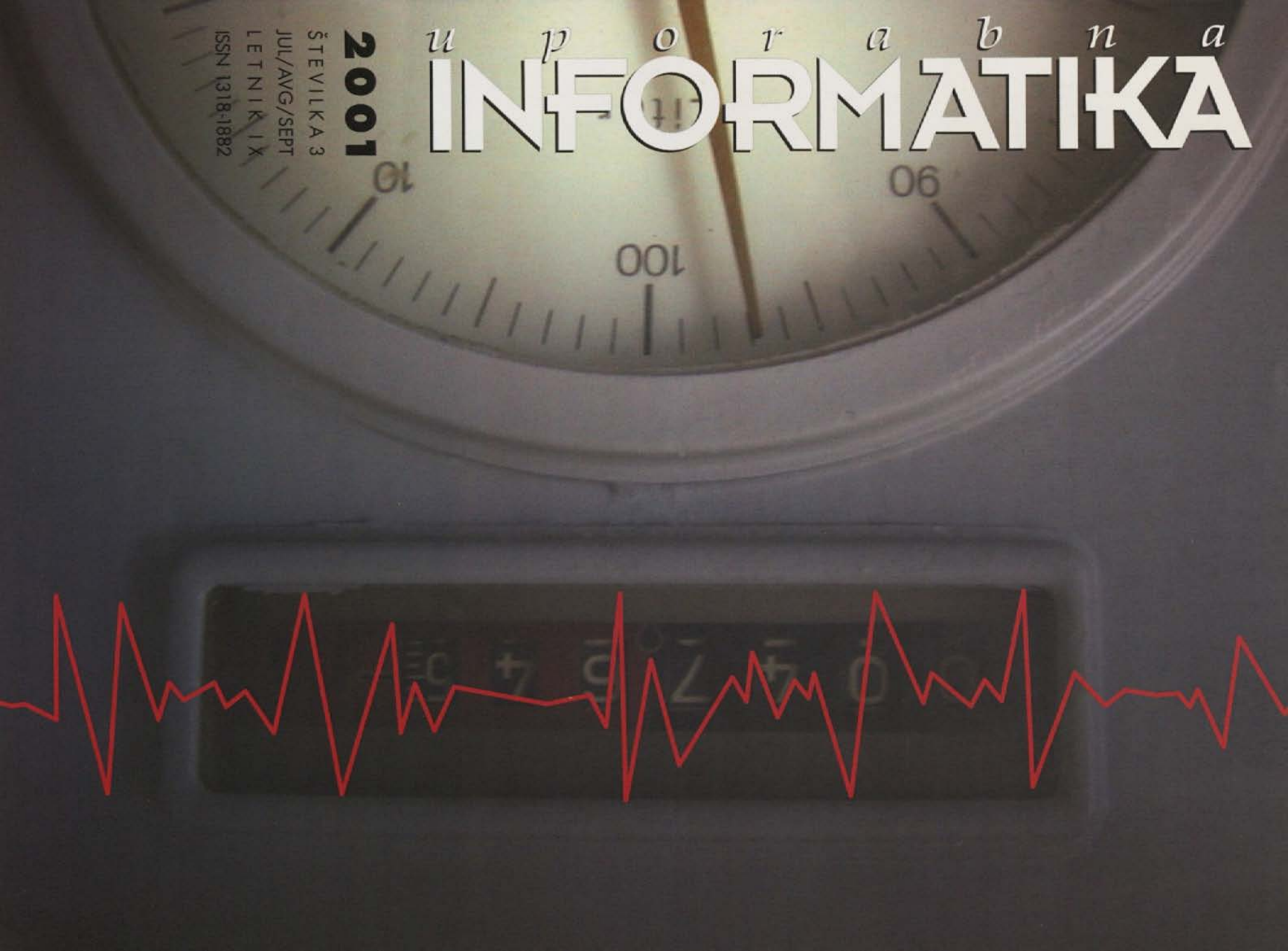


uporabna INFORMATIKA

2001
ŠTEVILKA 3
JUL/AVG/SEPT
LETNIK IX
ISSN 1318-1882

DONATORJI

ASTER

Nade Ovčakove 1, 1000 Ljubljana
Tel.: +386 01 589 42 00

gambit trade
računalništvo in informatika d.o.o.

Savska c. 3a, 1000 Ljubljana
Tel.: 01 437 63 33

nashuatec
Laserski tiskalniki in večnamenski stroji
ViboR

Brnčičeva 11b, 1231 Ljubljana
tel.: 01 561 33 21, faks: 01 561 12 54
domača stran: www.vibor.si
e pošta: info@vibor.si

MAOP®
Vaš partner v informatiki
MAOP RAČUNALNIŠKI INŽENIRING D.O.O., WWW.MAOP.SI

MARAND
Napredna računalniška hiša

Cesta v Mestni log 55, 1000 Ljubljana
Tel.: 01 283 33 77

www.menea.si
menea
d.o.o., internet trgovski center

Microsoft®

REPRO LJUBLJANA MS

rrc
RRC Računalniške storitve d.d.

Jadranska 21, Ljubljana
Tel.: 01 / 4778 500, Faks: 01 / 4255 229
www.rrc.si, info@rrc.si

SIQ ISO 9001 Q-231

SIEMENS

Dunajska 22, 1511 Ljubljana, Slovenija

SMART COM d.o.o.

Brnčičeva 45, 1001 Ljubljana, Slovenija
tel: + 386 01 56 11 606

SRC.SI

Tržaška cesta 116, 1000 Ljubljana
Tel.: 01 242 80 00 • Fax: 01 423 41 73
e-mail: src@src.si • http://www.src.si

vsebina

Zahvaljujemo se podjetju Marand d.o.o., Ljubljana, Cesta v mestni log 55,
za sponzoriranje domače strani Slovenskega društva INFORMATIKA

Navodila avtorjem

Revija Uporabna informatika objavlja originalne prispevke domačih in tujih avtorjev na znanstveni, strokovni in informativni ravni. Namenjena je najširši strokovni javnosti, zato je zaželeno, da so tudi znanstveni prispevki napisani čim bolj mogoče poljudno.

Članke objavljamo v slovenskem jeziku, prispevke tujih avtorjev pa tudi v angleškem jeziku.

Vsak članek za rubriko Strokovne razprave mora za objavo prejeti dve pozitivni recenziji.

Prispevki naj bodo lektorirani, v uredništvu opravljamo samo korekturo. Po presoji se bomo posvetovali z avtorjem in članek tudi lektorirali.

Polno ime avtorja naj sledi naslovu prispevka. Imenu dodajte naslov organizacije in avtorjev elektronski naslov. Prispevki za rubriko Strokovne razprave naj imajo dolžino cca 30.000 znakov, prispevki za rubrike Rešitve, Poročila, Obvestila itd. pa so lahko krajši.

Članek naj ima v začetku izvleček v slovenskem jeziku in Abstract v angleškem jeziku. Izvleček naj v 8 do 10 vrsticah opiše vsebino prispevka, dosežene rezultate raziskave.

Abstract naj se začenja s prevodom naslova v angleščino.

Pišite v razmaku ene vrstice, brez posebnih ali poudarjenih črk, za ločilom na koncu stavka napravite samo en prazen prostor, ne uporabljajte zamika pri odstavkih.

Revijo tiskamo v črno beli tehniki s folije, zato barvne slike ali fotografije kot originali niso primerne. Objavljali tudi ne bomo slik zaslonov, razen če so nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme itd. naj imajo belo podlago. Po možnosti jih pošiljajte posebej, ne v okviru članka.

Na koncu članka navedite literaturo, ki ste jo uporabili za prispevek, po naslednjem vzorcu:

Novak, F., Bernik, S.(1999): »Naslov članka«, ime revije, letnik, štev., str. 12-15

Bernik,S.: (1999): »Naslov knjige«, založba, kraj

Novak, F.(1999): »Naslov magistrskega dela«, magistrsko delo, univerza, fakulteta

Žagar, A.: »Naslov referata«, Dnevi slovenske informatike, Zbornik posvetovanja, Slovensko društvo INFORMATIKA (1998)

V besedilu članka se sklicujte na navedeno literaturo na način (Novak 1999).

Članku dodajte kratek življenjepis avtorja (do 8 vrstic), v katerem poudarite predvsem delovne dosežke.

Z vsa vprašanja se obračajte na tehnično urednico Katarino Puc. Prispevke pošiljajte na disketi in papirju na naslov Katarina Puc, Slovensko društvo informatika, Vožarski pot 12, 1000 Ljubljana, ali samo po elektronski pošti na naslov katarina.puc@drustvo-informatika.si.

Po odločitvi uredniškega odbora, da bo članek objavljen v reviji, bo avtor prejel pogodbo, s katero bo prenesel vse materialne avtorske pravice na društvo INFORMATIKA. Po izidu revije pa bo prejel plačilo avtorskega honorarja po tedaj veljavnem ceniku ali po predlogu glavnega in odgovornega urednika.

Naslov uredništva je:

Slovensko društvo INFORMATIKA, Uredništvo revije Uporabna informatika, Vožarski pot 12, 1000 Ljubljana
www.drustvo-informatika.si/posta

Revija Uporabna informatika bo brezplačno objavljala v rubriki Koledar prireditev datume strokovnih srečanj, posvetovanj in drugih prireditev s področja informatike. Obvestila naj vsebujejo naslednje podatke: ime srečanja, datum in kraj prireditve, naziv organizatorja, ime in telefonska številka kontaktne osebe. Pošiljajte jih na naslov: Slovensko društvo Informatika, za revijo Uporabna informatika, rubrika: Koledar prireditev, 1000 Ljubljana, Vožarski pot 12. Objavljali bomo vsa obvestila, ki bodo prispela 30 dni pred objavo revije.

Spoštovane bralke in bralci,

Danes si bomo zastavili vprašanje, čemu na začetku enaindvajsetega stoletja, ko vsak povprečno izobražen človek govori vsaj en tuj jezik, služi znanstveni in strokovni tisk v domačem jeziku? Ali je trud številnih skupin zanesenjakov, ki se večinoma brezplačno trudijo v uredniških odborih domačih revij sploh še smiseln in potreben. Ali kdo to sploh še potrebuje in ceni, denimo domača znanstvena in strokovna javnost, študentje in dijaki, šole in univerze? Vprašanje je povsem na mestu saj je sam rektor Univerze v Ljubljani prof. dr. Jože Mencinger je v prilogi Znanost (Delo 7. avgusta) izrazil dvom o pomembnosti znanstvenega in strokovnega tiska v domačem jeziku.

Če ima predstojnik najvišje in največje znanstvene, raziskovalne in pedagoške institucije prav, potem se moramo vsi prizadeti resno zamisliti nad jalovim poslom, ki ga počnemo, ko se mučimo z domačim jezikom. Posledic za nas Slovence in naš jezik po rektorju ne bo. Vse kar bomo strokovnega in znanstvenega napisali, bomo objavili v angleščini, v uglednih tujih revijah, kjer bo dostopno ne samo našim domačim strokovnjakom in znanstvenikom pač pa tudi celotni svetovni srenji, in tako ubijemo dve muhi na en mah. Obe univerzi bosta srečni, saj bodo vsa dela domačih strokovnjakov objavljena izključno v mednarodno primerljivih in cenjenih revijah. Strokovne in znanstvene razprave v domačih krogih bomo vodili v angleščini. Vsa domača strokovna posvetovanja bodo potem seveda tudi v angleščini. Za tiste 'uboge pare' iz prakse, ki se še niso naučile dovolj dobro tujega jezika, da bi lahko sodelovale na domačih strokovnih in znanstvenih srečanjih, bomo v prehodnem obdobju zagotovili prevajanje prispevkov domačih avtorjev iz angleščine v slovenščino. Ker bo slovenski strokovni jezik v večini strok pri današnjem tempu razvoja zelo hitro izumrl, bomo tudi vse učbenike od osnovne šole do univerz v bodoče pisali le v angleščini, kar bo prisililo šolajočo mladino, da se od malih nog nauči uporabljati pri učenju in študiju zgolj tujo literaturo, kar je tudi prav. Potreba po prevajanju najrazličnejših strokovnih navodil, priročnikov in programskih orodij v slovenščino bo odpadla, s čimer si bomo prihranili ogromne stroške.

Ukrepati je treba hitro, saj smo ravno sredi vstopanja v Evropsko unijo, kar nam ravno na jezikovnem področju povzroča ogromne težave. Smo šele na začetku prevajanja okrog 150.000 strani evropske zakonodaje v slovenski jezik, ki postane povsem odveč, če se država odloči, da je uradni jezik v pravu in upravi angleščina. Pametno bi bilo, da bi tudi lastne zakone začeli pisati čimprej kar v angleščini, na ta način bi si prihranili tudi njihovo prevajanje v vse uradne jezike unije.

Postopoma bomo začeli izvajati tudi vsa predavanja na vseh šolah v tujem jeziku, saj domačega strokovnega jezika ne bo več. Morda bi za nekaj časa ohranili pouk slovenskega jezika še v slovenščini. Ko pa bodo vsi, predavatelji in študenti dovolj dobro obvladali tuje izrazoslovje, pa ne bo več razlogov, da tudi slovenščine ne bi predavali v angleščini. Nekaj težav bo sicer še s slovensko literaturo, ki je v preteklosti nastala v slovenskem jeziku in jo bo treba prevesti. Pa tudi tu situacija ni brezizhodna. Lucidnosti največjih umov slovenskega naroda v preteklosti (Prešerna in nekaterih drugih) se imamo zahvaliti, da so tak razvoj predvideli že v devetnajstem stoletju in so za vsak slučaj nekaj del napisali v tujem jeziku. Naše šole bodo postale privlačne za tuje študente, na veliko bomo lahko razširili izvoz znanja, ki je bilo sedaj ograjeno s plotovi našega kranjskega jezika.

In kaj, če gospod rektor vendarle nima prav in znanstveni in strokovni tisk v lastnem jeziku za razvoj nekega naroda le ni tako nepomemben? Potem se bomo pač Slovenci kot narod samoukinili.

Glavni in odgovorni urednik
Mirko Vintar

Obletnice kot izkušnja in pozaba

Anton P. Železnikar
Ljubljana

Ta kratek zapis je posvečen 25. obletnici ustanovitve Slovenskega društva Informatika pa tudi izročilu, spominu in tisti izkušnji računalništva in informatike izpred desetletij, ki se je obdržala do danes.

Letos mineva 40 let od začetka študija *digitalne tehnike* na Fakulteti za elektrotehniko, 35 let od prvega *jugoslovanskega mednarodnega simpozija* za računalništvo in informatiko (prva dva sta bila v Ljubljani, drugi na Bledu), 30 let od *kongresa IFIP v Ljubljani* (1971) in 25 let od *ustanovitve Slovenskega društva Informatika* (1976) ter izhajanja mednarodnega *časopisa Informatica* (1977) pa tudi okroglih deset let (1990) od načrtovanega stečaja slovenske računalniške industrije Delta (kasneje Iskra Delta). K temu bi veljalo dodati še ustanovitev Odseka za digitalno tehniko na Institutu Jožef Stefan v letu 1961 in s tem začetek nenehnega razvoja in napredovanja obdelave podatkov pri nas in po svetu. Leta 1961 se je začela tudi kooperacija izdelave računalnikov v Sloveniji med Iskro (Zavodom za avtomatizacijo) in podjetjem Zuse, K. G., in sicer tranzistoriziranega računalnika Z23. Na IJS pa je stekel tudi razvoj t. i. dokumentacijskega dodatka (Dokumentationszusatz) za podjetje Zuse, kot dodatek računalniku in njegova uporaba v nemških bankah. Nastane vprašanje, kaj se je od naštetih dogodkov obdržalo do danes in kaj je dokončno utonilo v pozabo. Ali je neka pozitivna izkušnja ostala in kam se je slovenska računalniška in informacijska scena s svojo dejavnostjo in organiziranostjo sploh pomaknila?

Dobili smo novo državo in s tem novo politično in civilizacijsko okolje. Nekako po kongresu IFIP v Ljubljani, leta 1971, se je *kozmopolitizem* razumevanja in mednarodne povezanosti računalniškega in informacijskega umaknil v meje nekdanje države in še posebej slovenske republike. Nadaljevali so se vsakoletni mednarodni simpoziji za računalništvo in informatiko, ki so ostali dragocena navezava na tuje ustanove in posameznike v tedanjem času. Iz tega *simpozijskega druženja* se je npr. v Sloveniji konstituiralo področje *umetne inteligence*, Univerza v Edinburghu pa je celo prevzela v ime svoje fakultete naš slogan *računalništvo in informatika* (computing and informatics).

Leta 1976 smo bili primorani ustanoviti Slovensko društvo Informatika, ker nam po novi zvezni ustavi iz leta 1974 v Sloveniji niso dovolili imeti zvezno društvo, ki bi po logiki razvoja lahko nastalo iz Zveznega odbora za obdelavo podatkov pri JK ETAN. To bi lahko bila le zveza republiških društev. Slovenska oblast pa je dokazala, da se je duha nove državne ustave potrebno držati, čeprav to ni veljalo za druge (npr. Jurema v Zagrebu je postala zvezno društvo). Sploh pa se je dobro vrniti za kakšno desetletje nazaj, na začetek šestdesetih let, da bi celotno situacijo delovanja in pobude programa IFIP, ki smo ga želeli presaditi v domačo državo, bolje razumeli.

Čeprav je bila t. i. digitalna tehnika le neki skromen začetek študija, raziskovanja in inženirskih dosežkov, je v njenem ozadju ždelo to, kar smo takrat le slabo razumeli in o njem le sanjali. Kako narediti lasten računalnik in osvojiti znanje operacijskega sistema in tudi kompilatorja. V letu 1958 je namreč izšla prva verzija pravega visokega programirnega jezika, imenovanega Algol 58, dve leti kasneje pa že kar nekakšen sporazumen končen dosežek dotedanje prevajalske filozofije, prevajalnik za jezik Algol 60, ki je bil in ostal kar nekaj let dosežek non plus ultra na področju pravega visokega jezika in njegovega prevajalnika. Kot mlajšemu inženirju mi je bilo takrat nerazumljivo, kako lahko računalnik s svojim operacijskim sistemom in prevajalnikom uresniči izvajanje nečesa, kar je bilo v matematiki znano kot rekurzivna funkcija. Zanimivo, da je takrat nastal tudi prvi izvirni program za linearno programiranje v državi, ki je bil napisan v zbirnem jeziku računalnika Z23, narejen pa je bil po algoritmični metodologiji, ki jo je na podiplomskem študiju predaval prof. Alojzij Vadnal, programsko realiziral in objavil pa Lado Čatar skupaj z avtorjem tega prispevka v strokovnem jugoslovanskem časopisu Automatika.

Ifipovsko obdobje se je v Sloveniji oblikovalo na osnovi zdravega tekmovanja med Ljubljano in Beogradom. Zvezni atomski inštitut Boris Kidrič v Vinči pri Beogradu in Institut Jožef Stefan v Ljubljani sta razvijala naprave za digitalne meritve jedrskih parametrov in regulacijsko opremo za jedrske reaktorje. Hkrati je v Beogradu

nastal Jugoslovanski komite za elektroniko, telekomunikacije, avtomatiko in nuklearno tehniko, okrajšano JK ETAN, ali še krajše ETAN. V okviru tega obsežnega zveznega komiteja si je Slovenija izborila Zvezno komisijo za obdelavo podatkov (ZKOP), v kateri je tudi nastala pobuda za organizacijo svetovnega kongresa IFIP 1971 v Ljubljani. Pravzaprav je bila ZKOP s tem namenom tudi ustanovljena, hkrati pa je prevzela tudi organizacijo jugoslovanskih mednarodnih simpozijev najprej v Ljubljani (1966-67) nato pa na Bledu, najprej vsakoletno, potem pa sporadično do leta 1985. Tako se je predlog za včlanitev Jugoslavije v IFIP in za kandidaturo kongresa IFIP 1971 pojavil pred nekoliko presenečeno in nezaupljivo generalno skupščino IFIP v Jeruzalemu leta 1966. Predlog je bil opremljen z garancijsko listino zvezne vlade v Beogradu ter z listinami podpore Gospodarske zbornice Slovenije, republiške vlade, pristojnega ministrstva in mesta Ljubljane.

Kandidatura je bila leto kasneje v dramatičnem spopadu s kandidaturami Mehike in Čehoslovaške pridobljena in potrjena z zadostno večino na generalni skupščini IFIP v Mexico City, v jeseni leta 1967. Za akterje tega podviga (tajnik ZKOP je bil takrat Silvin Leskovar) je bila pridobitev kongresa za Ljubljano enaka nekakšni računalniški olimpijadi, saj je kongres z več tisoč udeleženci spremljala še ena največjih svetovnih razstav računalniške opreme in tehnologije na Gospodarskem razstavišču. Namen kongresa je bil pripeljati miselnost, organiziranost in razvojno spodbudo tedanje računalniške obdelave podatkov v Jugoslavijo in še posebej v domače slovensko delovno, izobraževalno, raziskovalno in gospodarsko okolje. Odmevi ljubljanskega kongresa doma in v tujini so bili kar presenetljivi (npr. visoka stopnja zadovoljstva udeležencev kongresa v Ljubljani), zato je prav, da se po tridesetih in več letih v ospredje postavijo tudi glavni zunanji podporniki kongresa. Tu je bil prvi ljubljanski župan Marijan Tepina, ki je predlog tudi prvi podpisal. Eskalacija predloga je potekala potem prek ministrstva za prosveto in kulturo, ki ga je vodil Tomo Martelanc, ki je zamisel na osnovi županove podpore takoj podpisal. Enako se je s pobudo strinjala tudi GZ SRS in ne nazadnje še podpredsednik tedanjega izvršnega sveta Beno Zupančič in z njim republiška vlada. Zvezna vlada je na osnovi teh priporočil in zakulisne politike naposled napisala priporočilno listino za generalno skupščino IFIP.

Bilo bi krivično, če ne bi povedali, da je začetno pobudo finančno podprlo podjetje Intertrade kot zastopnik tedaj največjega podjetja za proizvodnjo računalniških sistemov na svetu IBM. S to podporo je bil omogočen obisk pri tedanjem predsedniku IFIP, prof. Speiserju, ki je bil hkrati direktor razvojnega laboratorija IBM v Rüschlikonu pri Zürichu. Potovanje za podporo pobude se je nadaljevalo potem v Darmstadt in München, z obiskom pri prof. F. Bauerju, ki je bil nemški vplivni delegat v generalni skupščini IFIP, končalo pa na Dunaju pri prof. H. Zemaneku, avstrijskem delegatu in vodji avstrijskega laboratorija IBM.

Pisec teh vrstic je imel privilegij in štipendijo za obiskovanje letnih in zimskih šol Nata s področja baz podatkov, prevajalnikov, operacijskih sistemov in teoretskega računalništva. Na teh šolah so predavali tedaj svetovno znani profesorji Hoare, Dijkstra, Perlis, Gries itd. Danes so njihova dela domala pozabljena, tedaj pa so predstavljala vroče področje obsežnih razprav in publikacij.

Globalizacija sveta, gospodarstva, raziskav in komunikacij je prinesla nove možnosti in usmeritve v svet računalništva in informatike. Internet je presegel lokalno zmogljivost komuniciranja, ponudbe in znanja. Najbolj atraktivne so postale nove oblike publiciranja na internetu, skupinske interdisciplinarne raziskave in osebna povezanost raziskovalcev, razvojnih inženirjev in poslovnih partnerjev. Uveljavili so se strokovni, politični in ljubiteljski razpravljavski forumi, ne le mednarodni, temveč tudi slovenski. Politične stranke so z različnim znanjem, ustreznostjo in organizacijo postavile svoje forume. Na ljubiteljskem področju so zaživeli številni forumi nekdanjega radioamaterstva, danes razširjenega z uporabo računalniške tehnologije. Sramežljivo so se v javno razpravo na internetu vključili tudi oblastna struktura in nekateri vidni državni uradniki.

Če je bil IFIP 1971 v Ljubljani nazadnje le spodbuden mednarodni dogodek, potem bi si danes po naštetih letnicah in obletnicah želeli tudi česa podobno mednarodno odmevnega v Sloveniji. Mednarodna konferenca ECIS 2001 na Bledu v juniju 2001 (ECIS je kratica za The European Conference on Information Systems) gotovo sodi v kategorijo resnejših naporov mednarodne uveljavitve Slovenije na področju informacijskih sistemov. Prof. Jožetu Gričarju iz kranjske FOV in njegovi organizacijski ekipi velja zahvala za nadaljevanje neke mednarodne kongresne tradicije računalništva in informatike na Bledu. Domače prebivalstvo pa bi potrebovalo resnejšo pobudo za uporabo interneta, za poslovanje in mednarodno komuniciranje s podjetji in posamezniki globaliziranega sveta. Tako kot smo nekdaj stremeli k vsestranski uporabi računalnikov in računalniških metod v gospodarstvu in državnih ustanovah, bi morali danes omogočiti najširšo uporabo internetnih storitev s kolikor mogoče prijaznim in cenenim dostopom za vsakogar v državi, ki si to želi. S tem bi v današnjo provinco povrnili nekaj nekdanjega kozmopolitizma in se povzpeli v svet realnejših dosežkov, objektivnejših primerjav in mednarodnega poslovanja.

ANALIZA STORITEV CENTRA ZA PODPORO UPORABNIKOM

Jože Benčina, Janez Grad
Center Vlade za informatiko, Langusova 4, Ljubljana
Univerza v Ljubljani Visoka upravna šola, Gosarjeva 5, Ljubljana
joze.bencina@gov.si, janez.grad@vus.uni-lj.si

Izvleček

Pričujoči prispevek govori o kakovosti informacijskih storitev, ki se v veliki meri izkazuje z ravnjo zadovoljstva odjemalcev. Analizirali smo storitve podpore uporabnikom informacijske opreme in storitev v okolju javne uprave. Osrednja vloga na področju zagotavljanja informacijske infrastrukture v tem okolju je poverjena Centru Vlade za informatiko. Storitve podpore so organizirane v Centru za podporo uporabnikom. Zadovoljstvo uporabnikov smo merili z mnenjsko raziskavo; pri svojem delu smo uporabili merilni instrument SERVQUAL, statistične obdelave pa smo opravili s programskim paketom SPSS. Rezultate raziskave predstavljamo s treh vidikov. Najprej obravnavamo ugotovitve v zvezi z raziskovalno hipotezo in njeno zavrnitvijo. Nato sledita analiza razlik v zadovoljstvu s storitvami med posamezn mi skupinami uporabnikov in analiza vzrokov za ugotovljeno stanje. Poročilo o raziskavi zaokrožujemo s pregledom izsledkov in ugotovitev.

Abstract

Services Analysis of User Support Center

The paper deals with the problem of information service quality that reflects to a great extent the user satisfaction level. Our research effort was focused on user support services in Slovenian public administration delivered by the User Support Center, a department within the Government Centre for Informatics. We carried out a user satisfaction survey using the SERVQUAL measurement instrument. The necessary statistical testing was performed with help of the SPSS software package. Research results are presented from three points of view. Firstly, we discuss causes for rejection of the research hypothesis, then we analyse differences in satisfaction between individual population segments, and lastly we analyse root causes for the situation. At the end the paper brings a review of findings and conclusions.

■■■

1 Uvod

Prehod iz industrijske v postindustrijsko družbo se nam dogaja, ne glede na to ali si ga želimo ali ne. Potek dogajanja v prehodnem obdobju diktirajo najrazvitejše ekonomije, zasledovalci, ki želijo biti tekmovalno uspešni, pa se morajo že zdaj dejavno vključevati v razvoj, saj bi jih pasivno sprejemanje novosti pripeljalo v povsem podrejen položaj. Za majhno in krhko državo kot je Slovenija, bi bil tak scenarij poguben. Zato moramo omogočati in vzpodbujati prilagajanje na novo poslovno okolje na vseh področjih in na vseh ravneh. Vsakdo mora k temu prispevati svoj delež, pri čemer je še posebej odgovorna vloga javne uprave. Zagotoviti mora pravne in tehnološke osnove za razvoj elektronskega poslovanja in izpeljati preobrazbo svojih funkcij v elektronsko upravo. Če naj bo pri tem učinkovita in uspešna, morajo biti aktivnosti dobro organizirane in med seboj usklajene.

Eden od pomembnih dejavnikov razvoja slovenske e-uprave je Center vlade za informatiko, katerega delo in rezultati temeljijo na dosedanjih naporih in dosežkih pri razvoju in vzpostavljanju informacijsko komunikacijske infrastrukture, aplikativnih storitev in sistemov za podporo uporabnikom in vzdrževanje opreme. Dejstvo je, da učinkovitih in uspešnih elektronskih storitev brez ustrezne podpore odjemalcem preprosto ni. Tisto kar pri tem šteje, je strankino mnenje o kakovosti storitve, zato se vsa razmišljanja v zvezi s kakovostjo vrtijo okrog zadovoljstva strank, ugotavljanja ravni zadovoljstva in iskanja načinov za zvišanje ravni zadovoljstva strank.

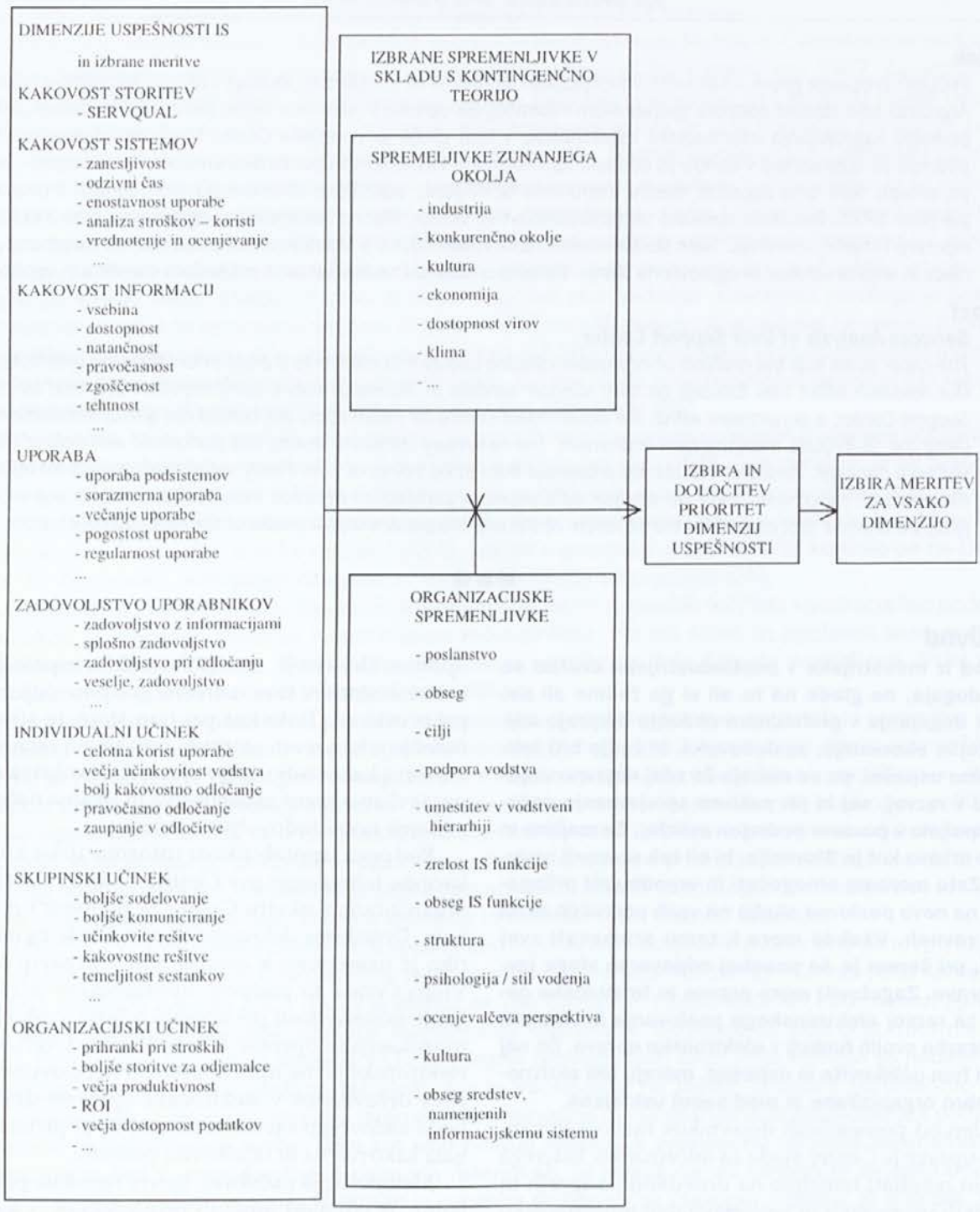
Podpora uporabnikom informacijsko komunikacijske tehnologije je v Centru vlade za informatiko organizirana v okviru Centra za podporo uporabnikom. Dosedanje delovanje Centra Vlade za informatiko je usmerjeno k zaposlenim v državni upravi. Vloga Centra za podporo uporabnikom je zagotavljanje učinkovitosti pri uporabi informacijsko telekomunikacijske opreme v tem okviru. Uveljavljanje elektronske javne uprave pomeni neposredno vključitev državljanov v elektronske upravne storitve, ki bodo zadovoljni s temi storitvami le, če jih bo spremljala kakovostna in učinkovita podpora.

Metodologija raziskave, katere rezultate predstavljamo, je eden od mnogih pripomočkov, s katerimi nadzorujemo kakovost storitev. Usmerjena je v ugotavljanje mnenja odjemalcev storitev, ki je temeljno

merilo ocenjevanja kakovosti storitev. Namen raziskave je bil poiskati odgovore na temeljna vprašanja o kakovosti storitev kot so:

- Kako so uporabniki zadovoljni ali nezadovoljni s storitvami Centra za podporo uporabnikom?
- Kaj so dobre in kaj slabe plati obstoječega sistema za podporo uporabnikom?
- Kateri so glavni vzroki za dobre oziroma slabe ocene uporabnikov?

Osnovni cilj raziskave je bil ugotoviti trenutno stanje zadovoljstva uporabnikov s storitvami Centra za podporo uporabnikom. Izpeljane cilje raziskave smo postavili na treh ravneh: na operativni ravni planirati ukrepe za izboljšanje kakovosti, sistemsko v



Slika 1: Model za izbiro spremenljivk in meritev uspešnosti informacijskih sistemov (IS Assessment Selection Model)

Vir: [7], str.18

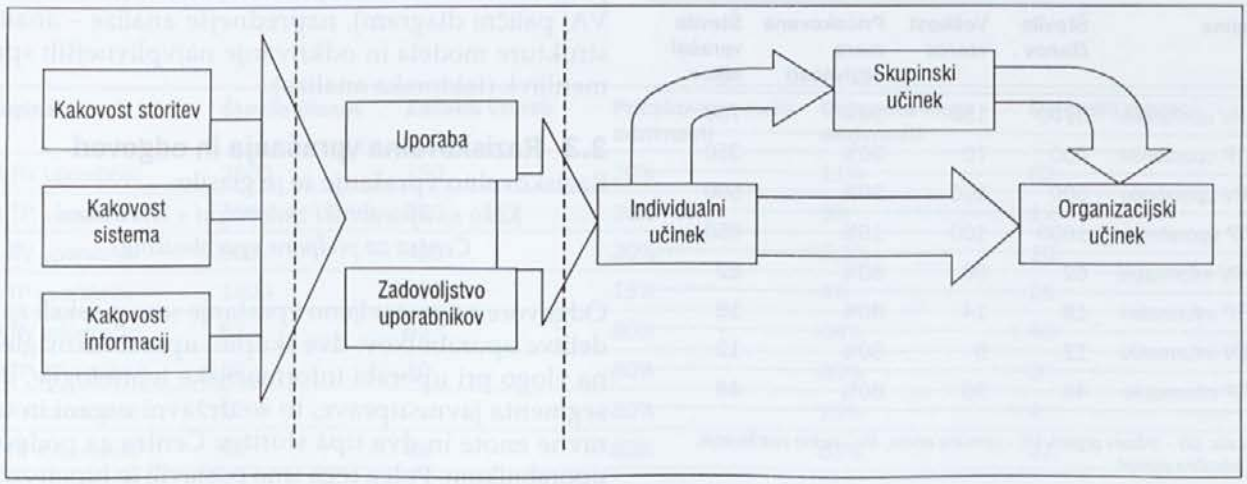
okviru obstoječega sistema predlagati organizacijske prilagoditve v smeri stalnega spremljanja kakovosti storitev, razvojno strateško podati usmeritve za usklajen nadaljnji razvoj storitve in zagotavljanja njene kakovosti.

2 Učinkovitost in uspešnost informacijskih sistemov, kakovost informacijskih storitev

Razvoj informatike je tako hiter, da se zdi, da vse nastaja sproti na novo. Seveda bolj poučeni opazovalec ve, da se za tem skriva bogata zapuščina, brez katere razvoj ne bi bil mogoč. Zato ne bo odveč, če na kratko predstavimo nekaj izhodišč, na katerih temeljijo razmišljanja o kakovosti informacijskih storitev. Uveljavljanje elektronskih storitev prinaša vse večje poenotenje segmentov, ki sestavljajo storitev, meje med posameznimi segmenti izginjajo. Zato so pri obravnavi kakovosti e-storitev bolj uporabni pristopi, ki upoštevajo celovito poslovno okolje, v katerem sta informacijsko telekomunikacijska infrastruktura in programska oprema integralni sistem celovitega poslovnega sistema.

Potreba po ocenjevanju prispevka informacijske funkcije pri povečevanju učinkovitosti in uspešnosti organizacije kot celote se je pojavila v poznih sedemdesetih letih [4], [5], [8]. Zgodnje meritve so bile osredotočene na zmogljivost (delati stvari na pravi način), kmalu pa je bil spoznan pomen merjenja učinkovitosti in uspešnosti (delati prave stvari) izrabe informacijskih sistemov [6]. Za celovito sliko problematike ocenjevanja kakovosti in produktivnosti informacijskih sistemov se je najbolje ozreti po celovitem modelu za ocenjevanje učinkovitosti informacijskih sistemov. Primer takega modela je predstavljen na sliki 1. Model vzpostavlja osem razsežnosti uspešnosti in predlaga spremenljivke in njim prirejene meritve. Izbira spremenljivk in meritev za ocenjevanje uspešnosti informacijskih sistemov mora biti prilagojena potrebam in ciljem organizacije kot celote. Pri tem moramo upoštevati tako organizacijske kot zunanje okoljske spremenljivke. Avtorji trdijo, da je treba algoritem za izbiro primernih razsežnosti, spremenljivk in meritev razviti za vsak poslovni primer posebej. Dobro sliko smernic za organiziranje meritev daje model, ki ga prikazuje slika 2. Model izvira iz del DeLonea in McLeana [2] z dodanima razsežnostima – s kakovostjo storitev in z vplivi skupinskega dela.

