vzorcih (podobnosti) | po poljih v dokumentu |

Iskanje po celotni vsebini

Z besedo - izrazom ali zaporedjem izbranih znakov preiskujemo celoten dokument od začetka do konca dokumenta. Postopek je enostaven za uporabo vendar zelo počasen in zato neprimeren za preiskovanje dolgih dokumentov, zato se uporablja le za specialne namene ali v kombinaciji z drugimi metodami za omejeno območje preiskovanja.

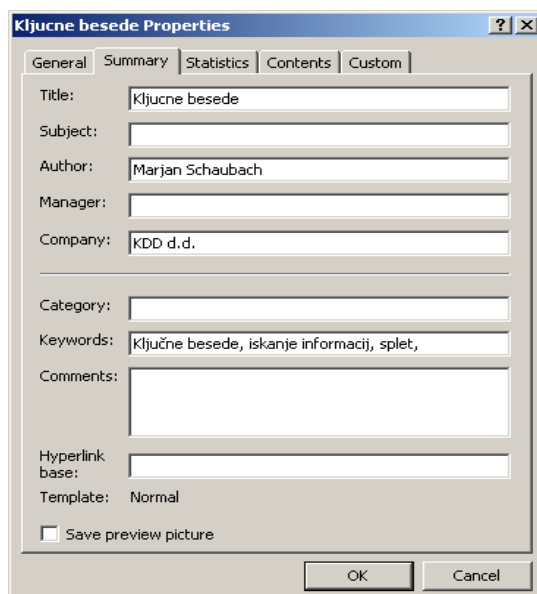
Iskanje po delu vsebine

Signatura je ključ, ki razvršča dokument po določenih vsebinskih kriterijih. Datoteka signatur je shranjena ločeno od dokumenta in je veliko krajša od originalnega dokumenta zato je iskanje veliko hitrejše. Ta način je najbolj pogost v knjižničarstvu.

Ključne besede lahko predstavljajo vsebino dokumenta in so v pomoč pri iskanju vsebine. Hitrejše iskanje se doseže, če so urejene po abecedi in shranjene kot »index datoteke«. Praviloma so članki v strokovnih revijah opremljeni s seznamom ključnih besed, ki vsebujejo od 5 do 15 pomembnih besed ali fraz, s katerimi avtor (ali avtorji, če jih je več) predstavi obravnavano snov oziroma temo članka. V posameznih primerih lahko ključne besede predstavljajo zelo koncentrirano vsebino.

Nekateri komercialna orodja za obdelavo teksta, kot je na primer MS Word97 in Word2000, imajo vključen algoritem za avtomatsko izločanje dokumentov po ključnih besedah, če so vpisane v lastnosti dokumenta.

Slika 29: Primer opisa »Lastnosti dokumenta - Properties« v Word2000



Poizvedbo dokumentov na sliki 29 s pomočjo ključnih besed omogočajo metapodatki, ki jih generira program MS Word.

Ključne besede se zato pogosto uporabljajo tudi pri opisu vsebine spletnih strani, elektronskih sporočil, člankih v časopisih in revijah ter poslovnih dokumentih. Praktičen pomen ključnih besed ne gre iskati pri ročni uporabi, so pa povzročile razvoj mnogih algoritmov, ki omogočajo avtomatsko zbiranje ključnih besed. Avtomatsko zbiranje temelji na dveh pristopih (Turney, 2002):

- **Zbirka ključnih besed** pomeni spisek predhodno definiranih besed, ki so v skladu z jezikovnimi in knjižničnimi pravili. Besede omogočajo kategorizacijo dokumenta v razrede s pomočjo modela. Dokument se pretvori v vektor, ki izraža njegove značilnosti. S tehnikami strojnega učenja pridemo do vektorja značilnosti dokumenta, ki je odraz spiska ključnih besed.
- **Izločanje ključnih besed** iz teksta dokumenta brez predhodnega seznama. Za izločanje ključnih besed se ne uporablja slovarjev in jezikovnih pravil. Tekst dokumenta se tretira kot področje kandidatov ključnih besed iz katerega je potrebno izločiti primerne in neprimerne kandidate. Vektor značilnosti dokumenta je izračunan iz primernih ključnih besed (fraz). Tehnike strojnega učenja so uporabljene za izgradnjo modela, ki klasificira besede kot ključne oziroma neključne. Značilnosti dokumenta vključujejo frekvenco in lokacijo ključne besede v dokumentu.

5.2.3. Medjezično iskanje

Medjezično iskanje pomeni, da je jezik iskalne zahteve različen od jezika ali jezikov, v katerih je izražena vsebina dokumenta oziroma dokumentov, ki jih iz zbirke prikaže iskalna zahteva. Iskalna zahteva je v jeziku **a**, dokumenti v zbirki pa v jeziku **a** in **b**. Preiskani bodo dokumenti v jeziku **a** in **b** in prikazani pripadajoči dokumenti v obeh jezikih.

Enojezično ali istojezično iskanje (ang. monolingual IR) je takrat, kadar sta iskalna zahteva in dokumenti v zbirki v istem jeziku. Medjezično iskanje v enem delu svoje definicije pokriva tudi enojezično iskanje. Večjezično iskanje (ang. multilingual IR) je najpogosteje uporabljen izraz, ki vključuje enojezično, medjezično iskanje, kakor tudi iskanje dokumentov v različnih jezikih.

Pri razvoju sistemov za medjezično iskanje je nujna uporaba IR metod, računalniškega jezikoslovja, računalniškega prevajanja in zelo pogosto tudi avtomatskega povzemanja (sumarizacije) besedil, povezovanje govora in druge. Medjezično iskanje vključuje prevajanje po katerem se bistveno razlikuje od pridobivanja informacij (IR), po načinu organizacije dokumentov v zbirkah, metodah avtomatskega indeksiranja (vektorske, probabilistične, latentno sematično indeksiranje ...), interpretiranju iskalnih zahtev in računanje relevantnosti pa sta si podobni.

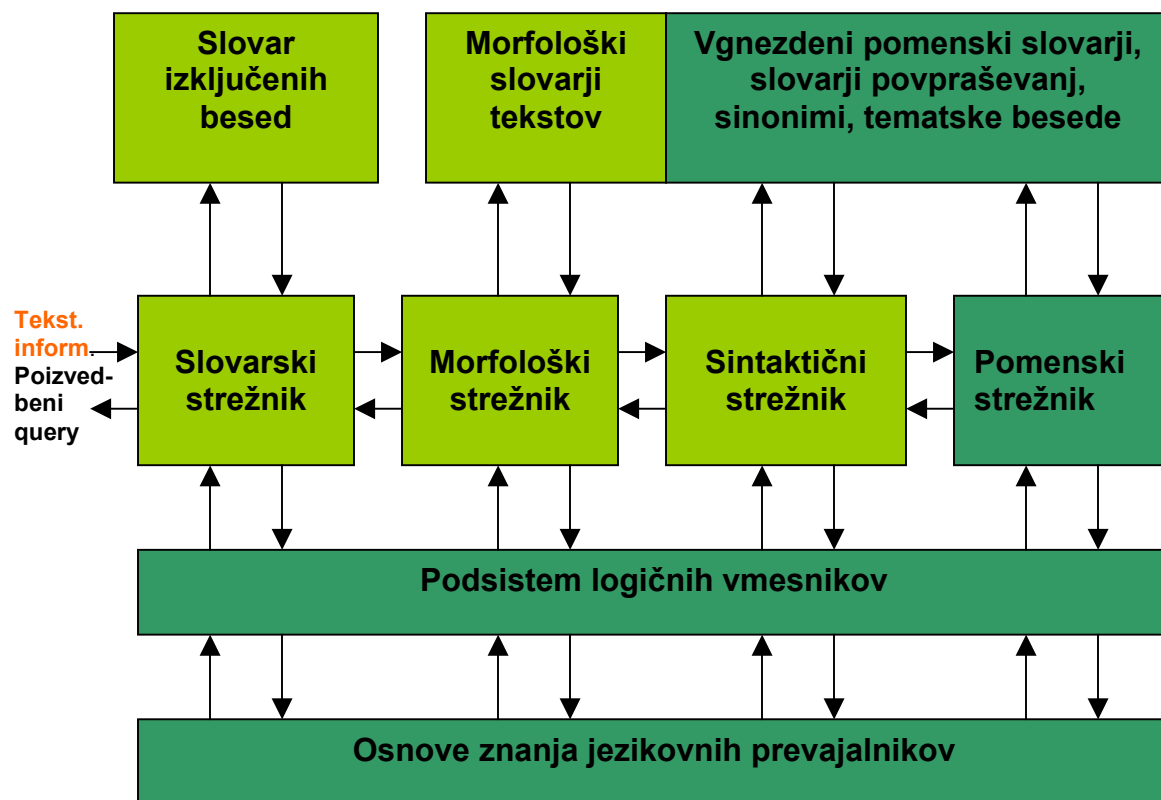
Inteligentni sistemi za pridobivanje tekstovnih informacij uporabljajo avtomatske postopke na vseh stopnjah jezikovnih analiz (leksikalne, morfološke, sintaktične in

semantične) in izkorišča prednosti, ki jih omogoča avtomatsko indeksiranje dokumentov, ekspertni sistemi in sistemi umetne inteligence.

Z razvojem inteligentnih IR sistemov se razvijajo tudi novi uporabniški vmesniki, ki omogočajo:

- Izvajanje poizvedbo v naravnem jeziku uporabnika.
- Dialog, ki poteka med uporabnikom pri postopku definiranja poizvedbe in inteligentnim sistemom pri kreiranju odgovora.
- Avtomatsko prevajanje uporabnikove poizvedbe iz njegovega naravnega jezika v formaliziran poizvedbeni jezik obstoječega sistema.
- Podporo iskanja z večpomenskimi besedami.
- Izvedbo poizvedbe s sinonimi in besedami, ki so povezane s tematiko.
- Povečano stopnjo uspešnosti poizvedb v dialogu z uporabnikom, ki omogoča sprotno primerjavo osnovne poizvedbe z odgovorom iskalnega sistema.
- Podporo avtomatskemu rangiranju semantike tekstovnih informacij.

Slika 30: Struktura jezikoslovnih procesorjev



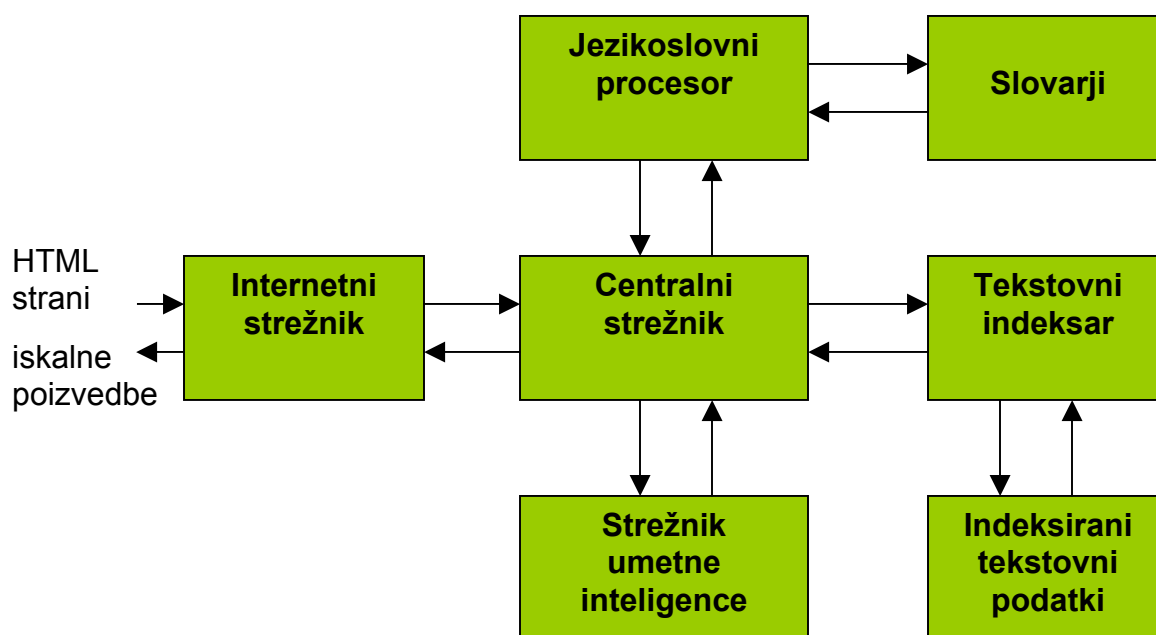
Vir: prirejeno po: <http://eng.stocona.ru/technology/informationRetrieval/>

Implementacija funkcionalnih lastnosti prikazanih na sliki 30 omogoča:

- popolno slovarsko analizo tekstovnih informacij narejeno na podlagi rezultatov predhodno opravljenih testiranj,

- enotno strukturo morfološkega slovarja, ki vsebuje vse morfološke in semantične oblike besed, vključno s sinonimi in vsebinsko podobnimi besedami,
- podrobno morfološko analizo, ki definira jezikovne posebnosti, ki so vključene pri poizvedbah tekstovnih informacij,
- iskanje tekstovnih informacij, ki vključuje sinonime in vsebinsko podobne besede,
- avtomatsko razčlenbo stavkov in medsebojno povezavo med členi,
- izločiti osnovne tekstovne informacije, ki so primerne za uporabniške poizvedbe,
- avtomatsko ocenitev pomembnosti posameznega stavka v besedilih in s tem omogočiti semantično popoln odgovor sistema pri poizvedbi.

Slika 31: Shema inteligentnega stroja za pridobivanje informacij



Vir: prirejeno po <http://eng.stocona.ru/technology/informationRetrieval/>

Na sliki 31 je prikazan model iskalnega stroja, ki nazorno prikazuje način delovanja inteligentnega sistema za pridobivanje informacij.

Primerjava tehnologij med klasičnimi in inteligentnimi sistemi za pridobivanje informacij ter njihove karakteristike so prikazane na sliki 32.

Slika 32: Primerjava tehnologij za IR

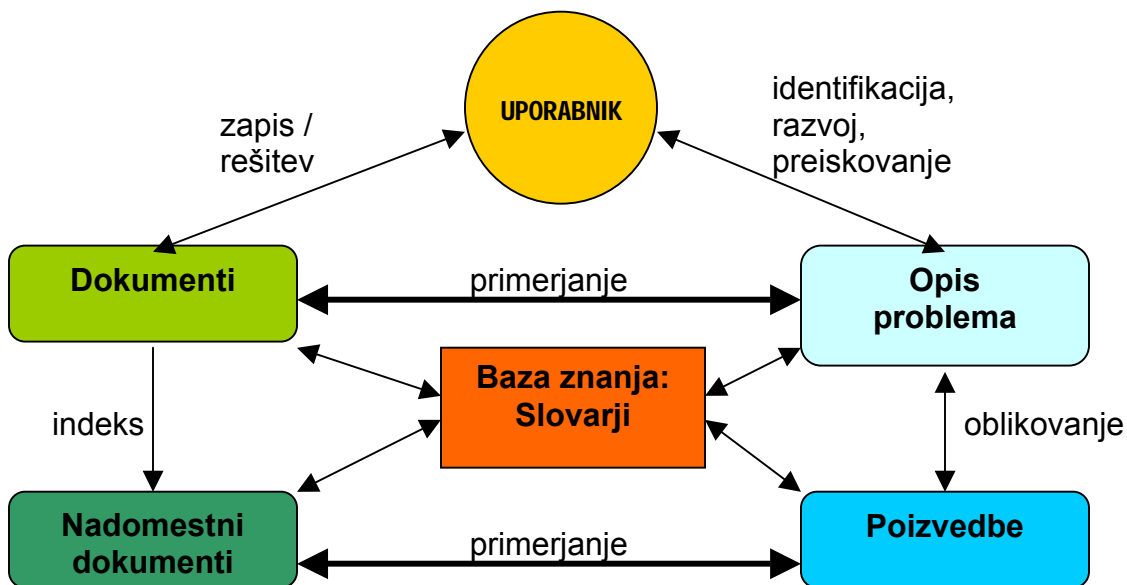
| Karakteristika sistema | Klasični sistemi | Inteligentni IR sistemi |
|-------------------------------------|---|---|
| STOPNJA JEZIKOVNE ANALIZE | <ul style="list-style-type: none"> ▪ leksikalno ▪ morfološko ▪ sintaktično (delno) | <ul style="list-style-type: none"> ▪ leksikalno ▪ morfološko ▪ sintaktično ▪ semantično |
| GLAVNE ZNAČILNOSTI SLOVARJEV | <ul style="list-style-type: none"> ▪ osnovne besede ▪ morfološka oblika besed | <ul style="list-style-type: none"> ▪ osnovne besede ▪ morfološka oblika besed ▪ sinonimi ▪ tematske besede ▪ semantika besed |
| TIPI POIZVEDB | <ul style="list-style-type: none"> ▪ ključne besede, predpisan poizvedbeni jezik | <ul style="list-style-type: none"> ▪ naravni poizvedbeni jezik ▪ poizvedbene besede |
| JEZIKOVNA PODPORA | <ul style="list-style-type: none"> ▪ slovenski ▪ angleški | <ul style="list-style-type: none"> ▪ slovenski ▪ vsi jeziki (v prihodnosti) |
| DIALOG SISTEMA Z UPORABNIKOM | Ni podprt | <ul style="list-style-type: none"> ▪ seznam z generirano listo ključnih besed ▪ seznam večpomenskih besed ▪ seznam semantičnega pomena odgovora sistema |
| OBLIKE ODGOVORA SISTEMA | <ul style="list-style-type: none"> ▪ določen seznam povezav z zbranimi ključnimi besedami | <ul style="list-style-type: none"> ▪ določen seznam povezav z zbranimi ključnimi besedami ▪ odstavki teksta, ki vsebujejo ključne besede ▪ obnovljiv indeksiran tekst; pomensko povezan z sistemskim odgovorom |

Vir: prirejeno po <http://eng.stocona.ru/technology/informationRetrieval/>

5.3. Digitalne knjižnice in vzpostavljanje povezav do informacij

Na področju skladiščenja informacij in hitrega ter učinkovitega dostopa do le teh se srečamo z različnimi izgradnjami digitalnih knjižnic, ki predstavljajo ključno tehnologijo za mrežne informacije. Različni modeli (*slika 33*) omogočajo razvoj informacijskih sistemov, ki uporabnikom zagotavljajo preiskovanje, brskanje in druge operacije.

Slika 33: Funkcionalni pogled na IR



Vir: prirejeno po *Digital Libraries, 2002*.

