

An abstract composition on a black background. A large, irregular shape is formed by layered, textured colors: a central blue area, surrounded by orange, red, purple, and green. Scattered around this central shape are numerous short, cylindrical sticks in various colors (red, yellow, blue, green, pink, orange).

u p o r a n a INFORMATIKA

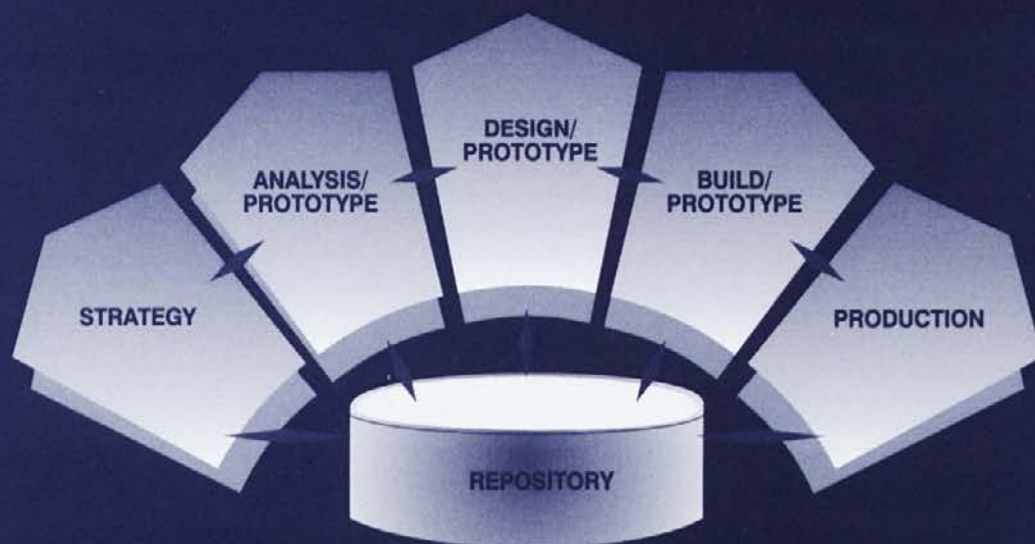
1993

ŠTEVILKA 2
OKT/NOV/DEC
LETNIK I

Aktualno
Ocenjevanje kakovosti programske opreme
Varnost v računalniških mrežah z dodano vrednostjo

PREDSTAVLJAMO ORACLE CDE (COOPERATIVE DEVELOPMENT ENVIRONMENT) USTREZNO OKOLJE ZA SKUPNO DELO

CDE so integrirana orodja za razvoj programov, ki omogočajo uporabnikom, programerjem in razvijalcem okolje za skupno delo. Vaše investicije v razvoj programske opreme so z odprtostjo in prenosljivostjo CDE popolnoma zaščitene pred poslovnimi in tehnološkimi spremembami, zaradi uporabe naprednih metod računalniško podprtega inženirstva.



**ORACLE
SOFTWARE d.o.o.**

Dunajska 156
(World Trade Center)
61000 Ljubljana
Tel.: 061/1687-004
Fax: 061/1685-009

**ŽIVLJENJSKI CIKLUS
RAZVOJA UPORABNIŠKIH
PROGRAMOV PO
PRINCIPU STREŽNIKA
IN ODJEMALCA.**

Oracle CDE podpira prilagodljiv, integriran življenjski cikel, primeren za izdelavo kakršnekoli programske rešitve - od najenostavnejše do najbolj komplicirane.

ORACLE®

Spoštovani bralke in bralci,

Ena od splošnih ugotovitev, glede katere smo si precej enotni, je, da nam za intenzivnejše vključevanje v gospodarske tokove razvitejšega dela Evrope skoraj na vseh področjih primanjkuje znanja. To velja v enaki ali pa še izrazitejši meri tudi za informatiko in računalništvo. Izobraževalni sistemi na tem področju morda še bolj kasnijo s prilagajanjem svojih učnih vsebin ter programov razvoju stroke in tehnologije kot na drugih, stabilnejših in nekoliko počasneje se razvijajočih področjih. Zato je vloga strokovnega tiska, med katerega prištevamo tudi našo revijo, toliko pomembnejša.

V prvi številki smo napovedali naša prizadevanja, da bi revija postopoma postala neke vrste strokovni forum, ki bo omogočal učinkovit in sproten prenos znanja, idej in informacij med akademsko ter raziskovalno sfero in prakso. Gre seveda za dvosmerno cesto. Na eni strani imamo univerzitetne izobraževalne institucije ter inštitute, na katerih je znanja kar nekaj, ki pa zelo težko zaide v naša podjetja, čeprav bi najbrž moralo služiti predvsem domačemu gospodarskemu razvoju. Na drugi strani pa imamo gospodarstvo, ki se zviija v krčih in svojih težav in problemov nima komu potožiti, da bi mu pomagal.

V taki situaciji bi bilo pričakovati, da bodo strokovnjaki na obeh straneh zasuli uredništvo s svojimi strokovnimi prispevki, vendar temu ni tako. Zakaj? Slovenci sicer veljamo za narod pesnikov, tudi proze napišemo kar precej, pri strokovnem, da ne govorimo o znanstvenem pisanju, pa je položaj povsem drugačen. Vzrokov je seveda več. Pisanje je bilo v preteklosti, kot morda najbolj čista oblika intelektualnega dela, povsem razvrednoteno, ne samo materialno, ampak tudi moralno. V želji, da bi domače znanje čim bolj izpostavili kriterijem in merilom mednarodne veljave, smo morda povzročili stanje, ki nikakor ni dobro za naš nadaljnji razvoj. Ko sem povabil nekaj priznanih strokovnjakov, univerzitetnih učiteljev s področja informatike, da bi kaj napisali za novo revijo, so mi nekateri kar naravnost povedali, da jih pisanje v domače revije ne zanima, saj jim to ne prinese skoraj nobenih točk za njihovo napredovanje v akademskem poklicu.

To seveda sproža celo vrsto vprašanj. Kakšna sta vloga in poslanstvo strokovnjakov, intelektualcev v naši družbi? Ali ni vsak strokovnjak, raziskovalec ali učitelj a priori tudi javni delavec, katerega moralna dolžnost je prenašati znanje na druge in to predvsem v domačem okolju.

Ali je objava članka v neki levi tuji znanstveni reviji res več vredna od prenosa znanja na generacije domačih študentov in praktikov? Upam, da bom s tem razmišljanjem vzbudil vsaj nekaj polemike v prizadetih krogih, ki jo bomo z največjim veseljem tudi objavili, morda pa bo kot revolt na to nastal tudi kakšen kvaliteten prispevek.

Veseli pa nas, da je naš poziv strokovnjakom iz prakse, kot kaže, padel na plodna tla. Pojavili so se že prvi odmevi iz različnih okolij, z zanimivimi prispevki, ki jih bomo začeli objavljati v tej in naslednjih številkah revije.

Informatika je še daleč od formalno urejene znanstvene discipline, ki bi razpolagala z vsem potrebnim inštrumentarijem, katerega izredno pomemben del je tudi strokovni jezik. Slovenci še vedno ne premoremo celovitega strokovnega slovarja za področje informatike. Po Turkovem Pojmovniku poslovne informatike je bilo sicer izdanih še nekaj manjših ali bolj specializiranih del na tem področju, kot je Simičev Pojmovnik itd.

Vendar nas tu glavnina dela še čaka. Ali je entity 'nosilec podatkov', 'predmet podatkov', 'objekt' ali pa kar entiteta, je še vedno predmet vročih razprav na mnogih omizjih. Zato vabimo k sodelovanju vse, ki jim ni vseeno, kako se opleta v naši stroki z jezikom.

Ker želimo čim bolj tekoče informirati člane našega društva tudi o dogajanju v društvu samem, pozivamo tudi vse vodje sekcij, da sproti poročajo o aktivnostih ali neaktivnostih le-teh.

Mirko Vintar
Glavni in odgovorni urednik

UVODNIK

AKTUALNO

- 5** *CENE BAVEC*
Strategija informatizacije na vladni ravni-da ali ne

STROKOVNE RAZPRAVE

- 10** *MARJAN PIVKA:*
Ocenjevanje programske opreme
- 14** *MITJA BORKO:*
Certificiranje sistemov kakovosti na področju programske opreme in informacijske tehnologije v svetu in pri nas
- 22** *BORKA JERMAN-BLAŽIČ:*
Varnost v računalniških mrežah z dodano vrednostjo
- 27** *VLADIMIR BATAGELI:*
Algoritmi za reševanje splošnega problema trgovskega potnika

POROČILA

- 33** *UROŠ PONIKVAR:*
Kam gre razvoj orodij CASE?
- 35** *NIKO SCHLAMBERGER:*
Informatika v državnih organih
- 36** *MARJAN PIVKA:*
Kakovost v programskem inženirstvu
- 37** *NIKO SCHLAMBERGER:*
East/West Communication

NOVOSTI

- 38** Načrtovanje in gradnja informacijskih sistemov
- 39** Dnevi slovenske informatike, Portorož '94
- 39** Včlanitev Slovenije v mednarodno organizacijo IFIP

KOLENDAR PRIREDITEV

- 40**

Izid te revije so finančno podprli:



VLADA REPUBLIKE
SLOVENIJE



CENTER VLADE ZA INFORMATIKO

KOMPAS

IngPOS_{d.d.}

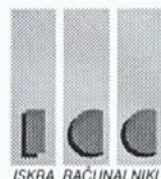
 **Ingres**

Tržaška 37, 61000 Ljubljana, tel.: 273-557, fax.: 273-460

Kompas IngPOS d.d. je ekskluzivni zastopnik ameriškega podjetja ASK Group Limited, ki nudi naj sodobnejšo relacijsko bazo podatkov INGRES™ in zastopnik firm WESTMOUNT™ in RIVA HUGIN SWEDA™.

Dejavnost podjetja:

- trženje, izobraževanje in tehnična podpora za relacijsko bazo INGRES
- svetovanje, projektiranje in izvedba rešitev z uporabo CASE orodij WESTMOUNT in razvojnih orodij INGRES.
- trženje integriranih poslovnih aplikacij in Hotelskega informacijskega sistema
- POS sistemi: razvoj, izobraževanje in trženje rešitev za gostinstvo in maloprodajo z uporabo registrskih blagajn IBM™ in RIVA HUGIN SWEDA



ISKRA Računalniki, d.o.o.

Tržaška 2, 61000 Ljubljana
tel.: (061) 214-455, 125-43-39, 125-82-12
fax: 214-087, telex: 31265ICC

Ob kombinaciji lastnega in kupljenega znanja ter s strateškimi zavezniki in dolgoročnimi poslovno tehnološkimi povezavami in partnerstvi z vodilnimi tujimi firmami (IBM, SIEMENS, OLIDATA, CHICHONY, SEAGATE, GENIUS, DELL, AST, WANG, APPLE, FUJITSU, MICROSOFT, NOVELL, BANYAN) zagotavljamo konkurenčno ponudbo produktov in rešitev informacijske tehnologije visoke kvalitete.

Razvojno-proizvodni in poslovni-tržni program podjetja:

- osebni računalniki, mikroročunalniški in miniračunalniški sistemi, podatkovni terminali, vhodno/izhodna računalniška periferija, podatkovne komunikacije za LAN in WAN mreže
- sistemska programska oprema
- uporabniški programi in rešitve
- izobraževanje, vzdrževanje in inženiring

STRATEGIJA INFORMATIZACIJE NA VLADNI RAVNI - DA ALI NE

Cene Bavec

KAM S SLOVENSKO INFORMATIKO?

Slovenija se počasi in z mukami prebija skozi fazo radikalnih sprememb, ki se bolj ali manj dotikajo vseh področij našega delovanja. Kot hiša iz kart se rušijo nekdanje resnice in pridobljene pozicije, ki so se zdele večne. Marsikaj se je spremenilo in porušilo tudi na področju informatike. Če drugega ne, smo v dveh letih izgubili primerjalno prednost pred vzhodnoevropskimi državami, na katero smo bili tako ponosni in od katere je marsikdo v Sloveniji tudi dobro živel. Upanje, da bomo svoje znanje vnovčili in postali most med računalniško razvitem zahodom in nerazvitem vzhodom, se je razblinilo v nič. Res je, da za vse nismo sami krivi, vendar je to bolj slaba tolažba.

Pred leti je bila Slovenija računalniško razmeroma razvita tudi zato, ker je bila v njej zbrana proizvodnja za jugoslovanski in vzhodni trg, nekaj pomembnih multinacionalk je vodilo jugoslovanske in deloma vzhodnoevropske posle iz Slovenije. Tako smo prišli do velikega števila kvalificiranih strokovnjakov, s tem pa se je posredno dvignila tudi splošna raven slovenske informatike. Po razpadu omenjenih trgov smo ostali s presežkom strokovnjakov, ki jih v danih gospodarskih razmerah težko ustrezno uporabimo, saj so se slovenske računalniške firme dobesedno sesule. Če k temu dodamo, da so se sesule tudi nekatere firme z velikimi računalniškimi centri, ki so v preteklosti nekaj dale za svojo informatiko, je slika trenutnega stanja zaokrožena. Veliko število majhnih preprodajalskih firm, ki so nastale v zadnjih dveh letih, sicer predstavlja rešitev za udobno preživetje posameznikov, še zdaleč pa ni najboljša rešitev z nacionalnega vidika.