Potreba po merjenju kakovosti storitev je rastla v skladu z večanjem vloge storitev v svetovnem gospodarstvu. Kakovost storitev ocenjujejo odjemalci. Osnovno vprašanje na tem področju je, kako pridobiti splošno mnenje odjemalcev o kakovosti naših storitev. Od tod se potem nadaljuje stratifikacija odjemalcev in solastnikov ali delničarjev podjetja, kar je lahko osnova za nadaljnje raziskave v smeri ugotavljanja zadovoljstva uporabnikov. Z raziskovalnimi napori v tej smeri so v osemdesetih letih začeli trije raziskovalci [10], kar jih je pripeljalo do oblikovanja metodologije in instrumenta za merjenje kakovosti storitev, ki so ga poimenovali SERVQUAL [10]. Instrument temelji na dveh vprašalnikih, ki se nanašata na dve oceni odjemalcev, obakrat z 22 trditvami in ustreznimi odgovori. Vprašalnik o pričakovanjih se nanaša na oceno uporabnikov o storitvah, s katerimi bi bili v vsakem pogledu zadovoljni, vprašalnik o zaznavah se nanaša na oceno storitev, ki jih odjemalci dejansko prejemajo. Navadno se ocenjuje s sedemstopenjsko Likertovo lestvico, kjer ocena 7 pomeni, da se uporabnik s



Slika 2: Celovit model za ocenjevanje uspešnosti informacijskih sistemov: organiziranje meritev

Vir: [7], str 17.

trditvijo povsem strinja, ocena 1 pa, da se ne more s trditvijo nikakor strinjati. V zvezi z uporabnostjo SERVQUAL-a na področju poslovno informacijskih sistemov lahko beremo različne ocene. Pri izbiri orodja za našo raziskavo smo se oprli na mnenje, da raziskave v zvezi z veljavnostjo in zanesljivostjo dokazujejo, da je SERVQUAL primeren instrument za raziskovalce, katerih cilj je ugotavljanje kakovosti storitev na področju informatike [7].

3 Raziskovalni pristop in metodologija

3.1 Stratifikacija, vzorčenje in tehnika zbiranja podatkov

V sistem podpore Centra za podporo uporabnikom je vključenih okrog 70 institucij z okrog 4000 zaposlenimi v državnih organih in okrog 60 institucij z okrog 2200 zaposlenimi v upravnih enotah. Večina institucij, o katerih govorimo, ima zaposlene informatike, ki so zadolženi za zagotavljanje nemotenega delovanja informacijskih sistemov in za skrb za razvoj. Posredovalci storitev se morajo prilagajati skupinam z različnimi potrebami, zato smo v raziskavi upoštevali štiri segmente populacije in v vsaki posebej obravnavali skupine, ki so vključene v redno vzdrževanje ločeno od tistih, ki prejemajo le osnovno tehnično podporo. To pomeni, da imamo opraviti z osmimi segmenti celotne populacije, kakor jih prikazuje tabela 1. S heterogenostjo izbranih vzorcev smo se spopadli s pomočjo petih kontrolnih spremenljivk (poznavanje storitev Centra za podporo uporabnikom, obseg uporabe informacijske tehnologije, starostne skupine, spol in stopnja izobrazbe).

Populacija informatikov je majhna, zato so vzorci kar segmenti kot celote. Segmenti populacije uporabnikov imajo precej večje članstvo, zato je bilo smiselno uporabiti naključno vzorčenje. Podatke smo zbirali s pomočjo spletnega vprašalnika. Uporabniki so spletni vprašalnik samostojno izpolnjevali. Vsem članom vzorcev smo poslali elektronsko sporočilo z naslovom URL, kjer se je nahajal vprašalnik.

Skupina	Število članov	Velikost vzorca	Pričakovana mera odzivnosti	Število vprašalnikov
DO RV uporabniki	3200	150	20%	750
DO TP uporabniki	450	70	20%	350
UE RV uporabniki	500	100	20%	500
UE TP uporabniki	1600	100	15%	650
DO RV informatiki	62	50	80%	62
DO TP informatiki	18	14	80%	18
UE RV informatiki	12	9	80%	12
UE TP informatiki	48	38	80%	48

Legenda: DO – državni organi, UE – upravne enote, RV – redno vzdrževanje, TP – tehnična pomoč.

Tabela 1:
Populacijski segmenti, velikost vzorcev, pričakovana mera odzivnosti

3.2 Orodja – SERVQUAL, Q-RATER 97 in SPSS

Celotna metoda se nanaša na iskanje 5 vrzeli med ocenami različnih konstruktov. Vrzeli od 1 do 4 raziskujejo verjetne vzroke za pomanjkljivosti v sistemu posredovanja storitev. Ukvarjajo se s štirimi splošnimi problemi, s katerimi se srečamo pri posredovanju storitev: nepoznavanje pričakovanj odjemalcev, napačni standardi kakovosti storitev, odmik pri posredovanju storitev, obljube ne ustrezajo dejanskemu stanju. Vrzel, ki smo jo merili, je vrzel 5 (razlika med oceno zaznave in oceno pričakovanj) [10]. Meritev temelji na dveh vprašalnikih za ocenjevanje pričakovane in zaznane kakovosti storitev. Za potrebe dodatnih pogledov in kontrolnih analiz vsebuje še dva kratka dodatna vprašalnika za zbiranje splošnih in demografskih podatkov in za razvrstitev razsežnosti kakovosti po pomembnosti. Uporabili smo skrajšani merilni instrument s 13 neodvisnimi spremenljivkami, ki tvorijo štiri razsežnosti kakovosti informacijskih storitev (zanesljivost, odzivnost, zaupanje in pozornost) [3]. Orodje za pripravo vprašalnikov je bil programski paket Q-RATER 97. Statistične obdelave smo opravili s pomočjo programskega paketa SPSS.

Pri načrtovanju obdelave podatkov smo uporabili pristop od preprostega k bolj zapletenemu in se odločili za naslednje zaporedje obdelav in analiz: analiza in razprava o meri odzivnosti, analize posameznih spremenljivk – odkrivanje in obravnava posebnosti v rezultatih (frekvenčne tabele, palični diagram), primerjanje dveh ali več spremenljivk – odkrivanje pomembnih zvez med spremenljivkami (T-test, ANOVA, palični diagram), naprednejše analize – analiza strukture modela in odkrivanje najvplivnejših spremenljivk (faktorska analiza).

3.3 Raziskovalna vprašanja in odgovori

Raziskovalno vprašanje se je glasilo:

Kako so uporabniki zadovoljni s storitvami Centra za podporo uporabnikom?

Odgovore na postavljeno vprašanje smo poiskali za tri delitve uporabnikov: dve skupini uporabnikov glede na vlogo pri uporabi informacijske tehnologije, dva segmenta javne uprave, to so državni organi in upravne enote in dva tipa storitev Centra za podporo uporabnikom. Poleg tega smo postavili še hipotezo, ki smo jo preverili za dva tipa storitev Centra za podporo uporabnikom:

Zadovoljstvo uporabnikov z rednim vzdrževanjem je bistveno večje kot zadovoljstvo uporabnikov s tehnično podporo.

Sestavo vzorcev smo preverili s hipotezo o kontrolnih spremenljivkah:

Med vzorci, pridobljenimi na osnovi kontrolnih spremenljivk, ni statistično pomembnih razlik v zadovoljstvu uporabnikov.

4 Rezultati raziskave

4.1 Odziv uporabnikov

Dejanski odziv uporabnikov je bil manjši od pričakovanega, podatki o pričakovani in dejanski odzivnosti so prikazani v tabeli 2. Eden glavnih vzrokov za slab odziv uporabnikov je bila slaba obveščenost uporabnikov o trudu za izboljšanje kakovosti storitev Centra za podporo uporabnikom.

V populaciji uporabnikov je povsem statistično sprejemljiv le vzorec za državne organe v rednem vzdrževanju. Poleg njega je le še vzorec uporabnikov v upravnih enotah s tehnično pomočjo kolikor toliko uporaben, medtem ko sta preostala vzorca le omejeno uporabna. Populacija informatikov kot taka je majhna, zato jo je bilo potrebno obravnavati s primerno mero previdnosti. Med skupinami informatikov sta dve s kolikor toliko sprejemljivo velikostjo vzorca (državni organi pod rednim vzdrževanjem in upravne enote pod tehnično pomočjo).

4.2 Testiranje ničelnih hipotez o kontrolnih spremenljivkah

Hipotezo smo preverili za pet kontrolnih spremenljivk posebej za uporabnike in posebej za informatike. Rezultati so osnova za dokončen razmislek v zvezi z združevanjem segmentov populacije in razlago pristranosti v skupnih vzorcih in so predstavljeni v tabeli 3. Ničelno hipotezo smo preverjali za obe skupini uporabnikov in za celotno populacijo. Znak + pomeni, da je ničelna hipoteza potrjena, znak - da je zavrnjena. Večje ali manjše razlike so se pojavile skoraj pri vseh vprašanjih za vse tri skupine, vendar smo lahko zaradi skromnih vzorcev hipotezo zavrnili le v dveh primerih [1]. Nekatere temeljne odnose pa smo lahko zaznali že tokrat.

4.3 Analiza razsežnosti zadovoljstva

Rezultati faktorske analize so nas postavili pred dilemo, ali skrčiti število razsežnosti na tri ali se še naprej držati strukture SERVQUAL metode. Glede na to, da je velikost vzorca majhna, tokrat prav gotovo ni bilo smiselno posegati v strukturo instrumenta, ki ga uporabljamo. Še več, glede na to, da so se ocene zaznane kakovosti razvrstile zelo podobno, kot je bilo predvideno, moramo ugotoviti, kako bi lahko vplivali na ocenjevanje pričakovanj. Prav gotovo je konstrukt pričakovanj manj jasen od zaznave, zato bi lahko z ustrezno akcijo obveščanja in izobraževanja uporabnikov dosegli, da bi se rezultati v obeh delih instrumenta obnašali podobno.

4.4 Raziskovalna hipoteza

Analiza kontrolnih spremenljivk je pokazala, da moramo pri obravnavi raziskovalne hipoteze razmisliti predvsem o vplivih dveh kontrolnih spremenljivk, to sta stopnja izobrazbe za uporabnike in starostne kategorije (po dveh vrednostih) za informatike. Sicer pa rezultati raziskave prikazani v tabeli 4 kažejo, da moramo hipotezo za skupni seštevek za populacijo kot celoto zavrniti ali celo postaviti nasprotno hipotezo:

Zadovoljstvo uporabnikov z rednim vzdrževanjem je bistveno manjše kot zadovoljstvo uporabnikov s tehnično podporo.

Skupina	Število članov	Začetni vzorec	Pričakovana mera odzivnosti	Dejanska mera odzivnosti	Dejanski vzorec
DO RV uporabniki	3200	750	20%	11%	82
DO TP uporabniki	450	350	20%	3%	12
UE RV uporabniki	500	400	20%	2,5%	10
UE TP uporabniki	1600	650	15%	4%	26
DO RV informatiki	62	62	80%	64%	40
DO TP informatiki	10	10	80%	30%	3
UE RV informatiki	12	2	80%	25%	4
UE TP informatiki	48	48	80%	55%	27

Legenda: DO – državni organi, UE – upravne enote, RV – redno vzdrževanje, TP – tehnična pomoč.

Tabela 2: Pregled odziva uporabnikov in dejanska velikost vzorcev

	Ničelna hipoteza			Bistvene razlike			Opomba
	U	I	Vsi	U	I	Vsi	
Poznavanje storitev CPU	+	+	+	Q4G	Q9G	odzivnost	Vrednosti: *ne poznam, poznam, zelo dobro poznam.* uporabniki – pristranost zaradi neodzivnosti (*ne poznam*). Višja ocena zadovoljstva za skupino *ne poznam.*
Obseg uporabe informacijske tehnologije	+	+	/	zanesljivost	Q9G, Q13G		Vrednosti: *malo – do 2 uri, normalno – od 2 do 4 ure, zelo veliko – več kot 4 ure.* Uporabniki – pristranost zaradi neodzivnosti (*malo*). Nižja ocena zadovoljstva za vrednost *zelo veliko.*
Starostne kategorije	+	-	+	odzivnost	skupaj	odzivnost	Vrednosti: *mlajši od 30 let, med 30 in 45 let, nad 45 let.* Uporabniki – nakazana možnost zavrnitve ničelne hipoteze. Dve skupini uporabnikov (< 35 in >= 35).
Spol	+	+	+	pozornost	zanesljivost	Q1G, Q3G, Q5G	Vrednosti: *ženski, moški.* Razlike temeljijo na psiholoških in sociоloških podlagah.
Izobrazba	-	+	+	skupaj, zanesljivost, pozornost			Vrednosti: *nižja – manj od VII. stopnje, višja – VII. stopnja in več.* Za informatike nepomembno - majhno število informatikov z nižjo izobrazbo.

Legenda: U – uporabniki, I – informatiki, Vsi – celotna populacija.

Tabela 3: Pregled rezultatov testiranja kontrolnih spremenljivk

4.5 Raziskovalno vprašanje

Raziskovalno vprašanje zahteva primerjavo ocen zadovoljstva uporabnikov s storitvami podpore med segmenti populacije. Analiza pomembnih razlik med osmimi segmenti populacije in njihovimi sestavljenkami je pokazala, da pride v poštev za predstavitev pet segmentov, postavljenih v tri skupine.

Skupina 1 –uporabniki, informatiki v državnih organih, informatiki v upravnih enotah

Informatiki v upravnih enotah (UE I) ocenjujejo kakovost storitev podpore uporabnikom precej višje kot uporabniki (U) in informatiki v državnih organih (DO I). Storitve centra za podporo uporabnikom so v okolju upravnih enot dokaj nove in so informatiki z njimi slabše seznanjeni. Zato so njihova pričakovanja nižja in s tem ocena zadovoljstva višja. Oceni zadovoljstva uporabnikov in informatikov v državnih organih sta si skoraj enaki. Rezultat je pričakovan, saj je vzorec uporabnikov v državnih organih prevladujoč in medsebojni vpliv med obema skupinama velik. Pri zanesljivosti in odzivnosti ni pomembnih razlik med ocenami po segmentih. Zanesljivost je najvišje ocenjena razsežnost, najmanj zadovoljni so uporabniki z zaupanjem, ki odraža mnenje uporabnikov o znanju izvajalcev in njihovi zmožnosti dati prave odgovore na njihova vprašanja.

	Vrsta podpore	N	Srednja vrednost	Standardna napaka	Sig.
Vsi	DO RV	102	,1027	,0283	
	UE TP	43	,2282	,0430	0,017
Uporabniki	DO RV	64	,0977	,0353	
	UE TP	19	,1886	,0582	0,212
Informatiki	DO RV	38	,1113	,0479	
	UE TP	24	,2595	,0621	0,062

Legenda: DO RV – državni organi, redno vzdrževanje; UE TP – upravne enote, tehnična pomoč.

Tabela 4: Tabela razlik v srednji vrednosti med rednim vzdrževanjem in tehnično podporo (samo primerni vzorci)

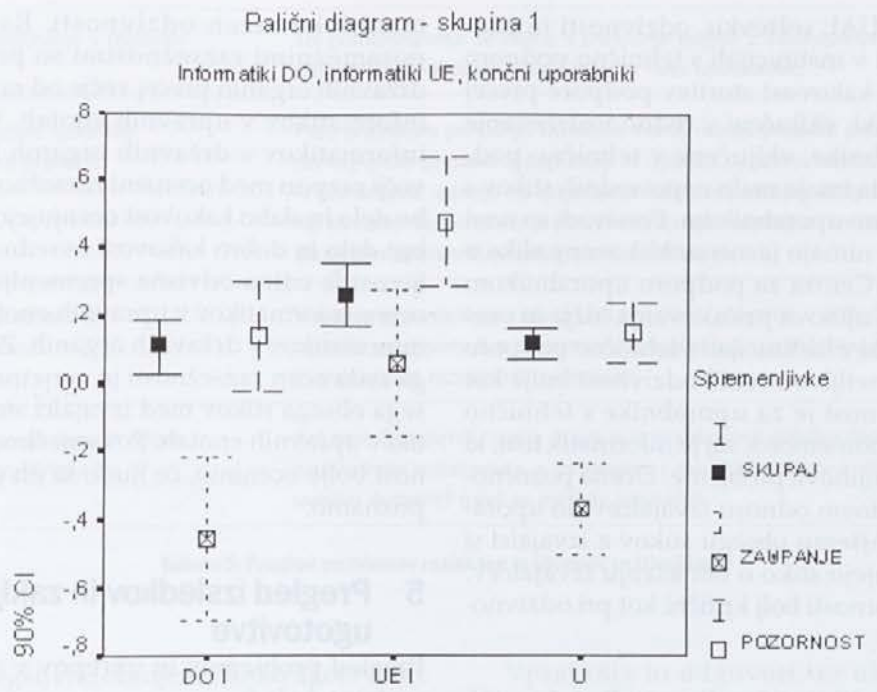


Diagram 1: Palični diagram – skupina 1

Skupina 2 –uporabniki glede na vrsto podpore

V drugi skupini opazujemo uporabnike glede na vrsto podpore, v katero so vključeni. Za redno vzdrževanje je značilno večje število neposrednih stikov med izvajalci podpore in uporabniki. Tehnična podpora je usmerjena k informatikom, ki so posredniki zahtev in rešitev med uporabniki in izvajalci podpore. Pri razlagi rezultatov moramo upoštevati dejstvo, da je v večini državnih organov vzpostavljeno redno vzdrževanje in pri večini upravnih enot tehnična podpora. Palični diagram za skupino 2 nazorno prikazuje razlike med obema vzorcema pri treh odvisnih spremenljivkah:

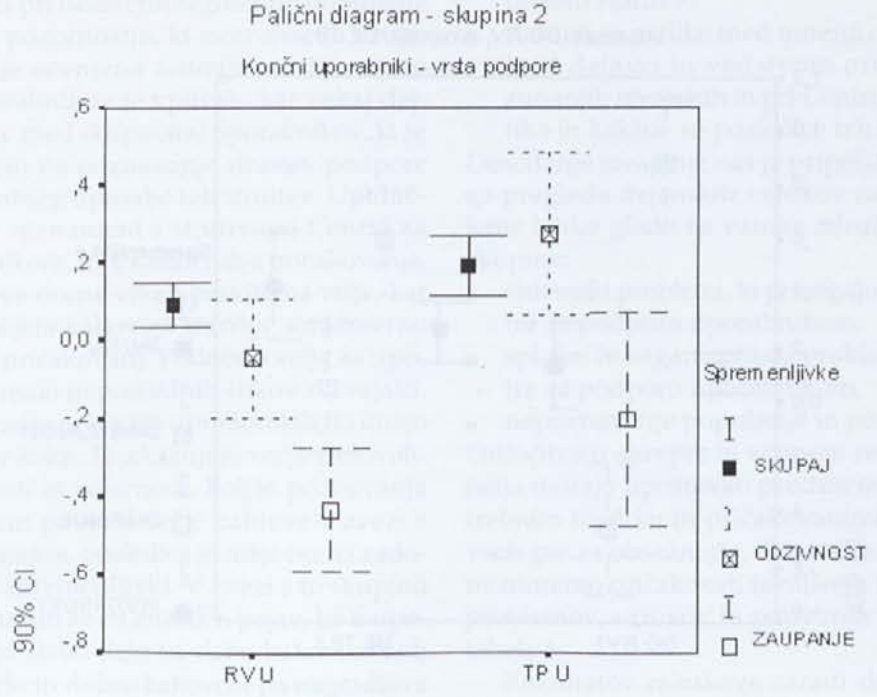


Diagram 2: Palični diagram – skupina 2

skupnem SERVQUAL seštevku, odzivnosti in zaupanju. Uporabniki v institucijah s tehnično podporo (TP U) ocenjujejo kakovost storitev podpore precej višje kot uporabniki, vključeni v redno vzdrževanje (RV U). Za uporabnike, vključene v tehnično podporo, je značilno, da imajo malo neposrednih stikov s Centrom za podporo uporabnikom. Ponavadi so novi v sistemu, zato še nimajo jasno izoblikovane slike o tem, kaj lahko od Centra za podporo uporabnikom zahtevajo. Zato so njihova pričakovanja nižja in ocena višja. Uporabniki v institucijah s tehnično podporo so nekoliko presenetljivo ocenili odzivnost bolje kot pozornost. Odzivnost je za uporabnike s tehnično podporo dokaj nepomembna, saj je informatik tisti, ki operativno rešuje njihove probleme. Ocena pozornosti temelji na vljudnem odnosu izvajalcev do uporabnikov. Kljub manjšemu obsegu stikov z izvajalci si uporabniki oblikujejo sliko o obnašanju izvajalcev. Očitno so pri pozornosti bolj kritični kot pri odzivnosti.

Skupina 3 – informatiki v državnih organih, informatiki v upravnih enotah

Za statistično obdelavo sta pri informatikih primerna le dva vzorca (informatiki v državnih organih – redno vzdrževanje in informatiki v upravnih enotah – tehnična podpora). Iz paličnega diagrama za skupino 3 je razvidno, da izkazujejo med tema dvema vzorcema statistično pomembne razlike vse odvisne spremenljivke razen odzivnosti. Razlike ocen med posameznimi razsežnostmi so pri informatikih v državnih organih precej večje od razlik med ocenami informatikov v upravnih enotah. Večja zahtevnost informatikov v državnih organih ima za posledico večji razpon med ocenami razsežnosti kakovosti. Slabo delo in slabo kakovost ocenjujejo bolj kritično, dobro delo in dobro kakovost ovrednotijo višje. Zanesljivost je edina odvisna spremenljivka, pri kateri je ocena informatikov v upravnih enotah nižja od ocene informatikov v državnih organih. Zamenjava vrstnega reda ocen razsežnosti je verjetno posledica manjšega obsega stikov med izvajalci storitev in informatiki v upravnih enotah. Povsem človeško je, da pozornost bolje ocenimo, če ljudi, ki jih ocenjujemo, bolje poznamo.

5 Pregled izsledkov in zaključne ugotovitve

Pregled problemov in ukrepov v zvezi z raziskavo podaja tabela 5.

O kakovosti storitev v absolutnem smislu na osnovi izsledkov ene raziskave ne moremo soditi. Glede na to, da je skupni SERVQUAL seštevek pozitiven, kar pomeni, da je ocena prejetih storitev višja od ocene pričakovane ravni storitev, lahko damo kakovosti storitev Centra za podporo uporabnikom pozitivno oceno. Če upoštevamo dejstvo, da je razsežnost

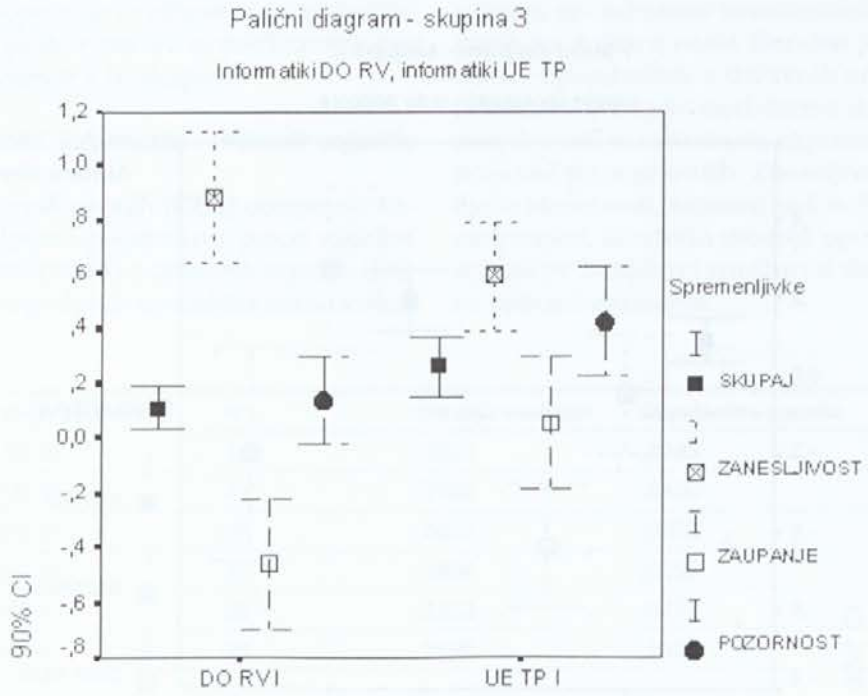


Diagram 3: Palični diagram – skupina 3

Majhna odzivnost uporabnikov v raziskavi	Tej pomanjkljivosti se bomo v prihodnje izognili z dvostopenjsko izvedbo naloge, najprej bomo obdelali informatike in nato uporabnike.
Veljavnosti in zanesljivosti raziskave ni bilo mogoče povsem preveriti	Pred pričetkom prihodnje raziskave bomo morali pridobiti potrebne dodatne demografske podatke o populaciji in izpeljati posebno raziskavo o lastnostih, ki pomembno vplivajo na dojemanje kakovosti storitev podpore uporabnikom. Na ta način bomo lahko pripravili ustreznejšo razslojitev in oblikovali posameznim skupinam uporabnikov prilagojene vprašalnike.
Ustreznost razsežnosti kakovosti smo lahko le delno ocenili	V zvezi s porazdelitvijo razsežnosti kakovosti moramo v prihodnjih raziskavah razrešiti predvsem dva problema: nejasnost pojma pričakovane kakovosti storitev in dvodelnost razsežnosti pozornosti.
Ocena zadovoljstva uporabnikov in s tem kakovosti storitev ni preverjena	Kot smo že omenili, bomo pravo oceno kakovosti storitev dobili šele z več zaporednimi raziskavami, s primerjavo z rezultati raziskav v drugih okoljih in z uvedbo dodatnih meril in meritev kakovosti.

Tabela 5: Pregled problemov raziskave in ukrepov za izboljšanje

zaupanje vedno negativno ocenjena, lahko ugotovimo, da vsebuje skupna pozitivna ocena o nekaterih segmentih storitev Centra za podporo uporabnikom tudi negativna mnenja. Zato enoznačne ocene ne moremo dati, temveč jo moramo oblikovati s pomočjo analize posameznih segmentov. Na ta način bomo lahko pripravili tudi ustrezne ukrepe za izboljšanje. Razvrstitev razsežnosti glede na oceno zadovoljstva je podobna za vse segmente populacije. Najnižjo oceno je dobilo *zaupanje*. Vzrok za tako oceno je pričakovanje uporabnikov, da bodo znali izvajalci odgovoriti na skoraj vsa njihova vprašanja. Druga najslabša ocena pripada *odzivnosti*, s tem da pri nekaterih segmentih populacije zamenja mesto s pozornostjo, ki sicer zaseda drugo mesto. Najbolje je ocenjena *zanesljivost*. Na oceno zadovoljstva uporabnikov je vplivalo kar nekaj dejstev. Gre za razlike med skupinami uporabnikov, ki se nanašajo predvsem na poznavanje storitev podpore uporabnikom in obseg uporabe teh storitev. Uporabniki, ki so slabše seznanjeni s storitvami Centra za podporo uporabnikom, so izkazali nižja pričakovanja, zato so bile njihove ocene vrzeli praviloma višje, kar pomeni, da je prejeta kakovost storitev sorazmerno višja od njihovih pričakovanj. Podobno velja za uporabnike, ki imajo malo neposrednih stikov z izvajalci. Do zanimive situacije pride pri uporabnikih, ki imajo z izvajalci pogoste stike. Ti izkazujejo večje zadovoljstvo pri *zanesljivosti* in *pozornosti*. Boljše poznavanje storitev pa obenem pomeni večje zahteve v zvezi z *odzivnostjo* in *zaupanjem*, posledica je nižja ocena zadovoljstva za ti dve spremenljivki. V zvezi s to skupino uporabnikov je zaznati še en značilen pojav, ko ti uporabniki vrednotijo slabo delo in slabo kakovost bolj kritično, dobro delo in dobro kakovost pa nagradijo z višjo oceno kot drugi uporabniki.

Vprašanja in odgovori ter ukrepi, ki jih lahko izluščimo iz rezultatov, so za nadaljnji razvoj storitve podpore uporabnikom zelo pomembna. Temeljna vprašanja, na katera moramo v tem okviru odgovoriti so:

- Ali so uporabniki prezahtevni?
- Ali so uporabniki dovolj seznanjeni z možnostmi in delovanjem Centra za podporo uporabnikom?
- Ali povzročamo pri uporabnikih nerealne želje in zahteve?
- Kakšna je povezava med tem, kar mislimo, da nudimo uporabnikom, in tem, kar oni zaznavajo kot prejeto storitev?
- Kakšne so razlike med mnenji o kakovosti storitev med delavci in vodstvom pri uporabnikih, pri zunanjih izvajalcih in pri Centru Vlade za informatiko in kakšne so posledice teh razlik?

Dosedanje izvajanje nas je pripeljalo do dokaj dobrega pregleda dejanskih vzrokov za težave. Vse probleme lahko glede na vzroke združimo v tri osnovne skupine:

- sistemski problemi, ki presegajo območje dela Centra za podporo uporabnikom,
- splošni in organizacijski problemi delovanja Centra za podporo uporabnikom,
- nepoznavanje populacije in potreb njenih članov.

Odločitve o ukrepih in vrstnem redu njihovega izvajanja morajo upoštevati predvsem razmerje med potrebnim trudom in pričakovanimi učinki. Skoraj pri vseh gre za obsežnejše, dalj trajajoče aktivnosti, zato ne moremo pričakovati takojšnjih rezultatov. Pregled problemov, vzrokov in potrebnih ukrepov prikazuje tabela 6.

Rezultatov raziskave zaradi skromnega statističnega vzorca sicer ne moremo upoštevati kot osnove za

oblikovanje gotove sodbe o dejanskem mnenju uporabnikov o storitvi podpore, lahko pa ugotovimo, da je uporabljeni pristop primeren.

V luči nadaljnjega razvoja informacijskih storitev in vzpostavljanja e-poslovanja in e-uprave je upoštevanje vloge odjemalca - stranke in njenega mnenja o kakovosti storitev ključnega pomena. Pristop, ki smo ga uporabili v tej raziskavi, je eden izmed mnogih načinov za ugotavljanje in zagotavljanje kakovosti e-storitev. Celovit sistem kakovosti e-storitev je naloga, pri kateri je treba uporabiti številne metode in orodja, med katerimi lahko nekatere uporabimo take kot so, druge pa prilagodimo ali jih izdelamo na novo. Izkušnje pričujoče raziskave kažejo, da morajo biti instrumenti za zagotavljanje kakovosti integralni del informacijskega sistema oziroma e-storitve. Občasna uporaba nekaterih instrumentov sicer pripomore k boljšemu razumevanju problematike in morebiti celo k boljši kakovosti, vendar ne zagotavlja trajne rasti kakovosti. Še večjo vlogo ima sistematičen pristop v smislu preventive in preprečevanja nezaželenih dogodkov ali trendov na področju zagotavljanja kakovosti.

Problemska skupina	Problem	Vzrok	Ukrep	Izvedljivost	Pričakovani učinek	Prioriteta
splošne omejitve	nezmožnost ugoditi posebnim zahtevam uporabnikov	omejitve s standardnim programskim okoljem	obveščanje in izobraževanje uporabnikov	normalna	odvisen od kakovosti akcij	srednja
		denarne omejitve pri nakupu programske opreme	priprava planov in obveščanje uporabnikov	normalna	dober	nizka
			določitev postopka za eskalacijo zahtevkov na strokovno službo	normalna	dober	visoka
splošni sistemski problemi	nezmožnost odgovoriti na vsa vprašanja uporabnikov	nepovezanost izvajalcev na različnih področjih	poenotenje sistema podpore uporabnikom / dogovor o ravni storitev	težja / projekt	zelo dober	visoka
		pomanjkljive informacije o aplikacijah in storitvah	oblikovanje postopka in spremljajočih dokumentov o prevzemu aplikacij in storitev v podporo / dogovor o ravni in obsegu storitev	normalna	zelo dober	visoka
delovanje Centra za podporo uporabnikom	nezmožnost rešitve problema	neopredeljena raven in obseg znanj izvajalcev podpore	določitev ravni in obsega znanja, izbira načina preverjanja, preverjanje	težja	dober	srednja
		prepočasno širjenje znanja na nova področja	oblikovanje načrtov za izobraževanje in usposabljanje	normalna	zelo dober	srednja
	težave z odzivnostjo, kadar uporabnik zahteva točno določenega izvajalca	preveč osebni odnosi med informatiki in izvajalci podpore	menjava izvajalcev, obveščanje uporabnikov	lažja	srednji	nizka
nepoznavanje populacije in potreb njenih članov	nezmožnost prilagajanja storitev posebnim potrebam uporabnikov	nepoznavanje potreb posameznih skupin populacije	projekt in raziskava o skupinah v populaciji	zelo težka / projekt	zelo velik	srednja

Tabela 6: Problemi, vzroki, ukrepi, prioritete

Izjemnega pomena dejavnosti na področju e-poslovanja se zavedamo vsi. Za raziskovalca željnega izzivov je na tem področju na voljo več kot dovolj vprašanj, na katera je treba odgovoriti. Zato je naša naloga, da se kolikor je mogoče posvetimo delu na tem področju in rezultate kar najhitreje in kar se da učinkovito uporabimo. Pri tem vsaj za okolje javne uprave velja, da si moramo znanje izkušnje izmenjavati in na ta način prispevati k hitremu in uspešnemu uveljavljanju e- poslovanja pri nas.

6 Literatura in viri

[1] Benčina J.:
Center za podporo uporabnikom – odkrivanje poti do kakovostnih storitev, magistrsko delo. Univerza v Ljubljani Ekonomska fakulteta, Ljubljana, 2000.

[2] DeLone W. H., McLean E. R.:
Information Systems Success: the Quest for the Dependent Variable. Information Systems Research, 3(1992), 1, str. 60-95.

[3] Kettinger William J., Lee C. C.:
Pragmatic Perspectives on the Measurement of Information Systems Service Quality. MIS Quarterly, Minneapolis, 21(1997), 2, str. 223- 240.

[4] King W. R., Rodriguez, J. I.:
Evaluating Management Information Systems. MIS Quarterly, Minneapolis, 2(1978), 3, str. 43-51.

[5] How to Survive a Management Assessment. MIS Quarterly, Minneapolis, 1(1997), 1, str. 11-17.

[6] McLean E. R.:
Assessing Returns from the Data Processing Investment. In F. J. Gruenberger (Ed.): Effective vs. Efficient Computing. Englewood Cliffs:
Prentice-Hall, 1973. str. 12-25.

[7] Myers Barry L., Kappelman Leon A., Prybutok Victor R.:
A Comprehensive Model for Assessing the Quality and Productivity of the Information Systems Function:
Toward a Contingency Theory for Information Systems Assessment. Information Resources Management Journal, 10(1997), 1, str. 6-25.

[8] Pitt L. F., Watson R. T., Kavan C. B.:
Service quality: A measure of information systems effectiveness. MIS Quarterly, Minneapolis, 19(1995), 2, str. 173-187.

[9] Rolefson J. F.:
The DP Check-up. Journal of Systems Management, 29(1978), 11, 38-48.

[10] Vavra Terry G.:
Improving your Measurement of Customer Satisfaction. Milwaukee: American society for quality, 1997, 476 str.

[11] Zeithaml V. A., Parasuraman A., Berry L. L.:
Delivering Quality Service: Balancing Customer Perceptions and Expectations. New York: The Free Press, 1990, 226 str.

◆

Mag. Jože Benčina je diplomiral na Fakulteti na naravoslovje in tehnologijo smer pedagoška matematika. V letu 2000 je magistriral na Ekonomski fakulteti na oddelku za upravljavsko informacijske sisteme. Zaposlen je na Centru Vlade za informatiko, kjer kot svetovalec vlade v sektorju za informacijsko infrastrukturo - programska oprema skrbi za delovanje sistema za podporo uporabnikom. Ukvarja se predvsem s problematiko zagotavljanja kakovosti elektronskih storitev.

◆

Dr. Janez Grad je magistriral iz matematike na Univerzi v Birminghamu, Anglija, leta 1973 pa doktoriral iz matematičnih znanosti na Vseučilišču v Zagrebu. Od leta 1973 do 1999 je sodeloval kot učitelj za informatiko na Ekonomski fakulteti, najprej kot docent, od leta 1979 dalje kot izredni profesor, od 1985 pa kot redni profesor. Sedaj pa je redni profesor informatike na Visoki upravni šoli v Ljubljani. Ukvarjal se je s programiranjem na računalniku in z reševanjem problema lastnih vrednosti in vektorjev matrik, v zadnjih letih pa se ukvarja z reševanjem problemov s področja operacijskega raziskovanja in s področja baz podatkov.

◆

NAPADI NA KRIPTOGRAFSKE SISTEME

Matej Šalamon, Tomaž Dogša
Fakulteta za elektrotehniko, računalništvo in informatiko
Univerza v Mariboru, Smetanova 17, 2000 Maribor
matej.salamon@uni-mb.si

Izvleček

V prispevku smo predstavili najpogostejše vrste kriptografskih napadov na simetrične in asimetrične kriptografske sisteme. Izbor vrste napada je odvisen od napadalcu razpoložljivih sestavnih delov kriptografskega sistema ter drugih informacij.

Primerjali smo odpornost simetričnih in asimetričnih kriptografskih sistemov, glede na dolžino uporabljenega ključa, obširneje pa smo predstavili napad z grobo silo. Navedli smo povprečni čas, ki ga posamezni napadalec ali skupine potrebujejo za preiskavo polovice vseh možnih ključev. V najslabšem primeru je lahko povprečni čas dvakrat daljši.

Opisali smo tudi napad na kriptografski sistem DES, v katerega je bilo leta 1999 z distribuiranim iskanjem tajnega ključa vlomljeno v rekordno hitrem času.

Abstract

Attacks against Cryptographic Systems

In this article we describe most frequently used crypto attacks against conventional or symmetric and public-key or asymmetric cryptographic systems. Type of attack selection depends on availability of cryptographic system components and other information to attacker.

Resistance of symmetric and asymmetric cryptographic systems is compared due to used key length. Brute force attack is circumstantially presented and average time needed to search half of the symmetric key-space is stated. Worst-case scenario could be twice as long.