5.4. Boolejeva metoda

Princip Boolejeve⁴ metode se pogosto razlaga z Venn-ovim diagramom, kjer posamezni ovali predstavljajo informacijski prostor na spletu. Vsak oval predstavlja zbirko dokumentov na spletu, ki vsebujejo besedo, ki pripada določeni vsebini.

Boolejeva logika vključuje tri logične operatorje s katerimi se pri iskanju konkretizira izločanje dokumentov:

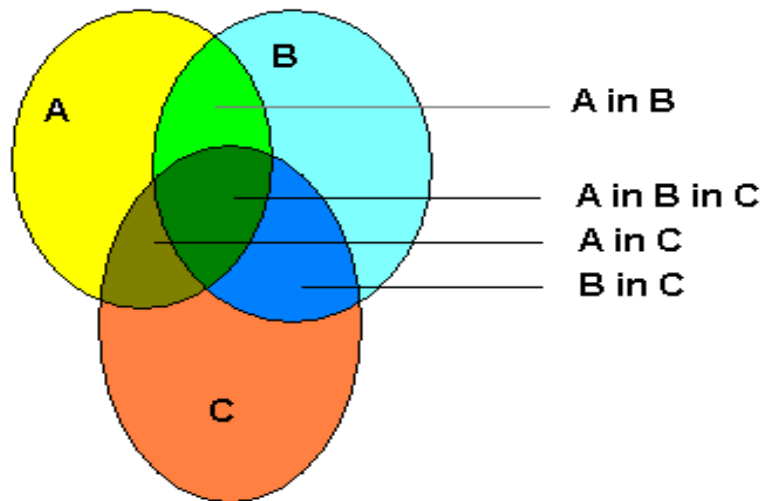
- In (AND)
- Ali (OR)
- Ne (NOT)

Na *sliki 34* je prikazana uporaba logičnega operatorja »In« pri obravnavanju dokumentov A, B in C.

Dodatni primeri metode: *priloga 1*.

⁴ George Boole angleški matematik

Slika 34: Princip Boolejeve metode



Sosedstvo besed

Pri iskanju dveh besed z operatorjem »AND« se ugotavlja le prisotnost besed kjerkoli v dokumentu. Včasih pa želimo izločiti dokumente, kjer dve besedi nastopata v logični povezavi in sta zapisani v istem stavku ali odstavku. Nekateri iskalni stroji dopuščajo tako iskanje z uporabo operatorja »NEAR«. Območje iskanja sosedstva je običajno med 9 in 15 besed in je odvisno od iskalnega stroja. Pri nekaterih iskalnih strojih je dolžina fiksna ([AltaVista](#): 10 besed) pri drugih pa jo lahko uporabnik določi do njene maksimalne vrednosti ([WebCrawler](#)), (Primer: "beseda **A** NEAR/15 beseda **B**").

Od oblikovanje iskalnih zahtev je odvisen rezultat iskanja. Priporočljivo je pričeti iskanje z preprostimi ukazi, ki jih nadgrajujemo, dokler ne dobimo želenih rezultatov.

5.5. Indeksiranje z LSA

Latentna semantična analiza (LSA) je relativno nova metoda pri računalniškem iskanju informacij. Slabost tradicionalnih metod preiskovanja dokumentov je v tem, da se išče in primerja določene izraze v dokumentu. Pri tem so najdeni dokumenti, ki po namenu in vsebini ne ustrezajo, čeprav vsebujejo iskani izraz. Posamezne besede in izrazi imajo lahko različne pomena, ki pri preiskovanju popolnoma ustrezajo zahtevam vendar dokument za uporabnika ni primeren. Drug problem pa so besede z enakim pomenom ali sinonimi, ki jih dokument vsebuje vendar se ne ujemajo z iskalnim izrazom.

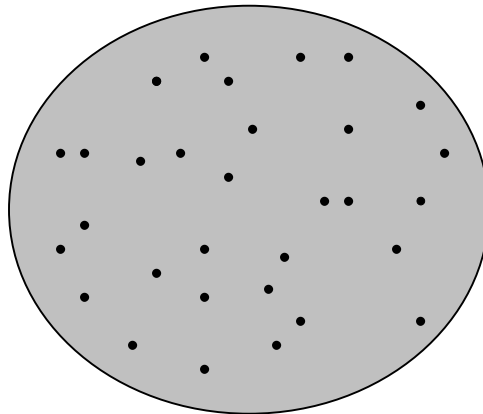
LSA pristop bazira na visoko urejenih strukturah asociativnih izrazov v dokumentih (»semantične strukture«) urejene na način, ki omogoča zaznati relevantne dokumente v poizvedovanjih na podlagi osnovnih izrazov. Uporabljena je posebna tehnika

razčlenbe posameznih izrazov - pomenov (SVD – singular-value decomposition) s katero se veliko matriko izraz-dokument razkroji v določeno skupino med 100 in 300 pravokotnih faktorjev, ki približno ustrezajo originalni matriki. Dokumenti so tako predstavljeni z vektorji izrazov oteženimi z faktorji. Poizvedbo predstavlja iskanje vektorjev navideznih dokumentov uteženih s kombinacijami pomenov. Vrnjeni so tisti dokumenti, ki imajo vrednost nad pragom funkcije kosinus.

5.5.1. Model vektorskega prostora

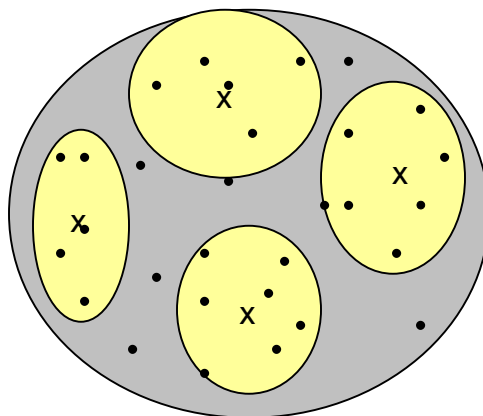
V večdimenzionalnem prostoru dokumentov, ki so predstavljeni kot vektorji, je vsak dokument predstavljen kot točka (slika 35).

Slika 35: Predstavitev dokumentov v vektorskem prostoru



Osnovna ideja vektorskega prostora je grupiranje podobnih dokumentov v skupine. Vsaka skupina dokumentov je predstavljena s povprečno vrednostjo, ki jo predstavlja center (na sliki 36 središče posamezne elipse označeno z »X«).

Slika 36: Skupine dokumentov v vektorskem prostoru



Skupine se generirajo na osnovi besed, ki so uporabljene v dokumentu in se prav tako grupirajo. Besede, ki imajo enak ali podoben pomen - sinonimi se razvrstijo v razrede. Tako razvrščene se uporabi za avtomatsko izdelavo tezavra.

Pri modelu vektorskega prostora so dokumenti predstavljeni kot realna vrednost vektorja, v katerem vsak element predstavlja frekvenco prisotnosti določene besede v dokumentu. Vektor dokumenta je prikazan kot zbirka grafično prikazane strukture besed. Slabost tega modela je veliko število ponavljajočih besed in večdimenzionalnost končnega vektorja, ki se odpravi s statističnimi metodami.

Tehnike vzpostavitve vektorskega prostora informacij se opirajo na predpostavki, da pomen dokumenta izvira iz vsebovanih besed oziroma izrazov.

Dokument je predstavljen kot vektor izrazov: $d = (t_1, t_2, \dots, t_N)$

t_j – pozitivno število, ki pove kolikokrat nastopa izraz i v dokumentu d

Podobno velja za povpraševanja: $q = (t_1, t_2, \dots, t_N)$

t_j – pozitivno število, ki pove kolikokrat nastopa izraz i v povpraševanju q

Vektorji dokumenta so običajno shranjeni v matriki izraz-dokument, kjer vrstica matrike predstavlja posamezne izraze, kolone pa posamezne dokumente v zbirki.

a_{ij} - je element matrike, kjer je i število nastopov izraza v dokumentu j .

5.5.2. Latentna semantična analiza (LSA) in razčlemba izrazov (SVD)

LSA je metoda pridobivanja informacij, ki omogoča kreiranje vektorskega prostora izbranih dokumentov in si prizadeva odpraviti slabost večdimenzionalnosti modela vektorskega prostora. LSA vektorski prostor ima relativno malo dimenzij (normalno med 100 in 300). Vsebinsko podobni dokumenti so predstavljeni v vektorskem prostoru podobno. Metoda je bila za potrebe pridobivanja informacij razvita v letu 1990 (Deerwester, Dumais, Furnas, Landauer in Harshman) in se je do danes prilagajala jezikovnim analizam.

Bistvo analize je matrika izraz-dokument, ki predstavlja število pojavljanj posameznega izraza v določenem dokumentu. Izračuna se vrednost SVD za vsak izraz in izloči majhne vrednosti v matriki elementov.

Razčlemba posameznega izraza (SVD - Singular Value Decomposition) omogoča razčlemba $t \times d$ v matriki izraz-dokument \mathbf{X} z naslednjimi produkti:

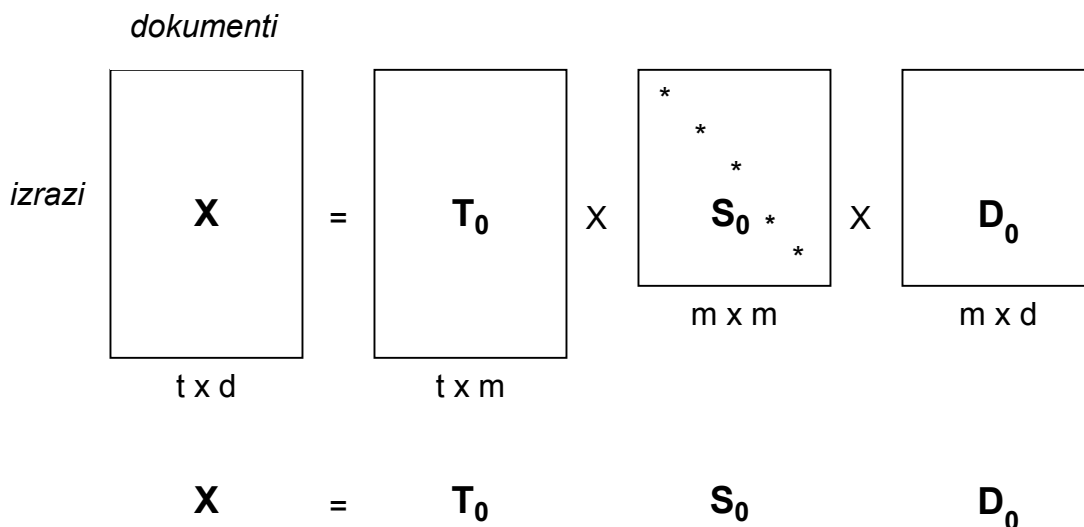
- $t \times m$ matrike \mathbf{T}_0 v vektorju izrazov
- preoblikovanje $d \times m$ matrike \mathbf{D}_0 vektorja dokumentov
- $m \times m$ diagonalne matrike \mathbf{S}_0 posameznih vrednosti

t – število vrstic v matriki \mathbf{X}

d – število kolon v matriki \mathbf{X}

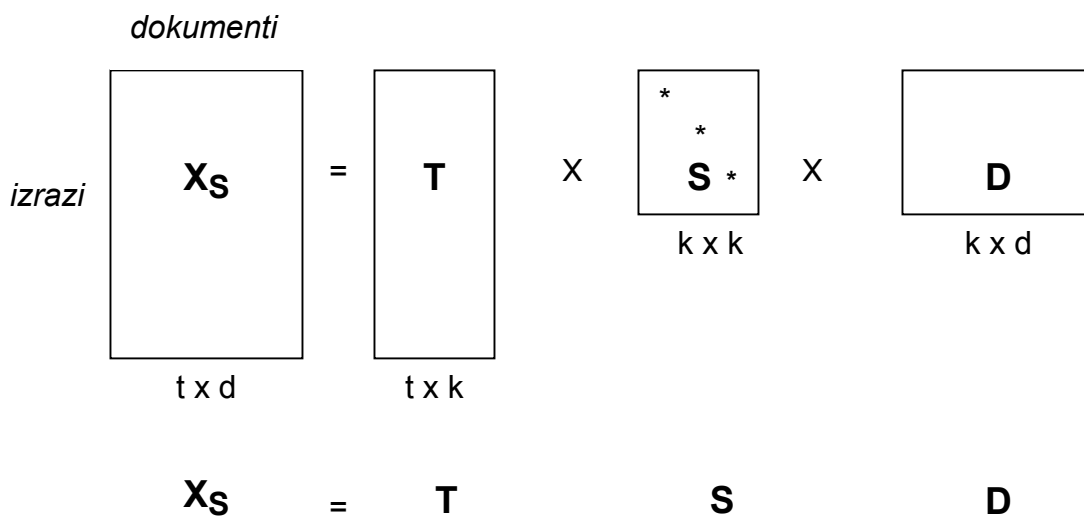
m – uvrstitev \mathbf{X} ($\leq \min(t, d)$)

Slika 37: Shematski prikaz razčlenbe vrednosti matrike $t \times d$ – izrazi po dokumentih



Na [sliki 37](#) je razvidno, da so matrike T_0 , S_0 in D_0 v popolni-celotni dimenziji. Metoda SVD omogoča, da z optimalnim prilagajanjem matrike zmanjšamo. Z razvrstitvijo diagonalnih elementov matrike po velikosti od največjega do najmanjšega tako, da tiste z vrednostjo 0 eliminiramo, kot je prikazano na [sliki 38](#).

Slika 38: Shematski prikaz skrčene matrike X_s zmanjšano število dimenzij $k(\leq m)$



Z brisanjem vrstic in kolon z vrednostmi 0 v matriki S_0 dobimo novo diagonalno matriko S in s skladnim brisanjem kolon matrike T_0 in D_0 dobimo ustrezne matrike T in D . Z množenjem tako dobljenih matrik dobimo matriko X_S katera ima dimenzije k , in je po vrednosti približno enaka X . Vrednost k predstavlja velikost redukcije, ki mora biti pravilno dimenzionirana. Dovolj velika, da še vedno zagotavlja realno strukturo podatkov brez nepomembnih detajlov. V praksi se uporablja operativne kriterije za vrednost k (*med 100 in 300*), ki zagotavljajo dobre iskalne pogoje.

LSA je avtomatičen matematičen algoritem za izločanje enakih pomenov besed uporabljenih v tekstu. Ne uporablja slovarjev zunanjih podatkov ali slovničnih pravil. Matrika v kateri besede predstavljajo vrstice in kolone dokument se predhodno transformirajo. Pogostost pojavljanja vsake besede se v matriki ovrednoti s funkcijo. Uporabi se SVD, ki predstavlja analizo faktorjev. Rezultat SVD-ja je zmanjšanje števila dimenzij matrike. Algoritem za razčlenbo matrike in s tem za zmanjševanje večdimenzionalnega vektorskega prostora daje rezultate, ki kažejo, da je podobnost pomenov besed blizu človeškemu razumevanju, vendar so pridobljeni rezultati odvisna od dimenzije.

Praktičen primer uporabe metode LSA je prikazan v [prilozi 2](#).

5.6. Iskalni stroji

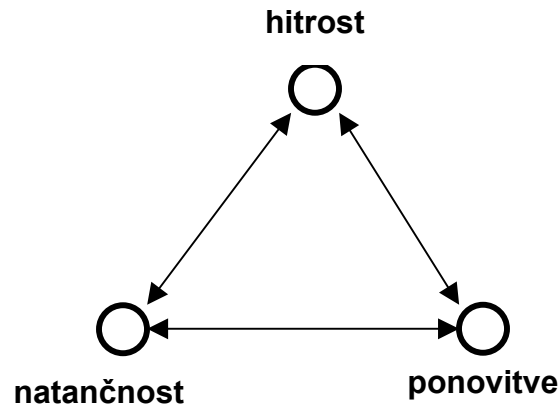
Po nekaterih ocenah [Kobayashi] 85% spletnih uporabnikov uporablja iskalne stroje ali kakršnakoli orodja za iskanje določenih informacij, ki jih zanimajo. Število objavljenih in dostopnih iskalnih strojev je zato v zadnjih letih skokovito naraslo (glej www.blueangels.net). Posledica takega množičnega iskanja so spletne strani (www.searchterms.com), ki objavljajo sezname najpogosteje uporabljenih iskalnih besed ali fraz. Iskalni stroji se večinoma financirajo z oglaševanjem oziroma so plačani od števila povezav na strani, ki jih uporabniki iščejo. Nedvomno je prav ta finančna spodbuda ena od najpomembnejših za velikanski razmah raziskav na področju iskanja informacij na spletu. Ključ do popularnega in uspešnega iskalnega stroja je razvoj novih algoritmov, ki so predvsem usmerjeni k hitri, zanesljivi in uporabni informaciji.

Iskalni stroji predstavljajo ogromne baze informacij o spletnih straneh. Te baze pa še zdaleč niso popolne. Po nekaterih ocenah iskalni stroji pokrivajo le majhen del (1/500) celotnega spletnega prostora.

5.6.1. Razvoj iskalnih strojev

Za ocenjevanje in vrednotenje iskanja informacij obstajajo pomembne razlike med klasičnim iskanjem in iskanjem informacij na spletu. Spletni uporabniki so do nekaterih lastnosti bolj strogi, kot klasični uporabniki. Interaktivni odzivni čas je na vrhu liste zahtev spletnega uporabnika, ki mu sledi točnost poizvedb, ki se odraža v številu uporabnih rezultatov izpisanih na prvi strani najdenih poizvedb. Če so uporabni rezultati že na prvi strani, listanje po naslednjih straneh ni potrebno. Učinkovitost iskalnega stroja je torej odvisna od hitrosti, natančnosti in številu ponovitev iskanja.