Ko se sprašujemo, kam naj se v bodoče usmeri slovenska informatika, smo polni lastnih idej in primerjalnih podakov iz dežel, ki bi jim bili radi podobni. Cilj je več ali manj jasen, vsaj zdi se nam tako, pot do njega pa je zelo vijugasta. Zato ni čudno, da se marsikdo počuti zgubljenega in si želi usmerjanja ali pomoči, med drugim tudi države. Vprašanje je, ali so take želje sploh upravičene in izvedljive, glede na stanje v katerem se država nahaja. Poleg tega je država večglavi zmaj, tako da človek nikoli ne ve s katero glavo naj se pogovarja in katera o čem odloča. Ravno zaradi tega bi morali jasno opredeliti, kaj naj država v skladu s svojo vlogo stori, predvsem pa minimum, ki bi ga morala opraviti. Posebej moram poudariti, da omenjena razmišljanja ne slonijo

na neposrednem državnem urejanju, ki presega ukrepe običajne v tržno razvitih državah. Sploh pa ne mislim na "spodbujevalne" državne ukrepe, ki smo jim bili priča v ne tako daljni preteklosti.

V bistvu bi se morali odločiti za enega od dveh pristopov, ali za skrbno izbrano kombinacijo. Prvi pristop, ki se, hvala bogu, uresničuje sam od sebe, pomeni, da je vsako področje informatizacije prepuščeno lastnim uravnalnim mehanizmom. Proizvodnja informacijske tehnologije je npr. podrejena samo tržnim zakonom, davčna in carinska politika sta del splošne ekonomske politike, znanstvena in raziskovalna dejavnost na področju informatike je utopljena v splošen raziskovalni koncept, država in javni sektor se informatizirata po lastnih parcialnih projektih, trg informacijskih storitev se rojeva v hudih mukah in podobno. S tem konceptom ni v bistvu nič narobe, saj bomo tudi z njim preživeli in bo vedno rezervna možnost, vprašljiva sta le njegova učinkovitost in čas, ki ga na žalost nimamo za razmetavanje. Drugi pristop pa je združujoč pogled na informatiko z vidika splošne državne strategije družbenoekonomskega in tehnološkega razvoja, ki omogoča zavestno vsklajevanje in prepletanje ukrepov različnih državnih resorjev v upanju, da bo prišlo do njihovega sinergizma.

ZAKAJ VLADNI UKREPI?

Pregled tujih vladnih strategij kaže, da ima le malo držav, predvsem so to azijske, posebno strategijo na področju razvoja, proizvodnje in uporabe informacijske tehnologije, ki pa praviloma ni bila javno objavljena. Večina razvitih držav nikoli ni imela posebne strategije, saj so informatizacijo urejali preko utečenih tržnih in upravnih mehanizmov ali v okviru širše tehnološke strategije. Eden od razlogov za sprejem posebnih vladnih strategij na tem področju je ugotovitev, ki je za nas še posebej pomembna, da so majhne države v drugačnem položaju kot velike. Za majhne ekonomije je informacijska tehnologija predvsem nekaj, kar morajo čim bolj učinkovito uporabiti, za velike pa strateško pomemben proizvod, ki ga hkrati tudi tržijo.

Kaj naj stori Slovenija, ki se nahaja v izredno pomembni in občutljivi razvojni fazi. Na žalost še vedno nimamo strategije družbenoekonomskega ali vsaj

tehnološkega razvoja, na katerega bi se lahko naslonila tudi strategija informatizacije. Zato je vprašljivo, ali je sploh smiselno sprejeti posebno strategijo na državni ravni, če ta ni integralni del neke širše strategije, saj informatika ni nikoli sama sebi namen in jo ne moremo ločevati od osnovne dejavnosti, ki naj bi jo podpirala. Kljub temu pa vrsta dejstev kaže, da je Slovenija v tako izjemnih razmerah, da bi morali razmisliti tudi o taki možnosti, čeprav ni optimalna.

Prepričan sem, da na področju razvoja, proizvodnje in uporabe informacijske tehnologije v Sloveniji ne moremo slepo sprejeti logike popolnega tržnega in državnega liberalizma ter pričakovati, da se bo sprožil samouravnavni mehanizem, ki bo sam od sebe urejal stvari. Zavedati se moramo, da še nimamo pravega trga, kot ga poznajo tržno razvite države, ki bi s svojimi mehanizmi usmerjal razvoj v smer, ki je za nas optimalna ali vsaj sprejemljiva. Po drugi strani tudi nimamo države z uveljavljenimi pravili igre, ki bi omogočala usmerjanje razvoja prek velikih državnih projektov ali morebitnih neposrednih državnih vlaganj. Da država v sistemskem smislu še ni zgrajena, je razvidno tudi iz skrajno pomanjkljive zakonodaje, ki je temeljni pogoj za delovanje trga in države. Zato stanja v Sloveniji ne moremo enostavno primerjati s stanjem v razvitih državah ali v državah na podobni razvojni stopnji, vendar z daljšo tržno tradicijo.

Že zelo površno razmišljanje nas napeljuje na zaključek, da bi bilo dobro, če bi država v svoji funkciji nekaj naredila na strateško tako pomembnem področju, kot je informatizacija. Odprto pa ostane vprašanje kaj, kdaj in kako. Informatiki vemo, da se zelo veliki in ambiciozni projekti radi ponesrečijo, zato ni odveč določena previdnost in postopnost. Začeti bi morali z zelo splošnimi usmeritvami, ki bi služile za pripravo nujno potrebnih kratkoročnih ukrepov Vlade RS. Šele v naslednjem koraku bi, če bi bilo to potrebno seveda, izdelali dolgoročno strategijo, ki bo v skladu s splošno razvojno in ekonomsko strategijo Slovenije.

PROIZVODNJA OPREME, DA ALI NE?

Ena od dilem, do katere se bomo morali opredeliti, je vprašanje, ali se bomo usmerili samo v učinkovito uporabo informacijske tehnologije, ki jo bomo uvažali, ali pa jo bomo tudi razvijali in proizvajali. Še pred kratkim je slovenska država izdatno pomagala razvoju in proizvodnji informacijske tehnologije, saj je težila k samozadostnosti tudi na tem področju, hkrati pa je predpostavljala, da je naša primerjalna prednost z vzhodnoevropskimi državami nekaj dolgoročnega. Vendar pa se lahko gremo informatizacije tudi brez lastne proizvodnje opreme. Nekatere azijske države so uspešen primer, ko se je država zavestno odločila in podprla tudi proiz-

vodno računalniške in komunikacijske opreme. Vrsta manjših razvitih evropskih držav pa se za obsežnejšo proizvodnjo opreme sploh ne zanima. Po mojem mnenju jim lahko mirno sledi tudi Slovenija, z zelo pomembnim dopolnilom, da se ne smemo in ne moremo izogniti proizvodnji programske opreme.

V odprti tržni ekonomiji je nosilec strategije razvoja in proizvodnje informacijske tehnologije gospodarstvo. Zato bo tudi v Sloveniji končno odločitev sprejelo samo gospodarstvo, vendar pa bo ta odločitev odvisna tudi od tega, ali bo vlada pri tem kaj pomagala, ali ne bo. Jasno nam mora biti, da brez državne spodbude proizvodnja informacijske tehnologije v Sloveniji ne more postati pomembnejša gospodarska panoga. Pa še v tem primeru je, zaradi izjemne mednarodne konkurence, izid zelo negotov. Aktivna davčna in carinska politika sta samo eno od orodij, ki jih ima vlada in jih lahko učinkovito uporabi. Druga možnost je združevanje razvojnih potencialov in proizvodnih zmogljivosti slovenskih firm pri državnih in infrastrukturnih projektih, ki so v glavnem proračunsko financirani in o njih odloča vlada. Mimorede, samo za telekomunikacije bomo v naslednjih desetih letih porabili okoli 2 milijardi USD. Tudi znanstveno raziskovalna politika, ki je vezana na državno financiranje, lahko neposredno poveča možnosti za tržno uspešno proizvodnjo.

To je samo nekaj elementov, ki kažejo na široko paleto vladnih mehanizmov, ki se lahko sprožijo zavestno in vsklajeno, ali pa delujejo medsebojno popolnoma ločeno, kot je to sedaj. Jasna in časovno stabilna strategija vlade v zvezi s temi mehanizmi, ki ni nujno vezana na neposredno finančno pomoč, je za gospodarstvo izredno pomemben razlog za odločitev za ali proti lastni proizvodnji na določenih segmentih. Postopoma bi se pokazale tudi primerjalne prednosti, ki bi jih posebej spodbujali. Po prvi oceni je to predvsem proizvodnja kvalitetne programske opreme in izdelava specializiranih celostnih rešitev, ki vključujejo aparaturno in programsko opremo.

DRŽAVNI IN INFRASTRUKTURNI PROJEKTI

Zelo učinkoviti so tudi posredni vladni ukrepi, kot je npr. združevanje sposobnejših proizvajalcev in ponudnikov storitev okoli velikih projektov informatizacije za državno upravo in javne službe, ki se financirajo iz proračuna. To je z zornega kota vlade daleč najcenejši ukrep, ki ne zahteva dodatnih finančnih sredstev. Zadostuje že samo usmerjanje obstoječih namenskih sredstev v projekte, ki so med seboj tehnološko in metodološko vsklajeni do te mere, da jih lahko združimo v logično zaključene večje projekte. S tem bi preprečili izredno razdrobljenost sedanjih projektov, ki so sami zase praviloma tako majhni, da izvajalcem ne omogočajo potrebne specializacije in dolgoročnega vlaganja v kvaliteto svojih izdelkov.

Veliko majhnih projektov le na videz spodbuja konkurenco in znižuje ceno, pogosto celo pod razumno mejo, saj je končni izid predvsem nezanesljivost in nizka kvaliteta izdelkov. Firme živijo iz dneva v dan in se sploh ne upajo pomisliti na specializacijo in kvaliteto, ki sta prvi pogoj za morebiten mednarodni prodor, hkrati pa ne čutijo potrebe po medsebojnem sodelovanju, saj so projekti tako razdrobljeni in unikatni, da z njimi lahko opravi vsak zase.

Vse razvite države so do sedaj podpirale domačo proizvodnjo aparaturne in programske opreme na ta način, da so dajale prednost svojim proizvajalcem in jih še posebej spodbujale k medsebojnemu sodelovanju in skupnemu vlaganju v razvoj. Tako so postopoma nastajale večje (za naše razmere) in izjemno kvalitetne firme, ki lahko preživijo tudi v ostri mednarodni konkurenci. V slovenski javni upravi ni niti sledu po takem pristopu. Določena izjema je le vsklajevanje projektov v okviru ožje državne uprave, pa še tu so izvzeti veliki resorji, kot sta notranje zadeve in obramba. Posebej pa kaže poudariti, da je cilj omenjenega vsklajevanja nadzor nad porabo finančnih sredstev in ne spodbujanje tehnološkega razvoja in kvalitetnega podjetništva, kar še zdaleč ni eno in isto. Oba cilja sta si v praksi pogosto celo v nasprotju, zato bi se morali na vladni ravni odločiti, kaj je tisto, kar želimo.

Evropska skupnost in države članice imajo za potrebe svojih uprav enake tehnološke standarde in predpisane metodologije (npr. GOSIP - Government Open System Interchange Profiles), ki jih brez vprašanja spoštujejo veliki in majhni ponudniki. Prehod naše uprave na te standarde bi bil šok in bi brez dvoma povzročil upor svobodnih strelcev, ki krojijo informacijsko usodo naših državnih resorjev, vendar bi imel izjemno ugodne dolgoročne učinke. Predvsem pa bi po kvaliteti in standardih izenačil naše proizvajalce in ponudnike storitev s tujimi in jim vsaj načelno omogočil vstop v mednarodne projekte.

Posebna zgodba so veliki infrastrukturni projekti, kot so telekomunikacije. Ker gre za izjemno velika vlaganja v tehnologijo, ki je za državo strateškega pomena, bi morali projekte obravnavati z različnih zornih kotov. Informatike bo npr. težko prepričati, da je izgradnja telekomunikacijskega omrežja in uvajanje spremljajočih storitev le stvar PTT (po novem Telekomu) in Ministrstva za promet in zveze. Za državo bi bilo iz čisto racionalnih razlogov veliko bolje, da bi pri podobnih projektih že v naprej zagotovila medresorsko sodelovanje in odločanje. Vendar to zahteva neko vsklajevanje nad ministrstvi, kar pa je trenutno zelo heretična ideja.

RAZISKOVALNO RAZVOJNA STRATEGIJA

Razvoj, proizvodnja in uporaba informacijske tehnologije

so dejavnosti, ki zahtevajo visoko stopnjo znanja, zato je razumljivo, da so močno naslonjene na akademsko raziskovalno sfero. Za Slovenijo je strateškega pomena, da poveže gospodarstvo, uporabnike in raziskovalno sfero, vendar ne le na papirju in na besedah. Trenutno stanje je vse prej kot spodbudno, saj ima človek občutek, da gre za tri različne svetove, ki se le občasno in naključno zblížajo. Po eni strani je res, da raziskovalne institucije nimajo pravih partnerjev v gospodarstvu, ki se bori za vsakodnevno preživetje in se izogiba dolgoročnim načrtom in investicijam. Res pa je tudi, da so prioritete na področju financiranja projektov s področja informatike izrazito akademske in le redko odražajo realne potrebe slovenskega okolja. V letošnjem letu se je celo zgodilo, da država skoraj ni financirala raziskovanj na področju informatike. Zato je znanstveno raziskovalna dejavnost eno od področij, kjer bi se morala država (Ministrstvo za znanost in tehnologijo ni dovolj) odločiti za svoje prioritete in za njimi stati tudi finančno.