We also describe a year 1999 attack against DES, in which cipher was broken in record time using distributed key search.

■ ■ ■

1. Uvod

Zagotavljanje tajnosti podatkov je zopet postalo aktualno, ko so se po internetu začela pošiljati zaupna sporočila. Vsako poslovanje prek interneta zahteva tajnost, celovitost in avtentičnost sporočil. Internet omogoča zelo hiter prenos velikega števila sporočil, vendar tudi zelo enostavno prestrezanje sporočil. Kot odgovor na ta problem so nastali razni širfirni in dešifrirni sistemi, ki jim pravimo tudi kriptografski sistemi. Njihova osnovna naloga je zagotavljanje tajnosti prenašanega sporočila. Z določenimi dodatnimi postopki lahko zagotovimo tudi celovitost in avtentičnost sporočil ter preprečitev utaje avtorstva in sprejema sporočila. Nepooblaščeno osebo, ki se želi dokopati do vsebine sporočila ali ga spremeniti, bomo poimenovali napadalec. Prva naloga napadalca je, da se dokoplje do sporočila. Če je le-to šifrirano, potem ima na razpolago dve možnosti. Prva je, da z analizo šifriranega sporočila razvozla vsebino. Temu postopku pravimo kriptoanaliza. Drug pristop je kraja ključa, s katerim lahko sporočilo dešifrira.

Pri kriptoanalizi nastopata dve konfliktni zahtevi. Prva je ta, da naj bodo kriptografski sistemi čim bolj varni, čim cenejši in vsakomur dostopni. Mnogo ljudi si želi popolno tajnost poslanih sporočil. Organizacije, ki se borijo proti kriminalu in protiobveščevalne organizacije pa tega vedno ne želijo, saj dobri kriptografski sistemi otežujejo njihovo delo. Te dileme ne bomo obravnavali v tem prispevku, ampak se bomo posvetili predvsem opisu raznih vrst napadov na kriptografske sisteme. Najprej bodo na kratko opisane tiste lastnosti kriptografskih sistemov, ki jih bomo v nadaljevanju potrebovali (podrobnejši opis glej v (Pavešić 1997). Obravnavane bodo splošne značilnosti napadov in primerjava med kriptografskimi sistemi glede njihove varnosti. Nato bo sledil kratek opis najpogostejših napadov.

2. Kriptografski sistemi

Kadar želimo zagotoviti zasebnost nekega sporočila, ga moramo pretvoriti v nerazumljivo obliko kar pomeni, da ga moramo *šifrirati*. Sporočilo mora biti šifrirano tako, da ga zna dešifrirati samo tisti, ki mu je sporočilo namenjeno, vsem ostalim pa mora biti njegova vsebina nerazumljiva. Sisteme, ki omogočajo šifriranje in dešifriranje sporočil, imenujemo *kriptografski sistemi*.

Pri šifriranju gre za transformacijo *odprtega sporočila* v nerazumljivo *šifrirano sporočilo* ali *tajnopis*. Tovrstna transformacija, ki se običajno izvaja kar z računalnikom,

poteka v skladu s *transformacijskimi tabelami* ali *šifrirnimi algoritmi*. Šifrirni postopek mora biti reverzibilen, saj je le v tem primeru tajnopis mogoče dešifrirati, to je pretvoriti nazaj v originalno odprto sporočilo.

Šifriranje in dešifriranje vhodnega sporočila poteka na osnovi *ključa*, ki mora biti tajen kar pomeni, da ga sme poznati samo pošiljatelj sporočila in tisti, ki mu je sporočilo namenjeno. Ključ, ki mora biti povsem neodvisen od odprtega sporočila, tvorijo izbrane vrednosti parametrov šifrirnega in dešifrirnega algoritma. Če za šifriranje in dešifriranje uporabljamo enak ključ, potem takemu sistemu pravimo simetričen kriptografski sistem[1]. Pri asimetričnih sistemih[2] imamo poseben ključ za šifriranje, ki je javen. Le s privatnim ključem lahko tajnopis dešifriramo. Glede na dolžino podatkov, ki jih v algoritmu obdelujemo, ločimo tokovne in blokovne šifrirne sisteme. Pri tokovnih se odprta sporočila šifrirajo po bitih, pri blokovnih pa se sporočilo razdeli na več velikih blokov[3], ki se nato šifrirajo.

3. Splošne značilnosti napadov na informacijski kanal in na sporočila

Eden izmed pogostih napadov na informacijski kanal je onesposobitev prenosnega medija. To lahko dosežemo s fizičnim (blokiranje voda) ali programskim posegom (blokiranje strežnika). V določenih primerih je mogoče tudi prisluškovati ali spreminjati lastnosti informacijskega kanala (npr. povzročitev prekomerne obremenitve). Če pri napadu ostane sporočilo nespremenjeno, potem gre za pasiven napad. Med pasivne napade štejemo prisluškovanje (prestrezanje) in analizo prometa sporočil:

- **Prisluškovanje:** To je direkten napad na zasebnost, ki je izvedljiv, če ima napadalec dostop do informacijskega kanala. Če prisluškovanja fizično ni mogoče preprečiti, potem moramo sporočila ustrezno šifrirati.
- **Analiza prometa:** Napadalec skuša z analizo prometa in z analizo značilnosti sporočil ugotoviti določene podatke o pošiljatelju in prejemniku (npr. identiteto).

Ker pri pasivnih napadih običajno ne ostane nobena sled za napadalcem, je tak napad težko opaziti. Zelo enostavna in popolnoma neopazna sta prisluškovanje in analiza prometa v mejah lokalnega omrežja. Za napad na sporočila, ki se prenašajo po drugih omrežjih, je treba najprej vdreti v enega izmed strežnikov, ki so vključeni v določeno lokalno omrežje.

Aktivni napadi povzročajo modifikacijo sporočila (podatkovnega toka) ali pa ustvarjajo lažno sporočilo (podatkovni tok). Ker gre za spremenjena sporočila, lahko zaznamo prisotnost aktivnih napadov. Razdelimo jih v tri kategorije:

- **Spreminjanje:** gre za napad na celovitost sporočila, zaradi katerega je lahko sporočilo spremenjeno ali zakasnjeno. Primer takšnega napada je sporočilo "Dovoli **Maji**, da dostopa do bančnega računa" spremenjeno v "Dovoli **Branku**, da dostopa do bančnega računa".
- **Ponovno pošiljanje:** napadalec prekopira sporočilo in ga kasneje (ob neprimernem času) ponovno pošlje (npr. naročilo za nakup delnic, ukaz za umik brigade).
- **Spreminjanje lastnosti informacijskega kanala:** napadalec v celoti preprečuje, spreminja ali ovira normalno komuniciranje. Npr. napadalec zaustavi vsa sporočila namenjena določenemu cilju. Drugi primer je prekomerna obremenitev omrežja s sporočili, kar privede do njegovega zloma.
- **Pretvarjanje:** napadalec se pretvarja za pooblaščeno osebo in izkorišča njene privilegije. Primer pretvarjanja je zajetje gesla, s katerim se napadalec lažno identificira in s tem pridobi določene privilegije.

4. Napadi in vdori v kriptografski sistem

Kakor hitro je iz tajnopisa mogoče izločiti originalno, odprto sporočilo, govorimo o vdoru v kriptografski sistem. Vdor je posledica uspešnega kriptoanalitičnega napada ali pa kraje ključa. V splošnem je odpornost kriptografskega sistema odvisna od vrste napada, njegov izbor pa od: zasnove šifrirnega sistema, ključa (dolžine ključa, njegovega distribuiranja) in napadalcu razpoložljivih informacij. Odpornost kriptografskih sistemov lahko z vidika napadalca predstavimo s količino napora, ki ga je treba vložiti za vdora.

Pred napadom mora napadalec oceniti ali je izbrani sistem sploh smiselno napasti in kakšna je najprimernejša vrsta napada. Kriptografski sistem je *računsko varen* (Stallings 1999), če so stroški vdora (dešifriranja) večji od koristi dešifriranega sporočila. Ker vrednost sporočila s časom pada, mora napadalec oceniti tudi čas, potreben za vdor.

Temelj varnosti vsakega kriptografskega sistema je ustrezen algoritem. Kljub temu, da je odpornost algoritma možno oceniti, se pogosto izkaže, da je dejanska odpornost nižja od ocenjene. Vzrok za zmanjšanje

1 *Tipičen predstavnik simetričnih kriptografskih sistemov je sistem DES (Data Encryption Standard).*
2 *Najbolj znan asimetrični kriptografski sistem je sistem RSA, poimenovan po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman).*
3 *64 in več bitna beseda.*

odpornosti je v raznih napakah, ki so nastale pri implementaciji. Posledice napak se kažejo v raznih hibah programske in strojne opreme. Poznavanje teh hib lahko zelo zmanjša varnost kriptografskega sistema. Prisotnost hib ugotavljamo z raznimi postopki preverjanja (npr. testiranje, formalno dokazovanje, itd.) (Dogša 1993). Ker so stroški testiranja zelo visoki, je zelo malo kriptografskih sistemov, ki bi bili izredno dobro preverjeni. Problem visokih stroškov testiranja izdelovalci kriptografskih sistemov rešujejo z distribuiranim testiranjem. V javnosti objavijo nekaj tipičnih informacij, ki so običajno napadalcu znane (npr. tajnopis, del odprtega sporočila in šifrirni algoritem[4]) in nato razpišejo visoko nagrado za vdor[5]. Pogosto mora napadalec tudi pojasniti svojo metodo, če želi prejeti nagrado. Z odpravljanjem najdenih napak, se veča varnost kriptografskega sistema. Mnogi so mnenja, da so zadovoljivo preverjeni le sistemi, ki so bili podvrženi distribuiranemu testiranju.

Tabela 1 prikazuje zanimivo primerjavo med odpornostjo simetričnih in asimetričnih kriptografskih sistemov, glede na dolžino uporabljenega ključa. Vidimo lahko, da je potreben za enako odpornost za simetrične šifrirne sisteme bistveno krajši ključ kot za asimetrične.

Vsaka informacija o kriptografskem sistemu in sporočilu pomaga napadalcu. Vrsta napada je odvisna od količine in vrste napadalcu razpoložljivih sporočil, njegovega znanja in računalniške podpore. Napadalcu lahko pomagajo zlasti naslednje informacije: vrsta algoritma, vsebina sporočila, vrsta sporočila (besedilo, slika, program itd.), jezik, v katerem je napisano sporočilo, statistične lastnosti jezika. S prikrivanjem teh informacij lahko dvigujemo varnost kriptografskega sistema. Napadalcu pri napadu koristita poznavanje določenih informacij in posedovanje sestavnih delov ali celotnega kriptografskega sistema:

- **skrivalni algoritem:** napadalec sumi, da je v množici sporočil skrit[6] tudi tajnopis. Npr. v eni izmed 100 slik je skrito sporočilo. Brez poznavanja skrivalnega algoritma napadalec ne more odkriti skritega sporočila, ki je lahko odprto ali šifrirano (Johnson, Jajodia 1998).
- **en tajnopis:** napadalec ima na razpolago samo tajnopis brez pripadajočega odprtega sporočila. Napadi, ki temeljijo samo na enem tajnopisu, so zelo redko uspešni. Eden izmed napadov, ki ga je možno izvesti tudi z delom tajnopisa, je napad z grobo silo[7], pri katerem napadalec poskuša vdreti sistematično - s preskušanjem vseh možnih ključev.
- **segmente odprtega sporočila in pripadajoče tajnopise.** Npr. v razpisu za napad na kriptografski sistem DES je bil znan tajnopis in začetek sporočila. Tudi v tem primeru je možno uporabiti napad z grobo silo.
- **šifrirni sistem,** s katerim lahko napadalec generira tajnopise, vendar ne pozna ključa, ker je le-ta npr. vgrajen v sistem. Napadalec lahko tvori poljubno število odprtih sporočil in tajnopisov in uporabi diferencialno analizo, kjer s premišljeno izbranimi sporočili[8] sklepa o pravilnosti ključa.
- **končno število tajnopisov in dešifrirni sistem,** vendar ne pozna ključa. Na podlagi analize tajnopisa in dešifriranega sporočila sklepa o uspešnosti napada. Napadi s tovrstnimi informacijami so običajni za asimetrične kriptografske sisteme.
- **celotni kriptografski sistem,** vendar ne pozna tajnega ključa. Napad lahko izvede s pomočjo izbranih odprtih sporočil in pripadajočih tajnopisov, ima pa tudi možnost izbire tajnopisov in pripadajočih dešifriranih sporočil. Na osnovi tega sklepa o pravilnosti izbranega ključa. Ta primer zelo redko nastopa.

V navedenih kategorijah količina informacij, katere napadalec pozna, narašča. Če napadalec uspe vdreti le s poznavanjem samo enega tajnopisa, potem velja, da je kriptografski sistem slab. Za vdor v večino dobrih šifrirnih sistemov je potrebnih več informacij.

Simetrični šifrirni sistem	ASIMETRIČNI šifrirni sistem	
	RSA	ECC (Elliptic Curve Cryptosystem)
40 bitov	274 bitov	57 bitov
56 bitov	384 bitov	80 bitov
64 bitov	512 bitov	106 bitov
80 bitov	768 bitov	132 bitov
96 bitov	1024 bitov	160 bitov
112 bitov	1792 bitov	185 bitov
120 bitov	2048 bitov	211 bitov
128 bitov	2304 bitov	237 bitov

Tabela 1:
Primerjava med dolžinami ključev potrebnih za enako stopnjo odpornosti v simetričnih in asimetričnih sistemih (Moscaritolo 1999).

4 *Izvršljivo kodo.*
5 *Primer: poziv, ki ga je razpisal laboratorij RSA za napad na kriptografski sistem DES - DES Challenge III: http://www.rsa.com/rsalabs/des3/*
6 *Veda, ki se ukvarja metodo skrivanja podatkov, se imenuje steganografija.*
7 *Angl.: brute force attack – exhaustive search.*
8 *Sorodna sporočila z določenimi razpoznavnimi vzorci.*

Kriptografski napadi se delijo (slika 1) glede na strukturo kriptografskega sistema, napadalcu razpoložljivih informacij in sestavnih delov kriptografskega sistema.

4.1 Najpomembnejši napadi na blokovne simetrične kriptografske sisteme

Za blokovne kriptografske sisteme je značilno, da šifrirajo naenkrat velik blok podatkov. Takšen princip varuje pred različnimi statističnimi analizami, s pomočjo katerih je mogoče sklepati o vrsti odprtega sporočila in informacijah, ki jih vsebuje. Kljub temu pa obstaja nekaj vrst napadov, ki so pri tovrstnih kriptografskih sistemih lahko zelo uspešni.

4.1.1 Napad z grobo silo - obširno iskanje tajnega ključa

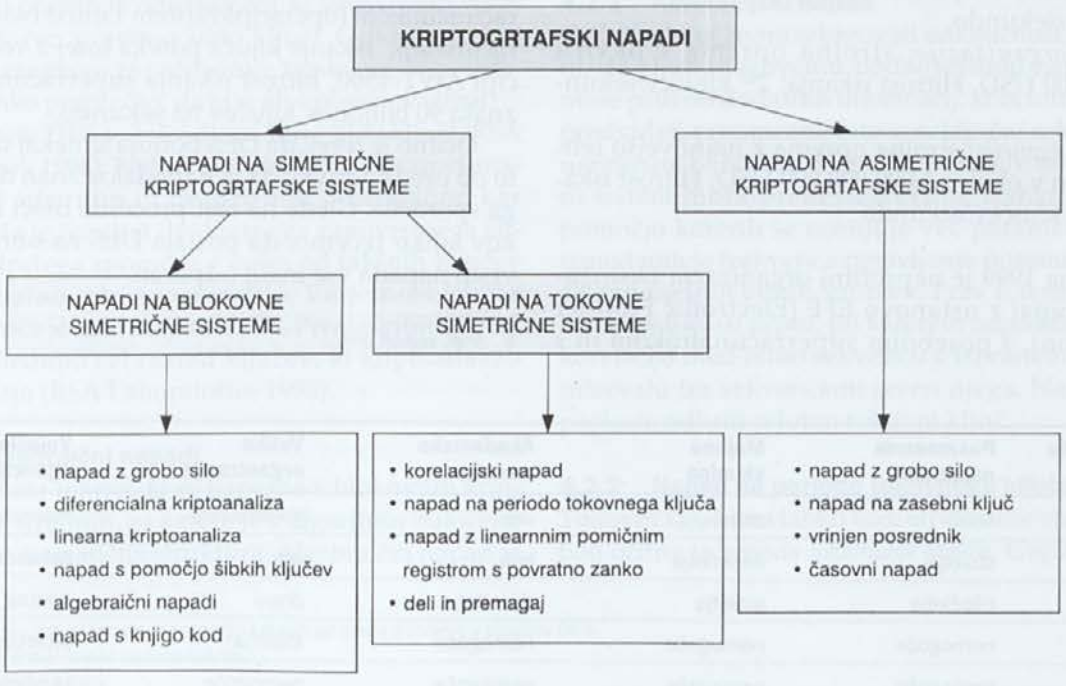
Obširno iskanje ključa, znano kot napad z grobo silo, je najpreprostejša kriptoanalitična tehnika, ki omogoča identifikacijo pravilnega tajnega ključa na osnovi poskusov z vsemi možnimi ključi. Pogoj za izvedbo tega napada je, da napadalec pozna:

- majhen del odprtega sporočila in pripadajoči tajnopis ali
- samo tajnopis, pri čemer mora imeti odprto sporočilo določene prepoznavne karakteristike.

Sam postopek je sestavljen samo iz treh korakov: izbor ključa, poskusno dešifriranje in ugotavljanje uspešnosti. Prva dva koraka je možno enostavno avtomatizirati, medtem ko lahko tretji v nekaterih primerih pomeni velik problem. Uspešnost, to je pravilnost ključa se kaže v tem, da je dešifrirano sporočilo smiselno. Če je znan vsaj del odprtega sporočila, potem je ugotavljanje ključa zelo hitro in enostavno. V kolikor napadalec dela odprtega sporočila ne pozna, lahko o njem ugiba, npr. mnogi dopisi se začnejo s »Spoštovani«. Če nima nobenih podatkov o sporočilu, je ugotavljanje uspešnosti ključa najdolgotrajnejši korak. Če ne pozna niti jezika, v katerem je napisano sporočilo, ali če gre za digitalno sliko, potem je napad z grobo silo največkrat neuspešen.

Napad z grobo silo je mogoče izvesti s strojno ali programsko opremo. Primeren je za odkrivanje tajnih ključev konstantne dolžine v simetričnih in asimetričnih kriptografskih sistemih. Ker je zelo obširen, zahteva ogromno časa in uporabo izjemno hitrih računalnikov. Napad na DES s 56-bitnim ključem bi namreč kljub uporabi danes najhitrejšega računalnika lahko trajal več sto let. Večjo računalniško moč je možno doseči z distribuirano kriptoanalizo. Iskanje ključa je razdeljeno na večje število računalnikov, ki so povezani v mrežo. Pri distribuiranem iskanju ključa vsak računalnik obravnava le del množice možnih ključev.

Tabela 2 prikazuje povprečni čas, potreben za vdor v simetričen kriptografski sistem. Uporabljena sta dva parametra: velikost ključa in hitrost preizkušanja. Če je hitrost 1 ključ/ms, pomeni, da mora računalnik v eni



Slika 1: Vrste kriptografskih napadov.

Velikost ključa	Število vseh možnih ključev	Čas za preiskavo polovice vseh možnih ključev: Hitrost dekodiranja: 1 ključ/μs	Čas za preiskavo polovice vseh možnih ključev: Hitrost dekodiranja: 10^7 ključev/μs
32 bitov	$2^{32} = 4.3 \cdot 10^9$	2^{31} μs = 35.8 min	2.15 ms
56 bitov	$2^{56} = 7.2 \cdot 10^{16}$	2^{55} μs = 1142 let	10.01 ur
128 bitov	$2^{128} = 3.4 \cdot 10^{38}$	2^{127} μs = $5.4 \cdot 10^{24}$ let	$5.4 \cdot 10^{18}$ let

Tabela 2: Povprečni čas potreben za napad z grobo silo pri dveh različnih hitrostih iskanja (Stallings 1999).

mikrosekundi generirati ključ, izvesti poskusno dešifriranje in ugotoviti uspešnost ključa. Tabela 3 prikazuje povprečni čas, ki ga potrebujejo posamezni napadalec ali skupine za preiskavo polovice vseh možnih ključev. V najslabšem primeru se seveda ti časi podvojijo.

Tabela 3 temelji na predpostavkah iz leta 1997:

- *posamezni napadalec:* samostojen računalnik z ustrezno programsko opremo. Hitrost iskanja: 2^{17}-2^{24} ključev/sekundo.
- *majhna skupina*: 16 računalnikov z ustrezno programsko opremo. Hitrost iskanja: 2^{21}-2^{24} ključev/sekundo.
- *akademsko omrežje*: 256 računalnikov z ustrezno programsko opremo. Hitrost iskanja: 2^{25}-2^{28} ključev/sekundo.
- *velike organizacije*: strojna oprema v okviru 1.000,000 USD. Hitrost iskanja: 2^{43} ključev/sekundo.
- *vojaške agencije*: strojna oprema z najnovejšo tehnologijo v okviru 1.000.000,000 USD. Hitrost iskanja: 2^{55} ključev/sekundo.

19. januarja 1999 je neprofitni organizaciji *Distributed.net*, skupaj z ustanovo EFF (Electronic Frontier Foundation), s posebnim superračunalnikom in s približno 100.000 osebnimi računalniki povezanih prek Interneta, uspelo postaviti hitrostni rekord v odkrivanju 56-bitnega DES-ovega ključa. Znan je bil tajnopis in začetek odprtega sporočila *"See you in Rome (second AES Conference, March 22-23, 1999)"*. Med 72,057,594,037,927,936 možnimi ključi jim je z akcijo *DES III Deep Crack* uspelo odkriti pravega v 22 urah in 15 minutah. Superračunalnik so zgradili na osnovi strogo namenskega čipa AWT-4500 Deep Crack, ki ga je izdelala firma AWT (Advanced Wireless Technologies). Čip se sestoji iz 24. identičnih iskalnih enot[9], ki delujejo z uro frekvence 40MHz in zmore testirati 60 milijonov ključev na sekundo (Kocher 1998). 64 takšnih čipov sestavlja, skupaj z ustrezno logiko za upravljanje, posebno matično ploščo. 29 takšnih plošč predstavlja šest računalnikov, ki skupaj s krmilnim PC računalnikom (operacijski sistem Linux) tvorijo superračunalnik. Iskanje ključa poteka torej z več kot 1800 čipi AWT-4500, hitrost iskanja superračunalnika pa znaša 90 bilijonov ključev na sekundo.

Očitno je torej, da DES ponuja le nekaj urno zaščito ob predpostavki, da je napadalcu znan del odprtega sporočila. Glede na rast procesne moči računalnikov lahko rečemo, da postaja DES na obravnavano vrsto napada vse manj odporen.

9 *Angl. search unit.*

Dolžina ključa	Posameznik napadalec	Majhna skupina	Akademsko omrežje	Velike organizacije	Vojaške agencije
40 bitov	tedni	dnevi	ure	milisekunde	mikrosekunde
56 bitov	stoletja	desetletja	leta	ure	sekunde
64 bitov	tišočletja	stoletja	desetletja	dnevi	minute
80 bitov	nemogoče	nemogoče	nemogoče	stoletja	stoletja
128 bitov	nemogoče	nemogoče	nemogoče	nemogoče	tisočletja

Tabela 3: Povprečni čas, ki ga porabi posameznik ali skupina za preiskavo polovice vseh možnih ključev (Moscaritolo 1999).

4.1.2 Diferencialna kriptoanaliza

Gre za zahteven in kompleksen napad, pri katerem ima napadalec šifrirni sistem, vendar ne pozna ključa (Ritter 2001). Šifrirni sistem napade tako, da izbira dve sorodni odprti sporočili in analizira dobljena tajnopisa. Pri tem pričakuje, da bo tudi v pripadajočih tajnopisih mogoče zaslediti podobnost, na osnovi katere bi lahko sklepal o ključu. S skrbno iterativno analizo dobljenih podatkov določi verjetnosti možnih ključev. Z najbolj verjetnim poskusi dešifrirati enega izmed tajnopisov.

4.1.3 Linearna kriptoanaliza

To je napad, pri katerem napadalec razpolaga z odprtimi sporočili, ki jih sam ne more poljubno izbirati, ter pripadajočimi tajnopisi (Ritter 2001). Do posameznih informacij o ključu pride na osnovi zadostnega števila parov odprtih sporočil in pripadajočih tajnopisov. Večje število takšnih parov poveča verjetnost uspešnega napada. Linearna kriptoanaliza sistema DES poteka tako, da poskuša napadalec na osnovi razpoložljivih parov vzpostaviti statistično linearno povezavo med vhodnimi in izhodnimi biti posamezne S-škatle[10].

Elementi diferencialne in linearne kriptoanalize so združeni v novi obliki napada, imenovani *diferencialno-linearna kriptoanaliza*[11].

4.1.4 Napad s pomočjo šibkih ključev

Znano je, da je varnost nekaterih kriptografskih sistemov odvisna tudi od vrednosti izbranega ključa. Pri nekaterih vrednostih se kriptografski sistem odzove z določenim pravilnim obnašanjem, ki lahko olajša vdor. Takim ključen pravimo šibki ključi. Odkritje šibkih ključev je zanimivo za načrtovalce kriptografskega sistema, saj lahko preprečijo, da bi si jih uporabnik izbral.

Za sistem DES so bili odkriti štirje šibki ključi (RSA Laboratories 1998). Njihov slučajni izbor povzroči enakost med šifrirnim in dešifrirnim postopkom, kar pomeni, da je rezultat dvakratnega zapovrstnega šifriranja odprtega sporočila z enim od takšnih ključev kar originalno odprto sporočilo. Verjetnost izbora takega ključa je zelo majhna (2^{-52}). Pri algoritmu IDEA lahko zasledimo cel razred ključev, ki kriptoanalizo zelo olajšajo (RSA Laboratories 1998).

4.1.5 Algebraični napadi

To je skupina tehnik, ki so uspešne v blokovnih kriptografskih sistemih, za katere je v algoritmu določena značilna matematična struktura. Algebraični napad je lahko zelo uspešen v primeru kriptografskega sistema, ki ga je mogoče razdeliti na posamezne podstrukture. Napadalec napada posamezno podstrukturo in na ta način poskuša vdreti v celotni sistem. Pojavi pa se vprašanje, ali je neki šifrirni sistem sploh mogoče predstaviti s podstrukturami. Za DES je znano, da to ni mogoče.

4.1.6 Napad s knjigo kod[12]

Napadalec zbira odprta sporočila s pripadajočimi tajnopisi, tvorjenimi z istim ključem. Ko zasledi tajnopis, ki ga ima v svoji knjigi kod, odkrije njemu pripadajoče odprto sporočilo. Tovrstni napad je primeren za napad na blokovne šifrirne sisteme, saj je le v tem primeru mogoče kontrolirati njegovo kompleksnost, ki zavisi od velikosti uporabljenih blokov in s tem števila elementov v knjigi kod.

4.2 Najpomembnejši napadi na tokovne simetrične kriptografske sisteme

Najobičajnejša varianta šifriranja s tokovnim kriptografskim sistemom je kombinacija tokovnega ključa[13] in odprtega sporočila. Tokovni ključ se generira na osnovi tajnega ključa. To je naključna sekvenca bitov, ki se na bitnem nivoju kombinira[14] z biti odprtega sporočila. Večina napadov na tovrstne sisteme je *ad hoc*, sicer pa so znani (RSA Laboratories 1998, 1995): korelacijski napad, napad na periodo tokovnega ključa, napad z linearnim pomičnim registrom s povratno zanko[15], deli in premagaj.

4.2.1 Korelacijski napad

Tokovni ključ mora izkazovati naključnost, kar pomeni, da kljub njegovemu podaljševanju napadalec ne more priti do dodatnih informacij, ki bi mu omogočile predvideti posamezne bite v naključni sekvenci - generiranem tajnopisu. Varen in zanesljiv tokovni šifrirni sistem mora prenesti številne *statistične teste*, s pomočjo katerih se ocenjuje več parametrov. Eden izmed njih je frekvenca pojavljanja posameznih bitov ali zaporednih bitnih vzorcev. Prav ti testi so osnova za t.i. *korelacijski napad*, pri katerem napadalec preverja korelacijo med bitno sekvenco v izbranem časovnem intervalu ter sekvencami izven njega. Na tej osnovi poskuša odkriti celoten tokovni ključ.

4.2.2 Napad na periodo tokovnega ključa

Tokovni ključ ima lahko tudi strukturne slabosti. Najbolj očitna je *perioda tokovnega ključa*. Gre za primere,

10 Angl. S-box – gre za tabele, s pomočjo katerih se izvaja šifriranje v sistemu DES.
11 Angl. differential-linear cryptoanalysis.
12 Angl. codebook attack.
13 Angl.keystream.
14 Običajno se izvaja logična operacija XOR.
15 Angl. linear feedback shift register.

pri katerih prihaja do prehitrih ponovitev določenega število bitov v tokovnem ključu. Razlog za to je prekratek tokovni ključ. Napadalec poskuša odkriti določen del tokovnega ključa - periodo, ki bi mu omogočil dešifrirati določene dele tajnopisa. Tovrstni napad opozarja, da je pri načrtovanju tokovnih šifrirnih sistemov treba paziti na minimalno periodo tokovnega ključa ali izbrati ustrezno vrednost njene spodnje meje.

4.2.3 Napad z linearnim pomičnim registrom s povratno zanko

Določene strukturne slabosti so lahko celo tako velike, da ponujajo napadalcu možnosti iskanja alternativnih poti za generiranje dela tokovnega ključa ali tokovnega ključa v celoti. Vodilni tovrstni pristop, ki omogoča reprodukcijo (izdelavo kopij) tokovnih ključev, je uporaba *linearnega pomičnega registra s povratno zanko*. Ta deluje tako, da na svojem vhodu prebere končno sekvenco bitov, na izhodu pa to sekvenco ponovno generira. Pri tem je pomembna dolžina registra, od katere zavisi dolžina prebrane ter kasneje ponovno generirane sekvence.

Varnost šifrirnega sistema se meri na osnovi *linearne kompleksnosti* sekvence, ki je določena z velikostjo linearnega pomičnega registra s povratno zanko, potrebnega za reprodukcijo te iste sekvence. Tokovni šifrirni sistem mora imeti torej čim večjo linearno kompleksnost.

4.2.4 Deli in premagaj

Razen iskanja ključa s pomočjo napada z grobo silo je znan tudi razred napadov, ki jih lahko opišemo z izrazom *deli in premagaj*[16]. V primeru tokovnih šifrirnih sistemov gre za napad na tokovni ključ, ki se generira na osnovi izbranega tajnega ključa. Napadalec uspe zajeti del tokovnega ključa in na osnovi tega prične z ugotavljanjem celotnega tajnega ključa. Z grobo silo napada posamezne dele tajnega ključa, pri čemer poskuša identificirati tisti del, ki ima zelo očiten in neposreden učinek na generiran tokovni ključ. Napad je tem uspešnejši, čim bolj se napadalcev tokovni ključ ujema z dejansko prisotnim tokovnim ključem. Rezultati napada *deli in premagaj* so lahko v pomoč tudi pri izvajanju zelo hitrih in učinkovitih korelacijskih napadov.

4.3 Najpomembnejši napadi na asimetrične kriptografske sisteme

Nekateri najpomembnejši napadi na asimetrične kriptografske sisteme so: napad z grobo silo, napad na zasebni ključ, vrinjeni posrednik[17] (MITM), časovni napad[18].

4.3.1 Napad z grobo silo

Podobno kot simetrične je tudi asimetrične kriptografske sisteme možno učinkovito napasti z grobo silo. Protiukrep je tudi tukaj enak: uporabiti je treba čim daljše ključe. Sistemi z javnimi ključi temeljijo na inverznih matematičnih funkcijah, katerih računska kompleksnost ne narašča linearno z dolžino ključa, ampak običajno precej hitreje. Ključ mora biti dovolj dolg, da napad z grobo silo ni praktičen, po drugi strani pa dovolj kratek, da sta šifriranje in dešifriranje dovolj hitra.

4.3.2 Napad na zasebni ključ

Napadalec poskuša na osnovi znanega javnega ključa generirati pripadajoči zasebni ključ. Ta napad je izredno zahteven, saj je povezava med javnim in zasebnim ključem zelo zapletena. Pri sistemu RSA temelji tovrstna povezava na faktoriranju velikih praštevil, kar je izredno dolgotrajen postopek.

4.3.3 Vrinjeni posrednik

To je napad, kjer se napadalec (oseba C) pojavlja kot posrednik (man-in-the middle) med pošiljateljem (oseba A) in prejemnikom (oseba B). Če želi zavzeti vlogo posrednika, mora imeti možnost prestrezanja sporočila, ki je namenjeno osebi B. Princip napada je naslednji: napadalec objavi svoj javni ključ in se pri tem izdaja za osebo B. Kadar želi oseba A poslati šifrirano sporočilo osebi B, uporabi njen javni ključ, ki pa je dejansko ključ napadalca - osebe C. Na ta način napadalec sprejema šifrirana sporočila, ki jih lahko brez težav dešifrira s svojim zasebnim ključem. Ko prebere sporočilo, ga šifrira s pravim javnim ključem osebe B in ji ga pošlje. Tovrstni napad se preprečuje s t.i. *potrditvijo* javnega ključa.

4.3.4 Časovni napad

Gre za zelo sodoben, računsko nezahteven in precej neopazen napad. Šifriranje različnih sporočil običajno traja različno dolgo. Če lahko napadalec meri čas, potreben za izvajanje šifrirne operacije, lahko pride na osnovi ponovljivih meritev in z uporabo verjetnosti in statistike, do pomembnih informacij o tajnem ključu, s katerimi se opravljajo šifrirni izračuni. Časovni napad je posebej nevarna oblika napada, saj zahteva le tajnopis. Deluje dobro tudi, če meritve niso posebej natančne. Uporablja se pri napadih na RSA, Diffie-Hellmanovo metodo in metode, ki temeljijo na

16 Angl. *divide and conquer.*
17 Angl. *man-in-the middle*
18 Angl. *timing attack.*

eliptičnih funkcijah. Proti časovnim napadom na RSA sta predlagana dva načina obrambe: dodajanje naključnih zakasnitev v računski del algoritma in dodatno predhodno šifriranje z nekim drugim algoritmom.

5. Sklep

Za absolutno preprečitev napadov bi bilo treba zagotoviti stalno fizično zaščito celotnega komunikacijskega sistema, kar pa je večinoma nemogoče (npr. internet, telefonsko omrežje,...). Dejavnosti, ki jih lahko uporabimo za reševanje opisane problematike, lahko razdelimo v naslednje kategorije: fizična preprečitev dostopa, odkrivanje napada, onemogočanje napada. Z zaščitnimi strežniki lahko zavarujemo lokalni del omrežja pred zunanjimi napadalci. Če smo zaznali napad in imamo tudi varnostne kopije sporočil, potem je možna tudi njihova rekonstrukcija.

Vsaka informacija o kriptografskem sistemu in sporočilu pomaga napadalcu. Vrsta napada je odvisna od količine in vrste napadalcu razpoložljivih sporočil, njegovega znanja in računalniške podpore. S prikrivanjem nekaterih podatkov o kriptografskem sistemu in sporočilu lahko povečujemo varnost kriptografskega sistema. Praviloma bo do napada prišlo, ko bo napadalec ocenil, da so stroški vdora (dešifriranja) manjši od koristi dešifriranega sporočila. Ker vrednost sporočila s časom pada, mora oceniti tudi, koliko časa potrebuje.

Ker se bosta kriptoanaliza in hitrost računalnikov neprestano dvigovala na višjo raven, bo treba tudi neprestano vzdrževanje kriptografskih sistemov, če želimo ohranjati potrebno varnost.

LITERATURA

[1] N. Pavešić (1997): *Informacija in kodi*, Univerza v Ljubljani

[2] W. Stallings (1999): *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice-Hall

[3] T. Dogša (1993): *Verifikacija in validacija programske opreme*, Tehniška fakulteta Maribor

[4] Vinnie Moscaritolo (1999): *http//www.vmeng.com/vinnie/crypto.html*

[5] N. F. Johnson, S. Jajodia (1998): *Exploring Steganography: Seeing the Unseen*, IEEE Computer, februar 1998, str.26-34

[6] Paul C. Kocher (1998): *Breaking DES*, RSA Laboratories' CryptoBytes vol. 4, Number 2, Winter 1998

[7] Terry Ritter (2001): *Research Comments from Ciphers By Ritter: http://www.ciphersbyritter.com/*

[8] RSA Laboratories (1998): *Frequently asked Question About Todays Cryptography* v4.0

[9] RSA Laboratories (1995): Technical Report TR-701: *Stream Ciphers*, July 1995

◆

Matej Šalamon je diplomiral leta 1994 in magistriral leta 1999 na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer je tudi zaposlen kot asistent za področje elektronike. Na raziskovalnem področju se ukvarja predvsem s kaotičnimi in kriptografskimi sistemi.

◆

Tomaž Dogša je docent na mariborski Fakulteti za elektrotehniko, računalništvo in informatiko, kjer predava na dodiplomski in podiplomski stopnji in vodi Center za verifikacijo in validacijo sistemov. Na raziskovalnem področju se ukvarja predvsem s preverjanjem programske opreme.

POSLOVNO MODELIRANJE Z UML

Mateja Izlakar, SKB banka d.d, Mateja.Izlakar@skb.si
Marjan Krisper, Fakulteta za računalništvo in informatiko, Marjan.Krisper@fri.uni-lj.si

Izvleček

Sistem za ravnanje z dokumenti, imenovan Document Management System (DMS), v SKB banki deluje že nekaj časa. Pred uvedbo samega sistema so bile definirane funkcionalnosti, ki jih mora sistem vsebovati in postavljen je bil koncept njegovega razvoja, delovanja in uporabe. V prispevku je predstavljen z uporabo diagramov UML razvojni cikel, ki vodi od definiranja potreb po uvedbi sistema do ciljev, ki jih želimo doseči, od procesa razvoja DMS in uvedbe storitev vanj do natančnejših opisov primerov uporabe in posameznih procesov, ki združujejo funkcionalnosti sistema in predstavljajo njegovo celotno delovanje. Predstavljene so tudi povezave med DMS in informacijskim sistemom banke.