Slika 39: Trosmerna učinkovitost iskalnega stroja



Vir: prirejeno po Kobayashi, 2000, stran 9

Natančnost iskanja je opredeljena z razmerjem med ustreznimi dokumenti in številom vseh najdenih dokumentov:

$$\text{Natančnost iskanja} = \frac{\text{Število ustreznih dokumentov}}{\text{Število najdenih dokumentov}}$$

Ponovitve pomenijo razmerje med vsemi ustreznimi dokumenti, ki so prikazani na več straneh ekrana:

$$\text{Ponovitve} = \frac{\text{Število ustreznih dokumentov}}{\text{Celotno število ustreznih dokumentov}}$$

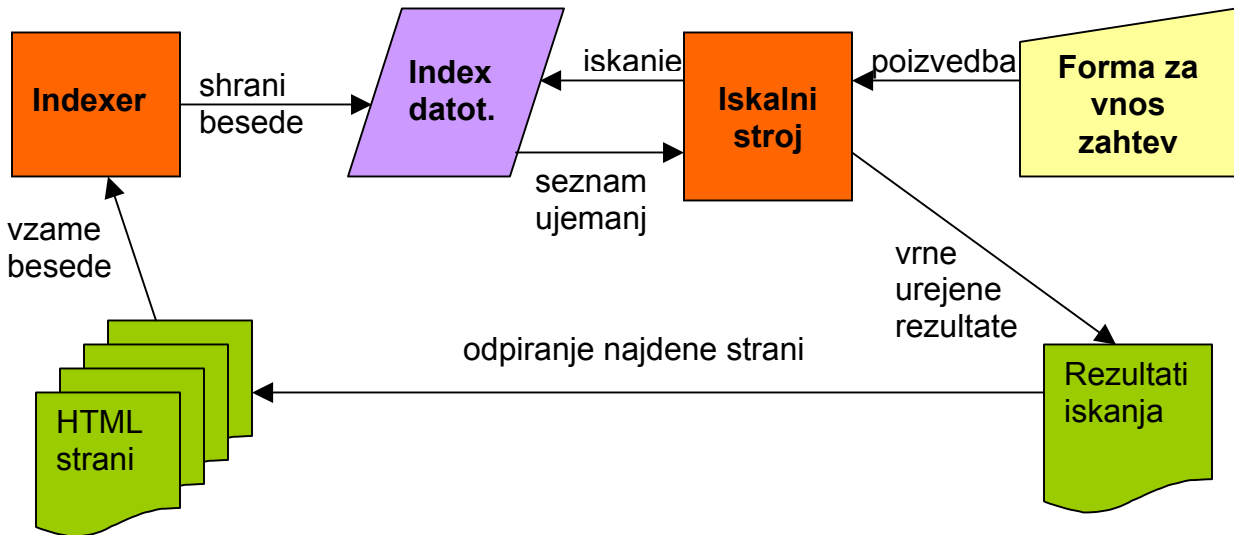
Število najdenih ustreznih poizvedb je v večini primerov preveliko in je za prikaz potrebnih (pre)več strani. Spletni uporabniki si prizadevajo osredotočiti se na iskanje in pridobiti le poizvedbe z visoko stopnjo zanesljivosti. Vsekakor imajo visoko stopnjo zanesljivosti avtorizirane strani zato so iskalniki, ki imajo povezave na avtorizirane strani bolj cenjeni. Spletni uporabnik se lahko izogne velikemu številu ponovitev z modificirano verzijo v kateri se upošteva le avtorizirane strani in prikaže le omejeno število (10 ali 20) najvišje uvrščenih dokumentov.

5.6.2. Delovanje iskalnih strojev

Iskalni stroj je aplikacija, ki išče določene podatke in vrne rezultat klientu običajno tako, da kreira HTML stran v določenem formatu. Večina iskalnih strojev uporablja indekse, ki jih proizvaja posebna indeksirna aplikacija. Zelo redki so iskalni stroji, ki preiskujejo podatke v realnem času, saj je takšno iskanje zelo zamudno.

Shematski prikaz delovanja iskalnega stroja prikazuje slika 40. Iskalniku se pošlje zahtevo za iskanje preko forme, ki vsebuje polje za vnos iskanega teksta in običajno tudi možnosti izbire nastavitvev iskanja. S klikom na zahtevo iskanja se podatki pošljejo v aplikacijo iskalnega stroja.

Slika 40: Shematski prikaz delovanja iskalnega stroja

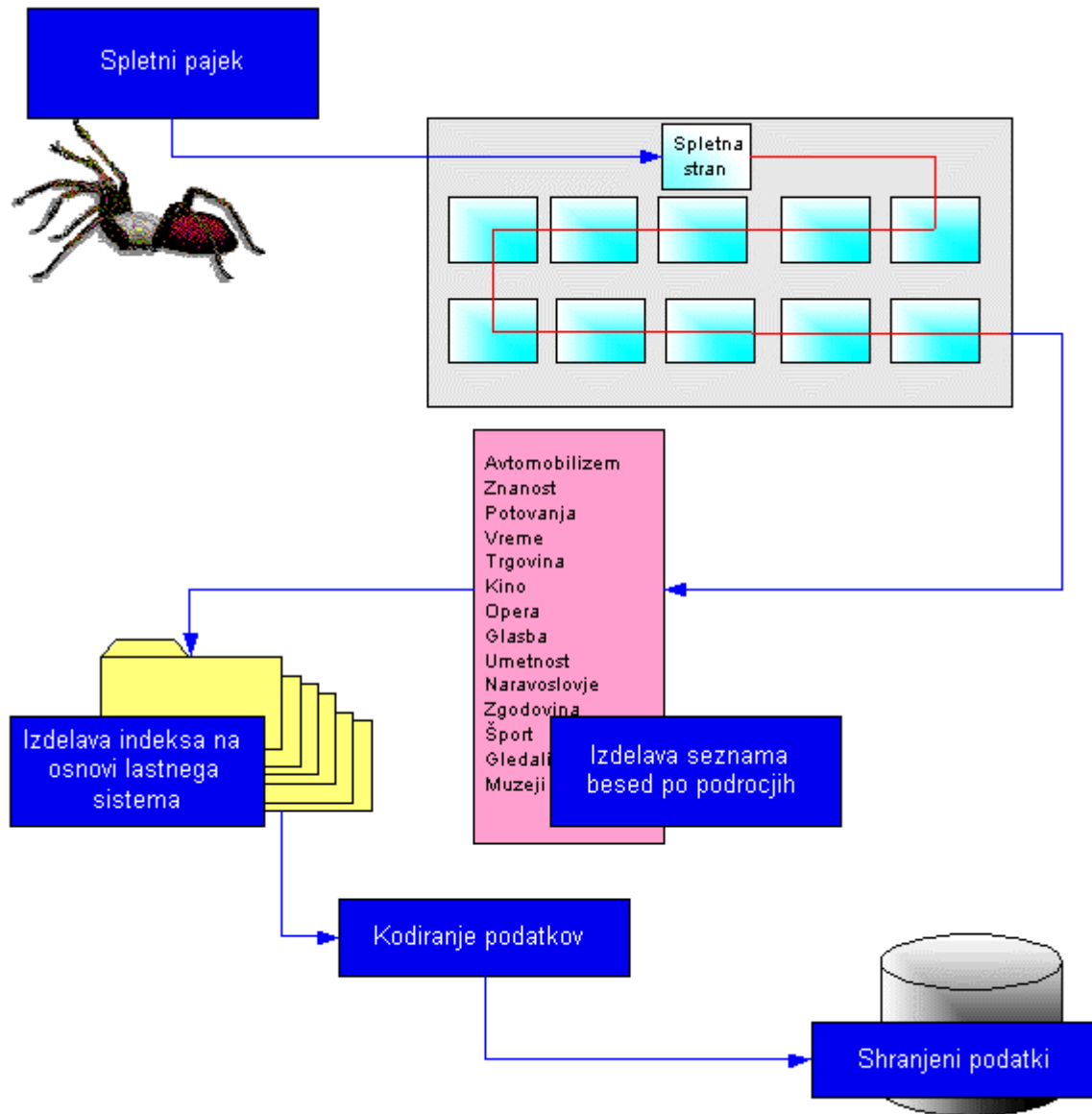


Vir: Prirejeno po [Search Tools Consulting](#)

Čeprav so načini delovanja različni, so vsem iskalnim strojem skupni majhni programi imenovani pajki (»spiders«, nekateri jih imenujejo tudi spletni roboti »robots« ali črvi »bugs«), ki prebirajo spletne strani po ključnih besedah. Kako so ključne besede obdelane in razvrščene je odvisno od lastnosti in namena iskalnega stroja. Iskalniki so narejeni za različna področja in različne profile uporabnikov. Preden nam iskalni stroj lahko pove, kje se nahaja informacija ali dokument ki ga iščemo, ga mora poiskati. Za iskanje informacij, ki se nahajajo na spletnih straneh, ki štejejo več sto milijonov je potrebno zgraditi sezname besed, ki se nahajajo na posameznih spletnih straneh. Proces gradnje seznama se imenuje »Web crawling«. Začetna točka izgradnje seznama je spisek pogosto uporabljenih strežnikov s popularno vsebino. Spider indeksira besede na straneh in sledi vsem najdenim povezavam na teh straneh. Na ta način potuje po vseh dosegljivih prostranstvih spleta.

Spletni pajek (slika 41) povzame vsebino spletnih strani in ustvari ključne besede, ki omogočajo uporabniku v realnem času poiskati spletno stran, ki jo iščejo. Spletni pajki so lahko tudi nevarni, ker svoje strani obnavljajo večkrat na dan ali celo večkrat na uro. S tem lahko povzročijo preobremenitev spletnih strežnikov, ki postanejo navidezno zamrznjeni. Skrbniki sistemov morajo biti zato pozorni na nove tehnologije spletnih pajkov, da pravočasno zaščitijo svoje sisteme pred namernimi ali nenamernimi motnjami, ki jih lahko pajki povzročijo.

Slika 41: Delovanje spletnega pajka



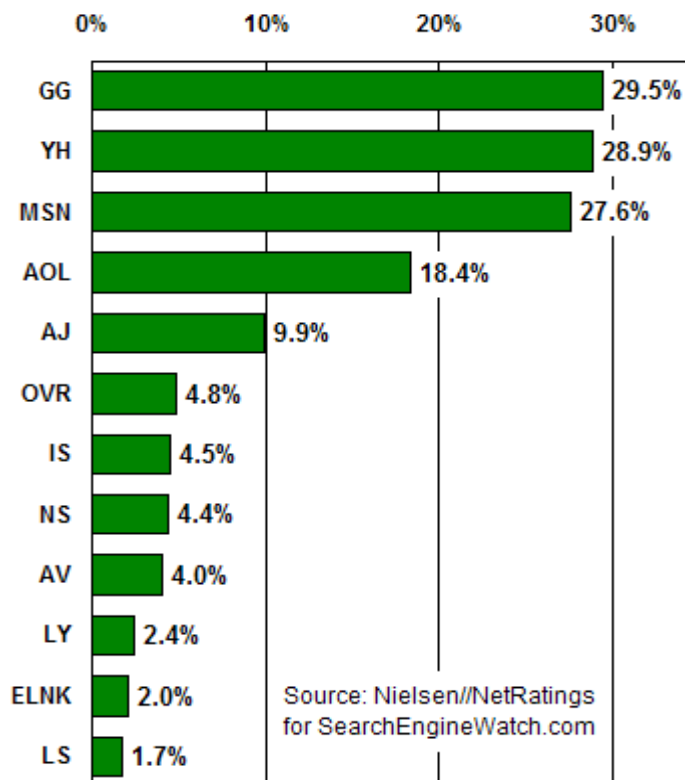
Vir: <http://persons.marlboro.edu/~jkramer/mis/wi-fall2002/week6.html#sework>

Med najbolj poznanimi primeri iskalni strojev so:

- [Google](#)
- [AltaVista](#)
- [HotBot](#)
- [Lycos](#)
- [Excite](#)
- [Overture](#) - plačljiv iskalni stroj

- »Overture« je posebni iskalni stroj, ki ga financirajo podjetja, ki oglašujejo svoje proizvode. Za vsako povezavo iz iskalnika na stran oglaševalca, le ta prizna določen znesek.

Slika 42: Razmerje uporabe iskalnikov v obdobju januar 2003 v ZDA



Legenda: GG=Google, YH=Yahoo, MSN=MSN, AOL=AOL, AJ=Ask Jeeves, OVR=Overture (GoTo), IS=InfoSpace, NS=Netscape, AV=AltaVista, LY=Lycos, ELINK=EarthLink.com, LS=LookSmart.

Slika 42 prikazuje najbolj popularne iskalnike v ZDA v januarju 2003. V diagramu ni zajeto število obiskov strani, upoštevane so le zahteve po iskanju več kot 60.000 uporabnikov.

5.6.3. Meta iskalni stroji

Meta iskalni stroji so stroji, ki iščejo po več iskalnih strojih. Odgovor je rezultat iskanja iz več različnih iskalnih strojev. Teoretično so to čarobna orodja za iskanje primernih rezultatov, v praksi pa so lahko rezultati precej zmedeni. Slaba stran preprostih metapodatkov za evidentiranje HTML dokumentov imenovanih metapovezav je, da so uporabni le za opis zbirk dokumentov, ki so dostopne preko spleta zato je obnavljanje in zbiranje povezav lahko zelo dolgotrajno. Pri zbiranju podatkov iz dveh ali več iskalnih strojev in kreiranju nove zbirke podatkov lahko pride do neskladja, ki je posledica različnega razvrščanja metapovezav z popolnoma drugim pomenom.

Primeri meta iskalnih strojev:

- [DogPile](#)
- [Mamma.com](#)
- [MetaCrawler](#)

Meta iskalni navigator je preprosto orodje, ki omogoča uporabo vmesnikov na različnih iskalnih strojih in istočasno iskanje na več strojih. Med najbolj znanimi sta:

- [Search.com](#) - preko 250 iskalnih strojev
- [Infomine](#) - preko 90 iskalnih strojev

Napredni iskalni navigatorji imajo vhodni vmesnik, ki pošlje poizvedbo na vse iskalnike (ali le na določene, ki jih definira uporabnik) tako, da eliminira podvojene rezultate in rangira rezultate iz različnih iskalnih strojev. Primeri:

- [2ask](#)
- [ALL-IN-ONE](#)
- [IBM InfoMarket Service](#)

5.6.4. Knjižnice

Tematske knjižnice so narejene in se vzdržujejo ročno s pomočjo urejevalnika in ne uporabljajo spletnih pajkov ali robotov. Vsebina je izbrana le iz določenih spletnih strani, ki izpolnjuje pogoje predhodno določenih izbranih kriterijev. Spisek virov je običajno naveden. V principu naj bi bile knjižnice manj obširne kot so podatkovne baze iskalnih strojev.

Knjižnice omogočajo povezave in preiskovanje po zelo obsežnih skladiščih informacij z specifično vsebino. V splošnem knjižnice omogočajo prikazovanje in pregledovanje posameznih strani po vsebinskih kategorijah. Običajno je iskanje po specifičnih informacijah zamudno, vendar so knjižnice dobro izhodišče za začetno iskanje, ko nimamo popolnoma jasnih osnov o temi za iskanje. Med najbolj znane knjižnice sodi Yahoo.

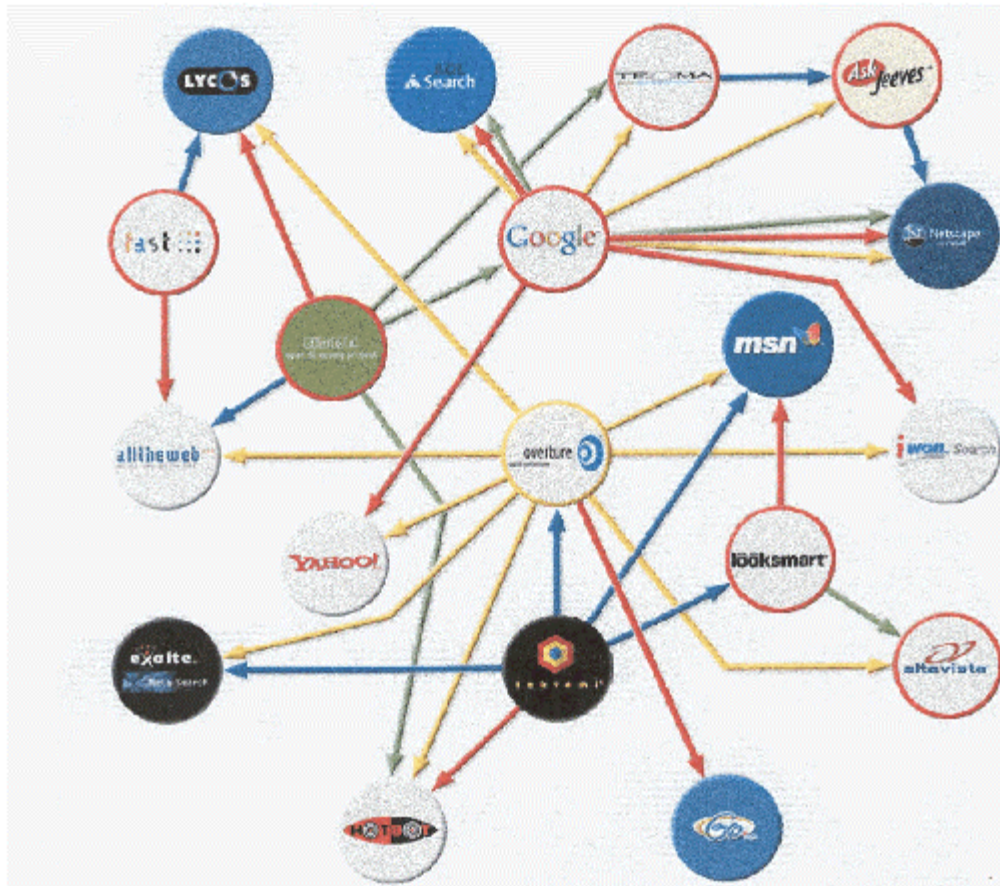
- [Yahoo](#)
- [LookSmart](#)
- [DMOZ](#) - the open directory project

Danes je linija med knjižnicami in iskalnimi stroji zamegljena, saj ima veliko knjižnic partnerstvo z iskalnimi stroji, ki preiskujejo te knjižnice in gradijo svojo podatkovno bazo. Medsebojne povezave iskalnih strojev prikazuje [slika 43](#).





Slika 43: Primer povezave iskalnikov

Povezave iskalnikov

na dan 1.12.2002



Legenda

-  primarni rezultati iskanja
-  sekundarni rezultati iskanja
-  rezultati iskanja po knjižnicah
-  sprejem plačanih rezultatov iskanja

Vir:prirejeno po www.bruceclay.com

5.7. Nevronske mreže

Svet je poln podatkov, ki z ustreznim zbiranjem in urejanjem postanejo informacije, če seveda imamo dovolj znanja in malo sreče. V današnjem kompleksnem in medsebojno povezanem svetu se rapidno povečuje število informacij shranjenih in izmenjanih v elektronski obliki. Vse te informacije so sicer dostopne vendar se pojavlja vprašanje kako jih zbrati in obdelati, da bodo uporabne. Zelo resnične so besede, ki jih je izrekel John Naisbitt: »Utopljam se v informacijah a smo lačni znanja«.

Svet je poln neurejenih virov podatkov, ki dejansko niso popolnoma zanesljivi, kot tudi ne znanje, ki bazira na tako pridobljenih podatkih.