Ko bi imeli vsaj okvirno strategijo informatizacije, bi veliko lažje izbrali tista raziskovalna in razvojna področja, ki neposredno podpirajo skupne cilje. S tem bi se izognili razdrobljenosti raziskovanj, ki ni le draga, ampak tudi neučinkovita. Selektivnost je nekaj povsem normalnega za tako majhno ekonomijo, kot je slovenska, vsa modrost je le v tem, da se izberejo prave prioritete. Na področju informatike je izbor razumnih prioritete še posebej zahtevna naloga, saj moramo upoštevati izjemno veliko parametrov, ki odražajo razvojne trende v svetu, poleg tega pa še vse domače možnosti in omejitve.

MEHANIZMI, KI SO V ROKAH DRŽAVE

Do sedaj smo povzeli le nekaj področij, kjer bi lahko država brez nepotrebne vmešavanja in z minimalnimi naporimi veliko storila zase in za slovensko informatiko. Najbrž bi morali omeniti še vlogo države pri vzpostavitvi trga informacijskih storitev, kar je z uporabniške plati ena prioritetenih nalog v bližnji prihodnosti. To je eno od tistih področij, kjer so si celo zahodnoevropske države privoščile precejšnje državne intervencije. Vendar je to zaključena in zahtevna tema, ki zasluži podrobnejšo obravnavo v posebnem prispevku.

Če ta razmišljanja nekoliko strnemo in se ne spuščamo v podrobnosti, potem je za informatizacijo pomembno, da država zagotovi:

- mednarodno združljivo zakonodajo, ki bo nudila varnost in stabilnost proizvajalcem in uporabnikom informacijske tehnologije;
- davčno in carinsko politiko, ki upošteva specifiko in spodbuja proizvodnjo in uporabo aparaturne in programske opreme;

- izgradnjo in delovanje tehnološko najsodobnejše infrastrukture, kot so telekomunikacije s spremljajočimi storitvami;
- tekoče uvajanje mednarodnih standardov in priporočil ter atestiranje strojne in programske opreme;
- prokurativo projektov javnega sektorja (standardizacija postopkov za nabavo opreme in storitev, standardizacija opreme in metodologij, kriteriji za kvaliteto);
- znanstveno raziskovalno delo, razvojne projekte in tehnološke parke na področju informatike;
- sistem izobraževanja (v okviru rednega študija in kot dopolnilno izobraževanje ob delu);
- organizirano promocijo Slovenije kot tehnološko napredne in poslovno zanesljive dežele;

Kot sem že omenil, lahko država uporablja omenjene mehanizme vsakega zase, kar bi v praksi lahko pomenilo, da se učinki posameznih ukrepov med seboj celo izničijo. Lahko pa jih uporablja tako, da v naprej predvidi njihove medsebojne vplive in poskuša doseči najugodnejše učinke. To pa je v osnovi že strategija, o kateri smo govorili.

KJE SO PROBLEMI?

Zakaj pravzaprav sploh zgubljam besede o vlogi države, bolje Vlade RS, pri razvoju slovenske informatike? Ali ni samo po sebi razumljivo, da vlada in njena ministristva naredijo svoje tudi na tem področju? Ali je informatika nekaj tako posebnega, da zahteva poseben pristop? Naj začnem odgovor na ta vprašanja z ugotovitvijo, da Vlada RS in slovenska državna uprava delujeta izrazito resorsko, kar pomeni, da ima vsako ministristvo ali vladna služba svoje naloge in finančna sredstva, ki se ne prekrivajo z ostalimi. Sistem je dovolj učinkovit, da omogoča delo pri tistih projektih, ki so vezani samo na en resor, postane pa zelo neučinkovit, ko se spopade z nalogami, ki jih ni mogoče pripisati samo enemu ministristvu. Vse skupaj postane še bistveno bolj zapleteno, ko naj bi se naloge tudi medministrsko financirale, zato takih projektov praktično sploh nimamo.

Informatika se, na žalost, dotika praktično vseh resorjev in zato nima matičnega ministristva, ki bi zanjo skrbelo v upravnem in finančnem pogledu. Ministristvo za znanost in tehnologijo bo šele po novi zakonodaji o pristojnosti ministristev verjetno dobilo tudi nekaj pristojnosti na področju splošne informatike in ne samo za njene znanstveno raziskovalne vidike. Sedaj te pristojnosti formalno nima. Vladni center za informatiko je pristojen za interno informatizacijo državne uprave in posredno tudi za tehnološko in metodološko vsklajevanje internih projektov ter prokurativo. Ministristvo za promet in zveze je v celoti pristojno za telekomunikacije, zato je moralo

Ministristvo za znanost in tehnologijo v letu 1993 nanj prenesti vse svoje projekte s tega področja. Ministristvo za ekonomske odnose in razvoj in Ministristvo za gospodarske zadeve sta pristojni za razvojne vidike in proizvodnjo informacijske tehnologije, Ministristvo za finance pa v celoti nadzoruje porabo proračunskih sredstev tudi v te namene. Ministristvo za notranje zadeve, Ministristvo za obrambo in Ministristvo za okolje in prostor pa so primer velikih uporabnikov informacijske tehnologije in naročnikov aplikativne programske opreme.

Ker v okviru Vlade RS nimamo dovolj močnih in operativnih mehanizmov, ki bi omogočali, če ne kar spodbujali, zapletena medministrska vsklajevanja in vodenje skupnih projektov, je zadeva z informatiko zapletena že samo zaradi formalnih razlogov. Posamezna ministristva se izogibajo vsklajevanju in ga pogosto razumejo kot vdor v svoje pristojnosti in samostojnost. Temu moramo dodati še vsebinske probleme, kot je pomanjkanje vladne strategije družbenoekonomskega razvoja, ki je trenutno izdelana le po nekaterih segmentih. Podobno velja za strategijo tehnološkega razvoja, ki naj bi sledila iz omenjene strategije. Šele potem pride na vrsto informatizacija.

Na koncu kaže omeniti verjetno najpomembnejši razlog, da bomo težko prišli v kratkem času do konzistentne strategije informatizacije Slovenije. Očitno je to tudi strokovno izredno zahtevna naloga, ki jo ne more opraviti država s svojim kadrovskim aparatom, ampak se mora nasloniti na zunanje strokovnjake in organizacije. Naloga je interdisciplinarna in bo zahtevala veliko vsklajevanja na strokovni ravni kot tudi v okviru vladnih resorjev, zato je eno leto za njeno izdelavo že zelo optimistična napoved. Na to nas napeljuje tudi razprava v okviru problemske konference o informatiki, ki je bila junija v Grimščah, ko je Ministristvo za znanost in tehnologijo predstavilo svoje poglede na to problematiko. Pokazalo se je namreč, da so pogledi posameznih institucij, še posebej vladnih, v osnovi odklonilni. Druge se sicer zavzemajo za neke vrste vladno strategijo, vendar le v tistem delu, kjer naj bi država nekaj financirala. Tudi mnenja posameznih strokovnjakov s tega področja so si bila pogosto v popolnem nasprotju.

ZAKLJUČEK

Če strnemo dosedanje ugotovitve, ki zajemajo le manjši del rezultatov dosedanega dela pri zasnovi splošne strategije informatizacije, se izkaže, da je priprava globalne vladne strategije v trenutnih razmerah zelo vprašljiva. Dejstvo je, da jo lahko sprejmemo le pod pogojem, da imamo jasno opredeljene omejitvene in spodbujevalne faktorje tako na strani države kot pri proizvajalcih in uporabnikih. Tega nimamo. Drugi pogoj je potrebno soglasje vseh prizadetih, vezano na skupne interese, saj

na silo ne moremo storiti ničesar. Tretji pogoj, ki ga do sedaj nismo omenili, pa je temu projektu naklonjeno politično ozračje, ki bi omogočilo prepotrebno vladno in medministrsko vsklajevanje in se odražalo tudi v namenskih sredstvih v državnem proračunu.

Problema se bomo morali lotiti postopoma. Posamezna ministrstva in vladne službe imajo svoje parcialne poglede in načrte, zato ne smemo misliti, da začenjamo od nič. Investicije v telekomunikacije in spremljajoče organizacijske spremembe so že v teku. Projekti informatizacije državnih resorjev se vsaj na papirju že vsklajujejo, v naslednjem letu bodo imeli raziskovalni in razvojni projekti s področja informatike večjo državno podporo in višjo prioriteto in podobno. V večji ali manjši meri se dela tudi pri drugih nalogah, ki smo jih prej že omenili. Še vedno pa med temi aktivnostmi ni nobene povezave. Zato je prioriteta naloga, za katero zadostuje že dobra volja in ustrezna organiziranost na vladni ravni, da začnemo v letu 1994 vsklajevati aktivnosti v okviru stalne medministrske koordinacije. Zelo veliko bi naredili, če bi se dogovorili za enotne kriterije, ki bi odražali globalne cilje, in prek njih vskladili državne razpise za opremo in storitve (to lahko storijo Ministrstvo za finance, Vladni center za informatiko in Ministrstvo za znanost in tehnologijo ob sodelovanju drugih zainteresiranih resorjev). Radikalna rešitev bi bila tudi hiter prehod na standarde, ki veljajo v Evropski skupnosti (GOSIP). Pozabiti ne smemo tudi na razpise za financiranje znanstveno raziskovalnih projektov in spodbujanja tehnološkega razvoja, ki bi jih morali obravnavati tudi z zornega kota državnih in infrastrukturnih projektov kot tudi širšega spodbujanja gospodarskih dejavnosti.

Ministrstvo za znanost in tehnologijo bo po spreje-

mu nove zakonodaje o pristojnosti ministrstev poslalo Vladi RS predlog, da kljub pomanjkanju širše vladne strategije sprejme nekatere operativne sklepe, ki bodo zagotavljali vsaj minimalno raven vsklajevanja med ministrstvi. Ministrstvo bo tudi posebej podprlo financiranje tistih raziskovalnih projektov, ki bodo kasneje strokovna podlaga za izdelavo dolgoročne državne strategije na področju informatizacije. Poleg omenjenih kratkoročnih in pragmatičnih ukrepov moramo pripraviti tudi dolgoročne usmeritve. Vseeno je, ali temu rečemo vladna strategija, ali pa kaj drugega, pomembno je, da imamo opredeljene skupne cilje, ki jih morajo v okviru svojih pristojnosti spoštovati vsi državni resorji.

Zaključek je preprost. Sloveniji bi zelo prav prišla globalna vladna strategija na področju informatizacije, če bi jo lahko pripravili in jo kasneje tudi uresničili. Če je ne bo, se bomo morali zadovoljiti s parcialnimi strategijami posameznih resorjev in včasih neuskkljenimi in nasprotujočimi se ukrepi. Resnično usodo informatike bodo krojile predvsem družbeno ekonomske razmere, kjer pa bo imela vlada vedno vmes svoje prste. Zato se hočemo ali nočemo ne bomo nikoli izognili vplivu države tudi na informatizacijo. Želeli bi le čimbolj strokovne in dolgoročno uspešne posege.

ZAHVALA

Čeprav so razmišljanja v tem prispevku izrazito osebna, se moram zahvaliti dr. Marjanu Krisperju in dr. Petru Stanovniku, ki sta sodelovala pri pripravi nekaterih dokumentov za potrebe Ministrstva za znanost in tehnologijo in sta mi ob tem pomagala pri razčiščevanju marsikatere dileme.

OCENJEVANJE PROGRAMSKE OPREME

Marjan Pivka
Univerza v Mariboru, Ekonomsko-poslovna fakulteta Maribor
Razlagova 14, 62000 Maribor

POVZETEK

Članek obravnava vprašanje ocenjevanja programske opreme in pokaže na razlike med ocenjevanjem, preskušanjem in testiranjem. Avtor poudarja, da je bistvo ocenjevanja v analiziranju semantične komponente programskega izdelka in analizira vprašanje merjenja količine kakovosti za posamezne karakteristike kakovosti po mednarodnem standardu ISO/IEC DIS 9126. Članek je delno povzet po referatu z enakim naslovom, ki je bil predstavljen na posvetovanju "Kakovost v programskem inženirstvu" septembra 1993 v Radencih.

ABSTRACT

In the paper, the differences between testing and assessing are analysed. Author emphasizes that assessment procedure is essentially a semantic analysis of software product. He researches measuring quality characteristics based on international standard ISO/IEC DIS 9126. The paper partly resumes the discourse author had at the Software Engineering Quality Conference, September 1993, in Radenci.