Abstract

Business Modeling with UML

A Document Management System (DMS) has already been implemented in SKB Bank for some time. Before the process of implementation all the functions, which should be included into the system, were clearly defined as well as the concept of development, activity and usage of the system. In the paper UML diagrams are used to introduce the whole development cycle of the DMS: from defining user needs to goals which should be achieved with the system implementation, from the process of development of the DMS process and implementation of different services to specifications of use cases and individual processes, which join different functions of the DMS and represent its full operation. Also, the connections between the DMS and the information system of the bank are presented.

1 UVOD

V sodobnem poslovanju se srečujemo z najrazličnejšimi računalniškimi podporami poslovanju. Večina teh podpor, informacijskih sistemov ali posameznih aplikacij, je namenjena ravnanju s podatki in informacijami. Na drugi strani pa se predvsem v obdobju podpiranja in avtomatizacije procesov srečujemo z dejstvom, da je proces mogoče učinkovito podpreti le, če obstaja informacijski sistem, v katerem so shranjeni podatki, ki se pretvarjajo v informacije, in sistem, ki omogoča delo z dokumenti. Zato je uvedba podpor za ravnanje z dokumenti, ki vključuje zajemanje, avtomatizirano obdelavo in arhiviranje dokumentov na elektronskih nosilcih postala potreba, močno izražena predvsem v okoljih, kjer obstajajo velike količine istovrstnih dokumentov.

Sodobni sistemi za ravnanje z dokumenti (Document Management System, DMS) ne omogočajo le skeniranja dokumentov in arhiviranja njihovih slik, temveč predvsem prepoznavanje podatkov na dokumentih, kar daje osnovo za njihovo nadaljnjo obdelavo. Zajemanje - skeniranje dokumentov je proces pretvarjanja dokumenta v papirni obliki v sliko dokumenta v elektronski obliki, največkrat v formatu PDF ali TIFF. Ta proces vključuje tudi indeksiranje dokumentov, da jih je kasneje mogoče poiskati, prikazati na ekranu ali natisniti. Zajemanje podatkov pa je proces, ki omogoča avtomatsko zbiranje informacij iz podatkov, prepoznanih na slikah skeniranih dokumentov. Tehnologiji ICR in OCR, ki ta proces omogočata, sta bistvenega pomena pri obdelavi dokumentov, saj dandanes omogočata zelo dobro in natančno prepoznavanje posameznih znakov, ne glede na to, ali so dokumenti izpolnjeni strojno ali ročno. To pomeni, da je ročnega dela pri popravljanju dvomljivo prepoznanih podatkov zelo malo. Avtomatsko prepoznavanje podatkov z dokumentov omogoča avtomatizacijo dela na področjih, kjer je bilo prej potrebno podatke z dokumentov v papirni obliki ročno vnašati v za to namenjene računalniške podpore. Podatke s slik skeniranih dokumentov je tako mogoče obdelovati, jih posredovati v informacijski sistem podjetja ali v posamezne aplikacije. Ne gre več zgolj za arhiv v elektronski obliki, ki nadomešča papirnega, temveč za celoten proces obdelave dokumenta od prejema le-tega v izvorni obliki prek avtomatske obdelave podatkov do njegovega arhiviranja. Slike dokumentov so lahko - prav tako kot aplikacije in drugi viri podatkov - vključene v »workflow« sistem, če ta obstaja.

Sodobni sistemi za ravnanje z dokumenti so zasnovani decentralizirano. To pomeni, da se enostavnejše funkcionalnosti, kot je skeniranje dokumentov, izvajajo na različnih mestih. Slike skeniranih dokumentov se nato po računalniškem omrežju pošljejo v centralno enoto, kjer se centralizirano izvajajo zahtevnejše funkcionalnosti, kot je prepoznavanje slik dokumentov, popravljanje podatkov v dvomljivo prepoznanih podatkovnih poljih, obdelava podatkov, prepoznanih z dokumentov ter arhiviranje podatkov in dokumentov.

Takšna organizacija dela se je v praksi izkazala za učinkovitejšo in stroškovno ugodnejšo. Možnost napak je manjša, saj zahtevnejše funkcionalnosti sistema uporablja ožja skupina rutiniranih operaterjev, ki svoje delo dobro obvladajo. Tudi nadzor nad delovanjem tako organiziranega sistema je boljši ter odzivni časi vzdrževalcev v primeru težav so krajši. Centralizirano arhiviranje dokumentov je varnejše in bolj učinkovito.

Ko govorimo o dokumentih, ki jih skeniramo, prepoznavamo, obdelujemo in arhiviramo na elektronskih nosilcih, mislimo največkrat na vhodne dokumente, torej na dokumente, ki jih podjetja prejemajo od svojih strank. Pod pojmom DMS pa lahko razumemo tudi sistem, ki skrbi za ravnanje z vsemi vrstami dokumentov, tudi tistimi, ki nastanejo v podjetju, ostanejo v podjetju ali pa postanejo izhodni dokumenti, poslani strankam. Popoln DMS bi skrbel za zajemanje vseh vrst dokumentov, skeniranih in tistih, ki nastanejo v podjetju z uporabo različnih orodij, tudi za elektronsko pošto ter vsebino spletnih strani, za njihovo obdelavo, shranjevanje, iskanje in distribucijo. Prihranki tako pri stroških kot tudi pri času, zdaj porabljenem za iskanje in reprodukcijo dokumentov, so lahko v primeru uvedbe takega sistema izredno veliki. Če želimo obvladovati celotne življenjske cikle dokumentov, je za celotno podporo takemu ravnanju z dokumenti potrebna kombinacija DMS in »workflow« sistemov, ki skupaj pomenita korak od delnih rešitev k celotnemu, enovitemu sistemu.

2 SISTEM ZA RAVNANJE Z DOKUMENTI V SKB BANKI

DMS v osnovi sestavljata strojna oprema in programska oprema. Pomemben del strojne opreme poleg strežnikov in delovnih postaj so skenerji, s pomočjo katerih zajemamo dokumente v sistem in tako pretvorimo sliko na papirju v elektronsko obliko.

Programska oprema, ki je sestavni del DMS, ni splošno namenska, temveč je izdelana po naročilu na podlagi zahtev naročnika. Po namenu je razdeljena v tri osnovne sklope: programsko opremo, namenjeno samemu skeniranju dokumentov, programsko opremo, ki omogoča prepoznavanje in popravljanje podatkov s slik skeniranih dokumentov ter obdelavo podatkov in programsko opremo, ki omogoča arhiviranje dokumentov na elektronske nosilce.

DMS je, tako kot druge računalniške podpore, namenjen nadomestitvi ročnega dela z avtomatiziranim. Njegova največja uporabnost se torej pokaže v primerih:

- ko imamo opraviti z velikimi količinami istovrstnih dokumentov, ki jih je treba učinkovito obdelati in arhivirati in
- ko potrebujemo hiter dostop do arhiviranih dokumentov v primeru reklamacij in poizvedb, da lahko stranki odgovorimo na njeno zahtevo v najkrajšem možnem času.

Vloga DMS pri njegovi uporabi v banki je tudi v tem, da podatkov o transakcijah z dokumentov v papirni obliki ni treba ročno vnašati v aplikacije, ampak je obdelava dokumentov v največji možni meri avtomatizirana. Funkcionalni deli sistema, ki to omogočajo, so naslednji:

- zajemanje (skeniranje) dokumentov,
- prepoznavanje podatkovnih polj na slikah skeniranih dokumentov,
- vnašanje popravkov v primeru nepopolne ali dvomljive prepoznave podatkov,
- pripravo podatkov za izvedbo transakcij in
- arhiviranje dokumentov na elektronske nosilce.

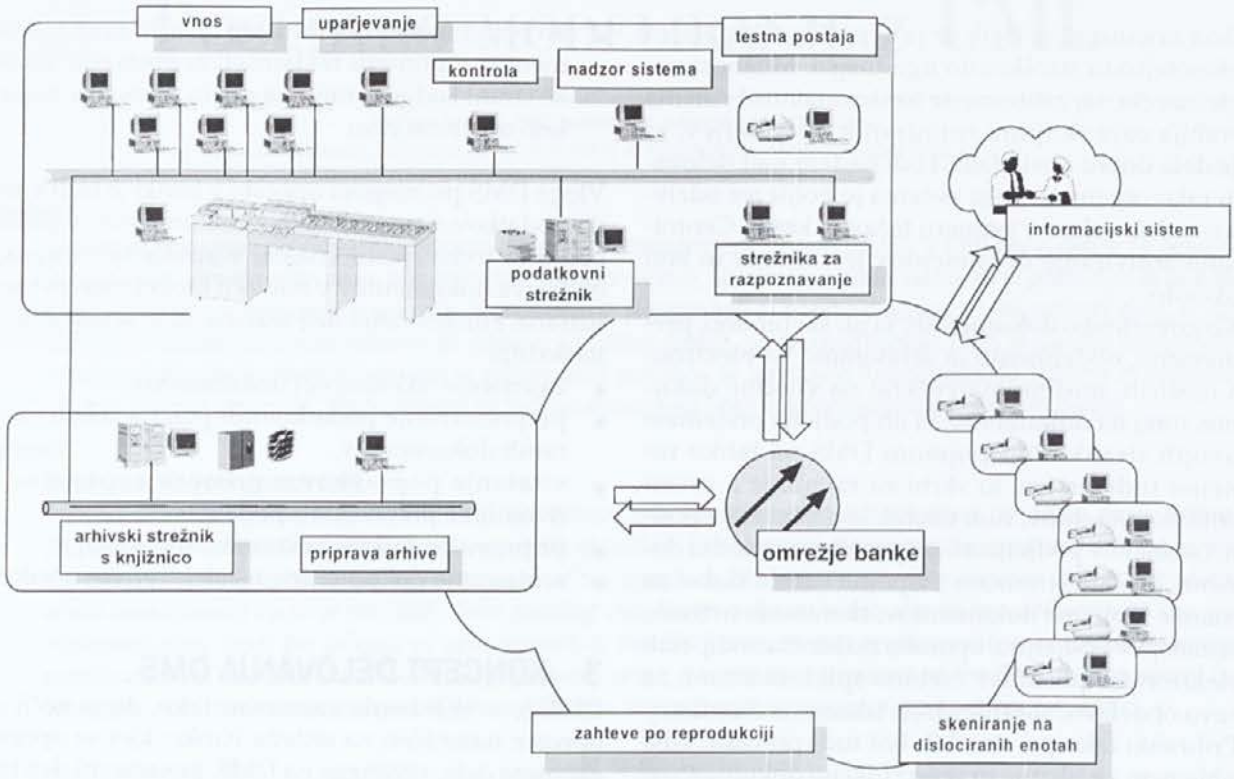
3 KONCEPT DELOVANJA DMS

DMS je v SKB banki zasnovan tako, da je večji del opreme nameščen na sedežu banke, kjer se opravlja glavnina dela, vezanega na DMS, posamezni deli tako strojne kot programske opreme pa so nameščeni v poslovalnicah banke. Dokumenti se zajemajo na sedežu banke in v poslovalnicah banke, prepoznavanje podatkovnih polj, vnašanje popravkov v dvomljivo prepoznana podatkovna polja, priprava podatkov za izvedbo transakcij in arhiviranje dokumentov na elektronske nosilce pa se izvajajo le na sedežu banke. Prav tako je zahteve za informacije ali reklamacije mogoče podati v tudi poslovalnicah banke, samo iskanje dokumentov pa se izvaja na sedežu banke.

Iz navedenega (slika 1) lahko vidimo, da se glavnina dela opravlja v obračunskem centru banke. Zakaj tako? Če bi hoteli vse funkcionalnosti DMS izvajati v poslovalnicah banke, bi morali poslovalnice opremiti z dodatno strojno in programsko opremo. To bi na eni strani občutno povečalo stroške sistema, na drugi strani pa bi zaposleni v poslovalnicah morali obvladati celotno delovanje sistema in izvajati vse njegove funkcionalnosti, kar bi povečalo obremenitev zaposlenih, ne pa poenostavilo njihovega dela. Bolj učinkovito je, da to delo opravlja skupina rutiniranih operaterjev na enem mestu v banki.

Delovanje DMS in njegove povezave z uporabniki na eni strani in drugimi sistemi na drugi strani lahko prikažemo v konceptualnem modelu. Bistveni koncepti, razvidni iz modela, so naslednji:

- dokument: predstavlja vhod v DMS in je v njem obdelan; odvisno od tipa dokumenta je le-ta lahko skeniran le za arhivo ali pa je v sistem zajet z namenom, da se na podlagi prepoznanih podatkov avtomatsko izvedejo transakcije;



Slika 1: Koncept delovanja DMS v SKB banki

- slika dokumenta: nastane s skeniranjem dokumenta ter predstavlja osnovo za prepoznavanje podatkov; slika dokumenta je arhivirana;
- podatki o dokumentu: pridobljeni so z razpoznavo s slike dokumenta in so osnova za izvedbo transakcij; podatki o dokumentu so arhivirani skupaj s sliko dokumenta;
- arhiv: arhivirane slike skeniranih dokumentov skupaj s pripadajočimi podatki;
- DMS sistem: strojna in programska oprema, namenjena obdelavi in ravnanju z dokumenti.

4 OBDELAVA DOKUMENTOV V SISTEMU

DMS najbolj služi obdelavi velikih količin istovrstnih dokumentov. To so dokumenti, izdelani na podlagi predpisanih, poenotenih obrazcev. Izgled dokumenta je torej vedno enak, njegova velikost, barva in razmestitev polj za vnos podatkov se ne spreminjajo, spreminja se le vsebina dokumenta. Primeri takih dokumentov, ki jih v banki dnevno obdelujemo v velikih količinah, so posebne položnice, posebne nakaznice, plačilni nalogi in čeki. Obdelavo teh vrst dokumentov smo najprej uvedli v sistem.

Primeri uporabe DMS sistema v SKB banki so predstavljeni v naslednjem diagramu uporabe:

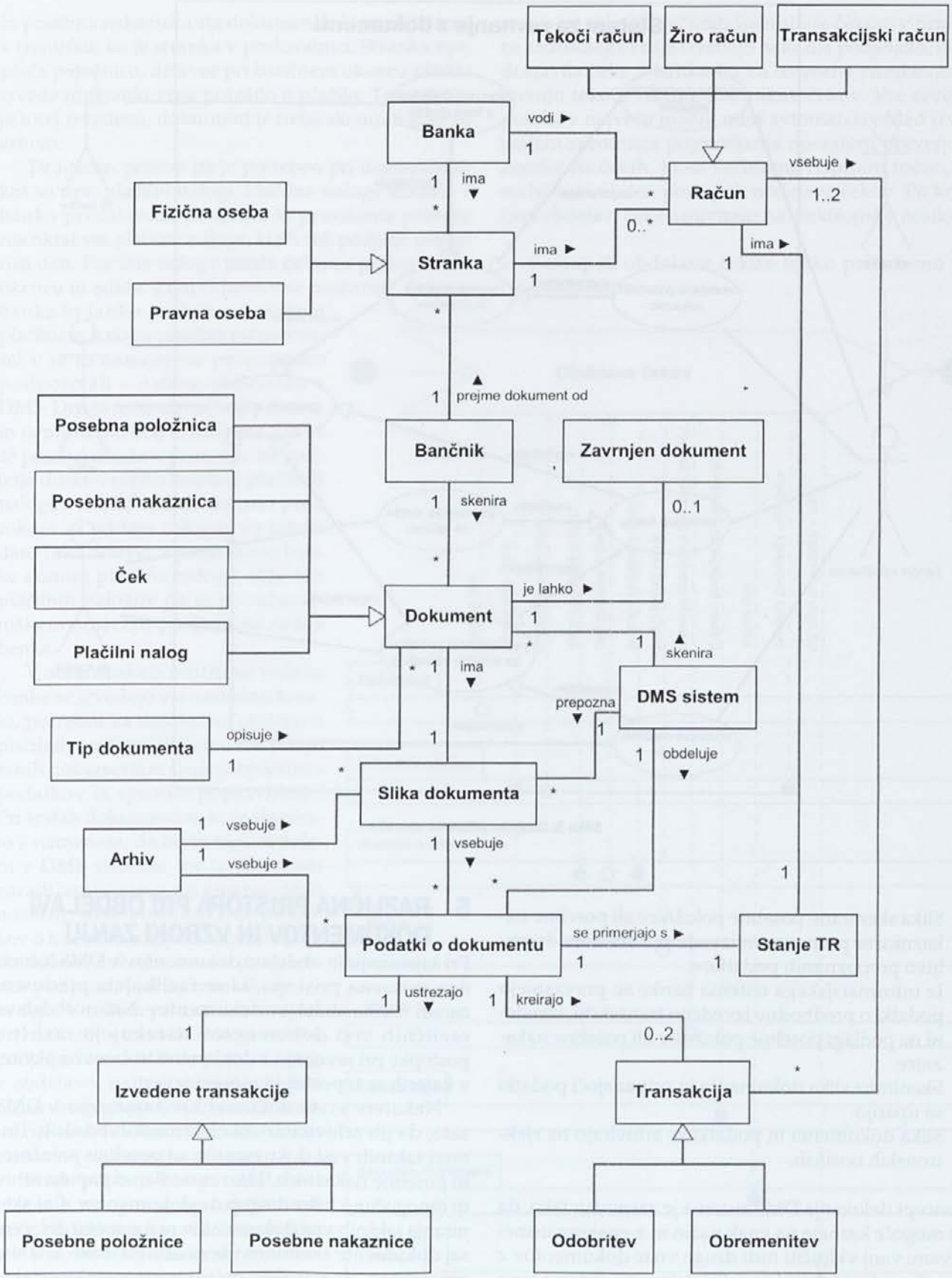
Kot je razvidno iz diagrama, obstajajo trenutno štirje osnovni primeri uporabe DMS:

- obdelava posebnih položnic
- obdelava posebnih nakaznic
- obdelava čekov in
- obdelava plačilnih nalogov.

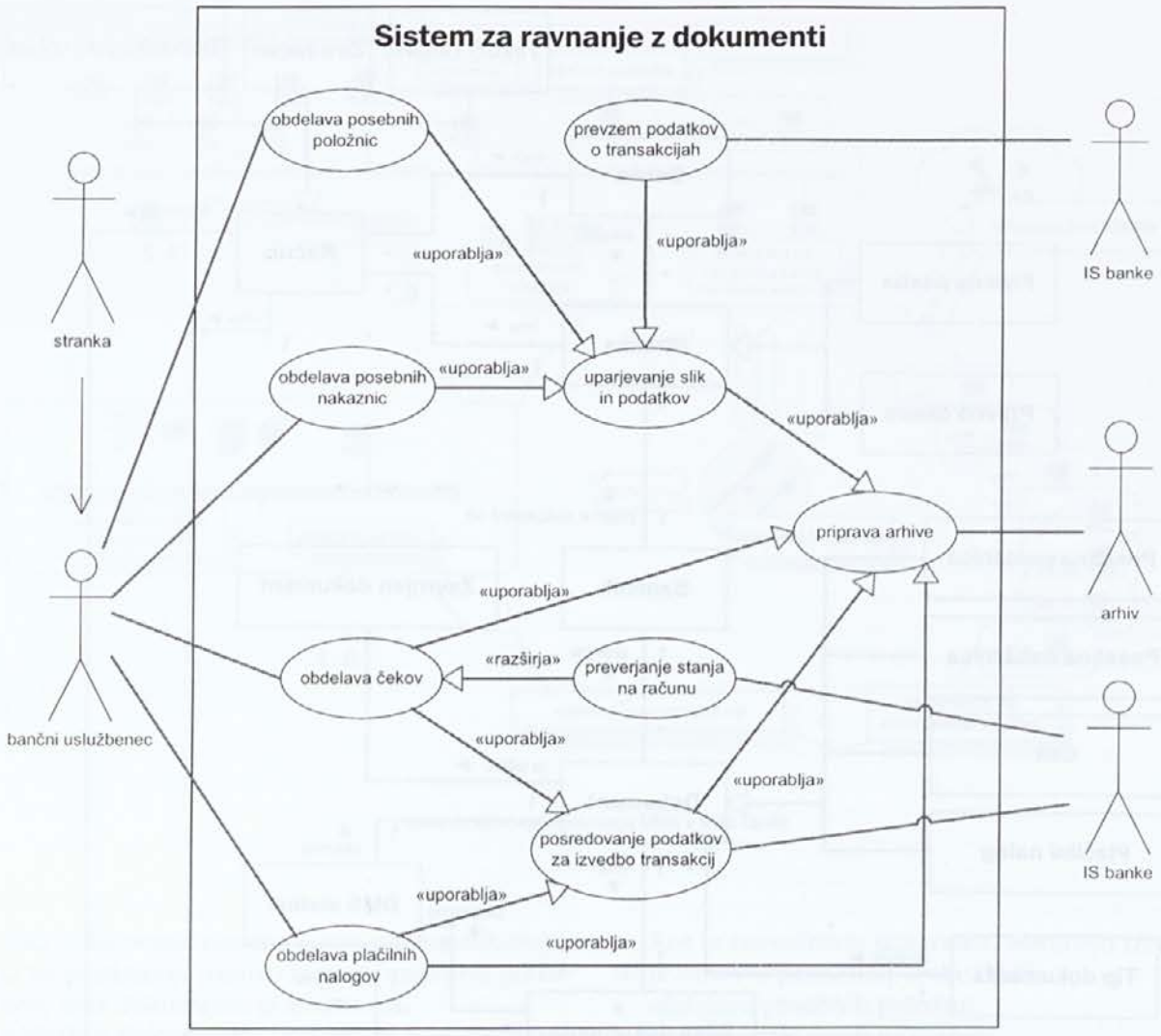
Za predstavitev in natančnejši opis posameznih primerov uporabe lahko uporabimo različne pristope in različne vrste diagramov UML. Primera uporabe »obdelava posebnih položnic« in »obdelava posebnih nakaznic«, ki sta pravzaprav enaka, saj gre le za dva različna dokumenta, ki se v DMS obdelujeta na povsem enak način, bomo predstavili z besednim opisom. Primera uporabe »obdelava čekov« in »obdelava plačilnih nalogov« bosta v nadaljevanju predstavljena z diagrami UML.

Primera uporabe »obdelava posebnih položnic« in »obdelava posebnih nakaznic« lahko opišemo na naslednji način:

- Stranka dostavi v banko posebno položnico, na podlagi katere se izvede plačilo ali posebno nakaznico, na podlagi katere se izvede nakazilo. Posebno položnico ali posebno nakaznico je po obdelavi treba arhivirati, zato se obdela v DMS.
- Bančni uslužbenec skenira posebno položnico ali posebno nakaznico.



Slika 2: Konceptualni model



Slika 3: Diagram primerov uporabe

- Slika skenirane posebne položnice ali posebne nakaznice se prepozna in izvede se korektura dvomljivo prepoznanih podatkov.
- Iz informacijskega sistema banke se prevzamejo podatki o predhodno izvedeno transakciji, izvedeni na podlagi posebne položnice ali posebne nakaznice.
- Skenirana slika dokumenta in pripadajoči podatki se uparijo.
- Slika dokumenta in podatki se arhivirajo na elektronskih nosilcih.

Koncept delovanja DMS sistema je zasnovan tako, da bo mogoče kasneje na enak način in z enakimi usmeritvami vanj vključiti tudi druge vrste dokumentov z drugih področij dela. Filozofija delovanja sistema torej ostaja enaka, spreminjajo in dodajajo se le vrste dokumentov.

5 RAZLIČNA PRISTOPA PRI OBDELAVI DOKUMENTOV IN VZROKI ZANJU

Pri zajemanju in obdelavi dokumentov v DMS ločimo dva osnovna pristopa, ki se razlikujeta predvsem zaradi načina obdelave dokumentov. Načini obdelave različnih vrst dokumentov narekujejo različne postopke pri ravnanju z dokumenti in časovne okvire, v katerih se ti postopki morajo izvesti.

Nekatere vrste dokumentov zajamemo v DMS zato, da jih arhiviramo na elektronskih nosilcih. Primeri takšnih vrst dokumentov so posebne položnice in posebne nakaznice. Tako zmanjšamo papirni arhiv in omogočimo hiter dostop do dokumentov. Čas skeniranja takšnih vrst dokumentov ni natančno določen, saj dokumente skeniramo le za arhivo. Tako si lahko privoščimo, da posebne položnice in posebne nakaznice, ki smo jih obdelali tekom dneva, naslednji dan zložimo v pakete in jih skeniramo. Posebna položnica

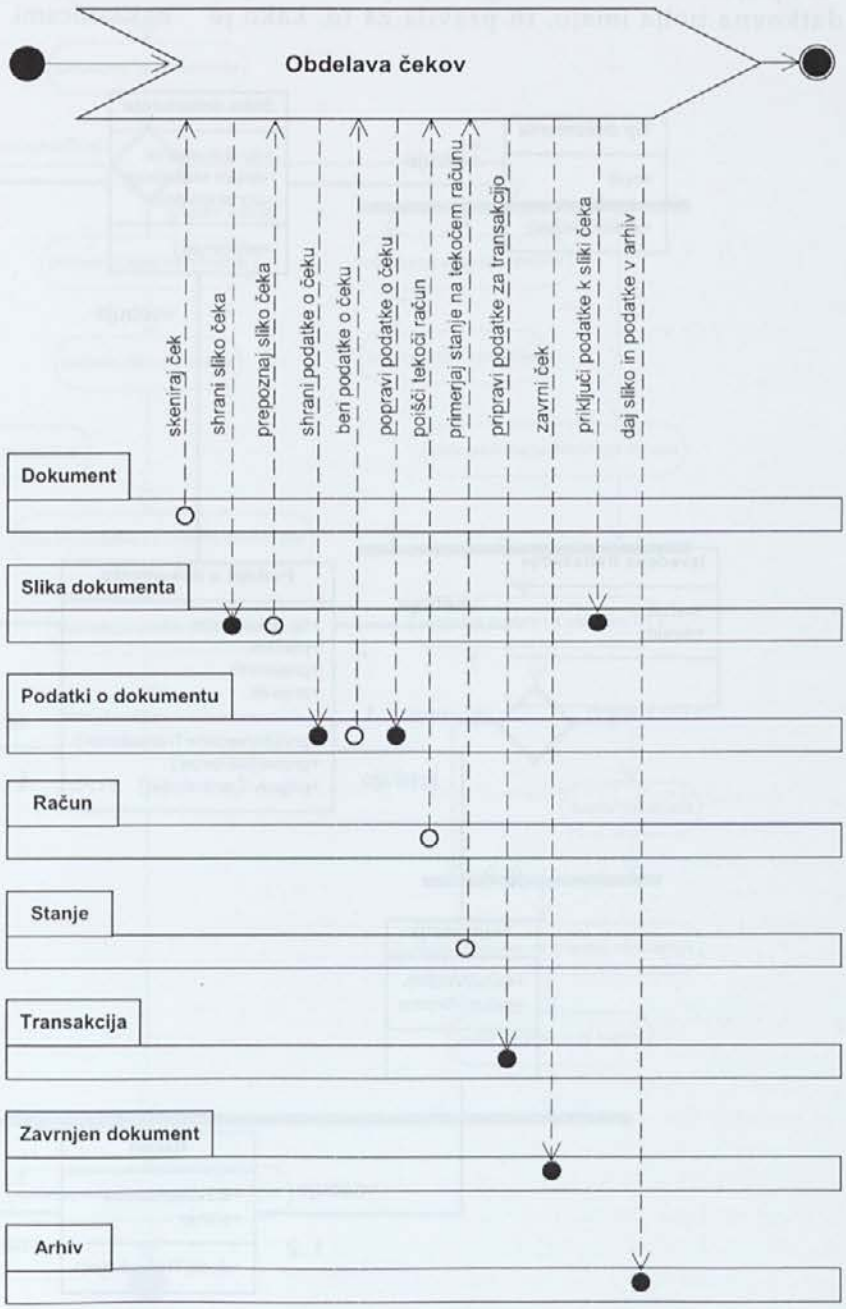
in posebna nakaznica sta dokumenta, ki ju obdelamo v trenutku, ko je stranka v poslovalnici. Stranka npr. plača položnico, delavec pri bančnem okencu plačilo izvede in stranki vrne potrdilo o plačilu. Transakcija je torej izvedena, dokument je treba skenirati le še za arhivo.

Drugačen pristop pa je potreben pri dokumentih kot so npr. plačilni nalogi. Plačilne naloge dostavi v banko predstavnik podjetja, ki praviloma prinese naenkrat vse plačilne naloge, ki jih želi podjetje plačati tisti dan. Plačilne naloge preda delavcu pri bančnem okencu in odide. Zdaj bi imeli dve možnosti: delavec banke bi lahko podatke o vsakem plačilnem nalogu posebej ročno vnesel v za to namenjeno programsko podporo ali – naloge obdelamo v DMS. Druga možnost je bolj prijazna in neprimerno bolj učinkovita, kar se še posebej izkaže v primerih, ko podjetje dostavi veliko količino plačilnih nalogov skoraj zadnjo minuto pred rokom za oddajo nalogov za tekoči dan. Tako delavec v poslovalnici banke skenira plačilne naloge, slike teh plačilnih nalogov pa se po računalniškem omrežju pošljejo na sedež banke.

V obračunskem centru na sedežu banke se izvedejo vsi naslednji koraki, potrebni za dokončno obdelavo plačilnih nalogov. Prejemu slik skeniranih dokumentov sledi prepoznava podatkov in sprotno popravljanje. Pri vrstah dokumentov, ki se skenirajo z namenom, da bodo tudi obdelani v DMS sistemu, ne le skenirani zaradi arhiviranja na elektronskih nosilcih, sledi posredovanje podatkov o transakcijah, pridobljenih s slik skeniranih dokumentov, v programsko podporo, kjer se transakcije izvedejo. V našem primeru se torej izvrši nakazilo s transakcijskega računa podjetja, ki je dostavilo plačilni nalog v obdelavo, na transakcijski ali žiro račun drugega podjetja. Izvedbi transakcije sledi še arhiviranje slike dokumenta na elektronske nosilce.

Enak pristop kot pri obdelavi plačilnih nalogov je uporabljen tudi pri v obdelavi čekov. Glavna razlika je v tem, da čeke, s katerimi so stranke plačale blago ali storitve, podjetja pošiljajo po pošti v obračunski center banke. Tam čeke skenirajo, preverijo stanja na tekočih računih imetnikov čekov, v primeru zadostnega kritja izvedejo nakazila podjetjem, ki so dostavila čeke v banko ter za ustrezne zneske obremenijo tekoče račune imetnikov čekov. Vse seveda poteka v največji možni meri avtomatsko. Med izvajanjem sprotnega popravljanja operaterji preverjajo zneske na čekih, ki so večinoma napisani ročno, in nadzirajo celoten postopek obdelave čekov. Po končani obdelavi čeke arhivirajo na elektronske nosilce.

Postopek obdelave čekov lahko prikažemo na naslednji način:



Slika 4: Proces obdelave čekov

6 STRUKTURA SISTEMA

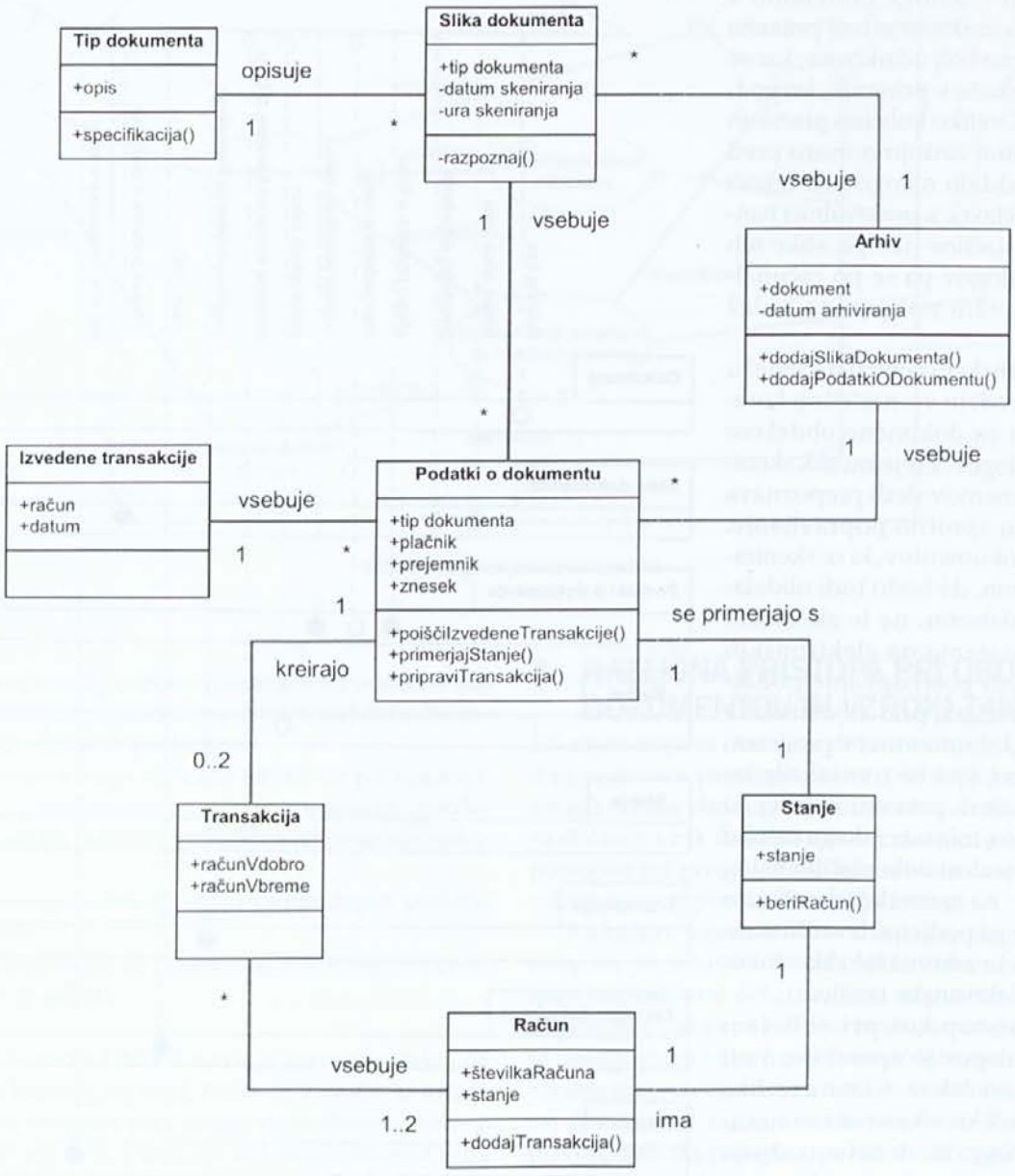
Struktura sistema DMS, ki služi kot osnova za razvoj programske opreme in uvedbo novega dokumenta ali nove storitve, je prikazana v razrednem diagramu (slika 5):

V razrednem diagramu so prikazani razredi, ki predstavljajo in sestavljajo programsko opremo sistema DMS.

Vsak dokument je določen s tipom dokumenta. Tip dokumenta definira strukturo dokumenta. Glede na določeni tip dokumenta se izvede celotna obdelava dokumenta. V tipu dokumenta je opisana razmestitev polj na dokumentu, vloge, ki jih posamezna podatkovna polja imajo, in pravila za to, kako je posamezna podatkovna polja treba obdelati. Podana so torej pravila igre, ki jim obdelava dokumenta mora slediti.

Pri tako zasnovani strukturi bo v prihodnosti, ko se bo pojavil nov tip dokumenta, za katerega bo določeno, da se bo obdeloval v DMS, enostavno dodajati nove vrste dokumentov. V razredu »tip dokumenta« je namreč navedeno vse, kar je potrebno vedeti o dokumentu in načinu njegove obdelave.