Rešitev vključuje oziroma zahteva preiskovanje podatkov, prečiščevanje podatkov (priprava podatkov za analize), analiza podatkov in končno prezentacijo na način, ki omogoča sprejemanje odločitev na osnovi znanja zgrajenega na pridobljenih podatkih. Ključna je raziskava in izločanje informacij na podlagi medsebojne odvisnosti podatkov, ki lahko privedejo do določenih spoznanj. V ta namen potrebujemo ustrezna orodja in tehnologije, ki so sposobna v neki meri nadomestiti človeške možgane pri pregledovanju, zbiranju in sortiranju ogromnih količin podatkov. To omogočajo empirični modeli, ki so sposobni hitro in natančno najti uporabne vzorce iz podatkov.

5.7.1. Pomen nevronske mreže

Nevronske mreže so matematična zgradba, ki oponaša procese, ki jih človek uporablja za prepoznavanje vzorcev, učenje nalog in reševanje problemov. Nevronske mreže karakterizira število in način povezav med posameznimi procesnimi elementi imenovanimi nevroni in uporabljenimi pravili učenja iz podatkov dobljenih iz omrežja. Vsak nevron ima prenosno funkcijo, ki je običajno nelinearna in generira posamezno izhodno vrednost iz vseh uporabljenih vhodnih vrednosti. Posamezne strukture nevronov in medsebojnih povezav, so običajno odraz arhitekture nevronske mreže. Učinkovitost nevronske mreže je odvisna od sposobnosti učenja iz izkušenj (iz zbranih in shranjenih zgodovinskih podatkov o posameznih problemih). Nevronske mreže se učijo identificirati vzorce z urejanjem in ocenjevanjem vrednosti, ki so odraz vhodnih podatkov. Učenje je lahko nadzorovano ali nenadzorovano. Pri nadzorovanem učenju se uporablja primere za katere so znane izhodne vrednosti. Primerjava med rezultati znanih primerov in nevronske mreže se uporablja pri testiranju in reguliranju povezav nevronske mreže. Pri nenadzorovanem učenju nevronske mreže identificirajo skupine (grupe) vhodnih podatkov, ki bazirajo na matematični definiciji intervalov.

V obeh primerih je nevronska mreža po uspešnem testiranju lahko predana v uporabo in služi za sprejemanje odločitev in aktivnosti ob spremembi vhodnih podatkov.

5.7.2. Tržne rešitve

Nevronske mreže na osnovi empiričnih modelov so uporabljene v mnogih tržnih aplikacijah. Obnašanje potrošnikov je z uporabo interneta možno raziskovati v realnem času. Modeli nevronske mreže lahko spoznavajo navade posameznikov in skupin uporabnikov, ki služijo organizacijam za specialne ponudbe. Z zbiranjem podatkov po posameznih tržiščih (na celotni zemeljski obli), lahko napovedujejo trende porabe v prihodnosti. Z raziskavo vzorcev nakupov se lahko zagotovi osnova za vzpodbujanje dodatnih nakupov ali uslug z prilagajanjem cene ali odobravanjem popustov v realnem času.

Za vsako organizacijo je pomembno, da obdrži stare stranke in si prizadeva poiskati nove ter jih privabiti k nakupu. Z nadzorom in preučevanjem procesov s strankami se skuša ugotoviti njihova pričakovanja in navade. Pomembno je poiskati vzorce aktivnosti, ki predstavljajo poskuse strank za odpravljanje različnih problemov s

katerimi se srečujejo, kot tudi pravočasno opozarjanje na potencialne probleme znotraj organizacije.

5.7.3. Varnostne rešitve

Vedno več informacij o posameznikih je dosegljivih na omrežju, vzporedno pa naraščajo tudi zahteve po zanesljivi in učinkoviti identifikaciji. Biometriji, ki bazira na fizioloških lastnostih posameznika se posveča veliko pozornosti pri učinkovitem prepoznavanju in potrjevanju identitete. Nevronske mreže so lahko osnova za stroje za prepoznavanje vzorcev kot so prstni odtisi, očesna mrežnica, glasovni zapisi, rokopisi ali celo tipkana pisava.

Podjetja, ki imajo interni računalniški sistem povezan na internet, morajo biti pripravljena na poskuse vdorov v sistem in zlonamerne poskuse. Nevronske mreže so lahko učinkovito sredstvo za učenje vzorcev sprejemljivih vsebin paketov in vhodov, ki lahko služijo kot dinamični varnostni požarni zid.

6. Informatika v KDD

6.1. Poslanstvo družbe

KDD je bila ustanovljena januarja 1995. Dejavnost družbe, kot jo opredeljuje Zakon o trgu vrednostnih papirjev, so opravljanje storitev izračuna, izravnave in zagotavljanja izpolnitve obveznosti, nastalih na podlagi poslov z vrednostnimi papirji, sklenjenih na organiziranem trgu vrednostnih papirjev, storitve vodenja centralnega registra nematerializiranih vrednostnih papirjev v skladu z Zakonom o nematerializiranih vrednostnih papirjih ter druge storitve v zvezi s poslovanjem z vrednostnimi papirji in uveljavljanjem pravic iz vrednostnih papirjev.

6.1.1. Zagotavljanje storitev KDD

KDD zagotavlja naslednje storitve (Pravila poslovanja KDD, 1996) :

- hramba in zbirna hramba vrednostnih papirjev, ki so bili izdani kot pisne listine,
- vodenje centralnega registra vrednostnih papirjev in s tem;
- vodenje stanja vrednostnih papirjev na računih članov KDD,
- vodenje stanja imetnikov vrednostnih papirjev,
- vodenje knjig imetnikov vrednostnih papirjev, ki se glasijo na ime, opravljanje prenosov vrednostnih papirjev s preknjižbo na računih članov KDD in na računih imetnikov vrednostnih papirjev;
- izračun in izravnava ter zagotavljanje izpolnitve denarnih obveznosti, nastalih na podlagi poslov z vrednostnimi papirji na organiziranem trgu in v zvezi s tem
- izračun skupnih denarnih obveznosti in terjatev posameznega člana KDD;
- ugotavljanje stanja denarnih terjatev in obveznosti posameznega člana KDD po pobotanju vzajemnih terjatev in obveznosti;
- zagotavljanje izvršitve plačila denarnih obveznosti in izpolnitve obveznosti prenosa vrednostnih papirjev.

6.1.2. Uporabniki trga vrednostnih papirjev

Poslovanje z vrednostnimi papirji v nematerializirani obliki poteka redno preko pooblaščenih članov KDD. Člani KDD so:

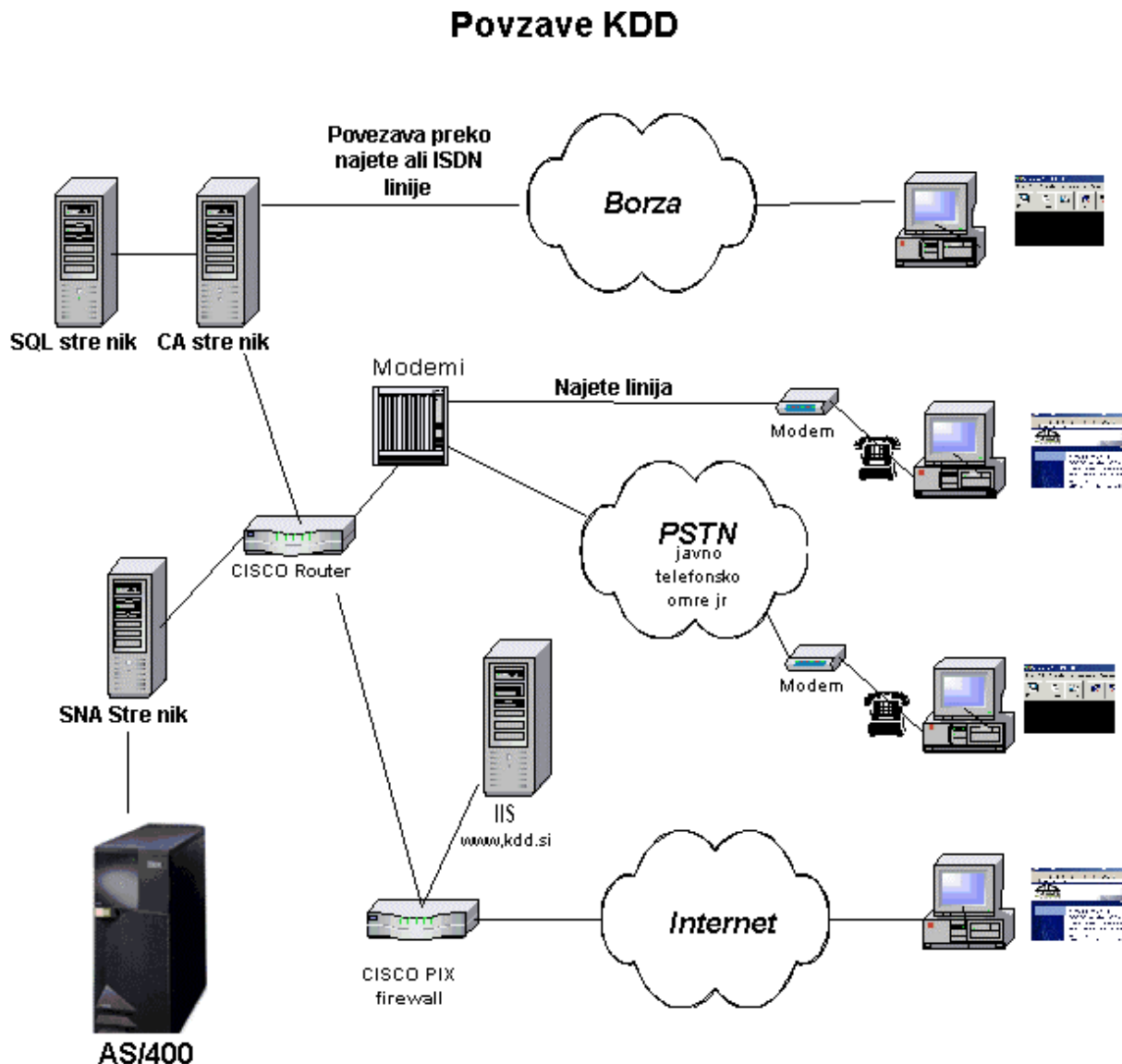
- banke ali borzno posredniške družbe,
- investicijske družbe in pooblaščene investicijske družbe,
- družbe za upravljanje in pooblaščene družbe za opravljanje,
- zavarovalnice,
- Republika Slovenija,
- Banka Slovenije.

Pojem **Član KDD** pomeni pravno osebo, ki jo KDD sprejme v članstvo in ima odprt enega ali več računov vrednostnih papirjev in sklenjeno pogodbo o pristopu k članstvu KDD.

Uporabniki trga vrednostnih papirjev so izdajatelji, ki z izdajo delnic pridobijo kapital za svoje delovanje. Izdajatelj je lahko podjetje, ki hoče razširiti proizvodnjo in dobi za to denar z izdajo nove emisije delnice, lahko je to država, ki izda obveznice.

Drugi uporabniki trga vrednostnih papirjev pa so investitorji, ki imajo denar in želijo ta denar vložiti čim bolj donosno z namenom po čim večjem dobičku. Investitorji (ali imetniki vrednostnih papirjev) so lahko tako fizične kot pravne osebe, lahko so domači ali tuji investitorji.

Slika 44: Povezave zunanjih uporabnikov s KDD



Vir: prirejeno po Burian at .al.

Na *sliki 44* so prikazane povezave zunanjih uporabnikov s KDD. Člani dostopajo do sistema KIS (AS/400) in intraneta na tri načine:

- preko Borze, ki je s KDD povezana preko najete linije,
- najete telefonske linije

- klicne telefonske linije

Notranje omrežje KDD je ločeno od interneta s požarno pregrado (ang. Firewall).

Člani KDD

Pooblašteni člani imajo dostop do informacijskega sistema KDD (v nadaljevanju KIS), ki poteka na sistemu IBM AS/400. Dostop do sistema (glej slika 44) imajo po najeti ali ISDN liniji preko SNA (System Network Architecture) strežnika. Razvit je bil v fazi osnovanja KDD, za podporo takrat znane funkcionalnosti. Nematerializirano vodenje centralnih registrov je relativno nov in specifičen pristop tako za Slovenijo, kakor tudi za ostale predvsem vzhodnoevropske države. Sistem je bil razvit v relativno kratkem času, s primerno tehnologijo in tehnološkimi rešitvami, ki so bile takrat dostopne. Dopolnjevanje in prilagajanje sistema uporabnikom, predvsem pa vzdrževanje takega sistema je oteženo in povezano z dolgimi intervencijskimi časi in visokimi stroški. Aplikativna oprema je bila napisana v jeziku tretje generacije (RPG) in je slabo dokumentirana. Osnovna oziroma celotna dejavnost KDD je neposredno odvisna od učinkovitega delovanja informacijskega sistema, zato se je pojavila potreba, da se na osnovi pridobljenih izkušenj in znanja z uporabo sodobnih tehnologij pripravi nov sistem. Sistem mora brez večjih pretresov in nevšečnosti na strani uporabnikov zamenjati obstoječi sistem.

Aplikacije novega KIS in registra se pripravljajo na podlagi poslovnega modela, ki temelji in je izpeljan iz obstoječega sistema, ter je usklajen s pravno ureditvijo in prakso poslovanja z vrednostnimi papirji. V izdelavi je nov informacijski sistem za vodenje centralnega registra vrednostnih papirjev (v nadaljevanju CRVP), ki se bo izvajal v najmodernejši tehnologiji odjemalec-strežnik (Client-Server). Nova programska oprema CRVP bo izdelana tako, da bo podpirala več jezikov in bo na razpolago tudi drugim (tujim) klirinško depotnim hišam.

Izdajatelji VP

Delniška knjiga

KDD je izdajateljem vrednostnih papirjev dolžna enkrat mesečno (stanje na zadnji dan v mesecu) in za potrebe skupščine delničarjev (stanje na dogovorjeni dan), posredovati podatke o stanju delnic po imetnikih (delniška knjiga - v nadaljevanju DK) na mediju, ki si ga izdajatelj izbere:

- disketa
- internet
- izpis v papirni obliki (v izrednih primerih)

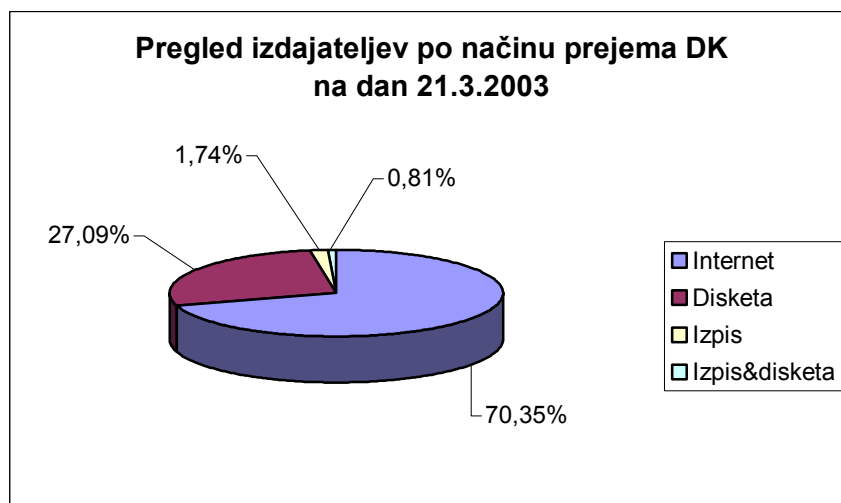
Pisanje podatkov na papir oziroma disketo ima vrsto slabosti:

- razpošiljanje po pošti je zamudno,
- nezanesljivo (možne poškodbe medija),
- zahteva ročno delo operaterja,
- reševanje reklamacij (v primeru nečitljive diskete; ponovna izdelava in pošiljanje)

Posredovanje podatkov preko intraneta ima zato več prednosti:

- avtomatska računalniška obdelava priprave podatkov,
- krajši čas priprave podatkov,
- varna in zanesljiva distribucija podatkov (SSL protokol),
- nižji stroški in čas dostave.

Slika 45: Pregled načina prejema DK



Vir: lastni

Uporabniki informacijske tehnologije KDD

Uporabnike sistema KIS, oziroma CRVP, torej lahko delimo v naslednje skupine:

- zaposleni v KDD,
- uporabniki pooblaščenih članov KDD,
- izdajatelji VP,
- uporabniki (potencialni kupci) programske opreme CRVP,
- spletni uporabniki

V KDD je preko 60 zaposlenih, ki uporabljajo PC računalnike povezane v lokalno mrežo. Uporablja se operacijski sistem MS Windows NT4, ki se postopoma nadomešča z MS Windows 2000 oziroma WindowsXP.

Pooblaščenih članov KDD je 60 in imajo različno število uporabnikov. Člani imajo dostop do intraneta, kjer se jim nudi splošna obvestila in podatke, ki se pripravljajo vsakemu članu v svojo mapo in sistema KIS preko SNA strežnika. Dostop do Intranete poteka po SSL protokolu s 128 bitnim kodirnim ključem.

Izdajatelji vrednostnih papirjev, ki imajo dostop do podatkov o imetnikih preko interneta je trenutno cca 650, ostali pa prejmejo enkrat mesečno disketo. KDD nudi Izdajateljem vrednostnih papirjev tudi program "Knjiga imetnikov" s katerim lahko pregledujejo in izpisujejo podatke o imetnikih po različnih kriterijih.

Sistem KIS je ime za aplikacijo vodenja registra vrednostnih papirjev, ki poteka na sistemu IBM AS/400.

6.1.3. Uporabljene tehnologije v CRVP

V novem sistemu bo integriteta podatkov in transakcij podprta z novimi rešitvami in tehnologijami, ki so dostopne danes in jih pri razvoju obstoječega sistema ni bilo, oziroma so bile preobsežne in s tem predrage. Namen prenove je tudi odpraviti oziroma zmanjšati napake pri zajemu transakcij in zagotoviti čim večjo kvaliteto podatkov (predvsem vhodnih). Težnja je, da bi bilo čimveč transakcij v novem CRVP elektronsko podpisanih (digitalni podpis). Prav tako je namen povečati integriteto podatkov z uporabo sistemskih rešitev (npr. z uporabo mehanizmov podatkovne baze).