1. OPREDELITEV PROBLEMA

V vsakdanjem življenju nas proizvajalci na različne načine prepričujejo, kako kakovostni so njihovi izdelki. Proizvajalci uporabljajo vse mogoče metode, od bolj ali manj agresivnih reklam, do plačanih mnenj in ocen različnih strokovnjakov, institucij in podobno. Tem in podobnim ocenam kot uporabniki verjamemo, ali pa ne. Vse prevečkrat se zgodi, da šele po določenem času, ko smo izdelek kupili in ga začeli uporabljati, ugotovimo, da nam ali ne ustreza, ali ne izpolnjuje vseh deklariranih funkcij, ali pa preprosto ne deluje kot je deklarirano. Čeprav so programski izdelki na tržišču šele 10 do 15 let, pa so bolj ali manj, odvisno od razvitosti tržišča in aktualnosti programskih izdelkov, uveljavljeni vsi znani načini preverjanja kakovosti: mnenja neodvisnih strokovnjakov, objavljena v strokovnih revijah, različna potrdila ali certifikati, naročene ekspertize, mnenja itd. Razlog, zakaj se je v tako kratkem času razvila cela vrsta načinov preverjanja programskih izdelkov, je preprost: uporabnik ni sposoben preverjati vseh deklariranih funkcij, niti definirati vseh svojih potreb.

Postavlja se vprašanje, ali od uporabnika lahko pričakujemo, da bo ugotovil, ali programski izdelek res izvaja vse deklarirane funkcije na deklariran način. Vsakdanja praksa kaže, da ne. Razvoj informacijske tehnologije in s tem tesno povezane programske opreme pa kažeta, da se to stanje le težko spreminja kljub večji osveščenosti uporabnikov.

Eden od načinov reševanja tega problema je, da ponudnik da kupcu potrdilo o ustreznosti izdelka. Potrdilo o ustreznosti ali certifikat je izjava, iz katere je razvidno, da programski izdelek ustreza določenemu standardu, predpisu, deklariranim funkcijam in podobno. Poznamo tri vrste potrdila o ustreznosti:

1. Potrdilo prve stranke (First party certificate). To potrdilo izda proizvajalec sam.
2. Potrdilo druge stranke (Second party certificate). Testiranje in izdajo potrdila je izvedel določen uporabnik.
3. Potrdilo tretje stranke (Third party certificate). To potrdilo izda neodvisna institucija na zahtevo proizvajalca.

Potrdilo o ustreznosti je končni rezultat procesa, ki ga imenujemo preskušanje in ocenjevanje. Cilj tega procesa je seveda ugotoviti, ali programski izdelek res ustreza zahtevam določenih standardov, predpisov in podobno. Certifikat je le formalna potrditev.

Neglede na certifikat pa ostaja formalna odgovornost uporabnika, da ugotovi, ali mu deklarirane funkcije izdelka ustrezajo ali ne. Certifikat sam torej ne daje nobene garancije, da izdelek izpolnjuje uporabnikova pričakovanja. Certifikat le potrjuje ustreznost izdelka določenim zahtevam, ki so običajno opredeljene v standardih in predpisih.

2. NIVO KAKOVOSTI IN KLASA KAKOVOSTI

Po definiciji mednarodnega standarda ISO 8402 Kakovost - slovar je klasa kakovosti definirana kot: "Kazalec kategorije ali nivoja kakovosti izdelka, procesa ali storitve, ki se nanaša na različne skupine zahtev za isto funkcionalno uporabo". Stopnja ali klasa ali razred kakovosti opredeljuje stopnjo funkcionalne dovršenosti nekega izdelka, procesa ali storitve. Namen opredeljevanja stopnje ali klase je pravzaprav poudariti odnos med stroški in funkcijami, ki jih neki izdelek, proces ali storitev, zadovoljujejo. Primer: Obračun proizvodnje ponuja na tržišču več proizvajalcev in vsak svoj izdelek deklarira za splošno uporabnega, cene pa so seveda različne. Kupec

ne ve, kateri izdelek naj izbere, zato je primoran analizirati vsakega ponujenega. Na koncu se, denimo, odloči za najcenejšega, ker ugotavlja, da izpolnjuje funkcionalne zahteve. Po nekaj mesečni uporabi ugotovi, da izdelek ne more slediti njegovemu razvoju in prisiljen je investirati v nov izdelek. Če bi bili programski izdelki označeni z razredom kakovosti, bi se uporabniki lažje odločali med različnimi proizvajalci tako iz vsebinskega, kot iz stroškovnega vidika.

Izdelek visokega razreda ali klase je lahko nekakovosten, če so posamezne funkcije proizvoda nekakovostno izdelane, imajo napake ipd. Dober primer za to je luksuzen hotel s slabo postrežbo. Ali programski izdelek, ki deklarirano izvaja celo vrsto funkcij, ni pa dokumentiran, nima zagotovljenega vzdrževanja, ima veliko število skritih napak, je neprijazen itd. Govorimo o nivoju kakovosti, ki opredeljuje, kako dobro je izdelek določene klase izdelan.

Nivo kakovosti opredeljuje stopnjo dovršenosti procesa, storitve ali izdelka. Ugotavljanje nivoja kakovosti je prav tako težavno. Tudi stopnja dovršenosti se s časom spreminja. To kar je bilo včeraj komaj mogoče (delo z več ekrani, grafična podpora ipd), je danes normalno.

Kakovosten izdelek, proces ali storitev zahtevajo visok nivo kakovosti za določen razred ali klaso kakovosti. To pa pomeni, da je tudi izdelek nizke klase lahko kakovosten in obratno: izdelek z deklarirano visoko klaso je lahko nekakovosten, če ni dovršen.

Klaso ali razred kakovosti lahko različno izražamo. Lahko s točkami (prva klasa), ali številkami (10 točk), ali pa kako drugače. V vsakdanjem življenju poznamo označevanje z zvezdicami za gostinske lokale in pet zvezdic pomeni pač lokal najvišje klase. V procesu izdelave programske opreme pa razvrščanja izdelkov, procesov ali storitev v različne klase ne poznamo. V naši državi zaenkrat nimamo izdelanih normativov, niti institucij, ki bi bile pooblaščenke za razvrščanje izdelkov v različne klase.

Tudi označevanje nivoja kakovosti je silno težavno, ker nimamo splošno sprejetih meril, ki bi izdelek, proces ali storitev, razvrstili na različne nivoje. Zato je označevanje nivoja kakovosti večinoma opisno. Primer: Help funkcija je lahko na dodatnem ekranu, dokumentacija za uporabnika in izvajalca je ločena, vgrajene so funkcije pomikanja ekrana v več oknih itd.

3. PRESKUŠANJE IN OCENJEVANJE PROGRAMSKE OPREME

Preskušanje je postopek, ko druga ali tretja stranka, to je laboratorij, priznan od proizvajalca in kupca, preskusi programski izdelek v skladu z določenim standardom ali predpisom. Če je izdelek preskus uspešno prestal, to pa pomeni, da je izdelek izdelan skladno z zahtevami standarda ali predpisa, izda preizkuševališče ustrezno poročilo. Tako poročilo se vselej nanaša na konkreten izdelek konkretnega proizvajalca. Tako poročilo ne razvršča enako imenovanih proizvodov različnih proizvajalcev v različne razrede ali klase kakovosti. Preskušanje je for-

malno gledano postopek, v katerem preskusni laboratorij preverja sintaktični in semantični vidik skladnosti med tem, kar je deklarirano za programski izdelek, in dejanskim stanjem.

Sintaktični vidik se nanaša na formalno skladnost med zahtevanim in pričakovanim, neglede na dejansko vsebino. Če standard zahteva da morajo vse deklarirane funkcije delovati tako kot je v dokumentaciji zapisano, potem je pa treba vse funkcije preskusiti in ugotoviti skladnost. Če predpisi ali zakoni nekaj zahtevajo, potem je treba preveriti, ali so rezultati programskega izdelka skladni s temi predpisi in zakoni. Rezultat preskušanja je odgovor DA (vsaj minimalna skladnost), ali NE. Rezultat preskušanja dveh enaki funkcionalni rabi namenjenih izdelkov ne pove, kateri je bolj kakovosten. Niti ne pove, kateri od njih izvaja več funkcij, je prijaznejši, bolj učinkovit itd.

Preskušanje ni testiranje programov ali izdelkov, s katerim odkrivamo napake v programih ter neskladnosti med definicijami in realizacijo.

Kadar govorimo o ocenjevanju programskega izdelka, pa ne mislimo le na njegov sintaktični, ampak tudi na njegov semantični vidik. To pomeni, da nas ne zanima le njegova sintaktična komponenta (skladnost s standardom, predpisom, zakonom,...), ampak tudi semantična, torej vsebinska komponenta iz vidika uporabnika in njegovih potreb. Zanimajo nas tiste lastnosti ali karakteristike izdelka, ki se nanašajo na njegovo vsebino in uporabnikovo okolje. Ocenjevanje programske opreme z razliko od preskušanja vsaj posredno vključuje tudi razvrščanje oziroma določevanje klase kakovosti in nivoja kakovosti izdelka. Nekateri avtorji (SCOPE) govorijo o razširjenem preskušanju. Zaradi vsebinske komponente procesa preskušanja pa je končni rezultat preskušanja ocena, ki je vsaj potencialno lahko osnova za rangiranje. Atributi ocenjevanja, torej lastnosti ocenjevanja, morajo biti tisti, ki jih zahtevata in pričakujeta stroka in uporabnik. Morajo biti enostavni za razumevanje, merljivi in rezultati meritev morajo biti ponovljivi. Pogoj merljivosti in ponovljivosti rezultatov merjenja lastnosti je zelo zahteven. Vendar pa le izpolnitev tega pogoja zagotavlja objektivnost ocenjevanja.

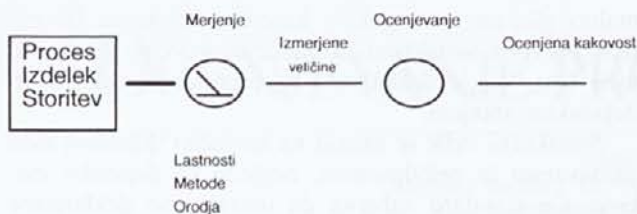
V zvezi z ocenjevanjem, ki je bistveno širše od preskušanja, pa nastopajo vsaj naslednji, vsebinsko zelo zahtevni in do danes še ne povsem rešeni problemi:

1. Katere so tiste karakteristike kakovosti programskih izdelkov, ki le-te najbolj ustrezno opredeljujejo?
2. Kakšen je pomen ali vpliv posameznih karakteristik kakovosti na kakovost celote?
3. Kako meriti (ugotavljati) količino posamezne karakteristike kakovosti?
4. Kako izraziti količino kakovosti za celoten izdelek?

3.1 Model postopka ocenjevanja

Model postopka ocenjevanja je preprost kibernetski model, ki ga prikazuje slika 1:

Problem, ki ga želimo poudariti v zvezi z ocenjevanjem, je, kako ugotoviti in izraziti količino posamezne last-



Slika 1: Kibernetski model ocenjevanja

nosti kakovosti. Na razpolago imamo široko paleto različnih metrik. Znani so na primer ciklomatično število, število vrstic kode, število operandov, operatorjev, stopnja vgnezenosti, vezljivost, sklopljenost itd. Vsaka od bolj ali manj znanih metrik pa se nanaša le na en vidik izdelka. Na primer na programsko kodo, kar pa je seveda daleč premalo za oceno celotnega izdelka po vseh mogočih karakteristikah. Še več! Kaže se potreba, da naj ocenjevanje upošteva tudi subjektivno, torej individualno mnenje ali oceno neke karakteristike. S tem pa je podatek iz objektivne metrike le eden od količinskih podatkov za ocenjevanje. Vprašanje je torej, s katerimi tehnikami ugotavljati količine kakovosti posameznih karakteristik in na tej osnovi izvajati ocenjevanje. Matematično gledano gre za proces preslikave ene metrične skale v drugo.

V programskem inženirstvu imamo na razpolago različne tehnike merjenja ali ugotavljanja količine posamezne lastnosti procesa ali izdelka. Vse seveda niso enako pomembne, niti niso primerne za vsako lastnost in za vsak primer. Nekatere se celo vsebinsko prekrivajo, niso eksaktne, celovite in še kaj. Pa vendar, teorija in praksa boljših ne pozna! V programskem inženirstvu so danes najbolj znane in v praksi uveljavljene naslednje tehnike:

- simulacija,
- testiranje,
- modeliranje,
- verifikiranje,
- programske metrike in
- preskušanje (kontrola).

Simulacija je tehnika, s katero prek nekega drugega sistema analiziramo dogajanje v obravnavanem sistemu.

Testiranje je postopek, s katerim odkrivamo napake v sistemu. Modeliranje se nanaša na razne modele zanesljivosti, stabilnosti, Markovi modeli ipd.

Verifikacija je proces formalne demonstracije sistema in njegovega pravilnega delovanja.

Programska metrika je proces pridobivanja in analiziranja podatkov o procesu, resursu ali izdelku na osnovi ustreznega modela.

Preskušanje (kontrola) je aktivnost preverjanja neke karakteristike na skladnost z doloženimi normami, predpisi itd.