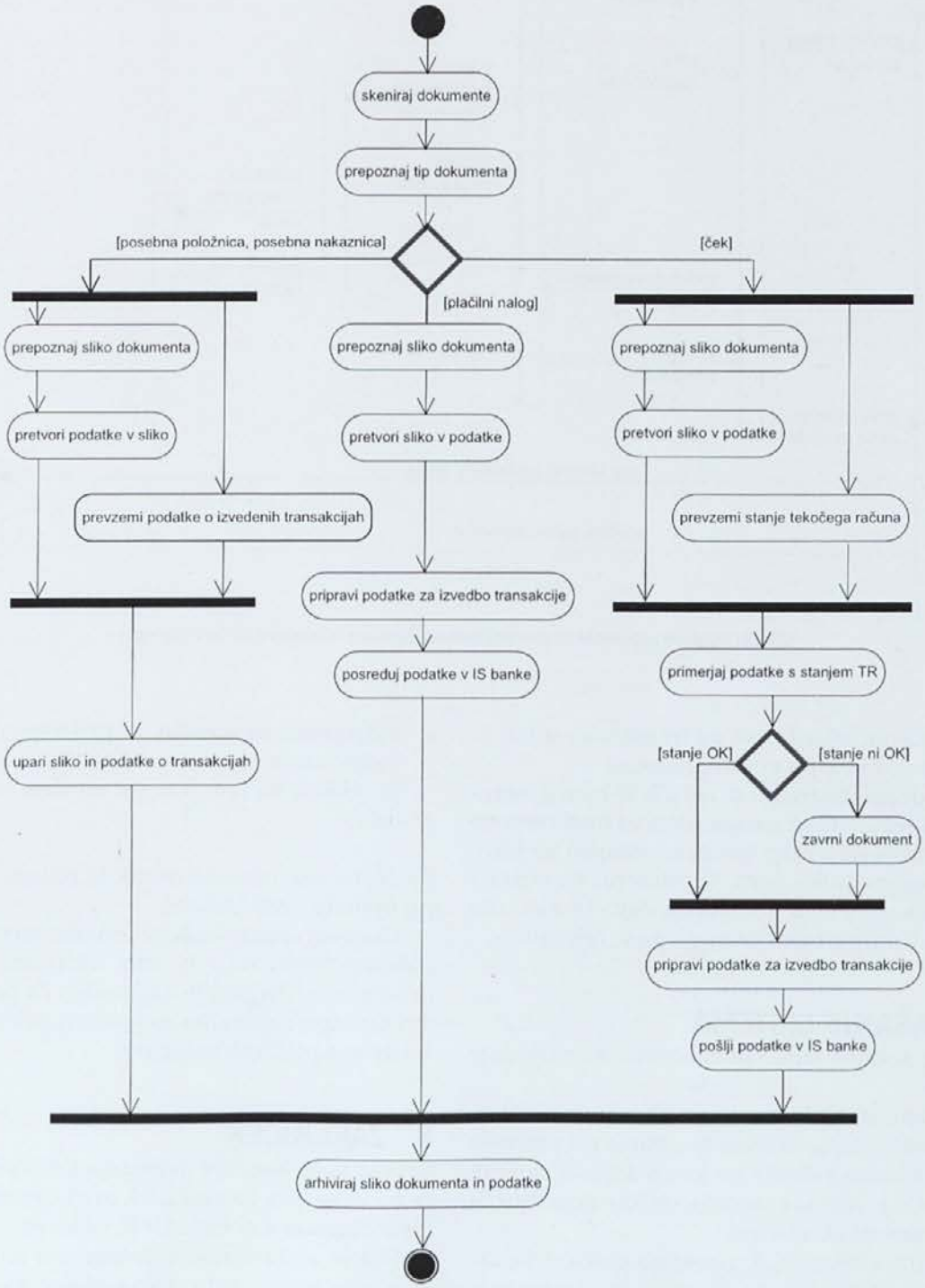
Povezave med DMS in informacijskim sistemom banke so razvidne iz štirih razredov. V razredu »izvedene transakcije« so zbrani podatki o že izvedenih transakcijah s posebnimi položnicami in posebnimi nakaznicami. Ti dve vrsti dokumentov sta namreč



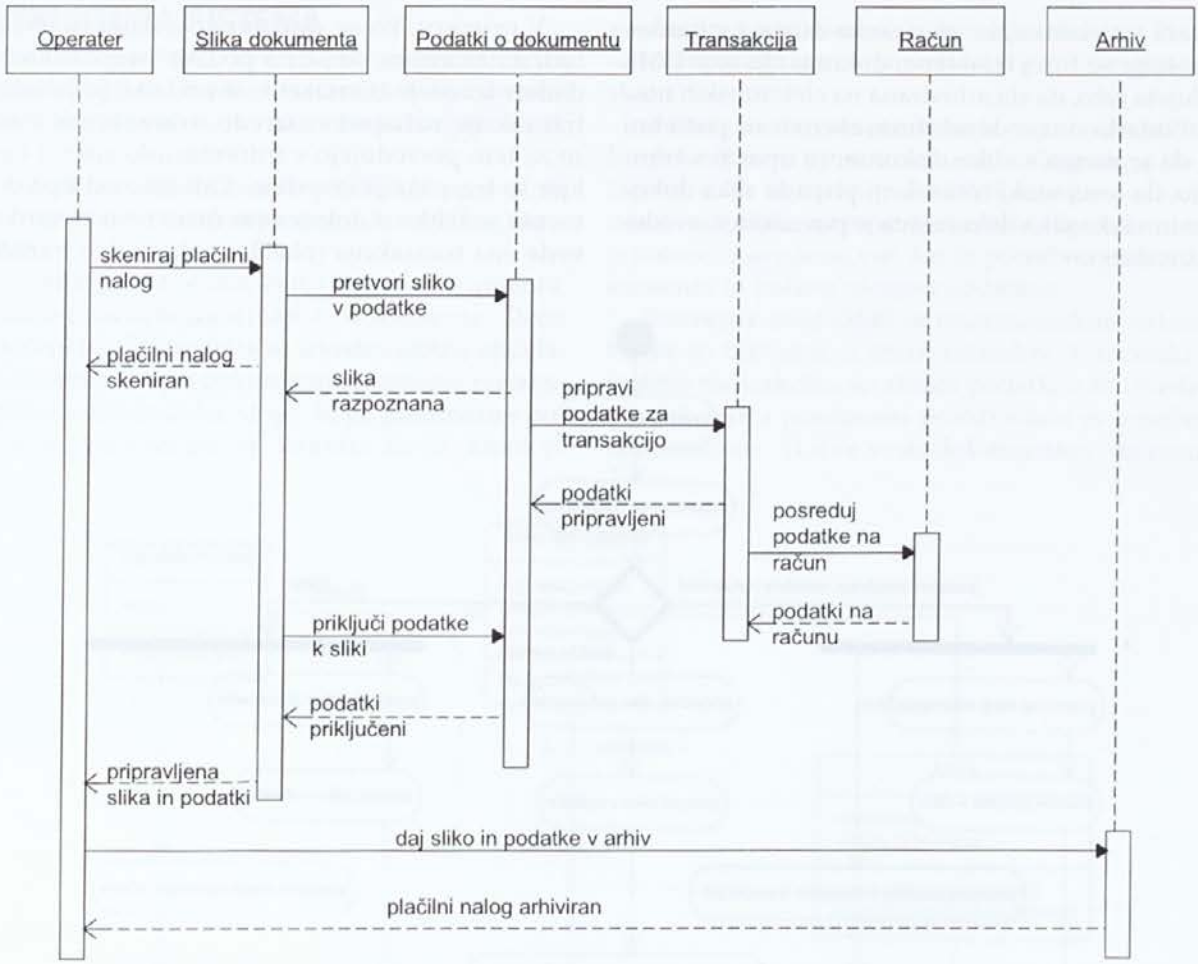
Slika 5: Razredni diagram za prikaz delovanja DMS

obdelani v trenutku, ko ju stranka dostavi v banko. Transakcije so torej izvedene, dokumenta se v DMS obdelujeta zato, da sta arhivirana na elektronskih nosilcih. Podatki o izvedenih transakcijah so potrebni zato, da je mogoče sliko dokumenta upariti s transakcijo, da torej vsaki transakciji pripada slika dokumenta in vsaka slika dokumenta je povezana z izvedeno transakcijo.

V primeru, ko se dokument v sistemu obdeluje tudi z namenom, da se na podlagi prepoznanih podatkov izvedejo transakcije, se podatki, pripravljeni z transakcije, nahajajo v razredu »transakcija«. Podatki se za tem posredujejo v informacijski sistem banke, kjer se transakcije izvedejo. Odvisno od tipa dokumenta se lahko v določenem časovnem trenutku izvede ena transakcija (plačilni nalog), dve transakciji



Slika 6: Diagram aktivnosti v DMS



Slika 7: Diagram zaporedja za scenarij primera uporabe »Obdelava plačilnih nalogov«

(ček: unovčenje, plačilo) ali pa transakcije sploh ni (posebna položnica, posebna nakaznica).

V razrednem diagramu se nahaja še razred »stanje«, ki služi temu, da se znesek na čeku med njegovo obdelavo primerja z razpoložljivim stanjem na tekočem računu imetnika čeka. V primeru, ko obstaja kritje za ček, se izvede unovčenje čeka in nakazilo remitentu, v nasprotnem primeru pa se ček zavrne.

7 OBNAŠANJE SISTEMA

Obnašanje sistema lahko ponazorimo na naslednje načine:

- z diagrami stanj, ki opisujejo obnašanje objekta, kako se obnašanje objekta spreminja pri prehodu iz enega stanja v drugo ter kateri dogodki spreminjajo stanje objekta razreda; prikazujejo možna stanja razreda ali sistema,
- z diagrami aktivnosti, ki opisujejo potek dela, aktivnosti in akcije, ki potekajo v sistemu ter omogočajo predstavitev sočasnih aktivnosti in
- z diagrami zaporedja, ki prikazujejo zaporedje sodelovanja objekta v interakciji in pri katerih je poudarek na tem, kaj sistem dela in ne kako to dela.

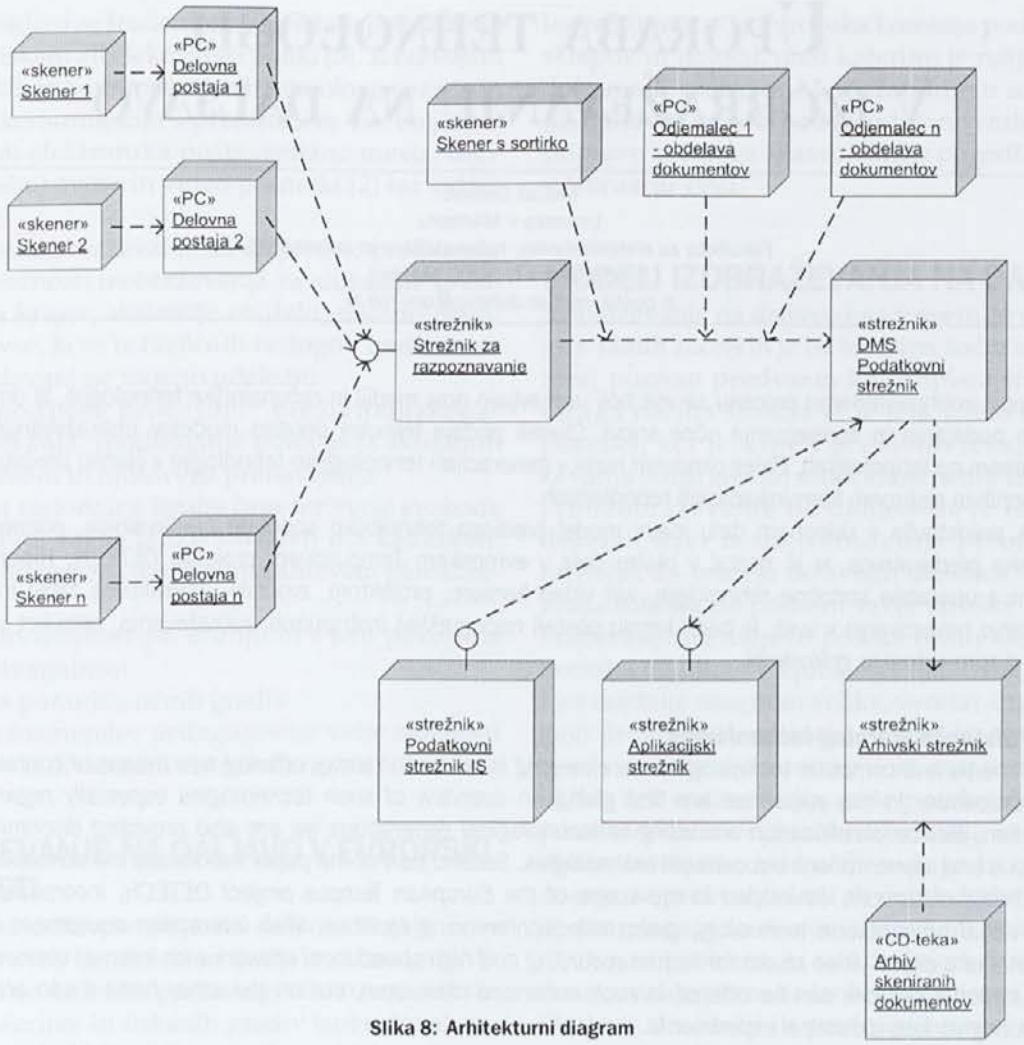
Poglejmo diagram aktivnosti, ki prikazuje dogajanja pri uporabi DMS (slika 6):

Diagram aktivnosti kaže izvedbo vseh aktivnosti v sistemu, podrobnejši opis aktivnosti pa lahko prikažemo v diagramih zaporedja. Za primer poglejmo diagram zaporedja za scenarij primera uporabe »obdelava plačilnih nalogov«:

8 ZAKLJUČEK

Čeprav je bil koncept delovanja DMS sistema s sliko že predstavljen, za zaključek predstavimo še arhitekturni diagram v notaciji UML (slika 8):

Sistem za ravnanje z dokumenti je v SKB banki zasnovan modularno, kar pomeni, da je nove elemente in funkcionalnosti mogoče enostavno dodajati,



Slika 8: Arhitekturni diagram

ne da bi bilo potrebno spreminjati zasnovo sistema. Prav tako je DMS povezan z informacijskim sistemom banke. Vse našteto omogoča, da je obdelava velikih količin istovrstnih dokumentov v največji možni meri avtomatizirana in zato učinkovita.

9 SPISEK UPORABLJENE LITERATURE

1. ERIKSSON, Hans-Erik; PENKER, Magnus: Business Modeling with UML: Business Patterns at Work, John Wiley & Sons, Inc., 2000, 459 strani.
2. LARMAN, Craig: Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design, Prentice Hall PTR, Upper Saddle River, New Jersey, 1998, 507 strani.
3. http://www.onbase.com, spletne strani, junij 2001.
4. http://www.matrix-logic.com, spletne strani, junij 2001.
5. http://www.kofax.com, spletne strani, junij 2001.
6. http://www.knowledgestorm.com, spletne strani, junij 2001.

◆

Mateja Izlakar je diplomirala na Fakulteti za računalništvo in informatiko v Ljubljani. Zdaj je študentka podiplomskega magistrskega programa Informacijski sistemi in odločanje na tej fakulteti. Zaposlena je v SKB banki d.d., kjer že nekaj let uspešno vodi projekt uvedbe Document Management System-a na različnih področjih poslovanja.

◆

Dr. Marjan Krisper je predstojnik katedre za informatiko na Fakulteti za računalništvo in informatiko Univerze v Ljubljani in od ustanovitve leta 1992 predstojnik Laboratorija za informatiko. Bil je soustanovitelj prve slovenske računalniške revije BIT in Revije za razvoj RR. Je član več znanstvenih in strokovnih združenj, med drugim ustanovitveni član AIS (Association for Information Systems) – svetovne zveze univerzitetnih učiteljev informacijskih sistemov, Slovenskega društva INFORMATIKA, Društva za umetno inteligenco in INFOS-a. Je avtor številnih raziskav, elaboratov, ekspertiz, znanstvenih in strokovnih sestavkov, z bibliografijo, ki obsega več kot 160 enot. Vodi številne projekte razvoja informacijskih sistemov in uvajanja metodologij razvoja v največjih sistemih v gospodarstvu, državni upravi in javnem sektorju.

UPORABA TEHNOLOGIJ V IZOBRAŽEVANJU NA DALJAVO

Matjaž Debevc
Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko
Smetanova 17, 2000 Maribor
e-pošta: matjaz.debevc@uni-mb.si

POVZETEK

V podpori izobraževalnemu procesu se vse bolj uveljavljajo novi mediji in računalniške tehnologije, ki omogočajo nove načine podajanja in sprejemanja učne snovi. Članek podaja trenutni pregled modelov izobraževanja na daljavo s poudarkom na tehnologijah. Poleg osnovnih razlik v generacijah tehnologij so tehnologije v članku predstavljene tudi po asinhronih in sinhronih komunikacijskih tehnologijah.

Članek predstavlja v sklepnem delu idejni model predloga tehnološko sodobne predavalnice, poimenovane hipermedijska predavalnica, ki je nastal v okviru dela v evropskem Tempusovem projektu DETECH. Hipermedijska predavalnica uporablja sodobne tehnologije, kot video kamere, projektorji, zvočniki, interaktivne table in računalniki z možnostjo povezovanja v svet, ki bodo kmalu postali nepogrešljivi instrumenti izobraževanja, tako kot so bili kreda in tabla, diaprojektorji in grafoskopi.

ABSTRACT

Using distance learning technologies

Digital media and computer technologies are emerging in education today, offering new means of content delivery and communication. In this paper we are first giving an overview of such technologies especially regarding distance education. Beside classification according to technological generations we are also providing discrimination to synchronous and asynchronous educational technologies. Second part of the paper introduces the conceptual model of a hypermedia classroom, developed in the scope of the European Tempus project DETECH, incorporating traditional audio-visual presentation technology, group videoconferencing facilities, Web interaction equipment (whiteboards), elements of a digital video studio for lecture recording and high speed local network with Internet connection. A variety of educational services can be offered in such enhanced classroom, but on the other hand it can also be used for conducting various didactical experiments.

UVOD

Razvojne spremembe v šolstvu so najbolj razvidne pri prehodu iz klasične družbe v informacijsko. Pomemben del sodobne informacijske družbe je izobraževanje na daljavo, to je uporaba sodobnih oblik izobraževanja z izdatno podporo informacijske tehnologije na vseh ravneh. Izobraževanje na daljavo postaja tudi v slovenskem prostoru pomemben člen v procesu vzgoje in izobraževanja, v visoko razvitih šolskih sistemih v tujini pa je že uveljavljeno kot dopolnitev izobraževalnega procesa.

Osnovni problemi, ki se pojavljajo pri uveljavljanju izobraževanja na daljavo, so predvsem povezani z učinkovitim uvajanjem, razvojem, organiziranjem in izvajanjem tega sodobnega načina izobraževanja, ki zahteva drugačen pristop pri načrtovanju in uvedbi učnih gradiv in preverjanja znanja. Tovrsten način izobraževanja pomeni nov izziv tudi za učitelje, ki žal niso izvedenci za uporabo novih tehnologij v izobraževalnem procesu. Učitelji se morajo soočati z novimi, ponekod celo skorajda nepremostljivimi ovirami, da bi lahko prišli v korak s spremembami, ki jih prinaša s seboj sodobna informacijska tehnologija.

IZOBRAŽEVANJE NA DALJAVO

Izraz izobraževanje na daljavo (distance education) zajema več pomenov in sicer po enem predstavlja sinonim za študij na daljavo, pri čemer se tovrstno izobraževanje pretežno nanaša na distribucijo študijskih materialov v akademskih okvirih. V drugem, sodobnejšem pomenu je izobraževanje na daljavo sinonim za izobraževanje na daljavo s pomočjo informacijske in komunikacijske tehnologije, ki vključuje tudi izobraževanje na domu [13]. Predvsem pa je to oblika posrednega izobraževanja, kjer sta učitelj in učenec med seboj fizično ali tudi časovno ločena. To pomeni, da je proces učiteljevega podajanja učne snovi ločen od procesa slušateljevega sprejemanja snovi [4].

Učno gradivo se študentom posreduje po različnih medijih v tiskani ali elektronski obliki [5]. Z razvojem računalniških in komunikacijskih tehnologij se za to in za osebno komunikacijo s profesorjem vse bolj uporabljajo tudi elektronska pošta, spletna mesta, digitalni (pretočni) avdio in video posnetki [2] ter videokonference.

Prednosti izobraževanja na daljavo so predvsem:

- večje možnosti izobraževanja za slušatelje iz oddaljenih krajev, slušatelje ob delu, telesno prizadete in vse, ki se iz različnih razlogov tradicionalnih predavanj ne morejo udeležiti
- boljša podpora procesom "vseživljenjskega" izobraževanja, spodbujanje podajanja aktualnih učnih vsebin in njihovega prenavljanja
- možnost racionalne izrabe časa ter večje svobode pri študiju, saj se lahko slušatelj uči kadarkoli. Navedeno ustreza današnjim zahtevam globalizacije
- večja samostojnost pri učenju in s tem povezana večja ustvarjalnost
- pestrejša ponudba učnih gradiv
- manjša obremenitev pedagogov ter večje možnosti za njihov individualni strokovni razvoj.

IZOBRAŽEVANJE NA DALJAVO V EVROPSKI SKUPNOSTI

Prvi začetki izobraževanja na daljavo segajo že v osemnajsto stoletje, ko so se ljudje v odmaknjenih krajih Severne Amerike po zaslugi takratnega razvoja poštnih storitev in tiskanih gradiv izobraževali samostojno, ne da bi jim bilo potrebno obiskovati izobraževalne ustanove. Prehod v računalniško obdobje v dvajsetem stoletju je prinesel s seboj tudi revolucijo na področju uporabe tehnologij v izobraževanju, tako da so se že pred desetimi leti vse bolj začela uveljavljati učna gradiva v elektronski obliki. Izobraževanje na daljavo se je kot alternativna oblika izobraževanja pričelo izraziteje uveljavljati sredi sedemdesetih in v začetku osemdesetih let, še posebej v ZDA, ko se je začel razvijati in uveljavljati internet [16].

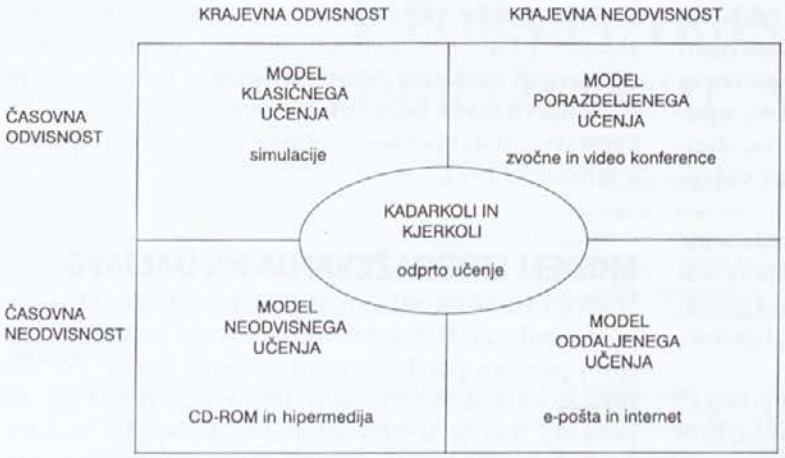
Tega trenda razvoja se zaveda tudi Evropska komisija, saj je v zadnjih nekaj letih določila kar nekaj smernic in iniciativ za razvoj izobraževanja na daljavo, kot so evropska iniciativa »**eLearning - Oblikovanje bodočega izobraževanja**" in iniciativa »**eEurope - Informacijska družba za vse**«. S temi iniciativami želi Evropska komisija, da bi Evropa prevzela vodilno mednarodno vlogo pri nadaljnjem razvoju interneta. Evropska komisija tudi želi, da bi se uporabnost svetovnega spleta bistveno razširila in bi se internet in izobraževanje na daljavo do konca leta 2001 privedla v vsako šolsko ustanovo, gospodinjstvo in urade. Poleg teh iniciativ je Evropska komisija podala kar nekaj sklepov in določil, med katerimi je najpomembnejši dokument vsekakor Memorandum o izobraževanju na daljavo, ki je bil eden od osnovnih izhodišč za pripravo predloga Maastrichtske pogodbe, podpisane v februarju 1992.

MODELI IZOBRAŽEVANJA NA DALJAVO

Izobraževanje na daljavo ima v svetu že dolgo tradicijo, v samih začetkih je bil tovrsten način izobraževanja torej poznan predvsem kot dopisni študij. Pomen takega načina študija se iz leta v leto povečuje, še posebej, ker je uspeh učenja in izvajanja izobraževanja boljši ali vsaj enak klasičnemu izobraževanju [1]. Izobraževanje na daljavo se je razmahnilo v deželah, kjer morajo študentje premagati velike razdalje, da pridejo do svojih učiteljev. Prebivanje v kraju šolanja pa pomeni večje stroške šolanja. Izobraževanje na daljavo poteka tudi v Sloveniji (Ekonomska fakulteta v Ljubljani [3], DOBA v Mariboru), kjer razdalje niso tako velike, vendar študentje izrabljajo druge prednosti takega študija, kot so: časovna neodvisnost, večja samostojnost, manjši dodatni stroški itd. Tak način študija je še posebej priljubljen pri povečevanju nivoja izobrazbe ljudi, ki so formalne oblike študija že zaključili, radi pa bi razširili svoje znanje, se prekvalificirali ali dobili dodatna znanja, ki jih potrebujejo na svojem delovnem mestu.

Pogost problem, ki se v zadnjem času pojavlja, je razumevanje pomena izobraževanja na daljavo. Velikokrat si učitelji in profesorji napačno razlagajo pojem tako, da vidijo v izrazu samo sistem zastarelega in okornega dopisnega izobraževanja, pri katerem nikdar ne bi imeli pravega stika s študentom [3]. Poleg tega je pogosto izražena tudi misel, da jim bo ta sistem prinesel samo dodatno delo in skrb. Sodobno izobraževanje na daljavo, kot je v veljavi danes po vsem svetu [10], ni samo posredovanje gradiva na daljavo, ampak srečamo v tem izrazu več modelov [9], ki so med seboj zelo različni. Sodobna učna okolja za potrebe izobraževanja na daljavo bi lahko razvrstili v štiri kategorije, kot prikazuje slika 1 [14].

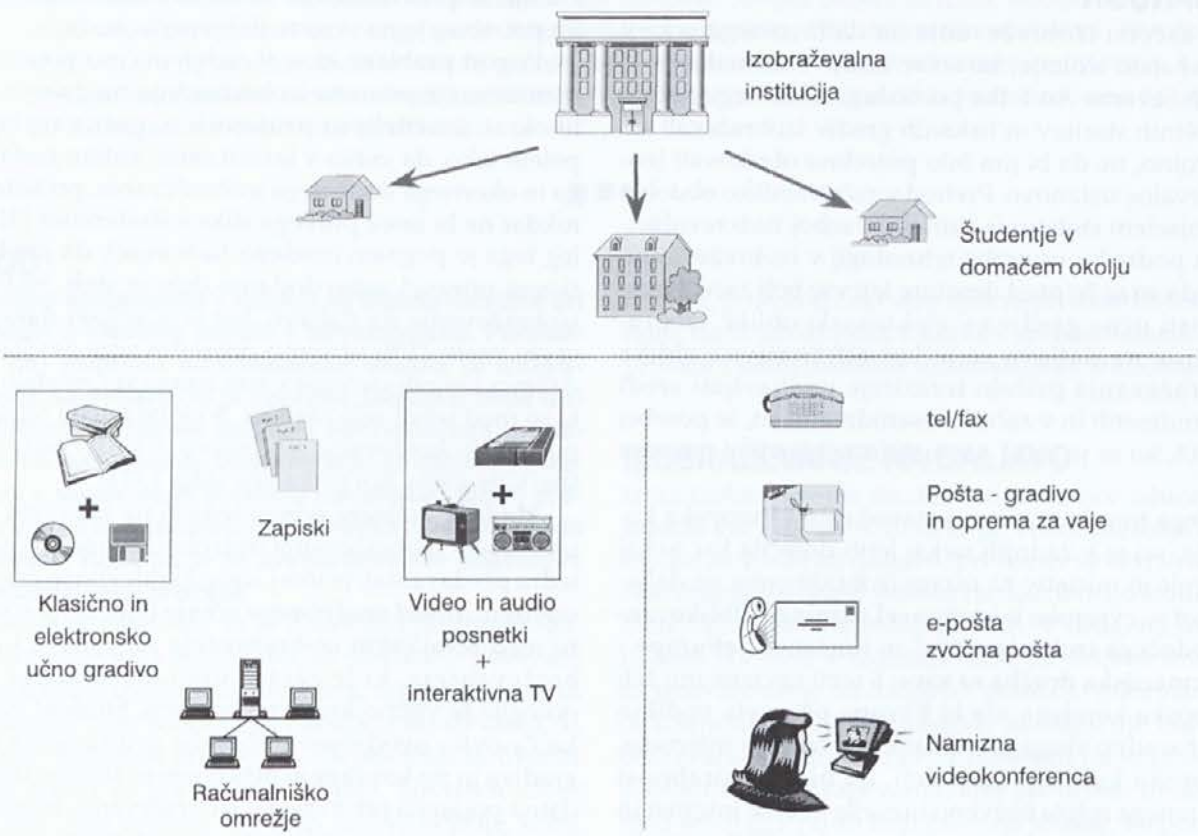
Model klasičnega učenja temelji na kontaktu med izvajalcem izobraževanja in izobraževancem (ex-katedra predavanja), je torej strogo krajevno in časovno odvisen. *Model neodvisnega učenja* temelji na kontaktu med izvajalcem izobraževanja na daljavo in izobraževancem, ki je zaradi uporabe sodobne tehnologije še vedno krajevno odvisen. Študent pa lahko časovno neodvisno uporablja pripravljena učna gradiva in po končanem neodvisnem študiju išče dodatna pojasnila pri izvajalcu izobraževanja. Študent je še vedno krajevno odvisen, obiskati mora izvajalca izobraževanja. *Model porazdeljenega učenja* izkorišča



Slika 1: Modeli različnih učnih okolij

sodobno tehnologijo, ki omogoča krajevno neodvisnost. Udeleženci so še vedno med seboj povezani istočasno. *Model odprtega učenja* bi lahko poiskali v elipsi, ki se nahaja v stičišču štirih modelov. Pozicija odprtega učenja je tudi smiselna, saj naj bi odprto učenje povzelo najboljše strani navedenih modelov.

Model neodvisnega učenja predstavlja enega najbolj zanimivih in aktualnih modelov izobraževanja na daljavo, ki se vse bolj uveljavlja tudi pri nas. Pri tem modelu se študentje zadržujejo večinoma v domačem okolju in prejemajo učno gradivo v klasični ali elektronski obliki. Poleg tega dobijo dodatne zapiske predavateljev, v katerih so označene opombe, kaj je v učnem gradivu najpomembnejše in na kaj naj bodo študentje pri učenju pozorni. Višji nivo ponudbe učnih gradiv predstavljajo video in zvočni posnetki predavanj, ki si jih lahko študentje nato ogledajo. Z razvojem računalniške tehnologije pa lahko pričakujemo, da se bodo študentje priključevali prek interneta v šolske računalniške informacijske in izobraževalne sisteme. Za komunikacijo med študenti in profesorji se lahko glede na to, kaj ima študent na voljo, uporabljajo za direktno komunikacijo telefon ali faks ter namizna videokonferenca. Za indirektno komunikacijo se uporabljajo navadna pošta, elektronska pošta, zvočna pošta ter v zadnjem času tudi video pošta. Za izvedbo vaj na domu lahko študentje dobijo tudi posebne poštne pakete, ki vsebujejo vse potrebno za enostavno izvajanje vaj na kateremkoli področju (slika 2).



Slika 2: Model neodvisnega učenja (levo: posredovanje učnega gradiva; desno: komunikacija)

Model odprtega učenja predstavlja klasični model, ki ga uporablja tudi Ekonomska fakulteta v Ljubljani [3]. Izobraževalna institucija uporablja študijske centre nameščene po državi, kjer so študentom na voljo tutorji, ki so v glavno pomoč profesorjem. Profesorji sicer občasno obiskujejo te centre, vendar se lahko uporabi tudi videokonferenca med matično izobraževalno institucijo in samimi centri. V tem primeru profesorju ni treba odpotovati posebej v posamezne študijske centre. Za učno gradivo dobijo študentje enako kot pri neodvisnem učenju material v klasični ali elektronski obliki, na disketah ali CD-jih. V zadnjem času se uveljavlja tudi DVD (Digital Versatile Disc). Zraven tega prejemajo študentje še zapiske predavanj in učne navigatorje za lažjo orientacijo pri študiju. Za višji nivo posredovanja učnega gradiva so na voljo večpredstavni video in zvočni posnetki, ki so na disketah, DVD-jih ali dosegljivi preko interneta [11].

Tretji model, ki je s finančnega vidika za izobraževalno institucijo težje dosegljiv, predstavlja **model porazdeljenega učenja**. V tem primeru se izvajajo klasična predavanja profesorjev pri običajnem pouku, vendar s to razliko, da imajo na voljo v razredu več video kamer in zmogljiv videokonferenčni sistem. To omogoča profesorjem, da posredujejo prek hitrega omrežja, kot so večkanalni ISDN, visokohitrostno optično omrežje ali omrežje ATM svoje predavanje v oddaljene razrede, v katerih so prav tako nameščene kamere in videokonferenčni sistem. Študentje imajo pri tem na voljo klasično učno gradivo in zapiske predavanj, tako kot so jih vajeni pri običajnih predavanjih. Za profesorje je ta sistem sicer najenostavnejši, saj uporabljajo svoj klasični pristop do predavanja, le s to razliko, da se je potrebno priučiti in navaditi delati s tehniškimi pripomočki. Sistem z omrežjem ATM v Sloveniji trenutno ne uporablja v praksi nobena izobraževalna institucija. Do sedaj so o tem prispevali samo predavanja na konferencah nekateri sodelavci Inštituta Jožef Stefan, Fakultete za elektrotehniko v Ljubljani in Fakultete za elektrotehniko, računalništvo in informatiko v Mariboru.

TEHNOLOGIJE ZA IZOBRAŽEVANJE NA DALJAVO

Taylor [15] je predstavil tehnološki okvir za modele izobraževanja na daljavo. Te oblike prikazujemo v tabeli 1.

Poleg te delitve na generacije, delimo tehnologije tudi glede na način komuniciranja, ki ga tehnologija dopušča, in sicer na tehnologijo na **enosmerno asinhrono in dvosmerno sinhrono komunikacijsko tehnologijo** [11].

Enosmerno asinhrono komunikacijo dopuščajo tehnologije kot npr.:

- **televizijski in radijski izobraževalni program**
  Televizija in radio posnemata in predvajata mnogo zanimivih in poučnih oddaj, katere si učenci lahko potem ogledajo doma. To dela učenca pasivnega. Oddaje ne more prekiniti in tudi ne zastaviti vprašanj, da bi s tem razjasnil razumevanje gradiva.
- **videokasete**
  Podobno vlogo kot televizija in radio imajo tudi kasete in videokasete. Tudi te delajo učenca pasivnega. Prednost kaset in videokaset pa je, da si lahko učenec sam določi čas poslušanja oziroma gledanja, lahko si posnetek ustavi, predvaja ponovno in večkrat.

Modeli izobraževanja na daljavo	Ustrezne tehnologije za posredovanje
Prva generacija – dopisovalni model	▪ tiskanje
Druga generacija – večpredstavni model . . .	▪ tiskanje ▪ zvočni trakovi ▪ video trakovi ▪ računalniško podprto učenje ▪ interaktivni video (disk in trakovi)
Tretja generacija – teleučni model . . .	▪ zvočne konference ▪ video konference ▪ zvočna grafična komunikacija ▪ TV in radijska telekonferenca
Četrta generacija – prilagodljivi učni modeli . .	▪ interaktivna večpredstavnost ▪ dostop do spletnih gradiv po internetu ▪ računalniško podprta komunikacija
Peta generacija – inteligentni prilagodljivi učni modeli . .	▪ interaktivna večpredstavnost ▪ dostop do spletnih gradiv po internetu ▪ računalniško podprta komunikacija z uporabo avtomatsko prilagodljivih odzivnikov

Tabela 1: Modeli izobraževanja na daljavo – tehnološki okvir

- **videodiski**
  Videodiski imajo podobne lastnost kot videokasete.
- **interaktivni video**
  Interaktivni video povezuje mikroračunalnik in videodisk v celoto. To je močan samokoračni (self-paced) sistem, ki pospeši učenčevo interaktivnost s snovjo predmeta skozi računalniško strokovno kontrolo. Interaktivni video je visoko individualiziran medij, ki narekuje samostojno učenje.
- **večpredstavnost**
  Večpredstavnost povezuje video, avdio, grafiko in podatke znotraj ene računalniške postaje v zaključeno celoto. Večpredstavni programi omogočajo učitelju izdelavo individualnih navodil in učnih načrtov, izvrševanje le teh ter uspešno prenašanje učnih izkušenj na učenca glede na učenčevo izbiro prostora in časa.

Dvosmerno sinhrono komunikacijo omogočajo:

- **interaktivna televizija**
  Interaktivna TV omogoča predvajanje poučnih oddaj, ki pa imajo v sebi interaktivno komponento, s katero je možna komunikacija z učnim sistemom na daljavo ali z učiteljem
- **satelitski dvosmerni prenos**
  V tem primeru se prenašajo video signali - digitalni podatki od satelita k uporabniku in nato nazaj. Tehnologija uporablja protokol TCP/IP za prenos (internet) in tako nudi možnost dvosmerne komunikacije po satelitski zvezi.
- **zgoščeni video**
  - **telekonference**
    Telekonference vključujejo telekomunikacijske tehnologije v najrazličnejša srečanja, izobraževalne delavnice, tečaje in razgovore med skupinami ali posamezniki na dveh ali več različnih mestih. Telekonference lahko uporabljajo avdio, podatke ali video komunikacije ali pa kombinacijo medijev.
  - **videokonference**
    Telekonferenca, na kateri se uporablja video tehnologija kot primaren način sporazumevanja, se imenuje videokonferenca. Ločimo tri vrste videokonferenc:
    - **enosmerni video, dvosmerni audio** - Študentje lahko gledajo in poslušajo učitelja prek televizije, vendar učitelj ne more videti učencev.
    - **dvosmerni video, dvosmerni avdio** - Učenci in učitelj se gledajo in govorijo med seboj. Pri tem se uporabljajo TV kamere in mikrofoni. Tehnologija dopušča prenose videa v obe smeri.
    - **večtočkovna videokonferenca**
      V tem primeru se več točk hkrati vključi v videokonferenco in se lahko vidi od enega do največ štiri hkrati na zaslonu. Na zaslon pa se praviloma pojavijo, ko začnejo z govorjenjem.

V okviru evropskega Tempusovega projekta DETECH »Development of the Department for Technology Supported Distance Education« [7], smo oblikovali tudi predloge za tehnološko podprto učenje. Projekt DETECH je bil v osnovi namenjen pomoči pri reorganizaciji univerzitetne uprave s ciljem, da se začne z razvojem študija na daljavo na univerzitetni ravni in z ustrezno tehniško pomočjo in je trajal od leta 1999 do leta 2001. Tako smo prej omenjeno klasično klasifikacijo tehnološke opreme dodatno razširili in jo porazdelili glede na kraj in čas, v katerem slušatelj komunicira z učiteljem ali z ostalimi slušatelji. S tega vidika razlikujemo štiri vrste tehnologij (tabela 2).

1. V skupino tehnologij, ki omogočajo prenos informacij na primer med učiteljem in slušateljem, ko se oba udeleženca nahajata ob enakem času na enakem kraju, sodijo tehnologije, ki so sicer značilne za tradicionalni študij, a se, kot že rečeno,

		KRAJ	
		enak	**različen**
ČAS	*enak*	*1.* ■ **interakcija zagotovljena** - sinhrone tehnologije - primer: projiciranje	*2.* ■ **interakcija zagotovljena** - sinhrone tehnologije - primer: telekonferenca, telefon. ■ interakcija ni zagotovljena
	različen	*3.* ■ **interakcija zagotovljena** - asinhrone tehnologije - primer: elektronska pošta ■ **interakcija ni zagotovljena** - primer: video, avdio, posnetki	*4.* ■ **interakcija zagotovljena** - asinhrone tehnologije - primer: elektronska pošta, novičarske skupine ■ **interakcija ni zagotovljena** - primer: tiskanje, zvočni in video posnetki, CD, DVD

Tabela 2: Vrste tehnologij glede na kraj in čas komuniciranja

uporabljajo tudi pri izobraževanju na daljavo, kot na primer projiciranje. Te tehnologije sodijo med sinhrone tehnologije in pri njih je slušatelj aktiven udeleženec.