Tehnologije in postopki, ki vodijo do lažje izpolnitve ciljev:

- pregled in racionalizacija vsebine sistema CRVP;
- definiranje natančnih pravil operativnega delovanja KDD;
- avtomatizacija poslovnih procesov s pomočjo uvedbe elektronskega načina poslovanja, upravljanja z dokumenti ipd;
- uporaba svetovnih standardov (ISIN, SWIFT, CFI, DNAfs,...);
- uporaba sodobnih tehnologij (nižja cena, hitrejši razvoj, večja nadgradljivost, prijaznejši grafični vmesniki, ipd.), kot so upravljanje z dokumenti, elektronska pošta, transakcijski sistemi, OLAP tehnologija, elektronsko pošiljanje, elektronsko potrjevanje in podpisovanje (digitalni podpisi) transakcij, internet/intranet, TCP/IP, ISDN, PKI (Public Key Infrastructure).

Delitev področja CRVP

Področji, na katera je projekt CRVP razdeljen sta tehnični in vsebinski. Delitev projekta na module, zaradi lažjega tehničnega prilagajanja in izdelave ter vključevanja funkcionalnosti v tako delitev, je sledeča:

- infrastruktura s potrebno strojno in sistemsko programsko opremo,
- ravnanje z dokumenti in sledenje delovnih procesov,
- podpora finančnemu in računovodskemu sektorju,
- članske aktivnosti in funkcionalnosti z uporabniškimi vmesniki,
- osrednja funkcionalnost CRVP s podatkovno bazo in transakcijskim delom KDD.

Operacijski sistem

Uporablja se operacijski sistem Windows 2000. Aplikacija bo tekla v okolju MTS, ki je del operacijskega sistema Windows 2000.

Podatkovna baza

Microsoft SQL Server 2000.

Komunikacija s klienti

Na strani KDD se bo uporabljal Microsoft Internet Information Server, na strani klienta pa Microsoft Internet Explorer 5 (ali novejši). Standard za komunikacijo s klienti bo HTML/XML preko HTTP, oziroma preko Microsoft Message Queue. Komunikacijo preko XML-a bo na strani strežnika izvedena s pomočjo Java paketov

“com.ms.xml.om”, “com.ms.xml.dso”, “com.ms.xml.parser” in “com.ms.xml.util”. Na strani klienta bo uporabljena podpora XML-u, ki je vgrajena v Internet Explorer 5.

Razvojno orodje in programski jeziki

Za načrtovanje podatkovne baze je uporabljen Platinum ERWin v povezavi z Rational Rose.

Za pisanje programov se uporablja Microsoft Visual Studio 6. Programski jezik je J++. Tam, kjer performanse J++ ne bodo zadoščale pa C++.

6.2. Analiza obstoječega stanja

6.2.1. Portal KDD

Portal KDD je bil izdelan in na spletnih straneh objavljen v letu 1999. Od prve objave do danes, se razen nekaterih vsebinskih sprememb ne razlikuje, zato se pripravlja sprememba izgleda in vsebine portala. Portal je potrebno redno vzdrževati in dograjevati z aktualno vsebino zanimivo za uporabnike. Dostop do strani, ki zahtevajo identifikacijo bi moral biti nedvoumen in ločen za izdajatelje in člane. Predvsem izdajatelji imajo probleme, z izbiro opravil namenjenim članom. Izvesti je potrebno personalizacijo tako, da so funkcije namenjene posameznim grupam uporabnikov (izdajatelji, člani, ostali uporabniki) jasno in popolnoma ločene tako, da jih ni možno niti po pomoti zamenjevati.

6.2.2. Navodila

Osnovna navodila za dostop do strežnika KDD dobijo člani in izdajatelji v pisni obliki po pošti takoj, ko KDD prejme seznam pooblaščenih oseb.

Izdajatelji VP

Splošna navodila namenjena praviloma izdajateljem so dostopna na naslovu www.kdd.si/datoteke. Poleg navodil je na tem naslovu tudi program »Knjiga imetnikov« v stisnjenem zapisu, katerega si lahko izdajatelji prenesejo na svoj PC in instalirajo. Pri prvem zagonu programa je potrebno le tega registrirati. Vsebina naslova je naslednja:

[Kako prenašamo datoteko z delniško knjigo preko interneta.doc](#)

[KI Navodilo za program - priloga.zip](#)

[KI Navodilo za program ver 1.2.zip](#)

[KNJIGA IMET NAROČILNICA .doc](#)

[KNJIGA IMET OPIS .doc](#)

[KnjigaImetnikov1.zip](#)

[KnjigaImetnikov2.zip](#)

[KnjigaImetnikov3.zip](#)

[KnjigaImetnikov4.zip](#)

[KnjigaImetnikov5.zip](#)

[Navodila za prenos programa Knjiga Imetnikov.txt](#)

[Poblast izd.doc](#)

[Pooblast izd internet.doc](#)

Člani - intranet

Člani imajo dostop do navodil preko članskega portala, ki je dostopen preko HTTPS protokola. Član, ki je istočasno tudi izdajatelj, lahko dostopa do podatkov svoje DK tudi preko intraneta (glej rubrika »Izdajatelji« [slika 46](#)). Dostop do obvestil in splošnih datotek, ki jih KDD pripravlja za svoje člane v različnih časovnih intervalih (mesečno, tedensko, dnevno ali med delovnim časom vsako uro), odvisno od vsebine in namena podatkov, je možen tudi preko interneta, medtem ko do vseh ostalih podatkov preko interneta nimajo dostopa.

Slika 46: Osnovna spletna stran za člane KDD



6.3. Predlog sprememb

6.3.1. Dostop do navodil

Uporabnikom je potrebno omogočiti dostop do navodil neposredno iz portala KDD.

6.3.2. Obveščanje neplačnikov

Način obveščanja neplačnikov. Na podlagi spiska neplačnikov, ki ga pripravi oddelek računovodstva, se neplačnikom odvzame pravico dostopa do podatkov. Pooblaščen oseb izdajatelja bi morala biti avtomatsko obveščena o odvzemu pravic.

Način obveščanja ob poravnavi obveznosti. Ko oddelek računovodstva izbriše izdajatelja iz liste neplačnikov, bi morala pooblaščen oseb prejeti E-pošto z obvestilom, da je dostop do datotek zopet možen.

6.3.3. Avtomatski prenosi – brez uporabe spletnega brskalnika

Avtomatski prenos omogoča poseben program, ki uporabniku, ki ima na svojem osebem računalniku instaliran veljaven certifikat, omogoči dostop do knjižnice z datotekami in kopijo datoteke. Zaradi različnih varnostnih omejitev se uporabljata dva programa, eden za dostop do podatkov na intranetu in drugi za dostop in prenos datotek preko interneta. Program se v obeh primerih zažene s parametri:

- uporabnik,
- geslo,
- lokacija in ime datoteke.

Avtomatski prenosi podatkov (datotek) so pomembni predvsem za člane, ki svoje datoteke prenašajo dnevno tako, da jih sprožajo iz seznama za avtomatsko izvajanje opravil (ang. Scheduled Tasks) in se prenesejo v njihovo podatkovno bazo »Back Office«, na določen dan ob določenem času. Predvsem so to dnevni prenosi, ki se pripravljajo pred začetkom delovnega časa. Take prenose običajno izvajajo skrbniki podatkovnih baz, ki imajo ustrezno računalniško znanje.

Zaradi pomanjkljivega računalniškega znanja izdajateljev, ki imajo težave že z osnovnimi računalniškimi ukazi, bi bilo smiselno pripraviti vmesnik za prenos podatkov njihove DK, brez uporabe spletnega brskalnika.

6.3.4. Pogosto zastavljena vprašanja

Na podlagi statistike evidenca pogostih vprašanj, ki jih uporabniki zastavljajo po telefonu ali elektronski pošti, bi bilo potrebno izdelati seznam pregleda vprašanj in odgovorov in jih objaviti na spletni strani tako, da so uporabnikom vedno na voljo. S tem bi se zmanjšalo število telefonskih klicev in prejete elektronske pošte.

Certifikat

- Zakaj potrebujemo certifikat?
- Kako preverimo ali je instaliran certifikat?
- Kako instaliramo certifikat?
- Kako odstranimo neveljaven certifikat?
- Seznam napak in opis rešitev.

Dostop do datotek

- Kako dostopamo do datotek?
- Kako prenesemo datoteko na svoj računalnik?
- Razpakiranje datoteke (pretvorba iz ARJ format v TXT)
- Zakaj pakiramo datoteke?
- Kako pregledujemo podatke DK?
- Napake - seznam znanih napak in opis rešitev.

Program »Knjiga imetnikov«

- Opis programa - kaj omogoča in zakaj se uporablja?
- Kako instaliramo program?
- Kako pridobimo pravico do trajne uporabe programa?
- Seznam napak in opis rešitev.

6.4. Programski paket ReactPro

Programski paket ReactPro je izdelek podjetja Repro MS iz Ljubljane. Namen programskega paketa je pregledovanje partnerjev in njihovih tehničnih problemov (spremljanje podpore in nudenje pomoči internim uporabnikom, kakor tudi zunanjim uporabnikom), ter uporabljene izkušnje in znanje shranjevati v bazi. V praksi je orodje preko interneta dostopno kjerkoli in v vsakem času. Narejeno je na podlagi Microsoft tehnologij za uporabo na spletu.

Odjemalec je spletni brskalnik, tako ima uporabnik enako okolje neglede kje se nahaja; na delovnem mestu, doma ali pri stranki. Na enak način je narejeno skrbništvo, ki je v celoti dostopno preko spleta.

V paket je vgrajen varnostni sistem, ki skrbi za beleženje nepooblaščenih dostopov in omogoča enostavno spreminjanje nivojev dostopa posameznim tipom uporabnika.

Trinivojska zasnova aplikacije (po priporočilih Microsoft WinDNA) omogoča hitrejše spreminjanje ter nadgrajevanje posameznih funkcionalnosti in prilagoditev. Objektna zasnova omogoča vključitev funkcionalnosti ReactPro v orodja zbirke MS Office.

6.4.1. Namen uporabe

V KDD se želi vzpostaviti centralno evidenco pomoči uporabnikom, ki bo služila lažji identifikaciji uporabnikov pri nudenju pomoči, ter evidenci pomoči in napak. Na osnovi evidentiranih dogodkov se bo zgradila baza na podlagi katere bodo možni različni vpogledi kot so:

- vrste napak oziroma problemov (Aplikacija, razvoj, internet,)
- način odprave problema (telefon, E-pošta, obisk na lokaciji, ...)
- opis odprave problema,

- pregled nespremenjenih problemov,
- statistika (število problemov, frekvenca, statistika po partnerjih, aplikacijah..)
- čas potreben za odpravo,
- status problema (prijavljen, v reševanju, odgovor posredovan)
- prioriteta reševanja.

Večino od navedenih pregledov programski paket ReactPro že omogoča.

6.4.2. Končni cilji

Končni cilj je vzpostaviti sistem za podporo uporabnikom, ki bo:

- evidentiral, spremljal in nadzoroval dogodke HD,
- obveščal uporabnike o problemih in njihovih rešitvah (po elektronski pošti),
- posredoval nerešene probleme odgovornim,
- shranjeval rešene probleme v arhiv,
- skrajšal čas od prijave problema do rešitve,
- zmanjšal stroške oddelka za pomoč uporabnikom.

6.4.3. Baza podatkov

Baze uporabnikov so v KDD že narejene, vendar so podatki razpršeni v različnih tabelah zato jih je potrebno združiti v enotno bazo.

Partnerji

V KDD se partnerji, oziroma uporabniki ločijo na podjetja:

1. Izdajatelji VP
2. Pooblašeni člani
3. Kupci programske opreme CRVP (druge depotne družbe, ki uporabljajo program CRVP)
4. KDD

Podatki o partnerju (prenos iz obstoječe baze):

- | | | |
|--|-------|----|
| 1. Naziv podjetja | | |
| 2. Koda* | A | 10 |
| 3. Matična številka | N | 15 |
| 4. Ulica | | |
| 5. Pošta | A | 7 |
| 6. Kraj | | |
| 7. Država | A | 3 |
| 8. Primarni tip (internet, disketa, izpis, disketa&izpis, ...) | A | 12 |
| 9. Datum izdaje | | |
| 10. Interval pošiljanja podatkov (dnevno, tedensko, mesečno) | | |
| 11. DK | (D/N) | |
| 12. Transakcije | (D/N) | |
| 13. Zastave | (D/N) | |

14. Knjižnica (ime knjižnice v kateri se hranijo podatki partnerja)
15. Geslo (dostopno le skrbniku programa)
16. Oznaka solventnosti (N-neplačnik; P-prisilna poravnava; S-stečaj)
17. Vrsta pogodbe
18. Direktor (ime in priimek)
19. Opomba
 - *Pri evidenci partnerjev prikaz kode (alfa 10 mest) in možnost iskanja partnerja tudi po kodi.

Kontaktne osebe

Podatki o kontaktni osebi, oziroma osebah partnerjev vsebujejo podatke (iz obstoječe baze):

1. ime in priimek,
2. elektronski naslov,
3. telefon,
4. telefaks,
5. uporabniško ime,
6. datum izdaje certifikata,
7. ime datoteke,
8. geslo,
9. zap. št. dokumenta (pooblastila),
10. opomba.

Problemi

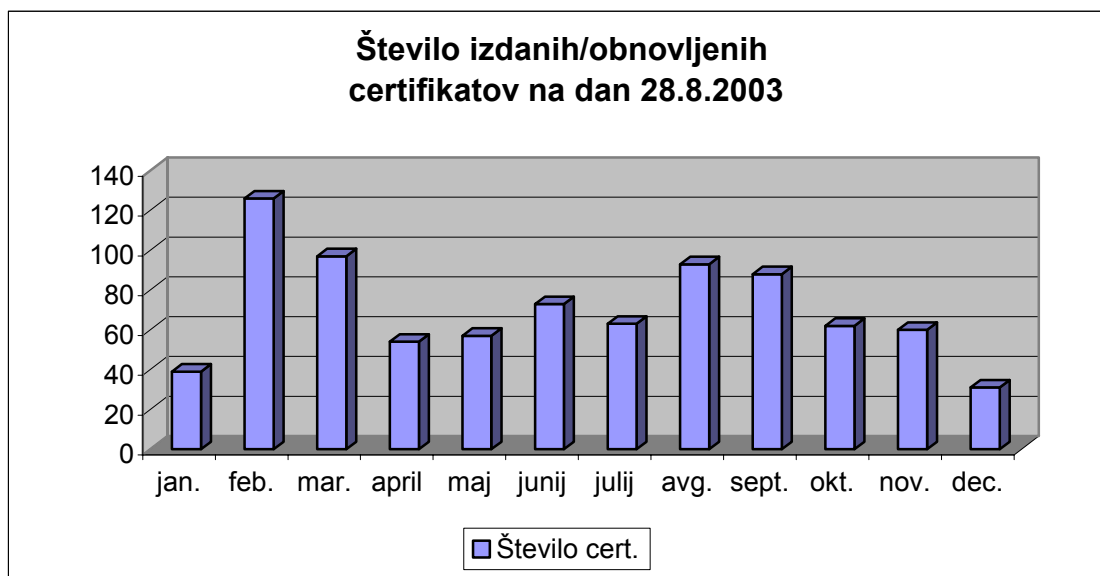
| Opis | 1 Izd. | 2 Član | 3 CRVP | 4 KDD |
|----------------------------------|-----------|-----------|-----------|----------|
| Certifikat | X | X | X | X |
| Dostop do Intraneta | | X | X | X |
| Dostop do spletne strani KDD | X | X | X | X |
| KIS (AS/400) | | X | | X |
| Omrežne komunikacije | X | X | X | X |
| Podatki DK | X | | | |
| Program CRVP ⁵ | | X | X | X |
| Program Knjiga Imetnikov | X | | | |
| Vsebina spletnih strani Intranet | | X | X | X |
| Vsebina spletnih strani WWW | X | X | X | X |
| SWIFT | | | | X |
| Neplačniki | X | X | X | |
| Programi za finance | | | | X |

V tabeli je groba razdelitev problemov in partnerjev pri katerih se pojavljajo. Certifikati, ki se uporabljajo za dostop do podatkov preko spleta veljajo eno leto, nato pa jih je potrebno obnoviti. Na leto je potrebno tako ročno izdelati preko 850 certifikatov.

⁵ CRVP je v testni fazi in ga člani še ne uporabljajo

Certifikati se pošiljajo pooblaščenim osebam izdajateljev VP in članom KDD.

Slika 47: Pregled izdelanih certifikatov po mesecih



S primerno podatkovno bazo v okolju Windows2000 je možno:

- avtomatizirati izdelavo certifikatov,
- obveščanje neplačnikov,
- avtomatizirati distribucijo popravkov programov.

S sistematičnim zbiranjem problemov, bi pogoste probleme objavili na internet strani v rubriki »Pogosto zastavljena vprašanja« (FAQ – Frequently Asked Questions).

Zbiranje problemov

Problemi se zbirajo na eni točki in sicer:

- dokumenti prejeti po pošti – pooblastila, preklici, itd.,
- dokumenti prejeti po telefaksu,
- elektronska pošta,
- telefonski klici.

Sistem dopisov naj bi se uporabljal le izjemoma, in le v primeru kjer se zahteva originalni žig in podpis (pooblastila, kontaktne osebe, ...). Pri tem bi bilo potrebno zagotoviti pretvorbo dokumenta v elektronsko obliko (telefaks to že omogoča) in prenos vpisanih podatkov v obstoječo bazo.

Sporočanje problemov po telefonu se bo postopoma opustilo razen pri izdajateljih VP, ki nimajo interneta. Le oseba, ki problem rešuje, bi lahko v primeru nejasno opisanega problema, poklicala uporabnika.

Prispelem dopisu je potrebno zagotoviti enotno identifikacijo. Pri vnosu v RP se problemi avtomatsko številčijo. Na prejeti dokument se vpiše številka problema in se ga arhivira.

Vnos problema

V programskem paketu RP poiščemo partnerja in njegovo kontaktno osebo in odpremo problem.

V oknu "Opis za tehnika" vpišemo problem partnerja. Opis lahko označimo, tako da ga bo videl tudi partner.

Okno "Opis za partnerja" izpolnimo, če želimo partnerju poslati drugačen opis, kot je opis problema.

Prioriteta reševanja problema:

- nizka,
- normalna,
- visoka.

Status problema je obvezen podatek in je lahko:

- odprt,
- v reševanju,
- čakamo strankine dodatne informacije,
- odgovor posredovan,
- rešeno,
- zaprto.

Kategorija - v tem poljem določimo kategorijo produkta:

- ni razvrščeno,
- aplikacija,
- razvoj,
- internet,
- exstranet,
- komunikacije.