3.2 Nivoji ocenjevanja

Izbira posamezne tehnike je odvisna ne le od obravnavane lastnosti, ampak tudi od kritičnosti obravnavanega

programskega izdelka ali njegovega dela (na primer programski modul). Dejstvo, da kritičnost programskega izdelka (ali njegovega dela) vpliva na izbiro tehnike ocenjevanja, vsiljuje odločitev, da je treba kritičnosti (rizičnosti) izdelka, ali z drugimi besedami pomenu izdelka za uporabnika, prirediti tehnike ocenjevanja. Manj kot je izdelek kritičen (na primer računalniške igrice), manj zahtevne so tehnike ocenjevanja. Bolj kot je programski izdelek rizičen (nevarnost za človeško življenje), bolj zahtevne so tehnike ocenjevanja (metrike, simulacije). Velja pa seveda splošno načelo, da zahtevnejši nivo ocenjevanja predpostavlja ustreznost vseh zahtev predhodnega nivoja. SCOPE projekt kot primer daje možnost ocenjevanja karakteristik kakovosti na štirih nivojih, označenih s črkami od A (najbolj zahteven nivo) do D (najmanj zahteven nivo). Za posamezen nivo ocenjevanja je treba izvesti:

Nivo D: Pregledati je treba uporabniško dokumentacijo, izvesti instalacijo ter preveriti, ali programi delujejo v skladu z dokumentacijo.

Nivo C: Zahteva oceno nivoja D, ter pregled specifikacije, zasnove izdelka in rezultate testiranja. Zahtevano je tudi funkcionalno testiranje skladno z specifikacijami.

Nivo B: Zahteva oceno nivoja C, pregledati je treba celotno proizvodno dokumentacijo, zahtevan je certifikat procesa po standardu ISO 9001 ali ekvivalentu. Izvesti je treba pregled specifikacije in zasnove ter ustrezna testiranja po načelu "bele škatle".

Nivo A: Zahteva oceno nivoja B, verifikacijo programske opreme (formalna, delno formalna, neformalna) in intenzivno testiranje po načelu "bele škatle".

Kdo pa je tisti, ki odloča, na katerem nivoju se bo izvedla ocena? V principu je to presoja in odločitev ocenjevalca in namena ocenjevanja. Ta odločitev pa se lahko spremeni na zahtevo uporabnika, kar pa se lahko nanaša le na zahtevo po višjem nivoju ocenjevanja, nikakor pa ne na zahtevo po nižjem nivoju.

Vidimo tudi, da se ocenjevanje na najnižjem nivoju, po vsebini prekriva s pojmom preskušanje, kakor smo ga v začetku opredelili.

3.3 Predlog tehnik ocenjevanja karakteristik kakovosti po ISO 9126

V Tabeli št.1 podajamo predlog tehnik ocenjevanja za posamezno karakteristiko kakovosti po ISO 9126 (ISO/IEC DIS 9126 Information Technology - Software product evaluation - Quality characteristics and guidelines for their use) za posamezen nivo ocenjevanja. Poudariti velja, da je to le predlog, oziroma nakazana povezava med tehnikami ocenjevanja, karakteristikami kakovosti in nivoji ocenjevanja (SCOPE). Pri tem ostaja popolnoma odprto vprašanje "kako" posamezno oceno izvesti na uvodoma navedenih splošnih principih merjenja: enostavnost, razumljivost, objektivnost in ponovljivost rezultatov. To vprašanje je prepuščeno ocenjevalcu in njegovemu "know how". Vsekakor pa velja poudariti, da si mora ocenjevalec, oziroma firma, ki ima ambicije ukvarjati se z ocenjevanjem po principu druge in tretje stranke, izdelati

ali kupiti ustrezno delovno okolje, ki integrira manualne in avtomatizirane postopke v integralno delovno okolje ocenjevalca.

4 STROŠKI OCENJEVANJA

Ocenjevanje programske opreme seveda ni samo sebi namen, ampak je predhodna faza vrednotenja, torej obravnava pragmatičnega vidika programske opreme. V procesu vrednotenja dajemo oceni individualni, ali nek splošno priznani pomen. Na primer certifikat ustreznosti, ali pripustitev v obratovanje. Stroški ocenjevanja morajo biti v koleraciji z riziki in ne smejo presegati močne izgube, ki bi nastala pri vrednotenju brez ustrezne ocene.

Kolikšni so dopustni stroški ocenjevanja je seveda težko reči. Odvisni so pa od velikosti programskega izdelka in nivoja zahtevnosti ocenjevanja. Sposobnost in znanje ocenjevalca seveda nista nepomembni, predpostavljamo pa organizacijsko, kadrovsko in tehnično usposobljenost ocenjevalca. Naše dosedanje izkušnje in empirični rezultati iz SCOPE projekta in izjave ocenjevalcev iz TÜV KOLN kažejo okvirno oceno potrebnega časa za ocenjevanje izraženo v človek/mesecih, kot jo prikazujemo v tabeli 2. Ponovno poudarjamo, da morajo biti stroški ocenjevanja za vsaj nekritične programske proizvode (nivo D in deloma C), nižji od možnih rizikov in odgovarjati poslovnemu interesu proizvajalca.

Tabela 1: Predlog tehnik ocenjevanja za karakteristike kakovosti po ISO 9126:

ISO karakteristika	Tehnika ocenjevanja	Nivo
Funkcionalnost	Kontrolni pregledi,inspekcije	D
	Sledljivost, testiranje	C
	Testiranje ("bela,siva" škatla)	B
	Formalni dokaz	A
Zanesljivost	Pregled načina programiranja (jezik, pripomočki,...)	D
	Preskusi v realnem okolju, stohastična analiza sistema, dovoljena odstopanja	C
	Zanesljivostni modeli	B
	Formalni dokaz	A
Uporabnost	Kontrola uporabniškega vmesnika	D
	Kontrola na standarde (GUI), čitljivost	C
	Laboratorijski test, anketa uporabnika	B
	Uporabnikov model	A
Učinkovitost	Izvajanje in meritve	D
	Benchmark testi	C
	Kompleksnost algoritmov	B
	Izvedba evaluacije performans	A
Vzdrževalnost	Kontrolne liste	D
	Statična analiza	C
	Kontrola pravil programiranja	B
	Analiza sledljivosti procesa	A
Prenosljivost	Instalacija	D
	Kontrola pravil programiranja	C
	Analiza predpostavk za okolja in platforme	B
	Ocena zasnove programov	A

Tabela 2: Ocena časa ocenjevanja

Nivo	Ocena časa v človek/mesecih za izdelek velikosti:		
	Majhen	Srednji	Velik
A	7 - 13	8 - 16	9 - 19
B	5 - 9	6 - 11	7 - 12
C	3 - 6	4 - 8	5 - 9
D	1 - 2	2 - 3	3 - 4

Med majhne programske izdelke štejejo vse tiste z do 10.000 vrstic kode in s približno 50 stranmi dokumentacije.

Srednje veliki so tisti programski izdelki z do 50.000 vrsticami kode in 200 do 300 stranmi dokumentacije. To so tipične rešitve za osebni računalnik.

Veliki programski izdelki so pa tisti, ki imajo preko 100.000 vrstic kode in več kot 400 ali 500 strani dokumentacije.

5. ZAKLJUČEK

V referatu smo analizirali vprašanje ocenjevanja lastnosti kakovosti programske opreme, kot jih opredeljuje mednarodni standard DIS 9126. Posebno pomembna so naslednja spoznanja:

1. Posamezne lastnosti kakovosti programske opreme ne moremo ocenjevati z enakimi tehnikami in na enak način neglede na vrsto in pomen programske opreme. Programsko opremo je smiselno razvrstiti na nivoje zahtevnosti ali kritičnosti ali pomembnosti. Najmanj kritični so izdelki, ki ne povzročajo izgub ali škode, najbolj kritični so tisti, od katerih so odvisna človeška življenja.
2. Ocenjevalec potrebuje za učinkovito in objektivno oceno ustrezno delovno okolje.
3. Stroški ocenjevanja morajo biti v skladu z namenom ocenjevanja in primerljivi z možnimi izgubami zaradi nakupa neustreznega izdelka. To spoznanje ima seveda izjemo pri programskih izdelkih, od katerih so odvisna človeška življenja.

UPORABLJENA LITERATURA:

- BOOLINGER T.B., MCGOWAN C.: A Critical Look at Software Capability Evaluations. IEEE Software July 1991.
- ISO 9126 ISO/IEC DIS 9126 Information Technology - Software product evaluation - Quality characteristics and guidelines for their use.
- IEEE Master Plan for Software Engineering Standards. Ballot draft, 1993.
- PIVKA M., KAJZER f., GRABNAR D.: Bodo AOP zaradi PC izumrli? Revija Biro, št.2 1993
- PIVKA M., BORKO M.: Survey of software practices and software quality assesment in Slovenia. 3rd European Conference on Software quality. Madrid, 1992.
- SCOPE EGS Esprit Project 2151 SCOPE. Software Assesment and Certification Programme Europe.

CERTIFICIRANJE SISTEMOV KAKOVOSTI

NA PODROČJU PROGRAMSKE OPREME IN INFORMACIJSKE TEHNOLOGIJE V SVETU IN PRI NAS

Mitja Borko
Slovenski inštitut za kakovost in meroslovje, Tržaška 2, 61000 Ljubljana

POVZETEK

Predstavljeno je področje uporabe standardov skupine SLS ISO 9000 s poudarkom na standardu (SLS) ISO 9000-3 ter področje uporabe standardov skupine SLS EN 45000. Opisana sta britanska shema TickIT ter koncept delovanja nove dogovorne skupine EOTC-ITQS. Podana je informacija o osnutku Zakona o standardizaciji s poudarkom na določitih, ki urejajo vprašanja postopkov akreditiranja, certificiranja in preskušanja. Na podlagi opisanih modelov je podan prvi celovitejši predlog za vzpostavitev mednarodno kompatibilnega sistema presoje in certificiranja sistemov kakovosti na področju programske opreme in informacijske tehnologije v Sloveniji.

ABSTRACT

The scope of SLS ISO 9000 and SLS EN 45000 standards is presented and the importance of (SLS) ISO 9000-3 outlined. British TickIT sectoral scheme and the concept of the work of EOTC-ITQS agreement group are described. The information on draft of the Standardisation Act is given and the items of accreditation, certification and testing procedures are discussed. The first proposal for the implementation of internationally compatible system of assessment and certification of quality systems on the field of software and information technology in Slovenia is presented.



1. UVOD

Področje informacijske tehnologije je eno od najhitreje se razvijajočih tehnoloških področij, računalništvo in programska oprema pa sta brez dvoma dve ključni in najbolj propulzivni sestavini tega razvoja. Naraščajo zahteve po kakovostni programski opremi; še zlasti to velja za kompleksno programsko opremo in tisto, ki je v uporabi v okoljih s posebnimi zahtevami. Kupci upravičeno zahtevajo kakovostne, zanesljive, uporabne in uporabniško prijazne, kompatibilne, zaščitene, lahko vzdrževalne, učinkovite in dobro dokumentirane proizvode programske opreme.

Tudi na področjih programske opreme in informacijske tehnologije je vse bolj izrazita zahteva, da dobavitelji kakovost svojih izdelkov zagotavljajo v okvirih vzpostavljenih in certificiranih sistemov kakovosti, ki ustrezajo zahtevam standardov družine ISO 9000. Koncept presoje ter certificiranja sistemov kakovosti pri razvoju, dobavi in vzdrževanju programske opreme postaja z izdajo standarda ISO 9000-3 ter vzporedno z uveljavljanjem standardov skupine EN 45000 predmet praktičnih implement-

acij sistemov preskušanja in certificiranja ter akreditacije v vse večjem številu držav pa tudi na evropskem nivoju.

Slovenija je v letu 1992 kot prve nacionalne standarde sprejela standarde družin SLS ISO 9000 in SLS EN 45000, pravkar pa je v postopku obravnave osnutek standarda SLS ISO 9000-3, ki opredeljuje smernice za uporabo standarda ISO 9001 pri razvoju, vzdrževanju in dobavi programske opreme.

2. STANDARD SLS ISO 9001

Mednarodni standard ISO 9001 je eden iz skupine treh mednarodnih standardov skupine ISO 9000 (1987), ki obravnavajo sisteme kakovosti dobaviteljev. Skupaj z drugimi standardi skupine ISO 9000 je bil v decembru 1992 izdan kot slovenski standard SLS ISO 9001: Sistemi kakovosti - Model zagotavljanja kakovosti v načrtovanju/razvoju, proizvodnji, vgradnji in servisiranju.

Uporablja se vselej, ko mora dobavitelj zagotoviti skladnost z zahtevami v različnih fazah procesa, ki lahko vsebujejo načrtovanje/razvoj, proizvodnjo, vgradnjo in servisiranje, oziroma ko mora dobavitelj dokazati, da obvladuje procese načrtovanja in dobave proizvodov. Ob tako vzpostavljenih sistemih lahko proizvajalci kakovost obvladujejo v vsaki točki poslovnega procesa in utemeljeno pričakujejo, da bodo proizvodi izdelani v tako obvladovanih procesih kakovostni in bodo v celoti izpolnjevali zahteve kupca ter vse druge, jasno specificirane zahteve. Določila tega standarda so usmerjena predvsem v preventivno delovanje z namenom, da se preprečijo neskladnosti proizvodov/storitev v vseh fazah od načrtovanja/razvoja do servisiranja.

Standardi skupine ISO 9000 so v preteklih letih postali osnova za vodenje in upravljanje kakovosti ter za vzpostavljanje sistemov kakovosti tako v proizvodnih podjetjih kot tudi v organizacijah, ki se ukvarjajo s storitvenimi dejavnostmi.