2. Med tehnologijami, ki omogočajo prenos informacij na primer med učiteljem in slušateljem, ko se oba udeleženca nahajata ob enakem času na različnem kraju, obstajajo tiste, kjer je interakcija slušatelja zagotovljena (telekonferenca, telefon, elektronsko klepetalno orodje), ter take, ki interakcije slušatelja ne omogočajo (televizija, radio). Pri telekonferenčnih prenosih, kjer je interakcija slušatelja zagotovljena, govorimo o že omenjenih sinhronih tehnologijah.
3. Tehnologije, ki omogočijo prenos informacij na primer med učiteljem in slušateljem, ko se oba udeleženca nahajata ob različnem času na enakem kraju, se za prenos znanja med učitelji in slušatelji uporabljajo v lokalnih študijskih centrih večjih univerz. Slušateljem je v teh centrih največkrat omogočen dostop do medijske opreme, kot so videorekorderji, računalniki z bazami podatkov in učnim gradivom ter knjige.
4. Tehnologije, ki omogočijo prenos informacij na primer med učiteljem in slušateljem, ko se oba udeleženca nahajata ob različnem času na različnem kraju, se ločijo na tiste, kjer je interakcija slušatelja zagotovljena, ter tehnologije, ki interakcije slušatelja ne omogočajo. V prvo skupino sodijo:
   - elektronska pošta (e-mail)
   - novičarske skupine (Usenet News)
   - računalniško podprta skupinska konferenca (NetMeeting)

HIPERMEDIJSKA PREDAVALNICA

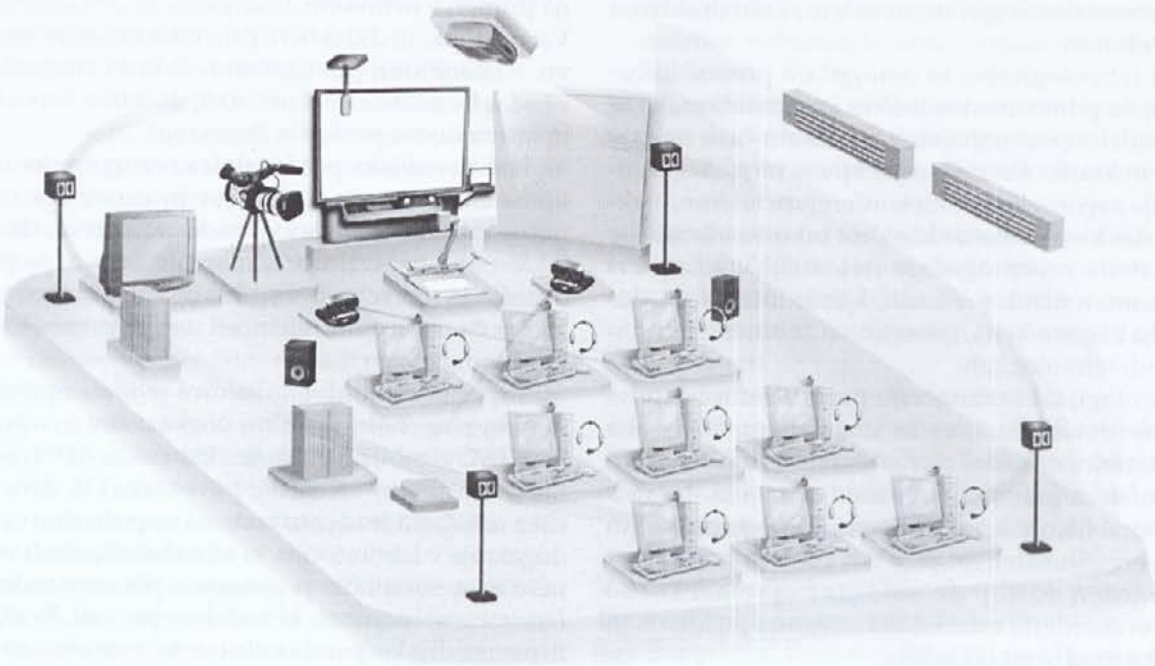
V okvir del v projektu DETECH je spadalo tudi oblikovanje predloga nove tehnološko sodobne predavalnice, ki smo jo poimenovali **hipermedijska predavalnica** (hypermedia lecture room). Hipermedija je sicer izraz, ki predstavlja večpredstavnostne dokumente, ki poleg hiperbesedilnih in grafičnih elementov vključuje tudi zvok in video kot osnove za povezave [131313]. Hipermedijska predavalnica v našem primeru vključuje videokonferenčno sobo in interaktivno sprotno video tehnologijo (streaming video) v novo učno okolje [2]. Razvoj takšne predavalnice poleg ustrezne pohištvene in zvočne opremljenosti učilnice zahteva tudi nabavo večjega števila strojne in programske opreme. Omenjena predavalnica se ponavadi uporablja v sodelovanju z drugimi univerzitetnimi učilnicami v lokalnem in mednarodnem okolju. Glavni cilj te predavalnice je, da učenec uporablja vso razpoložljivo tehnologijo s tem, da lahko posluša na primer predavanja na daljavo in komunicira s predavateljem na daljavo. Poleg tega lahko izvaja vajo na daljavo in pri tem ne bo imel občutka, da izvaja vajo, na primer, v nemškem ali angleškem laboratoriju [12]. Vsi postopki in didaktični prijemi bodo sicer na daljavo, s posebnimi povezavami ali linki (hyperlinks), vendar bo učenec imel občutek, da lahko neposredno in interaktivno posega v dogajanje.

Hipermedijska predavalnica omogoča povezovanje velikega števila slušateljev in zmanjšuje stroške potovanj predavateljev. Osnovna zahteva, da lahko takšen tip predavalnice učinkovito deluje , pa je hiter dostop do interneta z vsaj 10Mb/s ali celo bolje z 100 Mb/s s čimer so dane možnosti tudi za prenos kvalitetnega video posnetka.

Hipermedijska predavalnica je torej opremljena najprej z visokohitrostnimi povezavami in uporablja ali ATM, gigabitno omrežje, kabelsko, ADSL ali vsaj hitre dvosmerne satelitske povezave [11]. Živa video slika omogoča študentu tudi, da neposredno opazuje dogajanje v laboratoriju, ki se nahaja kjerkoli v internetu in se simultano pogovarja s pomočjo videokonference z asistentom, ki sodeluje pri vaji. Realizacija hipermedijske predavalnice bi morala izpolniti pričakovanja tako učiteljev kot še posebej študentov. Enaka oprema se predlaga tako za lokalno, kot tudi za oddaljeno lokacijo. Načrt, ki smo ga oblikovali kot predlog v okviru Tempusovega projekta DETECH je predstavljen na sliki 3.

Iz slike 3 je razvidno, da so za spremljanje dogajanja nameščene 3 video kamere, od katerih je ena digitalna video kamera za snemanje predavatelja, drugi dve kameri pa sta namenjeni za avtomatsko spremljanje študentov. Slednji sta tudi kameri, ki omogočata premik, »zoomiranje« in avtomatsko spremljanje gibanja v prostoru. Takšna kamera je na primer SONY DVI-31 kamera. V sprednjem delu prostora je nameščen televizijski zaslon za spremljanje dogajanja na oddaljenih lokacijah in za uporabo interaktivne televizije. Spredaj v desnem kotu je postavljeno platno, na katerega se projicira slika iz video projektorja, priključenega na predavateljev računalnik. Tu se lahko med drugim prikazuje tudi oddaljena lokacija, ki jo opazujejo lokalni slušatelji. Na sredini spredaj je postavljena elektronska tabla (white board) s projektorjem in posebno dodatno interaktivno tablo za predavatelja, s katero lahko krmili vso tehnologijo naenkrat. Na profesorjevi mizi se nahaja tudi dokumentacijska kamera. V prostoru so za boljši zvok razporejeni štirje prostorski zvočniki. Na stropu in na mizah so nameščeni mikrofoni, s katerimi lahko zajemamo zvok tako predavatelja kot študentov. Predavatelj mora imeti tudi brezžični mikrofon, ki mu daje največ svobode pri gibanju.

Za prenos audio in video signala ter podatkov na oddaljene lokacije se uporablja skupinski večtočkovni



Slika 3: Model hipermedijske predavalnice

videokonferenčni sistem. Ta je spravljen poleg glavnega računalniškega strežnika v omarici pri operaterju. Prenos lahko poteka preko ISDN, LAN, ATM, kabelskega in satelitskega omrežja. Pri operaterju je tudi omarica (A/V) z audio opremo, kjer se nahajajo zvočna krmilna enota in enota za odpravo odmeva, ojačevalnik za zvočnike, mešalna miza, mikrofonski pult, predvajalnik DVD, kasetofon, videorekorder, in druga oprema, ki je potrebna za delovanje celotnega sistema.

Pri tem morajo imeti tla za dosego dobre akustike stene in prostora grobo površino. Na tla se položi itison. Na stenah naj visijo zavese, ki dobro vpijajo zvok.

Pri postavitvi hipermedijske učilnice moramo na koncu še posebej upoštevati predavateljeve in slušateljeve zahteve, tako da bo uporaba tovrstne tehnologije čim enostavnejša in bo slušateljem na oddaljenih lokacijah omogočala enake pogoje za učenje kot lokalnim.

ZAKLJUČEK

Z oblikovanjem, razširitvijo in vse večjo priljubljenostjo interneta se moramo zavedati, da bodo generacije, ki prihajajo za nami, rasle s tem omrežjem, brez nas ali z nami. Tako, kot smo danes vajeni radia, televizije, računalnikov, bodo generacije za nami uporabljale in tudi zahtevale storitve interneta. In izobraževanje na daljavo je eden izmed najpomembnejših storitev, ki jih nudi to omrežje. Žal se v internetu čas meri v pasjih letih, kot se nekateri izražajo, kar pomeni, da razvoj s pomočjo interneta traja eno leto, namesto 7 let. Zato postaja nujno potrebno, da se razvoj izobraževanja na daljavo začne v Sloveniji čim hitreje, tako da bodo generacije, ki prihajajo, lahko že imele na voljo zmogljiva orodja in storitve, ki bi bile nadgradnja vsega, kar so do sedaj spoznali.

Da bi to uresničili na najbolj učinkovit način, je rešitev v čim večji informiranosti in usposabljanju uporabe tehnologij v izobraževanju s ciljem, da so tehnologije učinkovita in aktivna podpora profesorjem in učiteljem pri njihovem delu. Tudi vloga učitelja se z uvajanjem novih tehnologij temeljito spreminja in sicer iz vsestranskega strokovnjaka v mentorja mladim, ki jih bo znal usmerjati in uporabljati njihovo znanje v prid svojemu znanju in znanju celotnega razreda.

Idejni model hipermedijske predavalnice, ki smo jo oblikovali v okviru evropskega projekta DETECH in predstavili v tem članku, bi lahko služil kot osnova za oblikovanje sodobnih učilnic v vsaki izobraževalni

instituciji. Video kamere, projektorji, zvočniki, interaktivne table in računalniki z možnostjo povezovanja v svet bodo kmalu postali nepogrešljivi instrumenti izobraževanja, tako kot so bili kreda in tabla, diaprojektorji in grafoskopi.

LITERATURA

1 Andrakin, A. (1999). Survey Finds Online Education Equal to or Better than On Campus Learning. V: http://www.ecollege.com/ .

2 Bargeron, D., Gupta, A., Grudin, J. and Sanocki, E., "Annotations for streaming video on the Web: system design and usage studies," Computer Networks (Netherlands), Elsevier Science, 17 May 1999, Vol. 31, No. 11-16, pp. 1139-1153.

3 Bregar, L. (1998). Študij na daljavo na ekonomski fakulteti: izkušnje za prihodnost. Vzgoja in izobraževanje, 29, št.3, str. 14-20.

4 Bregar, L., Strategical Questions of Further Development of On-line Education in Slovenia, Round table - the Faculty of Economics. Vzgoja in izobraževanje, 29, nr.3, p.4-13., 1998

5 Carliner S., "An Overview of Online Learning", Bill Communications, http://www.lakewoodconferences.com/wp/

6 Chowdhury, A., Ratej, B., Debevc, M., Svečko, R.: Cable data network test trials in Slovenia, proceedings of the European Conference on Networks and Optical Communications 1998. Amsterdam, 1998, Pg. 192-199.

7 Debevc, M., TEMPUS PHARE Joint European Project DETECH, http://www.cded.uni-mb.si/tempus-detech.htm

8 Fritsch, H., D. Keegan, B. Vertecchi, VOCTADE: Development of knowledge in the field of vocational training at a distance in the European Union, Final report, http://www.fernuni-hagen.de/ZIFF/finalvoc.htm

9 IDE - Institute of Distance Education. (1999). Three Models of Distance Education, http://www.umuc.edu/ide/modldata.html .

10 International Association of Universities, Virtual Universities: Examples In Selected Countries, http://www.unesco.org/iau/tfit_examples.html

11 Minoli, D., Distance Learning Technology and Applications, Artech House, Norwood, MA, USA, 1996

12 Poindexter S.E., Bonnie S. H., "Using the web in Your Courses: What Can You Do? What Should You Do?", IEEE Control Systems, Vol. 19, No. 1, February, 1999, pp. 83-92

13 Slemnik, B., O'Dea, S. in Debevc, M., Angleško-slovenski besednjak izobraževanja na daljavo, UM FERI, 2001

14 Šmitek, B. (1999). Organizacija izobraževanja na daljavo s pomočjo sodobne računalniške tehnologije, Disertacija, Fakulteta za organizacijske vede, Kranj, str. 25

15 Taylor, J. C. (1999) Distance Education: The Fifth Generation, Proceedings of the 19th ICDE World Conference on Open Learning and Distance Education (Vienna, Austria, June 1999).

16 Zakon, H.R., "Hobbes' Internet Timeline", http://info.isoc.org/guest/zakon/Internet/History/HIT.html, 2000

◆

Dr. Matjaž Debevc je leta 1995 doktoriral na Univerzi v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko s področja tehniških znanosti. Je docent predmetnega področja Računalništvo in docent predmetnega področja Avtomatika in robotika. Poleg tega deluje od leta 1999 tudi kot predstojnik Centra za razvoj študija na daljavo Univerze v Mariboru. Njegovo področje delovanja so interakcija človek-računalnik, oblikovanje uporabniških vmesnikov, prilagodljivi uporabniški vmesniki, internetne aplikacije, kabelska televizija, izobraževanje na daljavo in podporne tehnologije za invalide. Je svetovalec združenjem in zavodom na področju izobraževalnih tehnologij. Za svoje delo na področju interakcije človek-računalnik je prejel nagrado UNESCO. Je tudi dobitnik nagrade za najboljši članek na konferenci in nagrad za svoje mentorstvo z mladimi raziskovalci. Je član IEEE, ACM in OCG.

◆

RAID in baza podatkov Oracle

Marija Kuhar[1], Borut Vovk[2], Miro Gradišar[3]

Izvleček

Varnost in zanesljivost informacijskih sistemov postajata vedno pomembnejša. V času, ko se poslovanje seli na spletne strani, je potreba po stalni dostopnosti podatkov vedno bolj pogosta. Hkrati se cena izpada sistema močno dviga, zaradi česar se pojavljajo nove strojne in programske rešitve, ki zagotavljajo boljšo zanesljivost, razpoložljivost in zmogljivost informacijskih sistemov.

Članek obravnava organizacijo diskov poimenovano RAID, ki poveča hitrost, razpoložljivost in zanesljivost računalniških sistemov. Predstavljeni so možni načini organizacije oziroma nivoji RAID, prednosti in slabosti le-teh, priporočljiva področja uporabe in analiza uporabe z vidika baze podatkov Oracle.

Ključne besede: RAID, zanesljivost, razpoložljivost, organizacija diskov, baza podatkov Oracle

Abstract

Raid and Oracle Database

Increased capacity requirements for network applications and better reliability in the time when significantly declined cost of storage per megabyte and high productivity losses give a fresh impetus to storage industry, which puts numerous solutions for improving overall better system performance on the market.

The article presents RAID storage systems and other supplements for improving overall availability and reliability of information systems. The article especially discusses the implementation of RAID systems in Oracle environment.

Key words: *RAID, reliability, availability, disk organization, Oracle database*

1. Uvod

Zadnjih nekaj deset let so se zmogljivosti procesorjev eksponentno večale. Približno vsakih 18 mesecev so se podvojile (1), kar pa ni moč reči za zmogljivosti diskov. V začetku sedemdesetih je bil povprečni čas dostopa do podatka na disku miniračunalnika nekje med 50 in 100 milisekundami. Dandanes se ti časi vrtijo okrog 10 milisekund. V mnogih vejah tehnične industrije je faktor sprememb 5 do 10 v 30 letih velika številka, v računalniški industriji, kjer dosega razvoj vrtoglave hitrosti, pa je tak napredek skromen. Razlika med zmogljivostjo procesorjev in diskov se tako iz leta v leto veča in seveda pomeni vedno večji problem, saj diski postajajo ozko grlo v procesu obdelave podatkov.

Na področju procesorjev se je veliko raziskovalo in tudi doseglo v smeri vzporednega procesiranja. Tako so znanstveniki v poznih osemdesetih začeli razmišljati tudi o paralelizmu na področju sistemov za shranjevanje podatkov. Leta 1988 so trije raziskovalci kalifornijske univerze David Patterson, Randy Katz in Garth Gibson objavili idejo o šestih različnih načinih paralelizma na področju organizacije diskov (2). Sistem je poimenovan RAID. RAID je kratica, ki danes pomeni *Redundant Array of Independent Disks* ali, če poskusimo to posloveniti – skupina neodvisnih diskov s preobiljem podatkov. Pri tem pomeni redundanca ali preobilje večkrat zapisane enake podatke ali osnovnim podatkom pridružene nadzorne podatke, ki so iz njih izračunani po določenem algoritmu, tako da je možno odkrivanje in odpravljanje napak. Glede tega bolj ali manj posrečenega prevoda velja omeniti, da je kratica RAID v začetku pomenila 'Redundant Array of Inexpensive Disks' – torej skupina poceni diskov, vendar je industrija idejo hitro spoznala za koristno in razvila praktične rešitve, ki so bile vse prej kot poceni. Zato so besedico 'Inexpensive' zamenjali za 'Independent'.

Glavna ideja je bila sestaviti črno škatlo, ki bo navzven izgledala kot en sam hiter in zanesljiv disk. Znotraj te črne škatle pa naj bi bilo več počasnejših in manj zanesljivih diskov ter krmilnik, ki naj bi skrbel za njihovo usklajeno delovanje.

Namen tega preglednega članka je predstaviti tehnologijo RAID in njeno praktično uporabo pri bazah podatkov Oracle, ki so v Sloveniji zelo razširjene. V nadaljevanju bomo opisali tehnologijo RAID in načine, kako lahko izboljšamo zmogljivost računalniškega sistema z uporabo različnih nivojev RAID, ki jih bomo med seboj primerjali. Opisali bomo različne možnosti uvedbe te tehnologije v prakso. Na koncu bomo podali pregled nad nivoji RAID, ki so zlasti zanimivi z vidika Oraclove baze podatkov in izvedli primerjavo tudi med njimi.

1 Grad d.d., Tržaška 118, 1000 Ljubljana, marija@grad.si
2 Gorenjska banka d.d., 4000 Kranj, borut.vovk@gbkr.si
3 Ekonomska fakulteta, Kardeljeva ploščad 17, 1000 Ljubljana, miro.gradisar@uni-lj.si

2. Tehnologija RAID

Razvoj tehnologije RAID koncem osemdesetih let so predvsem spodbujali naslednji takratni trendi (6):

- večanje potreb po velikih diskih zaradi novih omrežnih aplikacij
- hitrejši procesorji (stokratno povečanje zmogljivosti procesorjev napram samo štirikratnemu povečanju zmogljivosti diskov v istem obdobju) zahtevajo boljši vhodno izhodni (V/I) sistem
- zanesljivost sistema je v novih (omrežnih) aplikacijah vedno pomembnejša. Tehnologija RAID lahko prepreči izgubo podatkov, do katerih bi prišlo zaradi napak oziroma okvar diskov
- cena na enoto prostora na disku je močno padla in sistemi RAID so se razširili iz velikih računalniških centrov celo na področje delovnih postaj in namiznih računalnikov.

Zanesljivost delovanja kot velikokrat najpomembnejšo lastnost diskovnih sistemov lahko razčlenimo na (6):

- neobčutljivost na izpade (*fault tolerance*)
- majhno pogostost napak pri branju in pisanju
- visoko razpoložljivost.

V tabeli 1 so prikazani vzroki za odpovedi računalniških sistemov, kot jih je v svoji študiji leta 1995 predstavilo podjetje Intel Corporation.

Neobčutljivost na izpade posameznih komponent pomeni, naj bi bil sistem sestavljen tako, da posamezne komponente lahko odpovejo, vendar s tem ne povzročijo izpada sistema. Zrcaljenje diskov je najpogostejši način za doseganje neobčutljivosti na izpade, ki ga uporabljajo tudi sistemi RAID. Če odpove primarni disk, njegovo nalogo prevzame zrcalni disk in tako uporabnik opazi okvaro le kot počasnejše delovanje sistema.

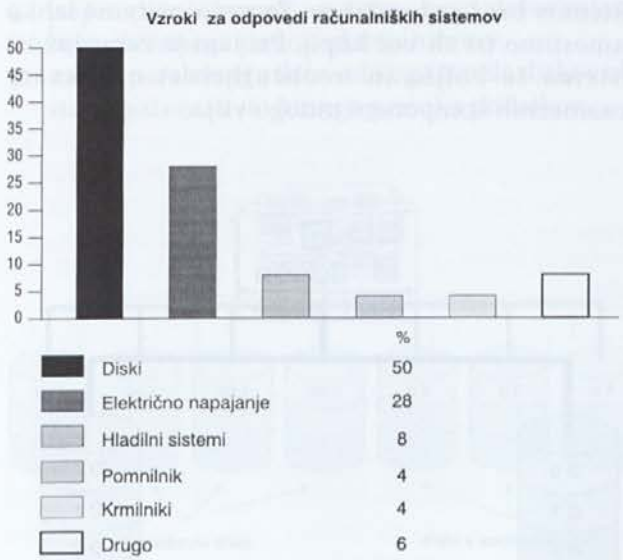


Tabela 1:
Razlogi za odpovedi računalniških sistemov (vir: Intel Corporation)

Majhna pogostost napak je naslednji pomemben dejavnik zanesljivosti. Napake sistema se lahko pojavljajo zaradi različnih vzrokov. Kadar le-te nastajajo zaradi vplivov okolja, na primer visoke temperature, so odpovedi posameznih komponent pogoste. Da se temu izognemo, je priporočljivo uporabljati komponente z visokim MTBF (kratica izhaja iz angleščine in pomeni povprečni čas med odpovedmi komponente - *mean time between failure*) in pomožne sisteme, kot so klimatske naprave, podvojeni sistemi napajanja in podobno. Nenazadnje lahko tudi programska oprema pripomore k majhni pogostosti napak. Programi, ki nadzorujejo delo sistema, lahko avtomatsko javljajo sumljive dogodke, ki nakazujejo na okvaro v obliki elektronske pošte ali sporočila na mobilni telefon dežurnega vzdrževalca.

Visoka razpoložljivost pomeni, da naj bi bil v nekem obdobju sistem čim dalj časa na razpolago. Visoka razpoložljivost je gotovo lastnost sistema, pri katerem niti okvara niti odprava te okvare ne povzročita izpada sistema. Visoko razpoložljivi diskovni sistemi morajo biti sestavljeni iz komponent, ki jih je mogoče zamenjati med delovanjem sistema. V ta namen se pogosto uporablja združevanje računalnikov v gruče (*clusters*), kjer je več strežnikov povezanih na isti diskovni sistem, da se omogoči uporabnikom dostop do programov in podatkov preko nadomestnega računalnika, če matični odpove. Seveda je v tem primeru za uporabnike ob delovanju vseh strežnikov pridobitev že to, da je zagotovljene več procesne moči za strežniško orientirane programe pri velikem številu uporabnikov.

2.1. Izboljšanje zmogljivosti sistema

V primerjavi z navadnimi diskovnimi sistemi omogočajo sistemi RAID izboljšanje zmogljivosti. Dejanske spremembe zmogljivosti diskovnega sistema RAID so odvisne od tega, kako je sistem zgrajen oziroma kakšen nivo RAID uporabljamo in od tega, kakšen je način dela s podatki. Pri uporabi zrcaljenja podatkov se zmogljivost v primerjavi z navadnimi enodiskovnimi sistemi pri branju podatkov povečajo, pri zapisovanju pa zmanjšajo. Pri sistemu zapisovanja paketov podatkov vzporedno na več diskov (*striping*), se poveča hitrost tako pri branju kot zapisovanju podatkov, vendar se zanesljivost sistema zmanjša. Nekateri sistemi RAID uporabljajo kombinacijo obeh principov in tako dosežejo hkrati pohitritev in povečanje zanesljivosti diskovnega sistema. Sistemi RAID so različnih tipov ali konfiguracij, ki jih literatura imenuje nivoji (*levels*).

2.2 Nivoji RAID

V uvodu omenjeni raziskovalci kalifornijske univerze so definirali 6 osnovnih nivojev RAID. Čeprav se govori o nivojih, tu ne gre za nikakršno hierarhijo, podrejenost

in nadrejenost posameznih nivojev. Gre le za 6 različnih konfiguracij, ki so pač tako poimenovane. Poleg teh šestih osnovnih konfiguracij se v praksi uporabljajo tudi kombinacije, izpeljane iz osnovnih. Opisi teh konfiguracij ter prednosti in slabosti so povzete po priporočilih proizvajalcev strojne opreme (8) (9) (11) in svetovalcih in združenjih (7) (10) (12).

2.2.1 RAID 0

Ta tehnika je poznana tudi kot *data striping*. Gre za razdeljevanje podatkov na več manjših blokov enake velikosti, ki omogočajo istočasno oziroma vzporedno branje ali pisanje na več diskov ali z njih in s tem občutno povečanje hitrosti. Skupina teh diskov je navzven vidna kot en sam velik in hiter disk.

Ker RAID 0 ne uporablja redundance podatkov, je tako od vseh konfiguracij glede prostora najvarčnejši. Prav odsotnost redundance pa je slaba stran. Ti sistemi niso neobčutljivi na izpade posameznih komponent, zato se v praksi največkrat uporabljajo le skupaj z drugimi nivoji RAID. Če odpove eden od diskov, izgubimo vse podatke in sistem stoji. Cena izpada je lahko bistveno višja kot prihranek pri nakupu diskovnega prostora. Učinek sistema je najboljši, kadar se uporablja čim večje število fizičnih diskov in kadar vsak krmilnik nadzira delo čim manj diskov, najbolje samo enega. Velikost posameznega bloka (*stripe*) podatkov mora biti skrbno pretehtana, sicer lahko dosežemo nasprotni učinek od zaželenega. S tako konfiguracijo dosežemo izjemno hitrost delovanja, ki je za nekatera področja zelo pomembna. Tako področje je na primer video, kjer je bistvena hitrost branja podatkov, saj je za kvaliteten zvok in sliko nujen neprekinjen dotok podatkov do procesorja.[4]. Značilnosti RAID 0 lahko strnemo v naslednje ugotovitve.

Prednosti:
- enostavnost sistema,
- preprosta izgradnja sistema,
- dobra zmogljivost.

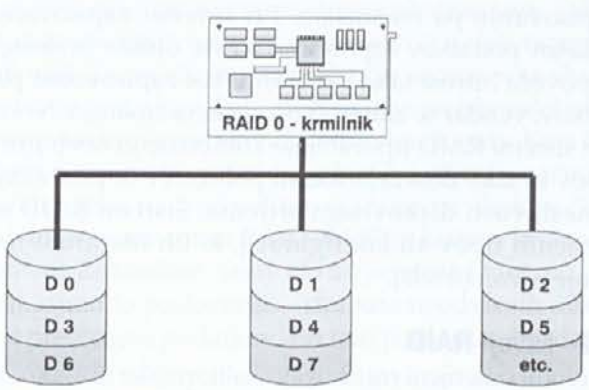
Slabosti:
- občutljivost na odpovedi,
- izguba samo enega diska povzroči izgubo vseh podatkov.

Priporočena področja uporabe:
- urejanje in predvajanje videa,
- urejanje slik, fotografij,
- aplikacije, ki potrebujejo velik pretok podatkov.

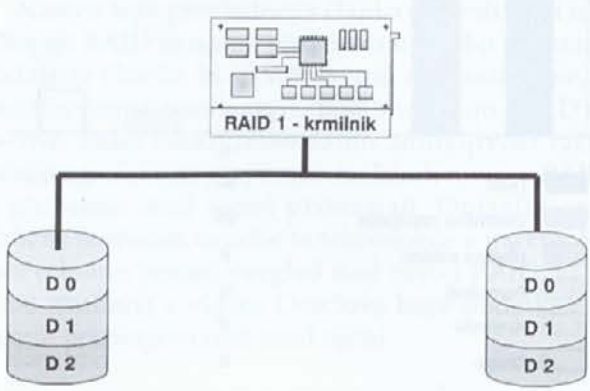
2.2.2 RAID 1

RAID 1 je najpreprostejši sistem, ki zagotavlja neobčutljivost na okvare posameznih komponent. Poznamo ga tudi pod imenom zrcaljenje. RAID 1 krmilnik razdeli diske v dve skupini. Vsak podatek vzporedno zapiše na obe skupini (slika 2). Za postavitev sistema sta potrebna vsaj dva diska. Če eden odpove, njegovo delo prevzame drugi in do izpada sistema ne pride. Pade le zmogljivost, dokler ne vstavimo nov disk. Ob izpadu še tega edinega diska odpove celoten sistem. Cena uvedbe sistema je zelo visoka, saj moramo celotno konfiguracijo podvojiti. Dodatno varnost pred odpovedmi sistema si zagotovimo s podvajanjem vseh komponent v sistemu (električno napajanje, pretvorniki, V/I vodila, itd.) in nakupom bolj kakovostnih komponent. Zaradi visoke ravni zaščite podatkov in enostavnosti uvajanja in vzdrževanja ta sistem priporočajo mnogi ponudniki sistemov za upravljanje z bazami podatkov, če že ne za celotno zbirko podatkov, pa vsaj za njene najpomembnejše dele. Zrcaljenje diskov je tudi edina konfiguracija RAID, kjer hitrost ni večja od hitrosti navadnih diskovnih sistemov brez redundance. Za večjo varnost lahko namestimo tri ali več kopij. Pri tem je zanesljivost sistema še boljša in neobčutljivost na okvare posameznih komponent mnogo višja.

4 *V tem primeru je priporočljivo uporabljati diske, kjer se ne izvaja tako imenovana termična rekalibracija – ponovno nastavljanje bralno pisalnega mehanizma diska zaradi spreminjanja dimenzij kot posledice pregrevanja.*



Slika 1: RAID 0 – »striping«



Slika 2: RAID 1 - zrcaljenje

Prednosti:
- teoretično dvakratna hitrost branja podatkov,
- visoka neobčutljivost na odpovedi komponent,
- pri odpovedi posamezne komponente ne izgubimo podatkov,
- enostavnost izgradnje sistema.

Slabosti:
- največja stopnja redundance (100%) od vseh nivojev RAID,
- najdražji sistem s stališča cene na enoto diskovnega prostora.

Priporočena področja uporabe:
- računovodski sistemi,
- finančni sistemi,
- aplikacije, ki potrebujejo zelo visoko razpoložljivost.

2.2.3. RAID 2

Nivo RAID 2 (slika 3) uporablja za odkrivanje in odpravo napak sistem, imenovan Hammingova koda. Za ta sistem potrebujemo vsaj 7 diskov. Za vsake 4 bite podatkov, kjer se vsak bit zapiše na svoj disk, se sproti izračunavajo in zapisujejo še 3 nadzorni biti. Ti nadzorni biti se izračunajo tako, da je v primeru odpovedi kateregakoli diska možno na podlagi informacij, zapisanih na ostalih šestih diskih izračunati vrednost okvarjenega bita in sistem nemoteno deluje. Slabost takih sistemov je veliko število diskov in krmilnikov, posebej če želimo zmanjšati odstotek redundantnih diskov. Šele pri uporabi 38 diskov (32 podatkovnih in 6 nadzornih) pade odstotek redundantnih bitov na 19%. Druga slabost je potrebna sinhronizacija diskov v sistemu, ki jo dosežemo tako, da diske namestimo na isto gred, kar je za proizvodnjo zelo zahtevno.

Prednosti:
- popravljanje napak »v živo«, med delovanjem, brez občutnega padca odzivnih časov,
- zaradi paralelnega dela velikega števila diskov obstaja možnost zelo hitrega pretoka podatkov,
- relativno preprost krmilnik v primerjavi s tistimi za RAID nivoje 3, 4 in 5.

Slabosti:
- na trgu se zaradi zapletenosti taki sistemi niso uveljavili,
- za implementacijo potrebujemo preveč diskov,
- delo vseh diskov mora biti sinhronizirano, kar ni lahko doseči.

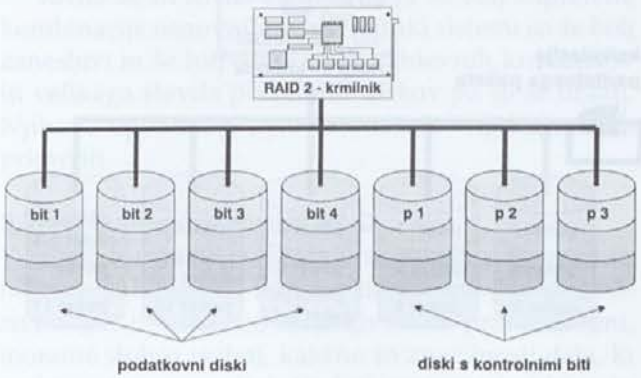
2.2.4 RAID 3

RAID 3 je poenostavljena verzija sistema RAID 2. Namesto Hammingove kode se za odkrivanje in odpravljanje napak uporablja le paritetni bit. V lihi paritetni shemi mora biti vsota vseh bitov liha, zato dobi paritetni bit vrednost 0 ali 1 glede na vsoto podatkovnih bitov. Podobno je v sodi paritetni shemi vsota vseh bitov soda. Postopek poteka tako, da se izračuna vsota podatkovnih bitov, nato pa se določi vrednost paritetnega bita, ki se zapiše na poseben vzporeden paritetni disk (slika 4). Če pride do izpada enega od diskov, ga moramo locirati, zatem pa lahko na podlagi informacij iz drugih diskov in paritetnega diska določimo vrednost podatka na disku, ki je odpovedal.

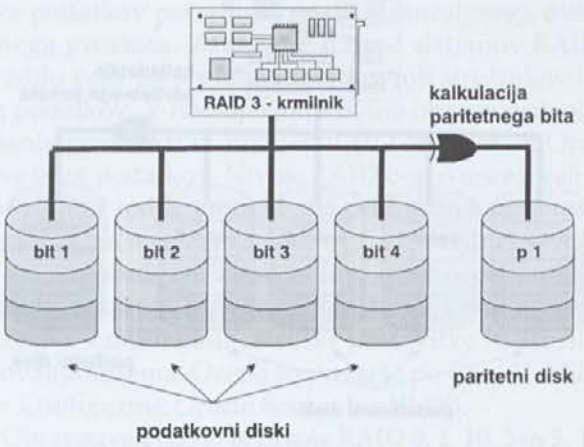
Prednosti:
- hitro branje in pisanje podatkov,
- odpoved enega diska ne vpliva močno na delovanje sistema,
- malo redundance podatkov.

Slabosti:
- kompleksni in dragi krmilniki,
- potrebno je zagotoviti sinhronizirano delovanje diskov,
- paritetni disk postane ozko grlo sistema pri pisanju velike količine podatkov.

Priporočena področja uporabe:
- urejanje in predvajanje videa,
- urejanje slik, fotografij,
- aplikacije, ki potrebujejo velik pretok podatkov.



Slika 3: RAID 2 – Hammingova koda



Slika 4: RAID 3 – paralelni prenos s pariteto

2.2.5 RAID 4

RAID 4 se od RAID 3 razlikuje po tem, da na posameznem disku ni zapisan le en podatkovni bit ampak en blok ali paket (slika 5). Tako se pri branju manjših količin podatkov lahko uporablja le enega ali samo potrebne diske, ne pa vse, kot je to treba pri RAID 3. Pri branju zato dosežemo zelo dobre rezultate, pri zapisovanju posebej manjših količin podatkov pa sistem deluje počasi, kajti tudi za najmanjšo spremembo podatkov znotraj bloka mora prej prebrati vse pripadajoče bloke na vseh podatkovnih diskih, da lahko obnovi pariteto. Prednost tega sistema je nizka cena dodatnega diskovnega prostora za kontrolne podatke v primerjavi z RAID 1 in fizično manj zapletena izdelava v primerjavi z RAID 2 in RAID 3. Zaradi slabih odzivnih časov pri zapisovanju podatkov se v strežniških bazah podatkov (npr. Oracle) ne uporablja, razen če aplikacija ne zahteva veliko sprotnega dodajanja, popravljanja in brisanja podatkov ali če nižja cena odtehta slabosti.

Prednosti:

- hitro in učinkovito branje podatkov,
- zaradi malo paritetnih diskov malo redundance podatkov.

Slabosti:

- zapleteni in dragi krmilniki,
- slaba zmogljivost pri zapisovanju in predvsem prepisovanju podatkov,
- počasno vzpostavljanje normalnega stanja ob izpadu ene komponente,
- pri pisanju velike količine podatkov paritetni disk postane ozko grlo sistema.

2.2.6 RAID 5

Sistem deluje podobno kot RAID 3 ali 4, le da je tu odpravljeno ozko grlo pri prepisovanju in brisanju podatkov. Paritetne informacije so namreč porazdeljene po vseh diskih v sistemu (slika 6). RAID 5 je danes na trgu najpogosteje uporabljan sistem take vrste. Zaradi majhne redundance podatkov je cenovno ugoden ob zelo dobrem odzivnem času pri branju podatkov in zmernem času zapisovanja. Ob izpadu enega diska le-tega lociramo in zamenjamo, potem pa sistem samodejno obnovi vsebino okvarjenega diska. En blok podatkov je lahko poljubne velikosti. Velja pa omeniti, da se z določanjem njegove velikosti da optimirati odzivne čase in konfiguracijo prilagoditi delovanju različnih sistemov. Pri obnavljanju podatkov po odpovedi in zamenjavi komponente je zmogljivost sistema močno zmanjšana.

V sistemih RAID 5 je najbolj problematično zapisovanje podatkov. Vsaka zahteva po zapisu sproži proces, sestavljen iz šestih korakov:

1. branje bloka, kamor naj bi zapisali nove podatke
2. branje pripadajočega primerjalnega bloka
3. odstranjevanje primerjalnih podatkov, ki naj bi bili prepisani
4. dodajanje novih primerjalnih podatkov
5. zapisovanje novih primerjalnih podatkov
6. zapisovanje novih podatkov.