Lokacija - definira način reševanja problema:

- telefon, e-pošta,
- obisk na lokaciji,
- posredovanje pogodbenim izvajalcem.

Operacijski sistem, izberemo iz seznama v kolikor je za reševanje problema pomemben.

Aplikacija - iz seznama izberemo aplikacijo partnerja.

- Access 98
- Access 2000
- IE 5.0
- IE 5.5
- IE 6.0
- CRVP
- Knjiga imetnikov

- IOS – evidenca osnovnih sredstev
- Osnovna sredstva
- Avtorski honorarji
- Osebni dohodki

Procesor – tip procesorja

- Intel Pentium
- Intel Pentium II
- Intel Pentium III
- Intel Pentium IV
- Power PC
-

Velikost pomnilnika - RAM

- 64 MB
- 128 MB
- 256 MB
- 512 MB ali več

Pogodba - izberemo tip pogodbe (še niso definirani)

Popravki - izberemo iz baze popravkov, če je bil popravek instaliran pri partnerju

Po končanem vnosu (izpolnjena morajo biti vsa obvezna polja) se problem doda v bazo. Odpre se novo okno, kjer se odločimo ali obvestimo partnerja po E-pošti o evidentiranju problema ali ne.

Razporejanje problemov

Ker se vsi prispeli dokumenti na internetu zbirajo na enem mestu, so dostopni vsem, ki so pooblaščen za reševanje problemov. Problem se po elektronski pošti pošlje v reševanje drugi fizični ali pravni osebe, če ga na prvi stopnji ne moremo rešiti.

Reševanje

Probleme rešujejo osebe, ki so za to odgovorne za posamezno področje. Ko je problem rešen, oseba, odgovorna za rešitev, o tem obvesti skrbnika HD-a. Skrbnik HD-a dokument označi kot rešenega tako, da vpiše datum rešitve. Skrbnik obvesti DU/osebo, ki je problem posredovala ter problem in njegovo rešitev vključi v intranet.

Vključevanje in iskanje problemov na intranet-u

Na intranetu je kreirana enotno vstopno točko za celoten HD. Skrbnik ima možnost dodeljevanja pravic partnerjem do vpogleda v njihove probleme.

Ustvarjanje baze znanja

Na osnovi rešenih primerov, se ustvarja baza znanja. V bazi so evidentirani vsi prejeti problemi in njihove rešitve. Najbolj pogoste probleme in njihove rešitve se lahko objavi v rubriki »Pogosto zastavljena vprašanja« (FAQ) na domači spletni strani.

6.4.4. Arhiviranje

Podatki se hranijo v SQL bazi podatkovnega strežnika. Arhiviranje podatkov poteka po ustaljenih, predpisanih postopkih.

6.4.5. Poročanje nadrejenim

Nadrejeni imajo neposreden dostop do podatkov. S filtriranjem lahko dobijo le tiste informacije, ki ustrezajo pogojem:

- Poraba časa za reševanje tehničnih problemov omogoča "Pregled ur" za obdobje, ki si ga sami izberejo.
- Statistika omogoča preglede po različnih kriterijih
- Nespremenjeni problemi 7 dni ponuja izpis vseh nerešenih problemov sedem ali več dni.

6.5. Konstrukcija in prikaz modela pomoči uporabnikom

Na *sliki 48* je prikazan model na prvem nivoju analize. Objekti modela so večinoma opisani v prejšnjih poglavjih zato bom navedel pomembnejše:

Uporabniški vidik predstavljajo informacijske storitve v zvezi z vrednostnimi papirji (vknjižbe, preknižbe, dedovanje, ...), denarno poravnavo borznih poslov, finančno računovodskih poslov, kot tudi raznih (upravno-administrativnih) informacij. Pod uporabniško podporo lahko štejemo le navodila, ki so trenutno vključena v portalu in nekaj podpore v aplikaciji KIS.

Informacijski sistem KDD predstavlja povezan IS vseh poslovnih funkcij v KDD, ki so v fazah njegovega planiranja, razvoja ali implementacije.

Upravljanje z znanjem predstavlja proces povezovanja metod in tehnik pridobivanja ter procesiranja podatkov in informacij, ki so plod inovativnosti in sposobnosti človeka.

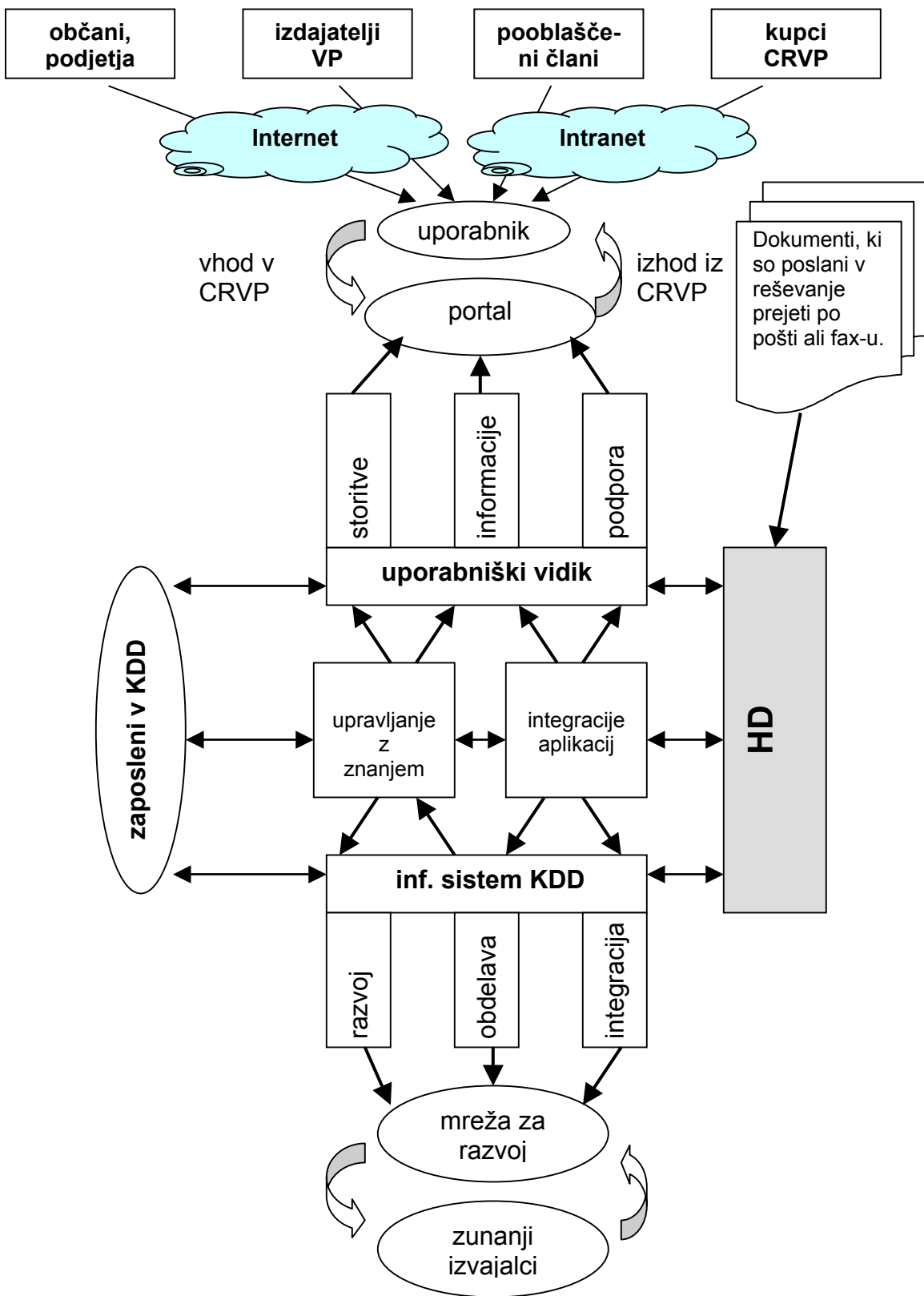
Integracija aplikacij je tehnološki proces povezovanja aplikacij oziroma delnih sistemov v celovit informacijski sistem.

Zunanji izvajalci predstavljajo usposobljene poslovne subjekte, ki izvajajo informatizacijo določenih področij (osebni dohodki, osnovna sredstva, itd) ali določene vsebinske naloge.

Portal predstavlja enotno vstopno točko integriranega IS v KDD. Preko interneta vstopajo občani, podjetja in izdajatelji. Z uporabo HTTPS protokola in kontrolo vstopa lahko izdajatelji prejemajo informacije o stanju in prometu njihovih vrednostnih papirjev. Kontrola vstopa in uporaba HTTPS-a se zahteva tudi za vstop v omrežje intranet.

HD predstavlja programski paket, kot je ReactPro, ki omogoča tehnično podporo preko internet in evidenco pomoči.

Slika 48: Model delovanja HD v okviru IS KDD



Vir: lastni

6.6. Ugotovitve ob prikazanem modelu

Sistem elementov računalniške podpore uporabnikom je obsežen in kompleksen zato je prikazan v obliki enostavnega modela.

Pomembno področje zagotavljanja ustreznega okolja za elektronsko poslovanje predstavljajo enotni tehnični standardi, ki danes temeljijo na principu objektnega modeliranja, podatkovnih skladišč in omrežnega računalništva in s tem povezanimi komunikacijskimi-podatkovnimi omrežji.

Sektor za razvoj IT v KDD si prizadeva upoštevati pravila in standarde pri izdelavi informacijskih rešitev, ki večinoma bazirajo na orodjih podjetja Microsoft, težje pa je to doseči pri zunanjih izvajalcih. Pri posodobitvah licenčne programske opreme, je neupoštevanje standardov lahko vzrok za nepričakovane težave, ki se odražajo v nedelovanje posameznih programov ali celo sistemov.

Pri dostopu zunanjih izvajalcev do IS je potrebno posebno pozornost posvetiti varovanju osebnih podatkov. Dostopajo lahko le do splošnih podatkov in testne baze.

Elektronska pošta je pomemben element, ki mora vsem uporabnikom v KDD omogočiti transparentno izmenjavo podatkov, tako na ravni intraneta, kot na ravni povezav s svetovnim omrežjem internet. Obravnavani model HD temelji na komunikaciji z uporabniki preko elektronske pošte in omogoča avtomatsko beleženje sprejetih zahtev za podporo in reakcij na prejeto zahtevo. Z uporabniki, ki nimajo elektronskega dostopa do KDD, se komunicira na klasičen način (telefon, pošta).

6.7. Analiza predlaganega modela

HD predstavlja infrastrukturo za nadzor in upravljanje storitev s področja podpore in pomoči uporabnikom, ki omogoča:

- spremljanje dejavnosti podpore in dogodkov, ki nastajajo ob izvajanju teh storitev na centru za podporo, pri nudenje poljubnih profesionalnih, specialističnih in intelektualnih storitev,
- spremljanje dejavnosti in dogodkov od naročila do zaključka aktivnosti,
- merjenje kvalitativnih in kvantitativnih učinkov teh storitev tako pri ponudniku, kot porabniku storitev z vidika vsebine, stroškov, porabe virov, učinkovitosti, odzivnih časov, itd.

Naročilo storitve

Programsko orodje omogoča uporabniku naročilo storitve centru za podporo, ki lahko predstavlja:

- prijavo napake, ali vnos naročila za njeno odpravo na različnih področjih,
- prijavo zahteve ali vnosa naročila za pomoč,
- prijavo zahteve za izvedbo poljubne storitve na področju poslovnih procesov ali drugih storitev.

Uporabniki imajo neposreden vpogled v naročila, pregled zgodovinskih dogodkov v procesu reševanja, ter aktivno komunikacijo z osebjem HD.

Posreden vnos naročila se izvaja s pomočjo operaterja na klicnem mestu, ki skrbi za vnos naročil prejetih po telefonu, telefaksu ali elektronski pošti.

Vnos naročila

Vnos naročila v sistem je možno opraviti neposredno ali posredno. Uporabniki lahko vnesejo naročilo preko spleta (internet, intranet) z neposrednim dostopom do aplikacije. S tem se razbremenijo zaposlene v klicnem centru, ki skrbijo za vnos naročil in njihovo posredovanje izvajalcem.

Spremljanje naročil

Programsko orodje omogoča spremljanje naročila od trenutka prijave, do izvedbe naročila oziroma rešitve problema. Naročilo se lahko spremlja po:

- vsebini naročila ali problema,
- zgodovinskih dogodkih posameznih aktivnosti,
- odzivnih časih ter trajanju posameznih aktivnosti,
- porabljenem času, materialu in vrednosti storitev (v primeru, ko jih zaračunamo),
- izvajalcih,
- statusu.

Upravljanje podatkov o partnerjih in kontaktnih osebah

Spremljanje podatkov partnerjev zajema pregled in spreminjanje pomembnih podatkov o podjetjih, in kontaktnih osebah. Naročilo se vedno nanaša na določeno podjetje ter pripadajočo osebo, ki je storitev naročila. Center za podporo uporabnikom lahko na podlagi zbranih zapisov o naročilih pridobi informacije, o pogostih napakah, ki so lahko povod za dodatno izobraževanje uporabnikov.

Večjezičnost

Programski produkt se lahko uporablja v različnih jezikovnih okoljih. Uporabniški vmesnik omogoča določanje jezika na nivoju posameznega uporabnika, skupine, podjetja, države ali regije.

Upravljanje z znanjem

Na podlagi shranjenih podatkov se gradi baze znanja, ki omogoča:

- uporabnikom; pregled in iskanje rešenih primerov (pogosto zastavljena vprašanja - FAQ),
- izvajalcem pomoči; iskanje že rešenih primerov,

Znanje predstavlja eno od najpomembnejših dobrin v podjetju. Baza znanja preprečuje odtok znanja ali zmanjševanje znanja v podjetju, zaradi fluktuacije zaposlenih ali drugih dejavnikov na katere nimamo vpliva.

Opisani način pomoči uporabnikom ustreza zastavljenim ciljem, ki so bili postavljeni v uvodu naloge.

7. Sklepne ugotovitve

Širok spekter uporabnikov z različnim nivojem računalniškega znanja, pri svojem delu uporabljajo različno strojno opremo, z različnimi operacijskimi sistemi in programskimi orodji. Z razvojem lastne programske opreme za vodenje centralnega registra vrednostnih papirjev, ki bo na voljo tudi tujim klirinško depotnim družbam, se bo krog uporabnikov še povečal, s tem pa tudi obseg pomoči. Obseg povečanja podpore uporabnikom bo odvisen tudi od kvalitete novega programskega produkta CRVP in prenovljenega portala družbe.

KDD izpolnjuje vsa priporočila (*opisana v poglavju 1.2.*), ki jih predpisuje skupina G30, razen priporočila št.9, ki govori o mednarodnih standardih. Pri svojem poslovanju se KDD sicer poslužuje predpisov in pravil različnih mednarodnih standardov, vendar sistema kakovosti še nima vpeljanega. Vodstvo se zaveda pomena sistema kakovosti, toda v fazi prenove informacijskega sistema je uvajanje sistema kakovosti preložilo na kasnejši čas.

Uporaba sodobnih informacijskih tehnologij zahteva drugačna, predvsem pa veliko širša znanja, tako pri načrtovanju informacijskih rešitev, kot pri pomoči uporabnikom. Pri izdelavi novega produkta CRVP, so uporabljene najnovejše tehnologije, ki se v svetu šele uveljavljajo, zato praktičnih izkušenj z njimi skorajda ni. Sistem temelji na objektnem, modularnem principu z uporabo večslojne arhitekture odjemalec-strežnik. Za povezavo oziroma uporabo obširnih podatkovnih baz, ki se nahajajo na starejšem računalniškem sistemu IBM AS/400, služijo SNA in SQL strežniki.

Povezave in poslovanje KDD z pooblaščenimi člani in drugimi uporabniki trga vrednostnih papirjev, preko intraneta oziroma interneta, si brez spletnih in aplikacijskih strežnikov danes ne moremo predstavljati.

Pri iskanju znanih rešitev, ki so objavljena na spletu, je poznavanje metod iskanja podatkov in informacij nujno potrebna. Sistemi iskanja informacij se bodo uporabljali in razvijali, dokler bo obstajala potreba po informacijah. Metoda LSA opisana v poglavju 5.5. je le droben kamenček v mozaiku, ki ga sestavljajo različni sistemi in metode, ki jih večinoma razvijajo univerze, računalniška podjetja in podjetja, ki imajo predvsem komercialni interes (Telcordia).

Na trgu se pojavljajo različni proizvajalci z orodji za spremljanje in upravljanje pomoči uporabnikom, med katere sodi tudi Repro d.o.o. s svojim programskim paketom ReactPro. Namen naloge ni bil iskati najustreznejše orodje, temveč izdelati model za zbiranja evidence pomoči, ki služi kot baza znanja, poleg tega pa omogoča različne preglede in poročila. Programski paket sicer ni pisan za potrebe KDD, vendar je tehnološko in z manjšimi popravki tudi vsebinsko ustrezen. Z znanjem in izkušnjami zaposlenih v IT, je verjetno bolj smiselno izdelati lastno orodje za podporo in pomoč uporabnikom, ki bo v celoti prilagojeno poslovanju družbe.

KDD potrebuje integrirano programsko orodje, kot je ReactPro, ki bi povečalo učinkovitost oddelka za pomoč uporabnikom, s tem pa tudi zadovoljstvo uporabnikov. Poročanje je eno glavnih komunikacijskih povezav med zaposlenimi in vodstvom.

Premalo oziroma pomanjkljivo poročanje vodi v subjektivno ocenjevanje rezultatov. Avtomatizirana orodja, učinkovita in enostavna za uporabo, lahko integrirajo poročila, kot sestavni del delovnih nalog, katerih rezultat so primerni in objektivni ukrepi. V okolju, kjer se resnično želi reševati probleme zato, da bi jih rešili, je potrebno znotraj lastnih zidov ustvariti odprto družbo, v kateri prevladujejo osnovna pravila poštenosti in objektivnosti. Objektivnost je dosežena takrat, ko za probleme ne krivimo posameznikov, temveč iščemo in ugotavljamo vzroke.