Danes si v svetu ni mogoče zamisliti resnejšega sodelovanja med poslovnimi partnerji, ne da bi se v zvezi z vprašanji o kakovosti sklicevali na enega od standardov skupine ISO 9000. Evropska skupnost je te standarde z oznako EN 29000 celo vgradila v temelje združevanja in sicer na tistem področju, ki obravnava pogoje za plasma industrijskih proizvodov na trge držav skupnosti ("Celoviti pristop evropske skupnosti k ocenjevanju skladnosti", resolucija sveta z dne 21. decembra 1989, oziroma "Moduli za različne faze postopkov ocenjevanja skladnosti, ki naj se uporabljajo v direktivah tehniške harmonizacije", odločitev sveta z dne 13. decembra 1990). /1/

3 STANDARD SLS ISO 9000-3 (osnutek)

Z razvojem informacijske tehnologije se bistveno povečuje obseg programske opreme. Prav zato postaja vprašanje vzpostavljanja sistemov kakovosti pri načrtovanju / razvoju, dobavi in vzdrževanju programske opreme vse bolj bistveno. Vendar pa je proces razvoja in vzdrževanja programske opreme drugačen od drugih industrijskih proizvodov.

Ob tako naglem razvoju tehnologije je bilo nujno potrebno zagotoviti dodatne smernice za sisteme kakovosti, kjer so vključeni izdelki programske opreme, ter pri tem upoštevati sedanje stanje te tehnologije.

Mednarodna organizacija za standardizacijo je že leta 1991 izdala standard ISO 9000-3: Standardi za vodenje in zagotavljanje kakovosti - 3.del: Smernice za uporabo in ISO 9001 pri razvoju, dobavi in vzdrževanju programske opreme, ki ga je pripravil njen tehnični komite ISO/TC 176 - Vodenje in zagotavljanje kakovosti.

Dokument temelji na standardu ISO 9001, vendar se z njim ne ujema popolnoma. Narava razvoja programske opreme je pač takšna, da so nekatere aktivnosti pov-

ezane le z določeno fazo razvojnega procesa, medtem ko druge veljajo za celoten proces. Smernice so bile sestavljene tako, da odražajo te razlike, dodatka A in B pa sta bila pripravljena kot pomoč pri sklicevanju na osnovni standard.

Struktura standarda ISO 9000-3: Standardi za vodenje in zagotavljanje kakovosti - 3. del: Smernice za uporabo in ISO 9001 pri razvoju, dobavi in vzdrževanju programske opreme, ki opredeljuje zgradbo sistema kakovosti pri proizvajalcih/dobaviteljih programske opreme, je naslednja:

- 1 Področje uporabe
- 2 Zveza z drugimi standardi
- 3 Definicije
- 4 Sistem kakovosti - zgradba
 - 4.1 Odgovornost vodstva
 - 4.2 Sistem kakovosti
 - 4.3 Interna presoja sistema kakovosti
 - 4.4 Ukrepi za odpravo napak
5. Sistem kakovosti - aktivnosti v življenjskem ciklu
 - 5.1 Splošno
 - 5.2 Pregled pogodbe
 - 5.3 Seznam zahtev kupca
 - 5.4 Načrtovanje razvoja
 - 5.5 Planiranje kakovosti
 - 5.6 Načrtovanje in izvedba
 - 5.7 Preskušanje in vrednotenje
 - 5.8 Prevzem
 - 5.9 Kopiranje, dobava in instalacija
 - 5.10 Vzdrževanje
6. Sistem kakovosti - podporne aktivnosti (fazno neodvisne)
 - 6.1 Upravljanje s konfiguracijo
 - 6.2 Obvladovanje dokumentov
 - 6.3 Zapisi o kakovosti
 - 6.4 Meritve
 - 6.5 Pravila, postopki in dogovori
 - 6.6 Orodja in tehnike
 - 6.7 Nabava
 - 6.8 Vključena programska oprema
 - 6.9. Usposabljanje

Dodatek A: Zveza med ISO 9000-3 in ISO 9001

Dodatek B: Zveza med ISO 9001 in ISO 9000-3

Standard ISO 9000-3 določa smernice, ki omogočajo lažjo uporabo standarda ISO 9001 v podjetjih, ki razvijajo, dobavljajo in vzdržujejo programske opreme. Obravnava predvsem primere v katerih je bila specifična programska oprema, kot del pogodbe, razvita v skladu z zahtevami kupca. Standard opredeljuje smernice v primerih, ko pogodba med dvema partnerjema zahteva

zagotovilo, da je dobavitelj sposoben razviti, dobaviti in vzdrževati izdelke programske opreme. Smernice so namenjene opisu predlaganih načinov kontrole in metod proizvodnje programske opreme, ki naj izpolni kupčeve zahteve.

To se doseže predvsem s preprečevanjem neustreznosti v vseh fazah, od razvoja do vzdrževanja. Smernice so primerne za pogodbeno razmerja pri izdelkih programske opreme ko:

- a) pogodba izrecno zahteva načrtovan dosežek in so proizvodne zahteve v obliki funkcijskih pogojev navedene, oziroma jih je potrebno določiti,
- b) se zaupanje v proizvod lahko doseže z dokazom dobaviteljeve usposobljenosti načrtovanja / razvoja, dobave in vzdrževanja. /5/

Navedeni standard je bil že v letu 1992 preveden v slovenščino, tehniški odbor MZT/USM TC QAS pa ga v okviru rednega postopka obravnava kot osnutek/predlog slovenskega standarda, ki naj bi bil izdan že letos. Priprava omenjenih standardov je nedvomno koristna tudi za nas, saj je jasno, da se bodo lahko tudi naši proizvajalci/dobavitelji programske opreme pri vzpostavljanju sistemov kakovosti ter uporabniki/kupci pri specifikaciji svojih zahtev v bodoče vse bolj naslanjali na določila navedenih standardov ter upoštevali v njih navedene zahteve.

Naši proizvajalci imajo možnost, da v smislu navedenih standardov vzpostavijo sisteme kakovosti in postopoma privedejo svoje podjetje do certifikata v smislu zahtev standarda ISO 9001 oz. standarda ISO 9000-3. Nekateri od proizvajalcev, zlasti tisti, ki vidijo svojo dolgoročno perspektivo v enakopravnem mednarodnem sodelovanju, se s pripravo poslovnikov o kakovosti ter vzporednimi organizacijskimi ukrepi sistematično pripravljajo na ta korak.

4 STANDARDI SLS EN 45000

V oktobru 1992 so bili izdani prvi slovenski standardi družine SLS EN 45000, ki so identični z evropskimi standardi EN 45000 (1989). Standardi določajo splošne kriterije za delovanje, ocenjevanje in akreditiranje preskusnih laboratorijev, vključno s kalibracijskimi laboratoriji ne glede na sektor v katerem delujejo ter kriterije za certifikacijske organe za področje certificiranja proizvodov, sistemov kakovosti in osebja. Namenjeni so preskusnim laboratorijem in organom za akreditiranje laboratorijev, kakor tudi drugim organom, ki se ukvarjajo s priznavanjem usposobljenosti preskusnih laboratorijev. Standardi pomenijo tehnično podlago in okvir za vzpostavitev nacionalnih sistemov akreditiranja, certificiranja in preskušanja.

5 TickIT - SHEMA CERTIFICIRANJA SISTEMOV KAKOVOSTI NA PODROČJU PROGRAMSKE OPREME IN INFORMACIJSKE TEHNOLOGIJE NA PODLAGI STANDARDOV EN 29001

Velika Britanija je država z najdaljšo tradicijo in izkušnjami na področju certificiranja sistemov kakovosti. V okviru britanskega nacionalnega programa kakovosti so že v osemdesetih letih vzpostavili akreditacijsko in certifikacijsko shemo in do danes so podelili že blizu 20000 certifikatov podjetjem, ki so lahko dokazala učinkovito upravljanje kakovosti v smislu zahtev standardov ISO 9000/EN29000/BS 5750.

Ministrstvo za trgovino in industrijo je v osemdesetih letih želelo postopke certificiranja sistemov kakovosti razširiti tudi na sektor programske opreme in informacijske tehnologije. Z namenom pomagati proizvajalcem v omenjenem sektorju je ministrstvo podprlo projekt in iniciativo certificiranja sistemov kakovosti in jo imenovalo "TickIT" (Tick: angl. kljukica, zaznamovalni znak, IT: informacijska tehnologija). Ob tem je Britansko društvo za računalništvo opredelilo organizacijo, postopke in pravila sektorske sheme, ki naj bi bila skladna z nastajajočimi dokumenti Komisije evropske skupnosti (Commission of the European Communities - CEC).

Namen iniciative "TickIT" je doseči celovito izboljšanje kakovosti programske opreme in informacijskih sistemov.

Projekt "TickIT", ki je danes že mednarodna iniciativa, opredeljuje smernice za formalno ocenjevanje in certificiranje sistemov upravljanja kakovosti programske opreme v smislu zahtev standardov ISO 9001/EN 29001/BS 5750 1.del (1987). Projekt, ki upošteva navedene (sodobne) mednarodne in evropske standarde upravljanja kakovosti, je bil med drugim izdelan z namenom, da se ustrezno vključi in upošteva pri nastajanju in pripravi direktiv Evropske skupnosti. Cilj je doseči najširše osvajanje najboljše prakse ter izpolnjevanje minimalnih zahtev, kot so postavljene v evropskem harmoniziranem standardu EN 29001.

Industriji programske opreme je ponujena shema certificiranja sistemov upravljanja kakovosti, ki zadovoljuje posebne potrebe industrije ter utrjuje zaupanje kupcev v dobavitelje programske opreme. Za akreditacijo organov certificiranja skrbi Nacionalni svet za pooblaščenje organov za certificiranje (National Accreditation Council for Certification Bodies - NACCB). Certificiranje sistemov kakovosti izvajajo neodvisni ("third-party") akreditirani organi za certificiranje.

Če naj bo sektorska shema uspešna, mora zadovoljevati potrebe zainteresiranih strank; kupci/uporabniki morajo zaupati, da je certificiranje s svojimi kvalifikacijskimi kriteriji dovolj zahtevno, proizvajalci/dobavitelji pa morajo biti prepričani, da je koncept certificiranja primeren za

njihove poslovne potrebe in da bodo dosežki certificiranja nekaj pomenili tako v poslovnem kakor tudi intelektualnem smislu.

Kriteriji akreditiranja morajo biti dovolj jasni in morajo hkrati dopuščati ustrezno primerjavo certifikacijskih znakov. V okviru sheme TickIT so zato obstoječi nacionalni kriteriji pooblaščenja poostreni; poostritev se nanaša na tri področja: registracija in usposabljanje presojevalcev, navodila ter praksa organov za certificiranje.

Vsi presojevalci v shemi TickIT so profesionalno preverjeni in potrjeni od Instituta za zagotavljanje kakovosti (Institute of Quality Assurance - IQA) in Britanskega računalniškega združenja (BCS) ter registrirani kot presojevalci sheme TickIT v okviru nacionalnega registra presojevalcev (National Auditors' Register).

Da bi zagotovili enakovredni status certifikatov, ki jih izdajajo različni organi, so bili sprejeti enotni pogoji certificiranja, ki so naslednji:

- **Uporaba imena in znaka "TickIT".** Ime in znak sta zaščitena in se smeta uporabljati le za označevanje pooblaščenega certificiranja,
- **Triletni cikel certificiranja.** Cikel certificiranja tvorijo začetno ocenjevanje in certificiranje, ki jima sledijo nadzorne aktivnosti in ponovno ocenjevanje po 3 letih,
- **Nadzor vložnikovih aktivnosti pregleda upravljanja sistema.** Organ za certificiranje v okviru letnega nadzora vključuje tudi preverjanje ali se pregled sistema kakovosti v podjetju ustrezno izvaja,
- **Medsebojno priznavanje certifikatov TickIT.** Ker obstaja le sistem pooblaščenega certificiranja bodo vsi udeleženci priznavali podeljene certifikate; bistveno pri tem je, da statusu certifikata ni mogoče oporekati,
- **Uporaba dokumentacije TickIT.** Za potrebe certificiranja je navodilo TickIT referenčni dokument, ki se uporablja v povezavi z dokumenti ISO 9000,
- **Presojevalci TickIT.** Presojevalci, ki izvajajo certificiranje in nadzor, morajo izpolnjevati zahteve za standardov za presojevalce (ISO 10011, 2.del, o.p.).

V shemi TickIT so na voljo posebna, strukturirana navodila za posamične potrebe.

Novo navodilo TickIT je razdeljeno v več delov:

1. Uvod
2. ISO 9000-3, uporaba ISO 9001 pri razvoju programske opreme
3. Navodilo za kupce
4. Navodilo za dobavitelje
5. Navodilo za presojevalce.