Prednosti:

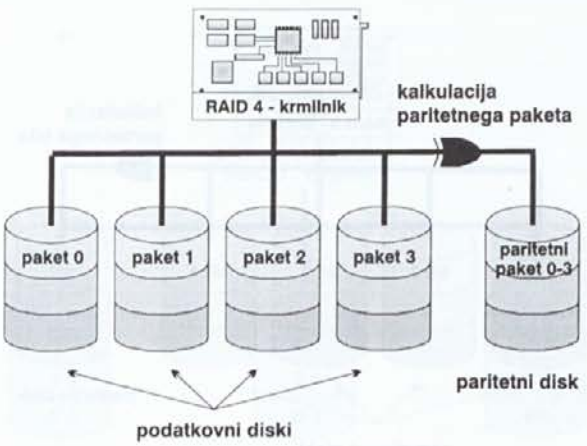
- hitro branje podatkov
- zadovoljiva hitrost zapisovanja podatkov
- malo redundantnih podatkov
- velika razširjenost.

Slabosti:

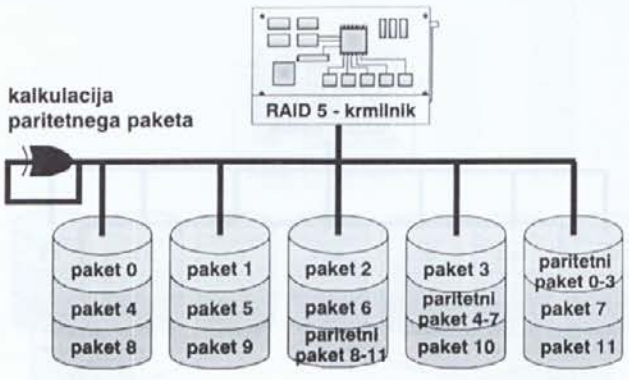
- zapleteni krmilniki
- zapleteno vzpostavljanje normalnega stanja ob izpadu ene komponente
- pri odpovedi ene komponente sistem sicer deluje, vendar se zmogljivost poslabša.

Priporočena področja uporabe:

- datotečni in aplikacijski strežniki
- strežniki za baze podatkov
- spletni strežniki in strežniki za elektronsko pošto
- intranetni strežniki.



Slika 5:
RAID 4 – neodvisni podatkovni diski s skupnim paritetnim diskom



Slika 6:
RAID 5 – neodvisni podatkovni diski s porazdeljenimi paritetnimi paketi

2.2.7 RAID 6

RAID 6 ima tako kot RAID 5 po več diskih porazdeljene paritetne informacije. Od RAID 5 se razlikuje v tem, da so paritetne informacije izračunane in zapisane dvakrat. Tako je ta sistem od nehibridnih (brez sestavljanja več osnovnih RAID konfiguracij skupaj) najzanesljivejši, vendar tudi zelo drag.

Prednosti:

- majhna občutljivost na odpovedi posameznih komponent
- idealna rešitev za sisteme, ki zahtevajo zelo veliko razpoložljivost in kjer si ne moremo privoščiti izgube podatkov.

Slabosti:

- zelo zapleteni in dragi krmilniki
- veliko redundantnih podatkov
- slabi odzivni časi pri zapisovanju podatkov
- zahteva po dodatnem disku zaradi dvonivojske paritete.

2.2.8 Drugi nivoji RAID

RAID 7 se kot izredno drag in zapleten sistem pojavlja zelo redko. Gre za asinhrono krmiljenje branja in pisanja podatkov, kar pomeni, da vsaki diskovni plošči pripada neodvisna gred, z internim operacijskim sistemom za krmiljenje in predpomnilnikom z vgrajenim paritetnim sistemom. RAID 7 je izredno zanesljiv, z odličnimi odzivnimi časi, vendar zaradi zahtevne izdelave zelo drag.

Skoraj vsi ponudniki diskovnih sistemov so razvili tako imenovane hibridne sisteme RAID, kjer se kombinirajo osnovni principi RAID. Najpogostejši so RAID 10, RAID 30 in RAID 50.

RAID 10 je kombinacija RAID 1 in RAID 0. Sistem je potemtakem tako kot RAID 1 dokaj neobčutljiv na odpovedi posameznih komponent in ima tako kot RAID 0 zelo kratek odzivni čas. Takšni sistemi so dragi, vendar vseeno precej razširjeni. Priporočljivi so za strežnike z bazami podatkov, kjer se zahtevata visoka zmogljivost in velika razpoložljivost.

RAID 30 in RAID 50 vsebujeta še bolj zapletene kombinacije osnovnih nivojev. Taki sistemi so še bolj zanesljivi in še hitrejši. Zaradi zahtevnih krmilnikov in velikega števila potrebnih diskov pa so še dražji. Njihova uporaba je zato smotrna le v dokaj redkih primerih.

2.2.9 Primerjava nivojev RAID

V tabeli 2 je predstavljena primerjava posameznih nivojev RAID (2). Če hočemo doseči sprejemljive odzivne čase in ustrezno zanesljivost ob primerni ceni, moramo dobro vedeti, kakšne so značilnosti dela, ki ga bo sistem opravljal. Vedeti moramo kolikšna je količina podatkov, kakšni so sprejemljivi odzivni časi pri branju, pisanju in obnovi sistema po okvari posamezne komponente ter kakšna je zahtevana varnost podatkov. Le tako se lahko odločimo za najprimernejši nivo RAID.

2.3. Izvedba RAID

Ponudniki sistemov za shranjevanje podatkov ponujajo nekaj načinov za namestitev RAID. Vsak od teh ima svoje prednosti in slabosti, ki jih je potrebno preučiti pred nakupom. Ti načini so:

- strežnik z vgrajenim krmilnikom za RAID, programsko krmiljenje RAID, v matično ploščo vgrajen RAID krmilnik ali kartica PCI s krmilnikom,
- zunanji RAID sistemi s poljem diskov v samostojnem ohišju, kjer je eden ali več takih sistemov povezanih s strežnikom ali delovno postajo. Posamičen samostojni RAID sistem lahko uporablja več strežnikov v večstrežniškem okolju,
- najboljša razpoložljivost podatkov je dosežena s kombiniranjem RAID sistemov in drugih komponent, ki povečujejo razpoložljivost računalniškega sistema, kot so brezprekinitveni napajalniki, gruče strežnikov, ko ob odpovedi enega prevzame delo drug strežnik itd.

Odpoved sistema povzroči stroške, med katere velikokrat ne moremo šteti le stroškov nakupa in zamenjave nove komponente, ampak tudi stroške izgube delovnega časa, izgubljenih podatkov, obnove podatkov, izgube dobrega imena podjetja in težav, ker stranke ne morejo dostopati do podatkov. Če so ti stroški veliki in če želimo povečati tudi hitrost delovanja, je pametno razmisliti o uvedbi sistema RAID. Nekateri proizvajalci sistemov RAID in uporabniki so v ta namen ustanovili organizacijo, imenovano RAID *Advisory Board* (RAD) (10), ki je definirala merila za zanesljivost sistema.

3. Sistemi RAID z vidika baze podatkov Oracle

Baze podatkov potrebujejo veliko zanesljivega diskovnega prostora. Zato se je največ sistemov RAID zgradilo prav za potrebe podatkovnih strežnikov in baz podatkov. V nadaljevanju bomo obravnavali obnašanje posameznih nivojev RAID ob uporabi Oraclove baze podatkov. Nivoje RAID bomo ocenjevali z naslednjimi sodili: zmogljivost pri naključnem branju, pri naključnem zapisovanju, pri zaporednem branju, pri zaporednem zapisovanju, pogostost izpada sistema, trajanje izpada, zmanjšanje zmogljivosti sistema v času izpada, stroški postavitve in stroški delovanja sistema. Ocene so povzete po Cary V. Millsap: Configuring Oracle Server for VLDB.

Obravnavali bomo le nivoje RAID 0, 1, 10, 3 in 5. Ti nivoji so v praksi najbolj razširjeni. Seveda je možno

Nivo RAID	Varnost podatkov	Odzivni čas pri branju	Odzivni čas pri pisanju	Odzivni čas pri obnovi sistema	Najmanjše potrebno število diskov	Primerna okolja za uporabo
RAID 0	slaba	zelo dober	zelo dober	N/A	N	nekritični podatki
RAID 1	odlična	zelo dober	dober	dober	2N x X (X = število nizov RAID)	majhne baze podatkov, transakcijski dnevnik, kritični podatki
RAID 2	dobra	zelo dober	dober	dober	N + 1	N/A
RAID 3	dobra	zaporedno branje: zelo dober transakcijski sistemi: slab	zaporedno pisanje: dober transakcijski sistemi: slab	ugoden	N + 1 (N = najmanj 2)	enouporabniška podatkovno intenzivna okolja (na primer obdelava videa)
RAID 4	dobra	zaporedno branje: dober transakcijski sistemi: dober	zaporedno pisanje: zelo dober transakcijski sistemi: slab	ugoden	N + 1 (N = najmanj 2)	baze podatkov in druge transakcijske obdelave z intenzivnim branjem podatkov
RAID 5	dobra	zaporedno branje: dober transakcijski sistemi: zelo dober	ugoden, razen če uporabljamo predpomnilnik za ponovno zapisovanje	slab	N + 1 (N = najmanj 2)	baze podatkov in druge transakcijske obdelave z intenzivnim branjem podatkov
RAID 6	odlična	zelo dober	slab	slab	N + 2	majhne in srednje velike baze podatkov s potrebo po veliki razpoložljivosti
RAID 10	odlična	zelo dober	ugoden	dober	2N x X (X = število RAID nizov)	podatkovno intenzivna okolja (dolgi zapisi)
RAID 30, RAID 50	odlična	zelo dober	ugoden	ugoden	N + 2 (N = najmanj 4, X = število RAID nizov)	srednje velike transakcijske baze podatkov in baze z velikim številom transakcij

Tabela 2: Primerjave nivojev RAID (Vir: http://www.del.com)

uporabiti tudi drugačne konfiguracije, predvsem hibridne ali sestavljene in pa konfiguracije z več kot enojnim senčenjem (3). O njihovih lastnostih se da sklepati na podlagi lastnosti osnovnih nivojev RAID.

3.1 RAID 0

Pravilno konfiguriran sistem RAID 0 lahko nudi izredno dobre rezultate pri vseh vrstah vhodno-izhodnih operacij, zaporednem (*sequential*) in naključnem (*random*) branju in zapisovanju podatkov. Tak sistem pride vpoštev le, kadar potrebujemo najcenejšo rešitev in zanesljivost ter razpoložljivost sistema nista tako pomembni.

Ocena sistema:

- Naključno branje: odlično, posebej če velikost zahtevanih podatkov, ki naj bi bili prebrani, sovpada z velikostjo bloka. Kadar so bloki premajhni, se zmogljivost pri naključnem branju lahko drastično poslabša.
- Naključno zapisovanje: enako kot branje.
- Zaporedno branje: odlično. Podobno kot pri naključnem branju je tudi tukaj zelo važna velikost posameznega bloka, ki mora biti usklajena z velikostjo bloka v Oraclovi bazi podatkov.
- Zaporedno zapisovanje - enako kot branje.
- Pogostost izpada sistema: velika. Izpad vsakega diska onemogoči delo baze podatkov in zahteva ponovno vzpostavitev sistema s pomočjo rezervnih kopij.
- Trajanje izpada: slabo. Pri vsakem izpadu je treba napako odkriti, pokvarjeno komponento zamenjati in obnoviti podatke. To je dolgotrajen proces.
- Zmanjšanje zmogljivosti v času izpada: slabo. Sistem v času izpada sploh ne deluje.
- Stroški postavitve sistema: odlično. RAID 0 je najcenejši od vseh RAID sistemov.
- Stroški delovanja: zelo slabo. Vsakokratno obnavljanje podatkov ob odpovedi posamezne komponente

zelo poveča skupne stroške sistema. Prav tako so postopki ob širjenju sistema z dokupom novih diskov precej zapleteni, kajti ves sistem je treba na novo postaviti.

3.2 RAID 1

Zrcaljenje diskov je najboljša tehnika za zmanjšanje pogostosti odpovedi. Rešitev je zelo uporabna, kadar želimo administratorju baze podatkov omogočiti razne posege v bazo, ki si jih pri drugih, cenejših sistemih ne bi mogli privoščiti.

Ocena sistema:

- Naključno branje: dobro. Obstajajo krmilniki, ki se za vsako branje posebej odločajo, katero od obeh kopij se splača uporabiti. Drugi diski lahko medtem delajo kaj drugega. Če krmilnik ne zna delati z vsakim diskom posebej, potem je zmogljivost enaka kot pri disku brez redundantnih podatkov.
- Naključno zapisovanje: dobro. V primeru, ko krmilnik zna delati z vsakim diskom posebej, je zmogljivost pri naključnem zapisovanju slabša kot pri samostojnem disku, če pa krmilnik omenjene lastnosti nima, potem je hitrost zapisovanja enaka samostojnemu disku.
- Zaporedno branje: zadovoljivo, enako kot pri navadnem, samostojnem disku.
- Zaporedno zapisovanje: zadovoljivo, enako kot pri navadnem, samostojnem disku.
- Pogostost izpada sistema: odlično. To je sistem, ki je najmanj občutljiv na odpovedi posameznih komponent, še posebej pri zrcaljenju na več diskov.
- Trajanje izpada: odlično. Če odpove samo ena komponenta, izpada sistema pravzaprav ni, ampak govorimo o delnem izpadu. Če odpovesta obe kopiji ali vse, če jih je več, seveda pride do izpada sistema.
- Zmanjšanje zmogljivosti v času izpada: odlično. Če odpove en disk, se hitrost delovanja ne spremeni. Po zamenjavi z novim se med obnovo podatkov hitrost začasno zmanjša.
- Stroški postavitve sistema: slabo. Potrebujemo dvakratno (ali celo večkratno) število diskov in RAID 1 krmilnike, ki sicer v primerjavi z RAID 3 in 5 niso najdražji, vendar vseeno dražji od navadnih.
- Stroški delovanja: zadovoljivo. Sistem ni najpreprostejši in najcenejši za vzdrževanje, vendar vseeno cenejši od tistih bolj zapletenih.

3.3. RAID 10

RAID 10 je kombiniran sistem, ki hkrati uporablja tehniko razporejanja blokov (RAID 0) in zrcaljenja (RAID 1). Tako dobimo zahvaljujoč zrcaljenju odlične rezultate z vidika neobčutljivosti na odpoved posameznih komponent in največje hitrosti pri vhodno izhodnih operacijah.

Ocena sistema:

- Naključno branje: odlično, če je nastavljena ustrezna velikost blokov. S krmilniki, ki znajo uporabljati optimizacijo RAID 1, kar pomeni branje samo enega diska, je hitrost branja celo večja kot pri RAID 0 sistemih.
- Naključno zapisovanje: odlično. Zaradi zahtev po dvojnem zapisovanju je sicer nekoliko slabše kot pri RAID 0, toda mnogo bolje kot pri RAID 5.
- Zaporedno branje: odlično. Enako kot pri naključnem branju je zelo pomembna usklajenost velikosti bloka z blokom v Oraclovi bazi.
- Zaporedno zapisovanje: odlično. Enako kot naključno zapisovanje.
- Pogostost izpada sistema: odlično. Enako kot RAID 1.
- Trajanje izpada: odlično. Enako kot RAID 1.
- Zmanjšanje zmogljivosti v času izpada: odlično. Enako kot pri RAID 1.
- Stroški postavitve sistema: slabo. Enako kot pri RAID 1, možni so celo dodatni stroški za zagotovitev principa RAID 0.
- Stroški delovanja: zadovoljivo. Tudi tukaj so seštete vse dobre in slabe lastnosti RAID 0 in RAID 1 sistemov. Vzdrževanje zahteva tehnično usposobljene kadre. Pri dograditvi sistema je potrebno letega na novo postaviti.

3.4. RAID 3

RAID 3 je odgovor na visoke stroške stoodstotnega podvajanja podatkov pri RAID 1. Ob odpovedi ene komponente sistem deluje dalje, medtem ko je komponento možno nadomestiti brez popolnega odklopa sistema, vendar je postopek zamuden in močno zmanjša čase izvajanja vhodno izhodnih operacij. Za večino baz podatkov ta rešitev ni primerna. Vpoštev pride le tam, kjer so stroški zelo pomembni in kjer je način dela tak, da ni veliko vpisovanja novih ter prepisovanja in brisanja obstoječih podatkov.

Ocena sistema:

- Naključno branje: slabo. Zaradi obveznega sinhroniziranega delovanja diskov je nemogoče vzporedno izvajati različne operacije.
- Naključno zapisovanje: slabo. Enako kot pri branju.
- Zaporedno branje: zelo dobro za sisteme z malo uporabniki, slabše za večuporabniške sisteme.
- Zaporedno zapisovanje: dobro za sisteme z malo uporabniki, slabše za večuporabniške sisteme.
- Pogostost izpada sistema: dobro. V primeru odpovedi ene komponente sistem ne odpove, pri odpovedi dveh pa je že potrebna obnovitev podatkov iz rezervnih kopij.
- Trajanje izpada: dobro. Ko izpad zaznamo, lociramo in zamenjamo pokvarjen disk, sistem sam vzpostavi podatke, ki manjkajo.

- Zmanjšanje zmogljivosti v času izpada: zadovoljivo. Dokler ne zamenjamo pokvarjene komponente, zmogljivost ni bistveno slabša. Ko pa namestimo nov disk in se sistem loti obnavljanja podatkov, zmogljivost začasno močno pade.
- Stroški postavitve sistema: zadovoljivo. Stroški odvečnih podatkov so relativno nizki, ker potrebujemo le en dodaten disk za nadzorne podatke. Potrebni so RAID 3 krmilniki, ki so v primerjavi s tistimi za RAID 0 in 1 dražji.
- Stroški izpada: zadovoljivo. Za vzdrževanje je potreben kader s posebnimi znanji, pri razširitvi je potrebno na novo postaviti sistem.

3.5. RAID 5

V RAID 5 sistemih je najbolj problematično zapisovanje podatkov, zaradi česar za baze podatkov ni priljubljen, je pa na trgu zelo razširjen na drugih področjih.

Ocena sistema:

- Naključno branje: odlično, če je sistem pravilno postavljen.
- Naključno zapisovanje: slabo. Delno lahko pomaga diskovni predpomnilnik, vendar se pri večjih količinah zapisanih podatkov tudi ta zapolni in sistem postane počasen.
- Zaporedno branje: odlično. Enako kot pri naključnem branju je pomembna pravilna postavitev sistema oziroma pravilna nastavitev parametrov.
- Zaporedno zapisovanje: dobro za sisteme z manj uporabniki. Pri večuporabniških sistemih in intenzivnem zapisovanju se diskovni predpomnilnik zapolni in zmogljivost močno pade.
- Pogostost izpada sistema: dobro. Sistem brez zaustavitve prenese odpoved enega diska, pri dveh istočasno pokvarjenih komponentah pa je potrebno obnoviti podatke iz rezervne kopije in medtem seveda sistem ne deluje.
- Trajanje izpada: dobro. Delni izpad traja toliko časa, da lociramo in zamenjamo odpovedano komponento.
- Zmanjšanje zmogljivosti v času izpada: zadovoljivo. V času delnega izpada, preden zamenjamo pokvarjeni disk, sistem deluje dobro, odzivnost se bistveno ne poslabša. Ko namestimo novo, prazno komponento in ko se prične samodejna obnova podatkov na novem disku, se delovanje sistema močno upočasni.
- Stroški postavitve sistema: zadovoljivo. Potrebujemo le en disk za odvečne podatke. Čim več diskov je v nizu, tem manjši je vpliv dodatnega diska na ceno celotnega sistema. Seveda se z večanjem niza zanesljivost sistema manjša. Krmilniki v RAID 5 so zapleteni in dragi, vendar precej razširjeni, kar jim kljub dragi proizvodnji znižuje ceno.
- Stroški delovanja: zadovoljivo. Inženirji, ki sistem vzdržujejo, morajo biti za to usposobljeni in imeti kar nekaj izkušenj. Ob razširitvi sistema je potrebno dokupiti cel nov niz ali če želimo dodati nove diske k že obstoječim nizom, je treba na novo določiti parametre.

3.6. Povzetek uporabe RAIDa v okolju Oracle

Tehnologija in cena diskov, vodil in krmilnikov se spreminjata. Zato je težko reči: »takšna konfiguracija je v takšnem primeru najboljša«. Vsekakor je najboljši pristop redno preverjanje razmer na trgu, to je razpoložljive ponudbe in vzdrževanje ter nadgrajevanje sistema, tako kot to narekujejo okoliščine in dovoljuje proračun (4).

V tabeli 3 (4) so predstavljene ocene delovanja posameznih RAID nivojev za specifične Oraclove datotečne podsisteme. Tabela je zasnovana tako, da je

Nivo RAID	Brez RAIDa	0	1	10	3	5
Zmogljivost z vidika kontrolnih datotek	2	1	2	1	5	3
Zmogljivost z vidika datotek *redo-log*	4	1	5	1	2	3
Zmogljivost z vidika sistemskih tabel	2	1	2	1	5	3
Zmogljivost z vidika sortiranja	4	1	5	1	2	3
Zmogljivost z vidika sistema *rollback*	2	1	2	1	5	5
Branje indeksiranih tabel	2	1	2	1	5	1
Zaporedno branje tabel	4	1	5	1	2	3
Intenzivno zapisovanje v bazo podatkov	1	1	2	1	5	5
Zaščita podatkov	4	5	1	1	2	2
Pristopni stroški in stroški vzdrževanja	1	1	5	5	3	3

Tabela 3: Primerjava nivojev RAID za baze podatkov Oracle

sistem RAID 10 vedno ocenjen z oceno 1 (najboljše), razen seveda pri stroških, kjer ima oceno 5 (najslabše). Drugi sistemi so ocenjeni glede na RAID 10.

4. Zaključek

Povečane zahteve po zmogljivosti strežniških sistemov in po večji zanesljivosti ob stalnem zniževanju cen sistemov za shrambo podatkov spodbujajo industrijo k razvoju vedno novih sistemov RAID in drugih dodatkov za splošno povečanje zmogljivosti prenosov V/I. Tehnike RAID, ki so bile doslej pretežno v domeni velikih sistemov, postajajo vedno bolj dostopne tudi manjšim podjetjem.

Sistemi RAID živijo v praksi že toliko časa in so že tako poznani, da so vsi proizvajalci podatkovnih baz, tudi Oracle, prilagodili svoje izdelke takim sistemom in izdali navodila in priporočila za to področje. Vendar pa se tudi programje baz podatkov hitro spreminja. Nove, izboljšane verzije, včasih z novimi funkcionalnostmi, včasih zanesljivejše, mnogokrat tudi ne, prihajajo kot po tekočem traku. Te novosti na področju programske opreme skupaj z novostmi in spremenjenimi karakteristikami strojne opreme strokovnjakom, ki morajo skrbeti za baze podatkov in načrtovati njihov razvoj, ne dovolijo počitka. Zahteve po razpoložljivosti delujoče baze podatkov se iz dneva v dan večajo. Varnost podatkov in zanesljivost, da ne pride do izgube podatkov, sta prav tako vedno pomembnejši. V času, ko se poslovanje seli na spletne strani, ko postaja zahteva po stalni dostopnosti podatkov vsakdanja, ko si ne moremo privoščiti zaustavitve sistema niti za izdelavo rezervnih kopij in sistemske posege in se cena izpada sistema drastično dviga, bodo sistemi RAID pridobivali na pomembnosti. V prihodnosti se pričakuje stopnjevanje takih zahtev, zato bo na teh področjih (varne, zanesljive baze podatkov, hitri, vedno večji diskovni sistemi) za strokovnjake in raziskovalce zagotovo dovolj dela in izzivov.

Pred uvedbo tehnike RAID je priporočljivo analizirati potrebe podjetja, predvsem dobro spoznati naravo baz podatkov, kajti pri posameznih nivojih RAID lahko z napačno izbiro dosežemo minimalne ali celo slabše rezultate kot pri navadnih diskih. Zaradi vse večjega pomena je razvoj na področju sistemov RAID in opreme za arhiviranje podatkov dokaj hiter in ga je potrebno spremljati, če želimo izbrati med vedno cenejšimi in boljšimi sistemi tistega, ki je najprimernejši za reševanje nalog v določenem praktičnem okolju, saj je dandanes zanesljiv in učinkovit informacijski sistem temelj dobrega poslovanja.

5. Literatura

1. Andrew S. Tanenbaum: Structured Computer Organization, Prentice Hall, 1999, četrta izdaja
2. Raid Technology White Paper, http: //www.dell.com/us/en/biz/topics/vectors_1999-raid.htm, marec 1999, 04.02.2001
3. E. Aronoff, K. Loney, N.Sonawalla: Oracle8 Advanced Tuning & Administration, Osborne/McGraw-Hill,
4. Cary V. Millsap: Configuring Oracle Server for VLDB, 01.03.1996,
5. Raid, http: //www6.tomshardware.com/storage/00q1/000329/, 04.02.2001
6. Raid Technology, The storage solution, http: // www.nstor.com, 04.02.2001
7. http: //www.fibrechannel.com, 04.02.2001
8. http: //www.raid-advisory.com, 12.05.2001
9. Abit Computer Corporation, BX133-RAID Users Manual, Rev. 1.00, Maj 2000
10. http://www.raid-advisory.com/rabguide.html#abouttherab, 14.03.2001
11. http://www.storagesearch.com/nstorart.html, 20.07.2001

◆

Marija Kuhar je diplomirala na višješolskem študiju pedagoške matematike in fizike na Fakulteti za naravoslovje in tehnologijo, smer matematika. Nato je pridobila univerzitetno izobrazbo na Fakulteti za organizacijske vede, smer Organizacijska informatika. Trenutno je vpisana na magistrski študij na Fakulteti za organizacijske vede, smer Management informacijskih sistemov. Zaposlena je v podjetju Grad d.d., kjer se ukvarja z razvojem integriranih informacijskih sistemov za srednja in mala podjetja.

◆

Borut Vovk je diplomiral na Fakulteti za organizacijske vede Univerze v Mariboru, smer informatika. Od takrat dalje je zaposlen v Gorenjski banki d.d. Kranj v Sektorju za informacijske sisteme. Sprva je opravljal dela programerja in analitika, od 1998 dalje pa je administrator baze podatkov. Njegovo delo je upravljanje in nadzor delovanja Oraclove baze podatkov. Prav tako se ukvarja z načrtovanjem in razvojem baze podatkov, podatkovnega skladišča in pripadajoče programske opreme v banki.

◆

Miro Gradišar je izredni profesor poslovne informatike. Diplomiral in magistriral je na Fakulteti za elektrotehniko v Ljubljani, doktoriral pa na Fakulteti za organizacijske vede v Kranju. Zaposlen je na Ekonomski fakulteti v Ljubljani, kjer predava predmete s področja poslovnih informacijskih sistemov, sodeluje pa tudi s Fakulteto za organizacijske vede. Osnovno raziskovalno področje je gradnja računalniških modelov za simulacijo in optimizacijo poslovnih procesov. Kot avtor ali soavtor je objavil pet knjig, 32 znanstvenih člankov in 46 referatov na domačih in tujih znanstvenih in strokovnih konferencah.

◆

Elektronsko prijavljanje v zdravstveno, pokojninsko in invalidsko zavarovanje

Tomaž Marčun, Irma Dovžan
Zavod za zdravstveno zavarovanje Slovenije
Miklošičeva 24, 1507 Ljubljana
tomaz.marcun@zzzs.si, irma.dovzan@zzzs.si

Povzetek

V letu 1987 je bil uveden nacionalni sistem enotnega prijavljanja v zdravstveno, pokojninsko in invalidsko zavarovanje, ki poteka na papirnih obrazcih. Obrazce pošiljajo zavezanci za plačilo prispevkov na Zavod za zdravstveno zavarovanje Slovenije (ZZZS), kjer se vnašajo še za potrebe Zavoda za pokojninsko in invalidsko zavarovanje (ZPIZ), Zavoda RS za zaposlovanje (ZRSZ) in Statističnega urada Republike Slovenije (SURS). Papirne obrazce je mogoče za določen del prijav nadomestiti z računalniškim izmenjevanjem podatkov med zavezanci in ZZZS in s tem izboljšati ažurnost podatkov in zmanjšati stroške na obeh straneh. Takšen sistem je možno uvesti za tiste prijave, kjer v skladu s pravnimi podlagami, ki urejajo to področje ni zahtevana predložitev prilog - uradnih potrdil, ki ne obstajajo v elektronski obliki. S podatkovnim povezovanjem z izdajatelji potrdil je mogoče del potrdil odpraviti. Pomemben predpogoj za uvedbo sistema je odprava mikrofilmanja obrazcev na ZPIZ in vzpostavitev nadomestnega elektronskega načina hranjenja podatkov.

Abstract

Electronic Registering into Health, Pension and Invalidity Insurance

In 1987, a national system of uniform registering into health, pension and invalidity insurance was introduced, applying paper forms. The paper forms are submitted by the contribution payers to the Health Insurance Institute of Slovenia (HIIS) where they are further entered for the purposes of the Pension and Invalidity Insurance Institute, the Employment Institute, and the Office for Statistics. In a segment of the registering operation, the paper forms can be substituted for electronic interchange of data between the contribution payers and the HIIS, thereby improving currency of data and saving costs to both parties. Such a system can be implemented in the cases of the registrations where the respective legal base does not specify submittal of attachments - formal certificates not available in electronic form. By means of data interchange with certificate issuers, a part of certificates can be made redundant. A vital condition to the implementation of such a system is the substitution of the present microfilm input of forms at the Pension and Invalidity Insurance Institute, for electronic data storage.

■■■

1. ENOTNO PRIJAVLJANJE V POKOJNINSKO, INVALIDSKO IN ZDRAVSTVENO ZAVAROVANJE

1.1. Zgodovina, obrazci in pravne podlage

Zavod za pokojninsko in invalidsko zavarovanje, Zavod za zdravstveno zavarovanje Slovenije (ZZZS) in Zavod Republike Slovenije za zaposlovanje (ZRSZ) so leta 1980 začeli izvajati projekt racionalizacije sporočanja in zbiranja istovrstnih podatkov za vodenje in vzdrževanje administrativnih evidenc o zaposlenih osebah in zavarovancih. Glede na to, da se večina podatkov iz teh evidenc uporablja tudi za izvajanje statističnih raziskovanj na področju dela, je k projektu pristopil tudi Statistični urad Republike Slovenije (SURS).

Od 1.1.1987 vsi navedeni zavodi in statistični urad uporabljajo podatke, zbrane iz skupnih obrazcev M-1, M-2, M-1A, M-3, M-3A in M-DČ, ki služijo za enotno prijavljanje oseb v zdravstveno, pokojninsko in invalidsko zavarovanje. Večnamenska uporaba enkrat zbranih in zajetih istovrstnih podatkov pomeni precejšnjo racionalizacijo tako za uporabnike evidenc, ki podatke potrebujejo za svoje delovanje, kot za dajalce podatkov pri izpolnjevanju njihovih zakonskih obveznosti.

Papirni obrazci so bili oblikovani v skladu z enotnimi metodološkimi načeli in standardi, upoštevajoč

vse specifične potrebe posameznih uporabnikov zbirk podatkov. Obrazci so ločeni glede na vrsto prijavnega postopka: prijava, odjava, sprememba podatkov, skupinske spremembe pri poslovnem subjektu, prijave družinskih članov.

1.2. Način poslovanja z obrazci

Obrazce izpolnjujejo in vlagajo zavezanci za plačevanje prispevka za socialno zavarovanje. Za osebe v delovnem razmerju in po teh osebah zavarovane družinske člane izvajajo prijavo njihovi delodajalci. Osebe, ki so same zase zavezanci za plačilo prispevka (samostojni podjetniki, lastniki podjetij, nosilci kmetijske dejavnosti, vrhunski športniki, ...), se prijavijo same. Podrobno so zavezanci določeni tudi za druge kategorije zavarovancev (brezposelni, itd.).

V določenih primerih se prijavljanje izvaja samo za pokojninsko in invalidsko zavarovanje (zaporniki, prejemniki starševskega dodatka, itd.) ali samo za zdravstveno zavarovanje (brezposelni prejemniki stalne denarne pomoči, upokojenci, vojni invalidi, veterani, vojaški obvezniki, prejemniki tujih pokojnin, itd.), v večini primerov pa za obe vrsti zavarovanj.

Zavezanci so dolžni prijave vložiti v 8 dneh od nastanka dogodka. Za zbiranje prijav in vnos podatkov so zadolžene prijavno-odjavne službe ZZZS. Zavezanci vlagajo prijave na eni od 56 izpostav glede na kraj sedeža zavezanca, poslovne enote ali poslovnega prostora, kjer oseba opravlja delo. Prijave lahko posredujejo neposredno v prijavno-odjavno službo ali jih pošljejo po pošti.

Prijavno-odjavna služba po uspešno opravljeni prijavi vrača izvod potrjenega obrazca vlagatelju kot dokazilo, da je bila prijava vložena.

1.3. Spremna dokumentacija

Zavezanci morajo pred začetkom prijavljanja oseb opraviti postopek prijave zavezanca. Ob tem morajo predložiti različno spremno dokumentacijo glede na vrsto zavezanca. Poslovni subjekti morajo predložiti obvestilo SURS o identifikaciji in razvrstitvi po dejavnosti, samostojni podjetniki morajo predložiti overovljen priglasitveni list, kmetje potrdilo o katastrskem dohodku itd. Spremno dokumentacijo je potrebno v nekaterih primerih predložiti tudi ob prijavi posameznega zavarovanca. Tujci morajo predložiti delovno dovoljenje, zaposleni pri zasebnem delodajalcu pogodbo o zaposlitvi, lastniki podjetja izpis iz sodnega registra, kmeti pa potrdilo o statusu kmeta in zdravniško spričevalo, ...

1.4. Pretok podatkov in dokumentov

Podatki, vneseni na ZZZS, se uporabljajo znotraj te institucije za potrebe izvajanja postopkov obveznega zdravstvenega zavarovanja. Isti podatki so podlaga za osvežitev podatkov na karticah zdravstvenega zavarovanja, ki so nosilec podatkov o zavarovancih in njihovem zdravstvenem zavarovanju. Podatki iz enotnih prijavnih obrazcev se usklajujejo s podatki iz Centralnega registra prebivalstva, Poslovnega registra Republike Slovenije in Registra teritorialnih enot, kar zagotavlja kvalitetno obravnavo enotnih prijav in ustrezen nivo točnosti in ažurnosti zbirk podatkov na ZZZS.

Mesečno se novo nastali podatki, vezani na pokojninsko in invalidsko zavarovanje na računalniškem mediju, posredujejo Zavodu za pokojninsko in invalidsko zavarovanje. V istem intervalu se sveži podatki o zaposlitvah oseb elektronsko posredujejo tudi na ZRSZ in SURS.

ZZZS opremlja obrazce z mikrofilmskimi številkami in jih posreduje ZPIZ, ki jih mikrofilma za potrebe vodenja arhiva uradnih dokumentov, ki izkazujejo pokojninsko dobo zavarovanca.

V letu 2000 (od 1.1.2000 do 31.12.2000) je 151.600 zavezancev vložilo 1.057.733 obrazcev. Podrobni podatki so razvidni v tabeli 1.

Ob upoštevanju stanja števila aktivnih zavarovanj na dan 31.12.2000, ki jih izkazuje tabela 2, lahko ugotovimo, da v povprečju letno zavezanci posredujejo 0,57 obrazca na zaposlenega in 0,47 obrazca na družinskega člana zaposlenega.

Tip obrazca	Število vlog
M1 (prijava zavarovanca-nosilca zavarovanja)	355.931
M2 (odjava zavarovanca)	352.120
M3 (sprememba podatkov zavarovanca)	89.708
Skupaj za zavarovance	**797.759**
M-DČ prijave družinskih članov	156.822
M-DČ odjave družinskih članov	103.152
Skupaj za družinske člane	**259.974**

Tabela 1: Število vloženih obrazcev v letu 2000 po vrstah obrazcev

2. ELEKTRONSKO VLAGANJE M-OBRAZCEV

2.1. Tehnična zasnova sistema

Analizirani sta bili dve možni tehnični rešitvi sistema elektronskega vlaganja M-obrazcev. Prva izvedba naj

Zavarovanci	1.397.388
Družinski člani	553.928
Skupaj	**1.950.316**

Tabela 2: Število aktivnih zavarovanj, stanje na dan 31.12.2000

bi temeljila na *neposrednem vpisu podatkov* prek internetne aplikacije, druga izvedba pa na *računalniškem posredovanju podatkov*. Najsodobnejša tehnologija bo omogočala še tretji način posredovanja podatkov z uporabo tako imenovanih *spletnih storitev*, kar bo prav gotovo aktualna rešitev, ko bo ta tehnologija dozorela in bodo širše uveljavljeni ustrezni standardi.

V podrobni analizi je bilo ugotovljeno, da prva izvedba ni najbolj aktualna zaradi naslednjih razlogov:

- vpis podatkov prek internetne aplikacije bi bil zamuden in zapleten, ker bi tovrstna aplikacija glede na obsežnost podatkov morala vsebovati številne kontrole vnosa podatkov, izbiranja in preverjanja šifer iz šifrantov, navzkrižnega kontroliranja podatkov;
- podatke bi bilo potrebno vpisovati ročno, čeprav pri večini večjih zavezancev že obstajajo v elektronski obliki v njihovem kadrovskem informacijskem sistemu;
- možni uporabniki takega načina dela bi bili predvsem manjši zavezanci, ki pa izpolnjujejo in vlagajo tudi manjše število obrazcev (po nekaj obrazcev na leto). Pri takšnem obsegu uporabe sistema je vprašljiva smotrnost naložbe v vzpostavitev sistema pri zavezancu.