8. LITERATURA

1. Bates Marcia J.; After the Dot-Bomb: Getting Information Retrieval Right This Time, UCLA Department of Information Studies, 2002, [URL:<http://www.hastingsresearch.com/net/08-net-information-retrieval.shtml#1>], 11.12.2002.
2. Bešter Janez et. al.: Zlivanje telekomunikacijskih omrežij in storitev. Ljubljana: Elektrotehniška zveza Slovenije, 1998. 111 str.
3. Bortniker Matthew, Conrad James M: Visual Basic 6 MTS. Birmingham: Wrox Press Ltd., 1999. 611 str.
4. Bosworth Seymour, Kabay M.E., Computer Security Handbook. New York: John Wiley & Sons Inc., 2002.
5. Bradley Phil: The advanced internet searcher's handbook. London: Library Association Publishing, 2002. 256 str.
6. Cooper James W.: Lexical Navigation; IBM Thomas J. Watson Research Center; Philadelphia, 1997, [URL:http://www.research.ibm.com/irgroup/lexical_navigation.htm], 11.12.2002.
7. Deerwester Scott et. al.: Indexing by Latent Semantic Analysis; University of Chicago; [URL: <http://lsi.research.telcordia.com>], 27.12.2002.
8. Deitel at all: e-Business & e-Commerce HOW TO PROGRAM. New Jersey: Prentice Hall, 2001. 1263 str.
9. Feghhi Jalal, Feghhi Jalil, Williams Peter: Digital Certificates. Massachusetts, Addison Wesley Longman, 1999. 453 str.
10. Feiler Jesse: Application servers: powering the Web-based enterprise. San Diego: Morgan Kaufmann, 2000, 302 str.
11. Ford Warwick, Baum Michael S.: Secure electronic commerce. New Jersey, 1997
12. Foxall James D.: Practical Standards for Visual Basic. Washington, Microsoft, 2000.
13. Gates Bill: Poslovanje s hitrostjo misli. Ljubljana: ORBIS, 1999. 359 str.
14. Hanke Johan-Christian: Spletne strani in HTML, Flamingo založba d.o.o, Šempeter pri Gorici, 2001, 102 str.
15. Hribar Peter: Internet: od elektronske pošte do navidezne resničnosti. Nova Gorica: Flamingo, 1996.
16. Hribar Peter: Spletne strani – zvižaje in nasveti, Flamingo založba d.o.o, Šempeter pri Gorici, 2001, 100 str.
17. Jackson Peter: Introduction to expert systems. Harlow: Addison-Wesley, 1999.
18. Jerman Blažič Borka: Elektronsko poslovanje na internetu. Ljubljana: GV Založba, 2001. 206 str.
19. Jerman Blažič Borka: Internet. Ljubljana: Novi Forum, 1996. 87 str.
20. Kintsch Walter: Metaphor comprehension: A computational Theory; University of Colorado, 2000, [URL:<http://lsa.colorado.edu/papers/metaphor.kintsch.pdf>], 20.01.2003.
21. Kobayashi Mei, Takeda Koichi: Information Retrieval on the Web, IBM Research, Tokyo Research Laboratory, 2000,
22. Kokol Peter: Inteligentni sistemi. Maribor: Fakulteta za elektrotehniko, 2001.
23. Kovačič Andrej, Vintar Mirko: Načrtovanje in gradnja informacijskih sistemov. Ljubljana: DZS, 1994. 316 str.

24. Kovačič Andrej: Informatizacija poslovanja, Ljubljana: Ekonomska fakulteta, 1998. 214 str.
25. Lacoste Gerard et al.: SEMPER – Secure electronic marketplace for Europe. Springer-Verlag, Berlin Heidelberg, 2000. 350 str.
26. Landauer Thomas K. et. all.: A Solition to Plato's Problem: The Latent Semantic Analysis Theory of Acquisition, Induction and Representation of Knowledge; University of Colorado, [URL: <http://lsa.colorado.edu>], 27.12.2002.
27. Landauer Thomas K. et. all.: How Well Can Meaning be Derived without Using Word Order? A Comparison of Latent Semantic Analysis and Humans; University of Colorado, [URL: <http://lsa.colorado.edu>], 27.12.2002.
28. Landauer Thomas K.: The computational basis of learning; University of Colorado, [URL: <http://lsa.colorado.edu>], 27.12.2002.
29. Levinson Jay Conrad, Rubin Charles: Gverilski marketing na internet-u. Maribor: ROTIS, 1996. 280 str.
30. Masand Brij at al.: Web Usage Analysis and User Profiling. Springer-Verlag, Berlin Heidelberg, 2000. 182 str.
31. Moniz Joseph: Enterprise Applicatiopn Architecture. Birmingham: Wrox Press Ltd, 1999. 787 str.
32. Moustafa A. Youssef: Cross Language Information Retrieval; University of Maryland College Park, April 2001, [URL: <http://www.otal.umd.edu/uupractice/clir/>], 11.12.2002.
33. Možina Stane et. al.: Management. Radovljica: Didakta, 1994.
34. Pfaffenberger Bryan: Protect your privacy on the Internet. New York: J. Wiley & Sons, 1997. 326 str.
35. Rector Brent, Sells Chris: ATL Internals. Massachusetts: Addison Wesley, 1999. 635 str.
36. Rich E.: Users are individuals: individualizing user models. International Journal of Man-Machine Studies 1983, str:199 do 214.
37. Rijsbergen C.J.: Information Retrieval, London: Butterworths, 1979,
38. Schneier Bruce: Secrets and lies. New York: J. Wiley & Sons, 2000. 412 str.
39. Starnes Jane K., Graves John, Justice Jacqueline: The complete Intranet Source for Information Professionals. Washington: Special Libraries Association, 1997.
40. Sterne Jim: Customer Service on the Internet. New York: John Wiley & Sons, Inc; 2000. 351 str.
41. Šuler Aleš: Visual Basic 5.0/6.0-Zvijače in nasveti. Nova Gorica: Flamingo, 2000. 129 str.
42. Taylor Donald H., Glezen G. William: REVIDIRANJE zasnove in postopki. Ljubljana: Slovenski inštitut za revizijo, 1996.
43. Toms Elaine G.: Serendipitous Information Retrieval; University of Toronto, Canada, [URL: http://www.ercim.org/publication/ws-proceedings/DelNoe01/3_Toms.pdf], 11.12.2002.
44. Toplišek Janez: Elektronsko poslovanje. Ljubljana: Atlantis, 1998.
45. Turney P.: Extraction of Keyphrases from Text: Evaluation of Four Algorithms; National Research Council Canada, 1997, [URL: <http://arxiv.org/list/cs.IR/recent>], 11.12.2002.
46. Turney P.: Learning to Extract Keyphrases from Text; National Research Council Canada, 1999, [URL: <http://arxiv.org/list/cs.IR/recent>], 11.12.2002.

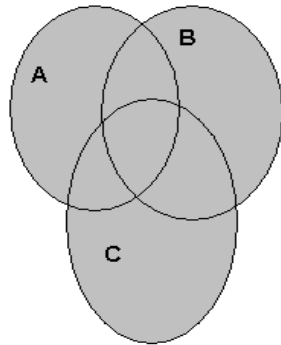
47. Turney P.: Mining the Web for Lexical Knowledge to Improve Keyphrases Extraction: Learning from Labeled and Unlabeled Data; National Research Council Canada, 2002, [URL: <http://arxiv.org/list/cs.IR/recent>], 11.12.2002.
48. Vacca John R.: Internet security secrets. Forster City: IDG Books, 1996. 758 str.
49. Zerdick Axel at all: E-CONOMICS Strategies for the Digital Marketplace. Berlin: Springer-Verlog, 2000. 330 str.

Viri

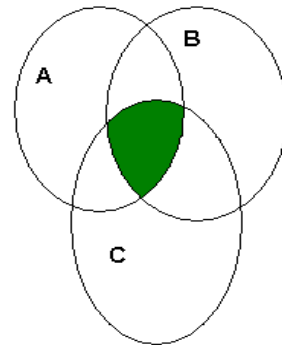
1. Bilten KDD, Centralna klirinško depotna družba d.d. Ljubljana, 1998.
2. Burian Saša at.al.: Interna dokumentacija CRVP, KDD d.d. Ljubljana.
3. Cimetiere Jean-Christophe, ASPs: Leading Us Into the Third Generation of IT, [URL: http://www.intranetjournal.com/articles/200003/asp_03_24_00.html], 18.3.2003.
4. Digital Libraries – Information Retrieval; [URL: <http://ei.cs.vt.edu/~cs5604/DL/DL6.html>], 12.11.2002.
5. ISO 9000 International standard, Geneva, Switzerland, 2000.
6. ISO 9001 International standard, Geneva, Switzerland, 2000.
7. ISO 9001 Slovenski standard; Sistem vodenja kakovosti, Urad Republike Slovenije za standardizacijo in meroslovje, december 2000.
8. IXTLAN, Portal [URL: <http://www.ixtlan-team.si/novice/prispevki/portal>], 13.11.2002.
9. Microsoft: Security Operations Guide for Windows 2000 Server, Prescriptive Guidance, Microsoft, 2002, 192 str.
10. Plavšak Nina: Pravni okviri informacijskega sistema centralnega registra nematerializiranih vrednostnih papirjev, KDD d.d., Ljubljana, 1999.
11. Portal [URL: <http://www.ixtlan-team.si/novice/prispevki/portal>], 13.11.2002.
12. Pravila poslovanja KDD - Centralne klirinško depotne družbe, KDD d.d., Ljubljana, 2001.
13. Pravilnik o poslovni skrivnosti in zaščiti podatkov, dokumentov in opreme v KDD d.d., Ljubljana.
14. STOCONA, The information technology of the intelligent information retrieval system; [URL: <http://eng.stocona.ru/technology/informationRetrieval/>], 11.12.2002
15. Wainwright Phil: The ASP Value Chain; 2001; [URL: http://www.aspnews.com/strategies/asp_basics/article/0,2350,4521_584731,00.html].

Priloge

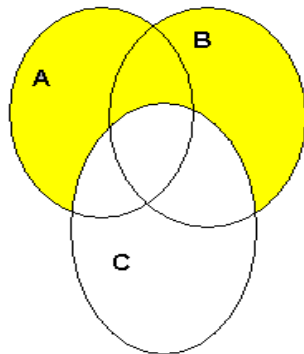
Priloga 1: Primeri iskanja z Boolejevo metodo



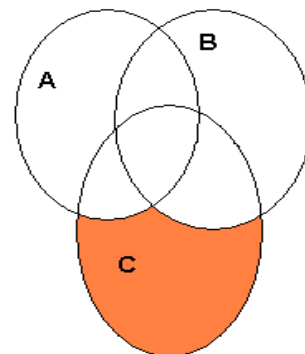
Dokumenti, ki vsebujejo besedo A, B, C



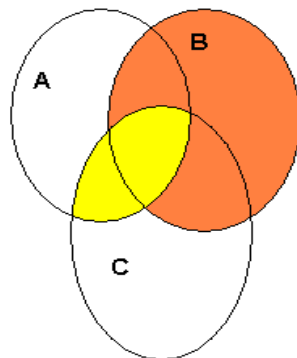
Dokumenti, ki vsebujejo besedo A in B in C



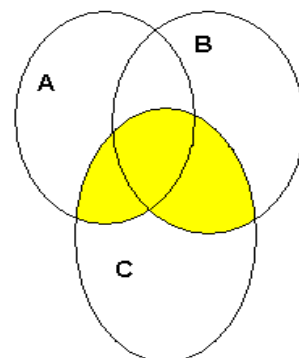
Dokumenti vsebujejo besedo A, B ne C



Dokumenti vsebujejo besedo C ne A ne B



Primer iskanja: A in C ali B



Peimer iskanja: A ali B in C

Priloga 2: Primer uporabe LSA

Podatki za izdelavo primera so vzeti iz članka [6], kjer so avtorji opisali primer z dvanajstimi besedami v naslovih devetih dokumentov. Dokumenti so razvrščeni v dva razreda. Razred »c« je povezan z računalništvom, drugi označen z »m« pa z diagrami.

Naslovi:

c1: **Human** machine **interface** for Lab ABC **computer** applications

c2: A **survey** of **user** opinion of **computer system response time**

c3: The **EPS user interface** management **system**

c4: **System** and **human system** engineering testing of **EPS**

c5: Relation of **user**-perceived **response time** to error measurement

m1: The generation of random, binary, unordered **trees**

m2: The intersection **graph** of paths in **trees**

m3: **Graph minors** IV: Widths of **trees** and well-quasi-ordering

m4: **Graph minors**: A **survey**

Tabela 1: Matrika **X** - besede po dokumentih (Vir: Deerwester)

| | D | O | K | U | M | E | N | T | I |
|---------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| Besede | c1 | c2 | c3 | c4 | c5 | m1 | m2 | m3 | m4 |
| Human | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| Interface | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| computer | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| User | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| System | 0 | 1 | 1 | 2 | 0 | 0 | 0 | 0 | 0 |
| response | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| Time | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| EPS | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| Survey | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Trees | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| Graph | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Minors | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

V tabeli 1 je prikazano kolikokrat se posamezna beseda (v tekstu izpisana ojačeno) pojavi v naslovu najmanj dveh dokumentov. Besede, ki se pojavijo le enkrat (samo v enem naslovu) v tabeli niso zajete. To v neki meri vpliva na vektorski prostor in s tem na utežene vrednosti besed, vendar se tako zmanjša računanje.

Tabela 2 prikazuje kolikokrat se posamezna beseda pojavlja v naslovu v kombinaciji z ostalimi besedami.

Tabela 2: Matrika besed

| | Human | Interface | computer | user | system | response | time | EPS | Survey | trees | graph | minors |
|-----------|-------|-----------|----------|------|--------|----------|------|-----|--------|-------|-------|--------|
| Human | X | 1 | 1 | 0 | 2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| Interface | 1 | X | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| Computer | 1 | 1 | X | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| User | 0 | 1 | 1 | X | 2 | 2 | 2 | 1 | 1 | 0 | 0 | 0 |
| System | 2 | 1 | 1 | 2 | X | 1 | 1 | 3 | 1 | 0 | 0 | 0 |
| Response | 0 | 0 | 1 | 2 | 1 | X | 2 | 0 | 1 | 0 | 0 | 0 |
| Time | 0 | 0 | 1 | 2 | 1 | 2 | X | 0 | 1 | 0 | 0 | 0 |
| EPS | 1 | 1 | 0 | 1 | 3 | 0 | 0 | X | 0 | 0 | 0 | 0 |
| Survey | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | X | 0 | 1 | 1 |
| Trees | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | X | 2 | 1 |
| Graph | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | X | 2 |
| Minors | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | X |

Primerjava dokumentov

Učinkovitost LSI (Latent Semantic Indexing) je odvisna od sposobnosti SVD za izločitev značilnosti iz pogostosti pojavljanja besed v zbirki dokumentov. V originalnem vektorskem prostoru so dokumenti predstavljeni v $X^T X$, simetrični matriki $d \times d$, kot skupni produkt vektorja vseh dokumentov predstavljenih z vektorjem frekvence besed. Vsaka kolona matrike $X^T X$ predstavlja torej skupni produkt vektorja dokumentov ustrezne kolone matrike X in dokumenta v zbirki. Vrednost kosinusa pomeni stopnjo podobnosti dokumentov i in j in je izražena kot:

$$\frac{(X^T X)_{(i,j)}}{\sqrt{(X^T X)_{(i,i)} \cdot (X^T X)_{(j,j)}}$$

Pravokotna matrika, kot je v našem primeru matrika $t \times d$ (besede in dokumenti), je razčlenjena kot produkt treh matrik:

$$X = T_0 S_0 D_0$$

T_0 – 9 dimenzij posameznih vektorjev za 12 besed

S_0 – diagonalna matrika 9 posameznih vrednosti

D_0 – 9 dimenzij posameznih vektorjev za 9 dokumentov

Tabela 3: Matrika $T_0 =$

| | | | | | | | | |
|------|-------|-------|-------|-------|-------|-------|-------|-------|
| 0.22 | -0.11 | 0.29 | -0.41 | -0.11 | -0.34 | 0.52 | -0.06 | -0.41 |
| 0.20 | -0.07 | 0.14 | -0.55 | 0.28 | 0.50 | -0.07 | -0.01 | -0.11 |
| 0.24 | 0.04 | -0.16 | -0.59 | -0.11 | -0.25 | -0.30 | 0.06 | 0.49 |
| 0.40 | 0.06 | -0.34 | 0.10 | 0.33 | 0.38 | 0.00 | 0.00 | 0.01 |
| 0.64 | -0.17 | 0.36 | 0.33 | -0.16 | -0.21 | -0.17 | 0.03 | 0.27 |
| 0.27 | 0.11 | -0.43 | 0.07 | 0.08 | -0.17 | 0.28 | -0.02 | -0.05 |
| 0.27 | 0.11 | -0.43 | 0.07 | 0.08 | -0.17 | 0.28 | -0.02 | -0.05 |
| 0.30 | -0.14 | 0.33 | 0.19 | 0.11 | 0.27 | 0.03 | -0.02 | -0.17 |
| 0.21 | 0.27 | -0.18 | -0.03 | -0.54 | 0.08 | -0.47 | -0.04 | -0.58 |
| 0.01 | 0.49 | 0.23 | 0.03 | 0.59 | -0.39 | -0.29 | 0.25 | -0.23 |
| 0.04 | 0.62 | 0.22 | 0.00 | -0.07 | 0.11 | 0.16 | -0.68 | 0.23 |
| 0.03 | 0.45 | 0.14 | -0.01 | -0.30 | 0.28 | 0.34 | 0.68 | 0.18 |

Tabela 4: Matrika $S_0 =$

| | | | | | | | | |
|------|------|------|------|------|------|------|------|------|
| 3.34 | | | | | | | | |
| | 2.54 | | | | | | | |
| | | 2.35 | | | | | | |
| | | | 1.64 | | | | | |
| | | | | 1.50 | | | | |
| | | | | | 1.31 | | | |
| | | | | | | 0.85 | | |
| | | | | | | | 0.56 | |
| | | | | | | | | 0.36 |

Tabela 5: Matrika $D_0 =$

| | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|------|-------|
| 0.20 | 0.61 | 0.46 | 0.54 | 0.28 | 0.00 | 0.01 | 0.02 | 0.08 |
| -0.06 | 0.17 | -0.13 | -0.23 | 0.11 | 0.19 | 0.44 | 0.62 | 0.53 |
| 0.11 | -0.50 | 0.21 | 0.57 | -0.51 | 0.10 | 0.19 | 0.25 | 0.08 |
| -0.95 | -0.03 | 0.04 | 0.27 | 0.15 | 0.02 | 0.02 | 0.01 | -0.03 |
| 0.05 | -0.21 | 0.38 | -0.21 | 0.33 | 0.39 | 0.35 | 0.15 | -0.60 |
| -0.08 | -0.26 | 0.72 | -0.37 | 0.03 | -0.30 | -0.21 | 0.00 | 0.36 |
| 0.18 | -0.43 | -0.24 | 0.26 | 0.67 | -0.34 | -0.15 | 0.25 | 0.04 |
| -0.01 | 0.05 | 0.01 | -0.02 | -0.06 | 0.45 | -0.76 | 0.45 | -0.07 |
| -0.06 | 0.24 | 0.02 | -0.08 | -0.26 | -0.62 | 0.02 | 0.52 | -0.45 |

$$X = T_0 S_0 D_0$$

S tem, ko obdržimo le prvi dve koloni matrike T_0 in prvi dve vrstici matrike D_0 dobimo približno vrednost $X_S = T S D$

Tabela 6: Matrika T, S in D

| T | S | D |
|----------|----------|----------|
| 0,22 | -0,11 | 3,14 |
| 0,20 | -0,07 | 2,54 |
| 0,24 | 0,04 | |
| 0,40 | 0,06 | |
| 0,64 | -0,17 | |
| 0,27 | 0,11 | |
| 0,27 | 0,11 | |
| 0,30 | -0,14 | |
| 0,21 | 0,27 | |
| 0,01 | 0,49 | |
| 0,04 | 0,62 | |
| 0,03 | 0,45 | |

Po množenju dobimo matriko X_S , ki sicer ni popolnoma enaka matriki X.