Certificiranje v shemi TickIT se nanaša na dobavo IT sistemov, pri katerih tvori proizvodnja programske opreme bistveni oziroma ključni del dobave. Kljub temu, da je TickIT osredotočen na proizvodnjo programske opreme, saj je to komponenta, ki določa moč in fleksibilnost in-

formacijskega sistema, je certificiranje vselej formalno definirano s sistemskimi pojmi. Programska oprema namreč ne more obstajati ločeno in se vselej uporablja v sistemskem okolju. Definiranih je nekaj modelov osnovnega poslovnega okolja, ki se lahko certificira v okviru sheme TickIT:

- Model 1: **Dobava celovitega informacijskega sistema.** Organizacija odgovarja za razvoj sistema, proizvodnjo, kopiranje programske opreme, dobavo in vzdrževanje. Model se nanaša na sistemske hiše ali na močne razvojne oddelke v lastni hiši.
- Model 2: **Dobava informacijskega sistema (programska oprema).** Organizacija ne dobavlja strojne opreme, ker jo naročnik že poseduje, vključuje pa odgovornost za verifikacijo delovanja sistema. Model se lahko nanaša na proizvajalce programske opreme in razvojne oddelke v lastni hiši.
- Model 3: **Dobava informacijskega sistema (embalirane komponente).** Sistem se lahko vzpostavi s pomočjo dobavljenih in/ali obstoječih komponent v lasti naročnika. Model se lahko nanaša na dobavitelje pisarniške avtomatizacije, prodajalce proizvodov programske opreme ali razvojne oddelke v lastni hiši.
- Model 4: **Podpora stranki in vzdrževanje.** Vzdrževalne aktivnosti vključujejo modifikacije programske opreme in/ali morebitne izboljšave dobavljene sistema. Model se lahko nanaša na primere, ko je organizacija originalni dobavitelj ali tretja stranka.

Pri pripravi vloge za pričetek postopka certificiranja je pomembna naloga vložnika, da definira področje poslovne aktivnosti, ki naj bo certificirana. To je pomembno zlasti zato, ker se certificirane organizacije vpisujejo v register certificiranih organizacij. Register uporabljajo kot referenco uporabniki in kupci zlasti v primerih, ko razmišljajo o potencialnih dobaviteljih kakovostnih proizvodov in storitev. Cilj v navodilu navedenega opisa je zagotoviti, da bo certificirani sistem kakovosti ustrezno pokrival področje poslovnih aktivnosti. Ni sicer specifičnih pravil za opis proizvajalčevega področja, vendar lahko naslednji opis služi kot tipičen primer:

"Dobava informacijskih sistemov vključno z <podroben spisec tipičnih sistemov> za <spisec pomembnejših sektorjev poslovanja, kot npr. finance, skladišče idr.> z uporabo <poljubna navedba specifične arhitekture strojne opreme in operacijskih sistemov za indiciranje tržne niše> vključno s sistemskim svetovanjem, usposabljanjem uporabnikov, vzdrževanjem sistema in pomočjo."

Navedbe v opisu služijo organu za certificiranje pri planiranju postopka presoje, ki vključuje izbiro projek-

tov in funkcij, ki naj demonstrirajo proizvajalčevo sposobnost, oceno trajanja presoje in izbiro presojevalcev s primernim strokovnim znanjem. /2/

V pripravah na vzpostavitev evropske sektorske sheme certificiranja na področju informacijske tehnologije je britanska shema TickIT od vsega začetka poudarjala svojo odprtost in evropsko usmeritev. Zaradi pomena programske opreme kot globalnega proizvoda in zaradi vzpodbude ostalim deželam, da vzpostavijo enakovredne sisteme certificiranja, so bili dosežki te sheme od vsega začetka na voljo javnemu sektorju. V tem smislu naj bi akreditirano certificiranje zagotovilo mednarodni poslovni potni list dobaviteljem programske opreme in informacijskih sistemov.

Slovenija je že v letu 1991 izrazila pripravljenost za uvedbo principov sheme TickIT in od leta 1992 obravnava shema TickIT Slovenijo kot zainteresirano državo.

6. ITQS - DOGOVORNA SKUPINA EOTC ZA OCENJEVANJE IN CERTIFICIRANJE SISTEMOV KAKOVOSTI NA PODROČJU INFORMACIJSKE TEHNOLOGIJE IN TELEKOMUNIKACIJ

Programsko inženirstvo je v primerjavi z elektronskim, mehanskim ali kemijskim inženirstvom relativno nova disciplina. Nova v razvoju in v prilagajanju je terminologija. Poudarek pri programskem inženirstvu je na razvoju in ne na multipliciranju izdelanih proizvodov. Obremenitve in obraba komponent na področju analize zanesljivosti programske opreme ne igrata pomembnejše vloge. Globalno razmišljanje o tem, da je potrebno tudi vprašanja ocenjevanja in certificiranja sistemov kakovosti na področju informacijske tehnologije in programske opreme obravnavati drugače kot na ostalih področjih, je zato aktualno in logično. Prav zaradi navedenih dejstev priprava že omenjenega standarda ISO 9000-3 v letu 1991 nikakor ni bila naključje.

Evropska organizacija za preskušanje in certificiranje EOTC (European organization for testing and certification), ki v državah Evropske gospodarske skupnosti in državah EFTA pokriva področje preskušanja in certificiranja, je v novembru 1992 oblikovala novo dogovorno skupino za presojo in certificiranje sistemov kakovosti na področjih informacijske tehnologije in telekomunikacij - ITQS (EOTC Agreement Group for assessment and certification of quality systems in Information Technology and Telecommunication).

ITQS deluje pod okriljem Evropskega komiteja za preskušanje in certificiranje na področju informacijske tehnologije ECITC (European Committee for Information Technology Testing and Certification), ki je vezan na or-

ganizacijo EOTC. Devet certifikacijskih organov iz sedmih držav Evropske skupnosti je v tem trenutku vključenih v to dogovorno skupino in sicer: AFAQ (Francija), AIB-Vinçotte (Belgija), BSI-QA (Velika Britanija), ElektronikCentralen (Danska), IMQ (Italija), KEMA (Nizozemska) ter TÜV Bayern, RW TÜV in TÜV Rheinland (Nemčija).

Cilj prizadevanj dogovorne skupine ITQS je promovirati koncept in implementacijo kakovosti ter sistemov kakovosti na področju informacijske tehnologije in telekomunikacij na temelju harmoniziranega ocenjevanja in certificiranja.

Z oblikovanjem te dogovorne skupine je zaključena prva faza priprav na vzpostavitev evropske sektorske sheme certificiranja sistemov kakovosti na področju informacijske tehnologije.

Podlaga za delo ITQS so standardi skupine ISO 9000, vsi certifikacijski organi pa dosledno izpolnjujejo zahteve standarda EN 45012.

Sodelovanje v dogovorni skupini ITQS ima vrsto prednosti:

- Organi certificiranja, ki so združeni v okvirih ITQS-a, zagotavljajo visoko stopnjo integritete in tehniške pristojnosti pri izvajanju presoje in certificiranja,
- Vsi sodelujoči organi certificiranja uporabljajo pri procesih presoje in certificiranja harmonizirane metode in postopke,
- Certifikat sistema kakovosti je vključen v centralni register ITQS-a in ga priznavajo v vseh sodelujočih državah,
- Princip harmonizacije dopušča koordiniran multinacionalni pristop, npr. presojo in certificiranje multinacionalnih podjetij s številnimi izpostavami v večih državah.

ITQS je za presojevalce pripravil harmonizirana navodila (European Information Technology Quality System Auditor Guide), ki naj zagotovijo konsistentno presojo sistemov kakovosti na področjih strojne opreme, programske opreme in storitve.

Navodila ITQS-a so identična z navodili TickIT sheme!

Ostale značilnosti v delu ITQS-a so strokovne delavnice, priprava harmoniziranih navodil za presojevalce, možnost prisostvovanja pri presojah, ki jih izvajajo drugi sodelujoči partnerji, izmenjava izkušenj ob skupnih poskusnih ocenjevanjih, medsebojno priznavanje certifikatov in centralni register certifikatov sistemov kakovosti.

7. ZAKON O STANDARDIZACIJI R SLOVENIJE (OSNUTEK 24.06.1993)

Za razpravo in sprejem v Državnem zboru je pripravljen osnutek Zakona o standardizaciji R Slovenije, ki bo

nadomestil dosedaj veljavni Zakon o standardizaciji (Ur.l. SFRJ, št.37/88 in 23/91).

Novi zakon v IV. poglavju ureja vprašanja akreditiranja, preskušanja in certificiranja. V sistemu akreditiranja opravlja Urad za standardizacijo in meroslovje naloge nacionalne akreditacijske službe (NAS).

Certificiranje se opravlja na področju proizvodov, storitev, osebje in sistemov kakovosti. Proizvodi, storitve in procesi morajo biti preskušeni in certificirani, če je to določeno s tehničnim predpisom, v smislu tega, 16. člena pa smejo preskušanje in certificiranje opravljati samo akreditirani organi.

Zakon v 20. členu ureja vprašanja veljavnosti listin o akreditaciji, poročil o preskusih, certifikatov o skladnosti in drugih listin izdanih v tujini, ki v R Sloveniji veljajo, če so izpolnjeni naslednji pogoji:

- če so bile te listine izdane v okviru mednarodnih sistemov preskušanja in certificiranja v skladu s pravili teh sistemov, pod pogojem, da je R Slovenija članica teh sistemov,
- če so bile te listine izdane na podlagi mednarodnih in večstranskih sporazumov, ki jih je sklenila R Slovenija.

Zakon o standardizaciji v 21. členu med drugim ureja tudi vprašanja označevanja z znaki skladnosti (ustreznosti). /7/

8 PREDLOG ZA VZPOSTAVITEV SLOVENSKEGA SISTEMA PRESOJE IN CERTIFICIRANJA SISTEMOV KAKOVOSTI (PROCESOV) NA PODROČJU PROGRAMSKE OPREME IN INFORMACIJSKE TEHNOLOGIJE NA PODLAGI STANDARDA (SLS) ISO 9000-3

Kako je torej vprašanje certificiranja sistemov kakovosti na področju programske opreme in informacijske tehnologije urejeno pri nas? Kateri pogoji za vzpostavitev evropsko in mednarodno primerljivega sistema certificiranja sistemov kakovosti na tem področju so že izpolnjeni in kaj bi bilo potrebno v prihodnje še storiti? Kakšno pomoč lahko glede presoje in certificiranja sistemov kakovosti v Sloveniji že v tem trenutku ter v bodoče ponudimo proizvajalcem in dobaviteljem na področjih informacijske tehnologije, strojne opreme, programske opreme in storitev? Poskušajmo odgovoriti na zastavljena vprašanja najprej tako, da iz dosedanjšega opisa povzamemo naslednje zaključke:

- Slovenija je leta 1992 izdala standarde skupine SLS ISO 9000,
- Slovenija je leta 1992 izdala standarde skupine SLS EN 45000,
- V Sloveniji je pripravljen osnutek Zakona o standardizaciji, ki predstavlja osnovo za vzpostavitev evropsko primerljivega sistema akreditiranja

preskusnih in kalibracijskih laboratorijev ter organov certificiranja,

- Zakon o standardizaciji ureja vprašanja certificiranja proizvodov, storitev, osebja in sistemov kakovosti,
- Osnutek standarda SLS ISO 9000-3 je v fazi rednega postopka sprejemanja in naj bi bil sprejet že letos,
- Slovenija je že v letu 1991 izrazila pripravljenost za uvedbo principov sheme TickIT in od leta 1992 obravnava shema TickIT Slovenijo kot zainteresirano državo,
- V Sloveniji spremljamo aktivnost EOTC ter v tem okviru tudi aktivnost njene dogovorne skupine ITQS,
- V Sloveniji pripravljamo projekt za vzpostavitev sistema preskušanja in certificiranja proizvodov programske opreme. Projekt, ki ga izvajata Ekonomsko poslovna fakulteta (EPF), Univerze v Mariboru, iz Maribora in Slovenski institut za kakovost in meroslovje (SIQ) iz Ljubljane, je bil 26.10.1993 predstavljen strokovni javnosti,
- Samostojno poglavje v projektu je namenjeno predlogu za vzpostavitev sistema presoje in certificiranja procesov (sistemov kakovosti) na področju programske opreme in informacijske tehnologije na podlagi standarda (SLS) ISO 9000-3,
- SIQ je v svojstvu preskusnega laboratorija in organa certificiranja pripravljen na ustrezno nacionalno akreditacijo.

Na podlagi navedenega lahko ugotovimo, da so izpolnjeni vsi ključni pogoji za vzpostavitev slovenskega, evropsko in mednarodno združljivega sistema certificiranja sistemov kakovosti na področju programske opreme in informacijske tehnologije na podlagi standarda (SLS) ISO 9000-3. Formalno je bil predlog za vzpostavitev tega sistema prvič podan v omenjenem projektu. /6/ Pričakujemo, da bo sistem pod okriljem MZT/USM vzpostavljen v letu 1994, oziroma najkasneje v letu 1995.

Splošno nacionalno shemo preskušanja, certificiranja in akreditacije je mogoče predstaviti kot odnos med udeleženci v sistemu t.j. ustreznim nacionalnim organom za akreditacijo in akreditiranimi organizacijami za preskušanje in certificiranje na eni strani ter proizvajalci in/ali uporabniki proizvodov na drugi strani. /4/

Za operativno vzpostavitev in nadzor nad delovanjem sistema skrbi Nacionalna akreditacijska služba (NAS). Ta po predhodni obravnavi vlog akreditira neodvisne institucije za izvajanje postopkov presoje in certificiranja sistemov kakovosti v smislu tretje osebe. Te institucije morajo dokazati, da v statusnem, organizacijskem in tehničnem smislu t.j. v pogledu opremljenosti in strokovnega znanja, ustrezajo kriterijem zadevnih standardov družine EN 45000. NAS tudi skrbi za stalen nadzor nad delom akreditiranih ustanov.