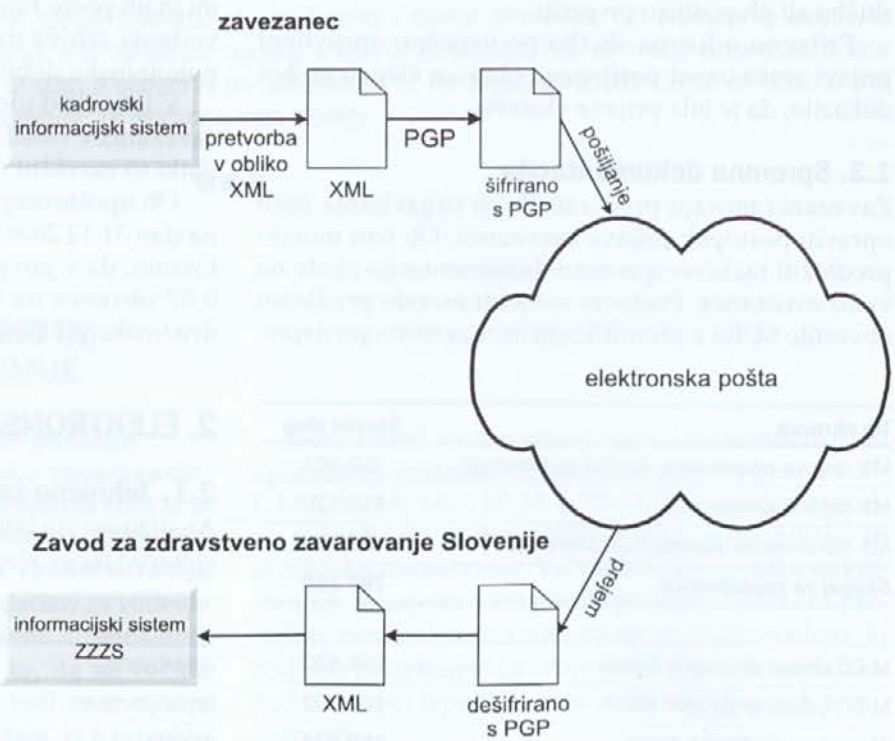
Iz navedenih razlogov je bila zato podrobneje analizirana druga možna izvedba z vzpostavitvijo računalniškega izmenjevanja podatkov. Tako izmenjevanje podatkov je možno široko vpeljati pri večjih zavezancih. Pri teh zavezancih pri večini prijav M-obrazcem ni potrebno prilagati druge uradne dokumentacije, večino potrebne spremne dokumentacije je možno ukiniti in nadomestiti z elektronskim izmenjevanjem podatkov med upravitelji zbirk podatkov (ZZZS, ZRSS in drugi).

Podrobna analiza je pokazala, da bi lahko v tak sistem vključili več tisoč zavezancev in v elektronski obliki izmenjali 600.000 obrazcev letno.

Zaradi tako velikega števila partnerjev mora sistem temeljiti na kar se da odprti, razširjeni in standardni tehnologiji. Izmenjevanje podatkov se bo zasnovalo na pošiljanju datotek prek splošne elektronske pošte. Za strukturiranje zapisa podatkov v datotekah bo uporabljen jezik XML. Z uporabo teh tehnologij zavezancem ne bo potrebno vložiti veliko virov v postavitev nove ali nadgraditev obstoječe tehnologije. Uporaba jezika XML bo omogočala kasnejšo nadgradnjo sistema v smeri spletnih storitev. Priprava podatkov na strani zavezancev mora biti čimbolj povezana v kadrovski informacijski sistem zavezanca, kar omogoča visoko stopnjo avtomatizacije postopkov in ažurno dnevno izmenjevanje podatkov.

Prenos osebnih podatkov po javnih omrežjih zahteva visoko stopnjo varovanja podatkov pred nepooblaščenim dostopom in uničenjem. Vgraditi je treba šifriranje, elektronsko podpisovanje, celovito sledenje, zanesljivost prenosa podatkov in arhiviranje celotnega prometa podatkov. V začetku uvajanja sistema bo šifriranje in elektronsko podpisovanje zagotovljeno z uporabo programa PGP. Postopek izmenjave javnih ključev in zagotavljanja istovetnosti zavezancev je moč izpeljati dokaj kvalitetno že v obstoječi organizacijski shemi, saj se mora vsak zavezanec pred vlaganjem M-obrazcev na ZZZS registrirati in ob tem predložiti ustrezna dokazila o obratovanju, pri večjih zavezancih pa obstajajo tudi drugi redni poslovni stiki in so zato ti partnerji ZZZS dobro poznani. Ko bodo v Sloveniji vzpostavljene ustrezne agencije, bo za varovanje podatkov moč uporabiti digitalna potrdila. Shemo celega sistema elektronskega vlaganja M obrazcev prikazuje slika 1.

Infrastruktura internetne elektronske pošte ne zagotavlja zanesljive dostave sporočila s podatki in zanesljivega obveščanja pošiljatelja o prispetju



Slika 1: Shema elektronskega vlaganja M-obrazcev

sporočila, zato je potrebno v sistem prenosa podatkov vključiti tudi potrjevanje uspešnosti prenosa v obliki povratnih potrditvenih elektronskih sporočil.

Zavezanci bodo podatke elektronsko posredovali v obliki pošiljke, ki bo lahko vsebovala več prijav, odjav ali sprememb zavarovanj. ZZZS bo pošiljatelja v kratkem času obvestil o uspešnosti prejema pošiljke in opravljenih formalnih kontrolah (dešifriranje, preverjanje XML-strukture pošiljke). V daljšem časovnem obdobju (do cca 2 dni) bo ZZZS prejeto pošiljko tudi podrobno preveril. Vsak elektronski dokument bo v celoti preverjen, avtomatsko evidentiran v ustrezne baze podatkov ali ročno razčiščen. Ko bodo vsi dokumenti znotraj pošiljke urejeni (prejeti ali označeni kot zavrnjeni), bo zavezancu poslano drugo sporočilo s podrobnimi podatki o uspešnosti prevzema posameznega obrazca. Postopek povzema slika 2.

Za zavezance bodo pripravljena podrobna vsebinska in tehnična navodila, ki bodo zavezancem v pomoč pri vključevanju v sistem, tudi pri testiranju. V testnem obdobju se bodo obrazci posredovali v papirni in elektronski obliki. Sistem se bo širil fazno in bo podrobno preverjen s pilotnimi partnerji.

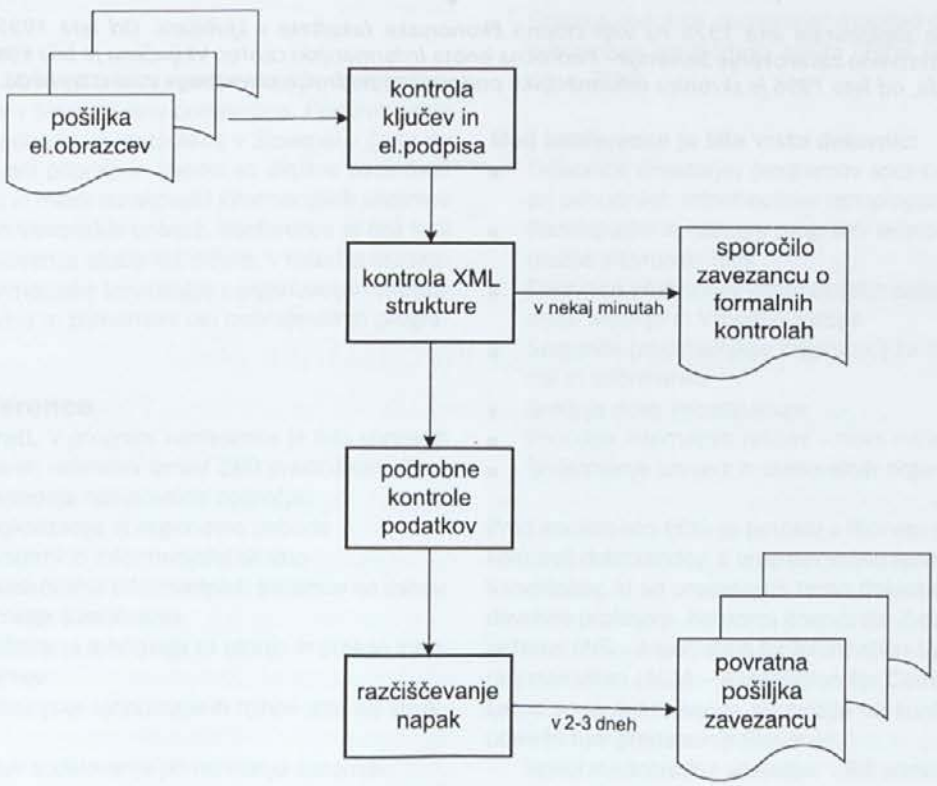
2.2. Organizacijske in tehnološke spremembe

Vpeljava opisanega sistema zahteva tudi organizacijske spremembe in celovito tehnološko podporo pri vseh vpletenih subjektih.

Pri zavezancih bo treba zagotoviti, da bodo kadrovske službe vodile ažurne evidence kadrovskega informacijskega sistema in sprotno evidentirale vse spremembe podatkov o zaposlenih. Izdelati bo treba tudi organizacijske in tehnične rešitve za kvalitetno informacijsko podporo za računalniško izmenjevanje podatkov in urejeno obravnavanje vseh povratnih sporočil ZZZS v zvezi z zavrnitvami ali uspešnim prejemom prijav.

Na Zavodu za zdravstveno zavarovanje Slovenije bo treba zagotoviti ustrezne organizacijske in informacijske rešitve za vzdrževanje in nadzor avtomatiziranega sistema prejemanja in pošiljanja podatkov. Referenti prijavnih služb, ki so pri poslovanju s papirnimi obrazci zadolženi za kontrolo, vpis, v izjemnih primerih pa tudi za izpolnjevanje obrazcev, bodo v novem načinu dela prvotno vlogo postopno v veliki meri zamenjali z vlogo kontroliranja in usklajevanja podatkov. Tako bo treba poskrbeti za zanesljivo arhiviranje vsega prometa podatkov za zagotavljanje sledi za reševanje problemov. Nekaj dodatnih organizacijskih in tehničnih rešitev bo potrebnih v času uvajanju sistema za pokrivanje aktivnosti priključevanja zavezancev (pomoč zavezancem, izmenjava javnih ključev, testiranje).

ZPIZ bo moral za primere elektronsko posredovanih M-obrazcev nadomestiti mikrofilmanje teh obrazcev z drugim sistemom zanesljivega arhiviranja



Slika 2: Prejem in kontrola podatkov, obveščanje pošiljatelja

podatkov v elektronski obliki, kar današnja tehnologija in veljavna zakonodaja seveda omogočata.

Določene spremembe so potrebne tudi v zakonodaji in drugih aktih, ki predstavljajo pravne podlage sistema. ZZZS je že dal ustrezne pobude in pripravil predloge dopolnitev.

3. ZAKLJUČEK

Elektronsko posredovanje prijav v obvezno zdravstveno, pokojninsko in invalidsko zavarovanje omogoča poenostavitev postopkov in zmanjšanje stroškov za večje zavezance, enostavnejše prejemanje podatkov, večjo ažurnost in točnost podatkov pri ZZZS in s tem tudi pri drugih institucijah, ki jim ZZZS posreduje podatke. Pomembne pridobitve sistem prinaša tudi zavarovancem, saj jim zaradi ažurnega in točnega urejanja podatkov o njihovem zavarovanju omogoča lažje koriščenje zdravstvenih storitev.

Na ZZZS je projekt razvoja opisanega sistema že v teku. Prvim zavezancem bo omogočeno, da bodo pilotne elektronske prijave posredovali že v prvi polovici naslednjega leta. ZZZS si želi tvornega sodelovanja vseh vpletenih institucij pri odpravljanju ovir za čim širšo uvedbo sistema, da bo možno sodobno storitev ponuditi vsem večjim zavezancem in s tem priti do očitnih javnih koristi.

VIRI

[1] Ministrstvo za delo, družino in socialne zadeve, Ministrstvo za zdravstvo, Statistični urad Republike Slovenije: Metodološko gradivo, I-Prijava podatkov za uvedbo in vodenje matične evidence pokojninskega in invalidskega zavarovanja, evidence zdravstvenega zavarovanja, evidence o sklenitvi delovnega razmerja (M-1, M-2, M-1A, M-3, M-3A, M-DČ), Ponatis z dopolnitvami, Ljubljana, 1998

[2] MARČUN Tomaž, DOVŽAN Irma: Elektronsko prijavljanje v zdravstveno, pokojninsko in invalidsko zavarovanje, Prispevek na Dnevih slovenske informatike, Portorož, 2001.

[3] DOVŽAN Irma, MARČUN Tomaž: Storitve Zavoda na Internetu, Prispevek na strokovnem srečanju Društva za medicinsko informatiko, Bled, 2000.

[4] KOŠIR, Franc, MARČUN, Tomaž: Elektronsko poslovanje – izkušnje in priložnosti, Zbornik, Statistični dnevi '99, Radenci, 1999 (str. 63-69), ISBN 961-6349-00-7

[5] Interna dokumentacija in podatkovni viri Zavoda za zdravstveno zavarovanje Slovenije, 2000-2001

◆

Tomaž Marčun je diplomiral leta 1991 na takratni Fakulteti za elektrotehniko in računalništvo. Od leta 1993 je zaposlen na Zavodu za zdravstveno zavarovanje Slovenije. Vodil je večje informacijske projekte, od leta 1996 je vodja Oddelka za razvoj v poslovni enoti Informacijski center.

◆

Irma Dovžan je diplomirala leta 1976 na višji stopnji Ekonomske fakultete v Ljubljani. Od leta 1995 je zaposlena na Zavodu za zdravstveno zavarovanje Slovenije - Področna enota Informacijski center. Vključena je bila v večje informacijske projekte Zavoda, od leta 1996 je skrbnica informacijske podpore za področje obveznega zdravstvenega zavarovanja.

Globalno sodelovanje v novem tisočletju

9. evropska konferenca o informacijskih sistemih – ECIS 2001
Bled, 27. –29. junija 2001
http://ECIS2001.fov.uni-mb.si

Organizatorji: Stalni odbor konference ECIS, Mednarodna zveza za informacijske sisteme, Fakulteta za organizacijske vede Univerze v Mariboru
So-organizatorji: Zveza računovodij, finančnikov in revizorjev Slovenije, Ministrstvo za šolstvo, znanost in šport, Slovensko društvo INFORMATIKA, fakultete, ki izvajajo program informatike na Univerzi v Ljubljani in Univerzi v Mariboru

Vsako leto je v drugi polovici junija organizirana tridnevna letna akademska Evropska konferenca o informacijskih sistemih (European Conference on Information Systems - ECIS). Konferenca združuje raziskovalne referate (research papers), referate o prigodkih (case study papers), panele (panels), referate o izobraževanju (teaching) in raziskovanje v teku (research in progress) ter sestanke. Pred konferenco poteka vsakokrat dvodnevni konzorcij doktorskih študentov (Ph.D. Doctoral Consortium), na katerega po enega izmed doktorskih študentov napotijo univerze evropskih držav in Izraela, ki izvajajo doktorski program informacijskih sistemov. Konference ECIS so bile doslej v naslednjih mestih: London, Amsterdam, Atene, Lizbona, Cork, Aix-en-Provence; junija 1999 je bila konferenca v Kopenhagnu, julija 2000 na Dunaju in od 27. do 29. junija 2001 na Bledu. Letošnja konferenca ECIS 2001 je bila prvič izven držav Evropske unije. Leta 2002 bo v Gdansku, Poljska, leta 2003 v Neaplju, Italija in leta 2004 v Turku, Finska. Fakulteta za organizacijske vede, Univerze v Mariboru je bila nosilka priprav konference v Sloveniji. Konferenca ECIS 2001 je imela naslov »Globalno sodelovanje v novem tisočletju« (Global Co-operation in the New Millennium).

Pomen za Slovenijo

Konferenca ECIS 2001 je bila za raziskovanje in razvoj informacijskih sistemov v Sloveniji zelo pomembna. Priprave nanjo so bile močna spodbuda za vrsto akcij v Sloveniji v času do junija 2001. Pri njeni pripravi in izvedbi so aktivno sodelovali profesorji, asistenti in mladi raziskovalci informacijskih sistemov na fakultetah obeh slovenskih univerz. Konferenca je bila tudi priložnost, da se Slovenija izkaže kot država, v kateri je raziskovanje uporabe informacijske tehnologije v organizacijah strateška razvojna sestavina in pomembni del izobraževalnih programov.

Program konference

Znanstveni referati. V program konference je bilo sprejetih prek 100 znanstvenih referatov izmed 280 predloženih. Razvrščeni so bili v naslednja raziskovalna področja:

- Globalizacija, lokalizacija in regionalne pobude
- Informacijski sistemi in informacijska družba
- Nove modeli raziskovanja informacijskih sistemov na osnovi interdisciplinarnega sodelovanja
- Posledice približevanja tehnologij za teorijo in prakso informacijskih sistemov
- Inovacije informacijske tehnologije in njihov vpliv na strukturo panog
- Inovativni modeli sodelovanja pri razvijanju sistemov
- Na znanju zasnovane organizacije: strukture in oblike sodelovanja
- Ekonomika digitalne ekonomije
- E-uprava
- Znanja in učenje v zvezi z informacijskimi sistemi: povpraševanje in ponudba
- Strategija informacijskih sistemov in organizacijska spremenba.

Uvodni referati so pokrivali široko področje, ki ga v povezavi z gospodarstvom proučujejo raziskovalci informacijskih sistemov:

- Trideset let kasneje (Anton P. Železnikar, Slovenija)
- Informacijska družba in poslovna revolucija – Evropska unija kot katalizator (Evropska komisija)
- Novi modeli poslovnih fakultet za novo ekonomijo (Howard Frank, University of Maryland, ZDA)
- Softver inženiring; Težave in priložnosti za strokovnjake informacijskih sistemov in informacijske tehnologije (Rudi Bric, Hermes Softlab, Slovenija)
- Uporaba informacijske tehnologije za gradnjo svetovnih povezav (Bernd Voigt, Lufthansa, Nemčija)
- Mobilno e-poslovanje: Izzivi za globalno sodelovanje (Kalevi Kontinen, Nokia, Finska)
- Gradnja sodobne ekonomije: mobilno poslovanje v okolju svetovnega brezžičnega spleta (Peter Keen, Keen Innovations, ZDA).

Med konferenco je bila vrsta delavnic:

- Delavnica direktorjev programov sodelovanja z univerzami pri ponudnikih informacijske tehnologije
- Raziskovalni in razvojni programi tehnologij informacijske družbe v Evropski uniji
- Delavnica profesorjev informacijskih sistemov in informatike držav Srednje in Vzhodne Evrope
- Sestanek predstavnikov organizacij za informacijske sisteme in informatiko
- Gradnja nove infrastrukture
- Ponudba internetnih rešitev – nova infrastruktura
- Sodelovanje univerz in svetovalnih organizacij.

Pred konferenco ECIS je potekal v Ribnem pri Bledu 3-dnevni konzorcij doktorandov. V program je bilo sprejetih 17 doktorskih kandidatov, ki so predstavlili temo doktorata in razpravljali z devetimi profesorji. Konzorcij financirata Zveza za informacijske sisteme (AIS – Association for Information Systems) in Zveza za računalništvo (ACM – Association for Computer Machinery). Letos se je doktorskega simpozija na konferenci ECIS prvič udeležil tudi predstavnik Slovenije.

Velika mednarodna udeležba: 388 udeležencev iz 36 držav.

M.P.

Program ECDL

1. Novi testni centri

Zaradi majhnega števila aktivnih testnih centrov (zaenkrat delujejo le trije pri družbah ISA – IT, d.o.o., KOPA, d.d. in SPIN, d.o.o.) se je Slovensko društvo INFORMATIKA odločilo, da ponovno razpiše prijavljanje testnih centrov. Pričakovali smo, da bomo z novimi testnimi centri, ki so sprejeli razpisne pogoje, sklenili pogodbe brez težav. Od 10 izbranih jih je do sedaj 8 podpisalo pogodbe.

V začetku julija smo obvestili vse izbrane ustanove in družbe, da bomo organizirali 2. delavnico za kandidate za inštruktorje in izpraševalce v drugi polovici septembra. Pogoj za udeležbo je, da organizacija sklene pogodbo in poravna svoje finančne obveznosti, kandidati pa morajo pridobiti certifikat ECDL.

Do srede septembra je izpolnila vse pogoje le ena organizacija, štiri pa delno (bodisi da še niso poravnale finančnih obveznosti ali pa kandidati še niso opravili vseh izpitov). Zato bomo organizirali drugo delavnico večkrat (prvič v Mariboru septembra, nato pa v Ljubljani). Tistim organizacijam, ki do konca leta ne bodo poravnale svojih finančnih obveznosti in ne bodo imele vsaj dveh certificiranih kandidatov za izpraševalce, ne bomo podelili koncesije.

2. Sofinanciranje ministrstva pri promociji in uvajanju ECDL

SDI je v okviru javnega razpisa za sofinanciranje projektov civilno družbenih iniciativ, ki ga je objavilo Ministrstvo za informacijsko družbo (MID), prijavilo projekt »Promocija in uvajanje ECDL v Sloveniji«. Posebna komisija MID je našo vlogo ocenila pozitivno in nam je zato MID odobrilo dobrih 1,8 milijona SIT sredstev za sofinanciranje tega projekta. Morda nam bo sedaj uspelo s programom ECDL tudi formalno 'prodreti' v državno upravo, še zlasti zato, ker so pogajanja Ustanove ECDL z Evropsko komisijo o tem, da bi certifikat ECDL postal standardno potrdilo o pismenosti na področju informacijske tehnologije, v zaključni fazi.

3. Prva gimnazija s programom ECDL pri nas

Škofijska klasična gimnazija v Šentvidu je prva srednja šola v Sloveniji, ki je v svoj učni program vključila program ECDL. Pri tem ji je pomagala družba Siemens, d.o.o. Družba Siemens nas je konec lanskega leta kontaktirala in dogovorili smo se za skupni nastop. Pri tem bi SDI kot nosilec licence s svojimi pooblaščenimi testnimi centri prevzel opravljanje izpitov in podeljevanje certifikatov ECDL, Siemens pa bi zagotovil vso potrebno opremo. Žal ni prišlo do realizacije tega dogovora.

Siemensovo sporočilo za medije vsebuje nekaj netočnosti in nejasnosti. Tako govori o 8 izvajalcih usposabljanja in testiranja v Sloveniji. V resnici imamo zaenkrat le 4 izvajalce usposabljanja (eden ni aktiven) in pet izvajalcev testiranja – testnih centrov (2 nista aktivna). Nosilci usposabljanja niso avtomatsko tudi izvajalci testiranja, ker morajo izvajalci testiranja dobiti pooblastilo za testiranje od nosilca licence, to je od SDI pri nas. Samo izobraževanje po programu ECDL, ki je javen (testna vprašanja pa so zaupna in jih dobijo le pooblaščeni testni centri), lahko opravljajo bodisi pooblaščeni centri ali druge izobraževalne ustanove.

Siemens je zagotovil Škofijski gimnaziji vso potrebno infrastrukturo, skupaj s programom za neposredno samoučenje. Zaenkrat je samoučenje možno le v angleščini (naši pooblaščeni centri šolajo kandidate v slovenščini in tudi izpiti so praviloma v slovenščini). Znanje zainteresiranih dijakov, ki bodo hoteli pridobiti Evropsko računalniško spričevalo, pa bodo lahko preverjali le pooblaščeni testni centri (po potrebi tudi v angleščini).

Odločitev vodstva gimnazije za uvedbo programa ECDL in tudi sodelovanje družbe Siemens je vredno vse pohvale. Upajmo, da bo tej inovaciji kmalu sledila še kakšna srednja šola, tako da bo maturantom omogočeno tudi potrdilo o pismenosti na področju informacijske tehnologije.

F. Žerdin

■

Prvo obvestilo in vabilo
k udeležbi in sodelovanju na devetem posvetovanju z mednarodno udeležbo

DNEVI SLOVENSKE INFORMATIKE 2002

17. do 20. april 2002, Kongresni Center Grand hotel Emona, Portorož

Slovensko društvo INFORMARTIKA prireja tudi deveto nacionalno posvetovanje informatikov in uporabnikov v tradicionalnem pomladanskem okolju Slovenskega Primorja. Namenjeno je vsem, ki se srečujejo s problematiko informacijskih tehnologij in spremljajočih dejavnosti v teoriji, v praksi in v poslu. Uveljavilo se je kot pregled dosežkov in možnosti slovenske informatike, ki v nobenem pogledu ne zaostajajo za inozemskimi. Tudi na DSI 2002 pričakujemo udeležbo in sodelovanje strokovnjakov, ki imajo interes, da bi s svojimi dosežki seznanili širšo strokovno javnost, obenem pa želijo razkrivati problematike, ki so lahko motiv in spodbuda za iskanje novih rešitev. Vsebinski okvir in razpored bo podoben kot prejšnja leta: predkonferenca, sekcije, okrogle mize in delavnice. Ob razvoju v smer informacijske družbe je nujno, da svoje dosežke primerjamo z dosežki drugih in da imamo možnost za obveščanje o novih spoznanjih. DSI 2002 bo omogočil oboje, posebej pa moramo poudariti interes sosednih držav za regionalno sodelovanje, ki je bilo uspešno zastavljeno na letošnjih dnevih slovenske informatike.

Ocenjujemo, da bo zanimanje za konferenco vsaj tako kot prejšnja leta, zaradi poudarjene mednarodne komponente pa lahko pričakujemo še večji mednarodni ugled in razpoznavnost. Vse, ki želijo svoja spoznanja, dosežke in probleme informirati informatike in uporabnike, vabimo k sodelovanju s praktičnimi in teoretičnimi prispevki. Pomnožite svoje znanje - delite ga z drugimi!

Generalna skupščina IFIP 2001

Letošnja generalna skupščina International Federation for Information Processing (IFIP) je bila letos v dneh od 1. do 5. septembra v Natalu, Brazilija. Generalna skupščina je pregled dela IFIP: poročila predsednika, sekretarja in teles - odborov, komisij in pododborov za preteklo obdobje enega leta ter spremljajoči sestanki, med katerimi je eden pomembnejših forum včlanjenih društev (Member Societies Forum). Razen tega se obravnavajo vprašanja članstva, prihodnjih sestankov in dogodkov, med katerimi so najpomembnejši svetovni kongres, generalna skupščina in sestanek izvršnega odbora IFIP. Slovensko društvo INFORMATIKA (SDI) je bilo sprejeto v IFIP leta 1998 na generalni skupščini, ki je bila eden od dogodkov na svetovnem kongresu IFIP na Dunaju in v Budimpešti. Predsednik SDI Niko Schlamberger je bil tedaj imenovan za člana odbora za marketing.

Na sestanku včlanjenih društev sta bili odmevni dve predstavitvi: predstavitev brazilskega društva Brasilian Computer Society in predstavitev Slovenskega društva INFORMATIKA ter njegovih novejših dosežkov: ustanovitev sekcije za jezik in skupaj z IFIP ustanovitev stalnega telesa za regionalno sodelovanje sosednih držav - IT STAR, ki je bil ustanovljeno na Dnevih slovenske informatike 2001. Temu so se želela pridružiti društva Slovaške in Češke, kar je bil znak, da je bila pobuda aktualna. IT STAR je odprt za vsa nacionalna društva, ki imajo interes za sodelovanje, IFIP pa bo v njem aktiven tudi v bodoče. V članstvo IFIP so bila sprejeta tri nova društva za informatiko: iz Čila, Litve in Zimbabveja. Z opazno pozornostjo je bilo sprejeta tudi informacija, da je naše društvo uradno imenovalo predstavnike v vse tehnične odbore IFIP, čeprav je bilo tudi nekaj splošne diskusije o tem, kaj je vloga nacionalnih predstavnikov v odborih. Priporočeno je bilo, da bi nacionalna društva udeležbo svojih imenovanih predstavnikov na sestankih odborov tudi finančno podprla.

Razen obveznih delov skupščine - poročila predsednika, finančnega poročila in poročil komisij in odborov IFIP so pomemben del vsake generalne skupščine volitve in imenovanja. Na letošnjih volitvah so bili izvoljeni Kurt Bauknecht, ki je bil predsednik IFIP v letih od 1995-1998, za častnega člana, za podpredsednike pa Klaus Brunnstein (Nemčija), Ricardo Reis (Brazilija in Prins Ralston (Avstralija). Za člane uprave (trustees) so bili izmed sedmih kandidatov na tajnih volitvah izvoljeni Qinsheng Wang (Kitajska), Anselmo del Moral (Španija), Jose Granado (Portugalska), Basie von Solms (Južna Afrika) in Niko Schlamberger. Slednja izvolitev je osebno priznanje, obenem pa čast tudi za Slovensko društvo INFORMATIKA in Slovenijo. Vsa poročila tehničnih odborov in zapisnik generalne skupščine so na ogled na naslovu *http://www.ifip.or.at/minutes/ga2001.htm.*

Podeljene so bile nagrade in priznanja Silver Core in Outstanding Service Award, ki ju prejmejo uredniki publikacij in posamezniki, ki so se pri delu v IFIP posebej izkazali.

Zanimiva je bila točka dnevnega reda generalne skupščine *prihodnji sestanki.* Na Dnevih slovenske informatike 2001 v Portorožu je predsednik IFIP Peter Bolerslev izrazil željo, da bi bil eden od prihodnjih dogodkov IFIP v Sloveniji. Na generalni skupščini je bil sprejet predlog, da bo sestanek Sveta IFIP v času od 4. do 7. marca 2002 na Bledu, generalna skupščina pa v času svetovnega kongresa IFIP 2002 od 1. do 4. septembra v Montrealu v Kanadi. Zaradi političnih okoliščin je bila spremenjena odločitev o svetovnem kongresu IFIP leta 2004, ki ne bo v Izraelu, temveč avgusta istega leta v Toulouseu v Franciji.

N.S

■

IFIP priporoča nove knjige

EMERGING PERSONAL WIRELESS COMMUNICATIONS
edited by Olli Martikainen, Jenni Hyvainen, Jari Porras, Lappeenranta University of Technology, Finland.
Proceedings of the Working Conference on Personal Wireless Communications (PWC'2001), sponsored by the International Federation for Information Processing (IFIP) and organized by IFIP Working Group 6.8. It was held in Lappeenranta, Finland in August 2001; http://www.wkap.nl/book.htm/0-7923-7443-6. ISBN 0-7923-7443-6, July 2001, 312 pp., EUR 165.00

GLOBAL ENGINEERING, MANUFACTURING AND ENTERPRISE NETWORKS
edited by John P.T. Mo, Division of Manufacturing, Science and Technology, CSIRO, Victoria, Australia, Laszlo Nemes, Chief Research Scientist, Commonwealth Scientific and Industrial Research Organization, Australia.
This state-of-the-art text is a collection of the effort of experts in the modelling, design and development of information infrastructures for global enterprises and networks working together in an active forum. This valuable new book will be essential reading and reference for researchers, engineers and managers at all levels involved in the present day business models of virtual enterprises and manufacturing networks. It is also a comprehensive text for students on enterprise integration, modelling methodologies and applications of information and telecommunication technologies; http://www.wkap.nl/book.htm/0-7923-7358-8 Kluwer Academic Publishers, Boston, ISBN 0-7923-7358-8, April 2001, 512 pp. EUR 230.00

COMMUNICATIONS AND MULTIMEDIA SECURITY ISSUES OF THE NEW CENTURY
edited by Ralf Steinmetz, Jana Dittmann, Martin Steinebach Institute IPSI, GMD-German National Research Center for Information Technology, Darmstadt
This volume contains papers presented at the fifth Joint Working Conference on Communications and Multimedia Security (CMS'01), which was sponsored by the International Federation for Information Processing (IFIP) and held on May 21-22, 2001, in Darmstadt, Germany. It constitutes essential reading for information security specialists, computer professionals, communication systems professionals, EDP managers and auditors, and researchers in the area; http://www.wkap.nl/book.htm/0-7923-7365-0. Kluwer Academic Publishers, Boston, ISBN 0-7923-7365-0, April 2001, 440 pp. EUR 202.00.

Vzgoja in izobraževanje v informacijski družbi	24. - 26. 10. 2001	Ljubljana	Univerza v Mariboru, FOV Institut Jožef Stefan, Ljubljana	http://lopes1.fov.uni-mb.si/is2001/ mojca.bernik@fov.uni-mb.si
8th Panhellenic Conference on Informatics	8. - 10. 11. 2001	Nicosia, CY	Greek Computer Society, Cyprus Computer Society, University of Cyprus	Manolopo@ucy.ac.cy
4th IFIP TC-11 WG 11.5. Working Conference on Integrity and Internal Control in IS	15. - 16. 11. 2001	Brussels, BE	IFIP TC-11	http://www.ifip.tu-graz.ac.at/TC11/CONF/IICIS2001
MICRO 34 – The International Symposium on Microarchitecture	1. - 5. 12. 2001	Austin, Texas,USA	University of Colorado, USA	www.microarch.org/micro34
14th Intl.Conf.on Testing of Communicating Systems	19. - 22. 3. 2002	Berlin, DE	WG6.1, GMD Fokus, BTU Cottbus	schieferdecker@fokus.gmd.de http://www.fokus.gmd.de/events/testcom2002
Work.Conf.on Formal Methods for Open Object-Based Distributed Systems	20. - 22. 3. 2002	Enschede, NL	WG6.1	rensink@cs.utwente.nl http://trese.cs.utwente.nl/fmoods2002
7th Conf.on Intelligence in Networks	8. - 10. 4. 2002	Saariselka, FI	WG6.7	kimmo.raatikainen@cs.helsinki.fi
3rd IFIP Work.Conf.on Infrastructures for Virtual Enterprises	2. - 3. 5. 2002	Vilamoura, PT	TC5, IFIP COVE Project, IST THINKcreative Project	cam@uninova.pt
Conf.on Security Visions and Perspectives in the Bright Age of Information Society	6. - 8. 5. 2002	Cairo, EG	TC11	hadidi@mailer.scu.eun.eg http://www.sec2002.eun.eg
11th Intl. World Wide Web Conference	7. - 11. 5. 2002	Honolulu, HI, US	WG6.4	david@hawaii.edu http://www2002.org/
Networking 2002	21. - 23. 5. 2002	Pisa, IT	WG6.2/3/8, CNR	enrico.gregori@cnuce.cnr.it http://www.cnuce.pi.cnr.it/Networking2002
IFIP WG9.4 Work.Conf.on ICTs and Socio-economic Development: Balancing global and local priorities	29. - 31. 5. 2002	Bangalore, IN	WG9.4	skrishna@iimb.emet.in http://is.lse.ac.uk/ifipwg94/Conference2002/ first_call.htm
IFIP WG2.6 Work.Conf.on Visual Database Systems	29. - 31. 5. 2002	Brisbane, AU	WG2.6, Univ.of Queensland, Queensland Univ.of Techn.	http://www.csee.uq.edu.au/~vdb6/
Intl.Conf.on Decision Making and Decision Support in the Internet Age	4. - 7. 7. 2002	Cork, IE	WG8.3, Univ.College Cork, Univ.Pierre et Marie Curie, Paris	fadam@afis.ucc.ie http://afis.ucc.ie/dsiage2002/
IFIP WG3.2 Work.Conf.on Informatics Curricula, Teaching Methods and Best Practice	10. - 12. 7. 2002	Florianopolis, BR	IFIP WG3.2, SBC	raul@inf.ufsc.br http://www.inf.ufsc.br/ifip2002/
IFIP Congress 2002	25. - 30. 8. 2002	Montreal, CA		George@cips.ca http://www.wcc2002.org

Pristopna izjava

Želim postati član Slovenskega društva Informatika

Prosim, da mi pošljete položnico za plačilo članarine SIT 5.200 (kot študentu SIT 2.400) in me sproti obveščate o aktivnostih v društvu.

(ime in priimek, s tiskanimi črkami)

(poklic)

(domači naslov in telefon)

(službeni naslov in telefon)

(elektronska pošta)

Datum: Podpis:

Včlanite se v Slovensko društvo INFORMATIKA.
Članarina SIT 5.200,- (plačljiva v dveh obrokih) vključuje tudi naročnino za revijo Uporabna informatika.
Študenti imajo posebno ugodnost: plačujejo članarino SIT 2.400,- in za to prejemajo tudi revijo.

Izpolnjeno Naročilnico ali Pristopno izjavo pošljite na naslov:
Slovensko društvo INFORMATIKA, Vožarski pot 12, 1000 Ljubljana.
Lahko pa izpolnite obrazec na domači strani društva
http://www.drustvo-informatika.si

INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET

Vse člane in bralce revije obveščamo,
da lahko najdete domačo stran društva na naslovu:

http://www.drustvo-informatika.si

Obiščite tudi spletne strani mednarodnih organizacij, v katere je včlanjeno naše društvo:
IFIP: **www.ifip.or.at**
ECDL: **www.ecdl.com**
CEPIS: **www.cepis.com**

INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET

Naročilnica

Naročam(o) revijo UPORABNA INFORMATIKA

- ☐ s plačilom letne naročnine SIT 4.600
- ☐ ..... izvodov, po pogojih za podjetja SIT 13.800 za eno letno naročnino in SIT 8.900 za vsako nadaljnjo naročnino
- ☐ po pogojih za študente letno SIT 2.000

Naročnino bom(o) poravnal(i) najkasneje v roku 8 dni po prejemu računa

_____

(ime in priimek, s tiskanimi črkami)

_____ _____

(podjetje) *(davčna številka)*

_____

(ulica, hišna številka)

_____

(pošta)

Datum: Podpis:

UPORABNA INFORMATIKA
ISSN 1318-1882

Ustanovitelj in izdajatelj:
Slovensko društvo Informatika, 1000 Ljubljana, Vožarski pot 12

Glavni in odgovorni urednik:
Mirko Vintar

Tisk: Prograf
Naklada: 700 izvodov

Revija izhaja četrtletno. Cena posamezne številke je 3.500 SIT.

Letna naročnina za podjetja SIT 13.800, za vsak nadaljnji izvod SIT 8.900.
Letna naročnina za posameznika SIT 4.600, za študente SIT 2.000.

Celotni Oraclov E-Business Suite.

	Oracle E-Business Suite
Marketing	✓
Spletna trgovina	✓
Prodaja	✓
Podpora uporabnikom	✓
Nabava	✓
Dobavna veriga	✓
Finance	✓
Človeški viri	✓
Aplikacijski strežnik	✓
Podatkovni strežnik	✓

Oraclove rešitve so razvite za povezano delovanje.

Aplikacije različnih proizvajalcev zahtevajo sistemsko integracijo.

Sistemska integracija stane veliko več kot sama programska oprema.

Razmislite o tem.

ORACLE®

SOFTWARE POWERS THE INTERNET™

www.oracle.si

AKTUALNO

STROKOVNE RAZPRAVE

REŠITVE