Tabela 7: Matrika X_S

| | D | O | K | U | M | E | N | T | I |
|---------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| Besede | c1 | c2 | c3 | c4 | c5 | m1 | m2 | m3 | m4 |
| Human | 0,16 | 0,40 | 0,38 | 0,47 | 0,18 | -0,05 | -0,12 | -0,16 | -0,09 |
| Interface | 0,14 | 0,37 | 0,33 | 0,40 | 0,16 | -0,03 | -0,07 | -0,10 | -0,04 |
| computer | 0,15 | 0,51 | 0,36 | 0,41 | 0,24 | 0,02 | 0,06 | 0,09 | 0,12 |
| User | 0,26 | 0,84 | 0,61 | 0,70 | 0,39 | 0,03 | 0,08 | 0,12 | 0,19 |
| System | 0,45 | 1,23 | 1,05 | 1,27 | 0,56 | -0,07 | -0,15 | -0,21 | -0,05 |
| response | 0,16 | 0,58 | 0,38 | 0,42 | 0,28 | 0,06 | 0,13 | 0,19 | 0,22 |
| Time | 0,16 | 0,58 | 0,38 | 0,42 | 0,28 | 0,06 | 0,13 | 0,19 | 0,22 |
| EPS | 0,22 | 0,55 | 0,51 | 0,63 | 0,24 | -0,07 | -0,14 | -0,20 | -0,11 |
| Survey | 0,10 | 0,53 | 0,23 | 0,21 | 0,27 | 0,14 | 0,31 | 0,44 | 0,42 |
| Trees | -0,06 | 0,23 | -0,14 | -0,27 | 0,14 | 0,24 | 0,55 | 0,77 | 0,66 |
| Graph | -0,06 | 0,34 | -0,15 | -0,30 | 0,20 | 0,31 | 0,69 | 0,98 | 0,85 |
| Minors | -0,04 | 0,25 | -0,10 | -0,21 | 0,15 | 0,22 | 0,50 | 0,71 | 0,62 |

Izračunane medsebojnih korelacij med posameznimi naslovi s popolno matriko (glej tab. 8) in po rekonstrukciji (glej tab. 9), ko obdržimo le dve vrstici ($X_S = T S D$), pokaže kako LSA vpliva na spremembo predstavitve korelacij. Rezultati prikazani v tabeli 9 pokažejo pričakovane rezultate.

Tabela 8: Korelacija med naslovi v večdimenzionalnem prostoru (matrika X).

| | c1 | c2 | c3 | c4 | c5 | m1 | M2 | m3 |
|----|-------|-------|-------|-------|-------|-------|-------|-------|
| C2 | -0,19 | | | | | | | |
| C3 | 0,00 | 0,00 | | | | | | |
| C4 | 0,00 | 0,00 | 0,47 | | | | | |
| C5 | -0,33 | 0,58 | 0,00 | -0,31 | | | | |
| M1 | -0,17 | -0,30 | -0,21 | -0,16 | -0,17 | | | |
| M2 | -0,26 | -0,45 | -0,32 | -0,24 | -0,26 | 0,67 | | |
| M3 | -0,33 | -0,58 | -0,41 | -0,31 | -0,33 | 0,52 | 0,77 | |
| M4 | -0,33 | -0,19 | -0,41 | -0,31 | -0,33 | -0,17 | -0,26 | -0,56 |

Tabela 9: Korelacija med naslovi v dvodimenzionalnem prostoru (matrika X_S)

| | c1 | c2 | c3 | c4 | c5 | m1 | m2 | m3 |
|----|-------|-------|-------|-------|-------|------|------|------|
| C2 | -0,91 | | | | | | | |
| C3 | 1,00 | 0,91 | | | | | | |
| C4 | 1,00 | 0,88 | 1,00 | | | | | |
| C5 | 0,85 | 0,99 | 0,85 | 0,81 | | | | |
| M1 | -0,85 | -0,56 | -0,85 | -0,88 | -0,45 | | | |
| M2 | -0,85 | -0,56 | -0,85 | -0,88 | -0,44 | 1,00 | | |
| M3 | -0,85 | -0,56 | -0,85 | -0,88 | -0,44 | 1,00 | 1,00 | |
| M4 | -0,81 | -0,50 | -0,81 | -0,84 | -0,37 | 1,00 | 1,00 | 1,00 |

Priloga 3: Pomen kratic

| | |
|---------|--|
| ACEs | Access Control Entries |
| ACL | Access Control List |
| AD | Active Directory |
| ADO | ActiveX Data Objects |
| ADSI | Active Directory Services Interface |
| AIA | Authority Information Access |
| ASP | Active Server Pages |
| ASP | Application Service Provider |
| B2B | Business-To- Business |
| B2C | Business-To- Customers |
| B2E | Business-To-Employee |
| BSA | Business Software Alliance |
| CA | Certificate Authority |
| CDP | CRL Distribution Points |
| CGI | Common Geteway Interface (standard, ki omogoča komunikacijo WEB strežnika z exsternimi programi) |
| COM | Component Object Model |
| CORBA | Common Object Request Broker Architecture |
| CPS | Certificate Practice Statement (Opis postopka delovanja) |
| CRL | Certificate Revocation Lists (Lista preklicanih certifikatov) |
| CSP | Criptographic Service Providers |
| DACL | Discretionary Access Control List |
| DBMS | Database Management Systems |
| DCOM | Distributed Component Object Model |
| DNA | Distributed interNET Arhitecture |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| DST | Digital Signature Trust Company |
| ECDSA | Eliptic Curve Digital Signature algorithm |
| EFS | Encrypting File System |
| EJB | Enterprise JavaBean |
| GDI | Graphics Device Interface (Grafični vmesnik) |
| HAL | Hardware Abstraction Layer (Sloj povezovanja strojne opreme) |
| HSM | Hardware Security Module |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICE-CAR | Interworking Public Key Certification on Infrastructure for Commerce, Administration and Research. |
| ICE-TEL | Interworking Public Key Certification on Infrastructure for Europe. |
| ISAM | Index-Sequential Access Method |
| ISAPI | Internet Server Application Program Interface |
| ISDN | Integrated Services Digital Network |
| ISO | International Standardization Organization |
| ISP | Internet Service Provider (Posrednik internet storitev) |
| KDC | Key Distribution Center |

| | |
|--------|---|
| LDAP | Local Directory Access Protocol |
| LPC | Local Procedure Call Facility (Lokalni postopki klicnih pripomočkov) |
| LRAs | Local registration authorities |
| MAC | Message Authentication Code (Mehanizem za zagotovitev neokrnjenih podatkov) |
| MD5 | (Enosmerna zgoščevalna funkcija) |
| MIME | Metoda prenosa podatkov |
| MS DTC | Microsoft Distributed Transaction Coordinator |
| MSMQ | Microsoft Message Queues |
| MTS | Microsoft Transaction Server |
| NIST | National Institute of Standards and Technology (Ameriški urad za standardizacijo) |
| OCLC | Online Computer Library Centre, Inc. |
| ODBC | Open Database Connectivity (Microsoft 1991) |
| OLAP | On-Line Analytical Processing |
| OLE DB | Object Linking and Embedding Data Base |
| OLE | Object Linking and Embedding |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| POP | Post Office Protocol |
| PSTN | Public Switched Telephone Network |
| RAID | Redundant Arrays of Inexpensive Disks |
| RDF | Resource Description Framework (Kodna shema metapodatkov za spletne dokumente) |
| RMI | Remote Method Invocation |
| ROI | Return of Investment |
| RSA | algoritma za javni ključ imenovan po avtorjih Rivest, Shamir in Adleman |
| SET | Secure Electronic Transaction (Protokol za varne elektronske transakcije) |
| SGC | Server Gated Cryptography |
| SGML | Standard Generalized Markup Language |
| SMTP | Simple Mail Transfer Protocol |
| SQL | Structured Query Language |
| SSL | Secure Socket Layer (Protokol za zaščito prenosa podatkov v spletu) |
| SVD | Singular Value Decomposition (Razčlemba posameznih vrednosti) |
| TCP/IP | Transmission Control Protocol/ Internet Protokol |
| TSL | Transport Layer Security |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator (Naslov vira v enotni obliki) |
| URN | Uniform Resource Names (enotna oblika nazivov) |
| VDM | Virtual DOS Machine (Navidezni stroj za izvajanje DOS aplikacij) |
| VMM | Virtual Memory Manager (Upravitelj navideznega pomnilnika) |
| VPN | Virtual private network (Navidezno privatno omrežje) |
| WMI | Windows Management and Instrumentation |
| WML | Wireless Markup Language |
| WOW | Windows on Windows (Okno v oknu, ko se izvaja WIN16 podsistem v okolju Windows NT, 2000 ali XP) |
| WSH | Windows Script Host |
| XML | Extensible Mark-up Language |

Priloga 4: Razlaga nekaterih kratic

ADSI Aktivni imenik je hierarhično urejen seznam predmetov v omrežju. Predmeti so shranjeni skupaj s svojimi lastnostmi, kar omogoča tudi iskanje predmetov po izbranih lastnostih. Taka funkcionalnost seveda ni sama sebi namen, ampak omogoča učinkovitejše delo uporabnikov in s tem dobro osnovo za postavitve "digitalnega živčnega sistema". Koncept digitalnega živčnega sistema podjetjem v hitro se razvijajočem in spreminjajočem poslovnem okolju omogoča konkurenčno prednost, ker je njihova infrastruktura zasnovana tako, da je učinkovita kljub nenehnemu spreminjanju poslovnih razmer. Čeprav se digitalni živčni sistem odziva in prilagaja spremembam, pa je treba imeti jasno vizijo, kaj želimo s postavitvijo infrastrukture doseči. Vizija je usmeritev, ki nam pomaga pri sprejemanju odločitev, da nas bodo te pripeljale v zeleno smer. Če se spremeni vizija, je običajno treba spremeniti tudi infrastrukturo.

BizTalk je nov pojem v poslovnem svetu, ki predstavlja poenotenje komunikacije na podlagi jezika XML med različnimi subjekti poslovanja, kot nadgradnja in razširitev dosedanjega sistema EDI/RIP - računalniške izmenjave podatkov. Spletne strani BizTalk.org so iniciativa podjetja Microsoft v želji, da se podjetja medsebojno dogovorijo in uskladijo standarde za izmenjavo podatkov. Kot pomoč pri tem Microsoft ponuja tudi izdelek BizTalk Enterprise Server, ki poenostavlja elektronsko komunikacijo med podjetji. Več o BizTalk.org na <http://www.biztalk.org> in <http://www.microsoft.com/biztalk/>.

DACL je varnostna kontrolna lista dostopov (**ACL**), ki omogoča varnostno zaščito določenemu objektu, lastnostim objekta ali posamezni lastnosti objekta. Vsaka aktivna mapa (Active Directory) objekta v Windows 2000 ima dve povezani listi dostopov: neomejena kontrolna lista dostopov (DACL), ki vsebuje spisek uporabnikov, skupin uporabnikov in imen računalnikov, ki se jim dovoljuje ali prepoveduje dostop do objekta. Kontrolna lista dostopov vsebuje spisek entitet (SID) s pravicami kot so pravica do branja, pisanje ali vse pravice (ACE). Kontrolna lista dostopov do sistema (SACL) definira kateri dogodki (kot so dostopi do podatkov) se bodo beležili za uporabnika ali skupino uporabnikov.

DCOM je kratica za model porazdeljenih objektnih komponent (ang. Distributed Component Model), ki sodi med pomembne proizvode Windows DNA. Model opisuje aplikacije, ki delujejo na več računalnikih istočasno. COM se uporablja za izvajanje aplikacije na enem računalniku, DCOM pa lahko komunicira preko različnih transportnih protokolov (TCP/IP, IPX/SPX, HTTP, ...) z računalniki na katerih tečejo različni operacijski sistemi (WindowsNT, Windows2000, Unix, Sun Solaris, ...). Podpira aplikacije, ki so napisane v različnih programskih jezikih kot so VB, C++, COBOL in drugi.

EFS je novi vmesnik v Windows 2000, ki ščiti občutljive podatke v datotekah shranjenih na diskih, ki so formatirani po načinu NTFS. EFS uporablja simetrični ključ za kriptiranje v povezavi z javnim ključem za zagotavljanje zaupnosti podatkov v datotekah.

HAL zagotavlja skupno programsko podporo strojnih enot kot so sistemska ura, nadzor pomnilnika, funkcije istočasnega izvajanja več opravil in sistemskih vodil.

JDBC pomeni enako kot ODBC, le da operacija poteka v Java okolju.

KDC je mrežni servis, ki oskrbuje sejo z začasnimi »vozovnicami« in ključi v avtentikacijskem protokolu Kerberos. V Windows 2000 teče KDC kot privilegiran proces na vseh domenskih kontrolerjih. KDC uporablja AD za upravljanje z občutljivimi prijavnimi informacijami kot je uporabniško ime in geslo.

LDAP je protokol za servisiranje map, ki deluje pod TCP/IP. To je osnovni protokol uporabljen za dodajanje, spreminjanje in brisanje informacij shranjenih v aktivnih mapah (AD) ali poizvedovanje po podatkih AD. Klienci in LDAP združljive aplikacije za delo z AD morajo uporabljati LDAP, če želijo pridobiti podatke in delati s podatki iz AD. Z pravimi pooblastili lahko uporabimo katerokoli LDAP združljivo aplikacijo za poizvedovanje, urejanje, dodajanje, spreminjanje ali brisanje informacij v AD.

MIME je običajna metoda za prenos podatkov, ki nimajo teksta po elektronski pošti. MIME zakodira netekstovne podatke kot ASCII tekst in potem dekodira nazaj v originalni format, ko je prenos zaključen. S/MIME je razširjen MIME, ki podpira varno elektronsko pošto, ki vključuje kriptiran prenos, pošiljateljev elektronski podpis in integriteto podatkov.

MS DTC Microsoft Distributed Transaction Coordinator je integriran v SQL strežnik in je vitalnega pomena za MTS. Poleg drugih funkcij v procesiranju transakcij le te preverja ali so pravilni in pripravljene za izvedbo.

ODBC je vmesnik med aplikacijo in podatkovno bazo, ki bazira na SQL standardu in predstavlja naslednje komponente: aplikacijo, podatkovno bazo, gonilnike za podatkovno bazo, gonilniki upravljanja (driver managers) za različne baze (Oracle, SQL Server, DB2, itd).

OLE DB je nabor ActiveX vmesnikov podjetja Microsoft, kateri lahko dostopajo do podatkov in je zamenjava za starejši gonilnik ODBC.

SGC (Server Gated Cryptography) je nadgradnja SSL protokola s 128 bitno kriptografijo. Zagotavlja varno izmenjavo podatkov med dvema strankama povezanima z TCP/IP, ki so čitljive samo njima in se brez njune vednosti ne morejo spremeniti.

SGML Standardiziran splošni opisni jezik. Uporablja se za elektronsko oblikovanje in prenos obsežnih podatkov, kot so tehnična dokumentacija za proizvodnjo letal in ladij. Podatki so označeni z opisi (zaznamki), ki predstavljajo strukturo znotraj dokumenta in so med seboj povezani. Opis definira posamezne dele dokumenta, njihovo strukturo in logične povezave. To omogoča hitro iskanje po vseh dokumentih.

SQL je jezik za izdelavo poizvedb, katerega začetki segajo v leto 1970. Kasneje ga je razvil IBM za upravljanje relacijskih baz. Zardi preproste sintakse se uporablja tudi danes v kombinaciji z drugimi jeziki kot so Cobol, C, C++, Visual Basic ali Java. Struktura SQL-a kjer so zahteve po izvedbah shranjene kot podatki in ne kot program, ki je naložen v pomnilniku, so združljive z HTTP, ki je (stateless) protokol brez običajnih programskih ukazov. Večina današnjih podatkovnih baz je osnovana na relacijskih modelih, ki za upravljanje uporabljajo SQL kot primarni jezik. Zaradi te standardizacije je možno povezovati podatkovne baze različnih proizvajalcev v standardno arhitekturo in oblikovanje, ki jo uporabljajo aplikacijski strežniki.

SSL je odprt standard, ki ga je razvil Netscape Communications za vzpostavitev varnega komunikacijskega kanala pri izmenjavi zaupnih informacij, kot so na primer številke kreditnih kartic. Razvit je bil za izmenjavo elektronskih finančnih transakcij na spletu, vendar dobro deluje tudi na drugih servisih na internetu.

TLS je standardni protokol uporabljen za zagotavljanje varne spletne komunikacije na Internetu in Intranetu. Omogoča overjanje strežnikov in klientu zagotavlja varen kanal zaupnih podatkov s kriptiranjem.

URI je nabor znakov, ki se uporablja za identifikacijo pripomočkov (kot na primer datoteke) kjerkoli na Internetu. URI vključuje enotna imena pripomočkov (URN) in nespremenljiva imena nahajališč (URL).

WML jezik za označevanje pri brezžičnih komunikacijah

XML je kratica za samoopisni jezik. Za razliko od jezika HTML, kjer so vsebina in podatki za prikaz le-te med seboj združeni, XML poenostavlja izmenjavo podatkov med različnimi računalniškimi sistemi in omogoča jasno ločitev vsebine od prikaza. Jezik je razširljiv, prav tako pa so razširljive tudi sheme, ki temeljijo na tem jeziku. XML podpira več organizacij, med večjimi tudi Microsoft, IBM in Oracle. Več o jeziku XML na <http://www.w3.org/XML/>.