Certifikacijski organ sprejema vloge za certificiranje

sistemov kakovosti, izvaja postopke certificiranja ter izdaja certifikate. Certifikacijski organ skrbi tudi za stalen nadzor proizvajalcev, tako da periodično ugotavlja stanje certificiranega sistema kakovosti.

Akreditirane institucije so s svojo funkcijo nekakšen vmesnik med vladnim organom in industrijo ter neodvisen arbiter v odnosu med proizvajalci/dobavitelji in uporabniki/kupci (slika 1).



Slika 1: Shema slovenskega sistema akreditiranja ter presoje in certificiranja sistemov kakovosti na področju programske opreme in informacijske tehnologije na podlagi standarda (SLS) ISO 9000-3

Predlagani sistem certificiranja sistemov kakovosti na področju programske opreme in informacijske tehnologije se v celoti vključuje v koncept praktične uvedbe slovenskega Zakona o standardizaciji.

Predlagatelji projekta smo prepričani, da lahko z njim ponudimo našim proizvajalcem in dobaviteljem tisto pomoč, ki jo od "države" potrebujejo pri enakopravnem vključevanju v mednarodno menjavo na področju informacijske tehnologije in programske opreme.

Za vzpostavitev predlaganega sistema bi bilo smiselno in potrebno izpeljati naslednje aktivnosti:

- Pri MZT prijaviti raziskovalno nalogo ter pripraviti projekt za vzpostavitev evropsko kompatibilnega (infrastrukturnega) sistema certificiranja sistemov kakovosti na področju programske opreme in informacijske tehnologije,
- Pod okriljem in v sodelovanju z USM vzpostaviti sistem v katerem naj bodo dosledno upoštevani principi evropske sektorske sheme certificiranja sistemov kakovosti na področju informacijske tehnologije,

- Akreditirati preskusne laboratorije in organ(e) certificiranja,
- Formalno se vključiti v shemo TickIT ter v delo dogovorne skupine ITQS,
- Zagotoviti mednarodno priznavanje izdanih poročil o presoji in izdanih certifikatov.

Vprašanje vloge "države" se postavlja ob vsakršnih priložnostih. "Država" lahko npr. priskoči na pomoč tako, da podpre tovrstne projekte, vzpostavi sektorske sisteme preskušanja in certificiranja, omogoči vključevanje v regionalne in mednarodne sisteme, pomembno področje pa je v vključevanju domačih zakonov in predpisov, zlasti s predpisi Evropske skupnosti, ipd. "Država" vsekakor lahko pomaga, zlasti na področju infrastrukturnih projektov, nikakor pa ni "Deus ex machina". Slej ko prej lahko tudi na tem področju največ stori svobodno tržno podjetništvo in njegova pobuda. //

UPORABLJENA LITERATURA:

- 1/ Borko M.: Pregled dejavnosti mednarodnih, evropskih, tujih in domačih organizacij za standardizacijo pri pripravi standardov in vzpostavljanju sistemov preskušanja in certificiranja programske opreme, Zbornik referatov specializiranega posveta "Preskušanje in certificiranje programske opreme", SIQ (prej IKM), Ljubljana, 15.1.1992
- 2/ Borko M.: "TickIT", (britanska) shema certificiranja sistemov kakovosti na sektorjih programske opreme in informacijske tehnologije na podlagi standardov EN 29001, Zbornik referatov specializiranega posveta "Preskušanje in certificiranje programske opreme", SIQ (prej IKM), Ljubljana, 15.1.1992
- 3/ Borko M.: Certificiranje sistemov kakovosti na področju programske opreme in informacijske tehnologije v svetu in pri nas, Zbornik referatov specializiranega posveta "Kakovost v programskem inženirstvu", Radenci, 23-24.9.1993
- 4/ Soljačič V.: Sistem certificiranja v Republiki Sloveniji (osnutek 1, 1993-07-21), USM, Ljubljana, 1993
- 5/ ISO 9000-3 (1991): Quality management and quality assurance standards - Part 3: Information Technology - Software product - Quality characteristics and guidelines for their use.
- 6/ Sistem preskušanja in certificiranja kakovosti programskih proizvodov v Sloveniji, (Projekt MZT, št.: 82 - 6148 - 92), EPF - Maribor in SIQ-Ljubljana, Maribor - Ljubljana 1993.
- 7/ Zakon o standardizaciji, (osnutek) - Državni zbor R Slovenije, Ljubljana, 24.06.1993

RAZVOJ, DOBAVA IN VZDRŽEVANJE PROGRAMSKE OPREME POT DO CERTIFIKATA SLS ISO 9001 / (SLS) ISO 9000-3/

Prvi korak na poti k certifikatu je storjen v trenutku ko podjetje jasno opredeli svojo politiko kakovosti in sprejme odločitev o vzpostavitvi sistema kakovosti v skladu s kriteriji kot v standardih skupine ISO 9000, ki so danes tudi že slovenski standardi z oznako SLS ISO 9000.

Na področju proizvodnje, dobave in vzdrževanja programske opreme je v veljavi standard (SLS) ISO 9000-3: Standardi upravljanja in zagotavljanja kakovosti - 3. del: Smernice za uporabo ISO 9001 pri razvoju, dobavi in vzdrževanju programske opreme. Osnutek slovenskega standarda je že v rednem postopku, sam standard pa bo sprejet še letos.

Proizvajalec mora ta standard predvsem podrobno preučiti in ugotoviti, kako bi lahko korak za korakom izpolnil vse zahteve standarda ter na njegovi podlagi zgradil svoj lasten sistem kakovosti. V ta namen mora proizvajalec sam ali pa s pomočjo svetovalnih organizacij pripraviti t.i. Poslovnik o kakovosti (Quality Manual), dokument v katerem je sistem kakovosti podjetja podrobno opisan. Najprimerneje je, če je Poslovnik o kakovosti napisan skladno s strukturo standarda ISO 9000-3 tako, da je mogoče v vsakem trenutku, točko za točko, ugotavljati skladnost sistema kakovosti z zahtevami standarda.

Naslednji korak je povezan z vzpostavitvijo stikov s pooblaščen, neodvisno institucijo, ki naj bi izvedla certifikacijski postopek za katerega so značilne naslednje aktivnosti:

- informativni in pripravljalni razgovori,
- vložitev vloge za pričetek certifikacijskega postopka,
- predpresoja,
- certifikacijska presoja,
- ponovna presoja in
- rutinske presoje.

Pri presoji sistema kakovosti se vselej ugotavlja:

- ali ima podjetje vzpostavljen sistem kakovosti?
- ali je sistem vzpostavljen v skladu s standardom ISO 9001 (ISO 9000-3)?
- ali sistem kakovosti učinkovito deluje?
- ali je sistem kakovosti ustrezno vzdrževan?

V kolikor se s presojami ugotovi, da je sistem kakovosti skladen z zahtevami standarda se poroči o presoji posreduje certifikacijski komisiji skupaj s priporočilom za podelitev certifikata in registracijo sistema kakovosti. S certifikatom se potrjuje, da ima podjetje vzpostavljen sistem kakovosti in da ga tudi vzdržuje.

Nadzor certificiranega sistema kakovosti se izvaja dvakrat letno, veljavnost certifikata pa je potrebno za sistem kakovosti po ISO 9001 (ISO 9000-3) obnoviti po treh letih.



VARNOST V RAČUNALNIŠKIH MREŽAH Z DODANO VREDNOSTJO

Borka Jerman-Blazič
Laboratorij za odprte sisteme in mreže, Institut Jožef Stefan
61111 Ljubljana, Jamova 39

Povzetek

Prispevek je pregled funkcij varnosti, ki se uporabljajo v računalniških mrežah z dodano vrednostjo (Value Added Network - VAN). Na kratko so opisane zahteve uporabnikov po varnih komunikacijah in najpreprostejše grožnje, ki so jim izpostavljeni komunikacijski sistemi. Predstavljeno je tudi ogrodje odprtega varnostnega modela (Open Secure Model - OSM), ki definira varnostne funkcije in servise, ki se uporabljajo v odprtih mrežah. Opisani so varnostni mehanizmi za zagotavljanje varnostnih servisov in funkcij.

Abstract

Article gives an overview of security functions, used in computer value added network systems. User demands for secure communications and the most simple threats, to which communication systems are exposed, are shortly described. Open Secure Model - OSM framework, defining security functions and services, used in open networks, is also presented, together with security mechanisms for ensuring security services and functions.



1. UVOD

Informacija pridobi na vrednosti takrat, ko se izmenja oziroma prevzame. Da pa bi se izmenjala ali prevzela, mora biti prenešana ali dostavljena. Potreba po učinkovitih in varnih načinih prenosa danes narašča hitreje kot narašča računalniška obdelava informacij in podatkov. Izmenjava informacij in podatkovne komunikacije so postali integralni del sodobnih informacijskih sistemov.

Izmenjava informacij je proces v okviru storitev, ki jih nudijo mreže z dodano vrednostjo. Te mreže navadno povezujejo uporabnike z različnimi informacijskimi servisi. Posamezne mreže se razlikujejo po strukturi in servisih, ki jih nudijo uporabnikom. Nekateri servisi so precej splošni, drugi pa so lahko zelo specializirani. Vsestranska mreža z dodano vrednostjo (VAN) mora imeti naslednje splošne komponente:

- osnovno prenosno infrastrukturo,
- splošne ali generične servise,
- obdelavo transakcij,
- uporabniške programske rešitve,
- podatkovno bazo,
- upravljanje mreže in pomoč uporabnikom.

Generični ali splošni servisi so servisi, ki jih uporablja širok krog odjemalcev. Zanje je značilno, da niso

specifični za nobeno aplikacijo oziroma vejo industrije. Primer takšnih servisov so npr. elektronska pošta, masovni prenos podatkov, elektronska izmenjava podatkov (Electronic Data Interchange - EDI) in informacijski servisi, ki pomagajo vodstvenim ali strokovnim kadrom pri vodenju. VAN ne potrebuje geografsko obsežne infrastrukture (Wide Area Network - WAN), vendar jo navadno poseduje. V najbolj preprostem primeru VAN lahko zagotovi le preklapljanje paketov, v bolj dognanih sistemih pa nudi konverzijo protokolov za podporo široke palete različnih storitev in s tem zagotavlja popolno povezanost vseh naprav in sistemov, ki jih potrebujejo njihovi odjemalci.

S posebej dodanimi varnostnimi servisi je mogoče zgraditi odprto, popolnoma povezano mrežo na kateremkoli zahtevanem nivoju varnosti.

2. ODPRTE MREŽE IN GROŽNJE

Povezanost in varnost sta nasprotujoči si zahtevi. Vendar odprtost, kot jo razumemo danes, ne pomeni pomanjkanja varnosti, temveč medsebojno povezanost in sposobnost medsebojnega delovanja sistemov v različnih organizacijah in od različnih proizvajalcev.

Ko je odprt, distribuirani sistem zgrajen, postane zelo pomembno, da definiramo zahteve uporabnikov s stališča varnosti komunikacij. Glede na to, kateri servis komunikacijskega sistema uporabljajo, lahko uporabniki zahtevajo različne nivoje varnosti. Običajno se uporabniki zanimajo za naslednje vidike varnega komuniciranja:

- identiteta stranke, s katero komunicirajo,
- da nihče drug ne more prisluškovati seji med dvema računalniškima sistemoma,
- da nihče ne more neodkrito izbrisati, spremeniti ali dodati informacij, ki se izmenjujejo z drugo stranjo,
- da se v primeru spora obveze, dogovorjene med sejo, lahko kasneje brez večjih dvomov zagotovijo z nepristransko sodbo.

Zaskrbljenost uporabnikov izhaja iz dejstva, da so komunikacijski sistemi in nanje priključeni viri pogosto tarča groženj. Grožnje se lahko nanašajo na samo komunikacijsko mrežo ali na neavtoriziran dostop do lokalnega sistema, kjer je komunikacijska mreža uporabljena le kot medij za dostop.

Definiramo lahko tri kategorije vrednosti, ki so lahko resno ogrožene znotraj globalno povezane mreže:

- viri v mreži,
- prenešene informacije,
- odnosi med strankami.

Lokalni sistemi in viri, ki so dostopni skozi komunikacijski kanal, morajo biti zaščiteni. Tudi komunikacijski sistem sam je tak vir in mora biti zaščiten. Upabniki komunikacijskega sistema pričakujejo, da bodo komponente komunikacijskega sistema prisotne in da bodo vselej delovale. V tem smislu sta uporabnost in stabilnost servisov prav tako vrednosti komunikacijskega sistema in potrebujeta zaščito. Informacije so dejanska vsebina komunikacij. Neavtoriziran dostop do informacij z izgubo ali spremembo zapisanega lahko uniči vrednost informacije. Tej kategoriji pripadajo tudi informacije, ki se hranijo lokalno in so dostopne prek omrežja. Odnosi med strankami so naslednja osnovna vrednost komunikacij. Brez zaupanja v avtentičnost druge stranke so vse komunikacije z njo brez vrednosti. Zaupanja vredni odnosi s stranko pomenijo, da zaupamo v identiteto stranke in v delovanje komunikacij.

Vse te vrednosti komunikacijskega sistema so izpostavljene dvema v osnovi različnima vrstama groženj, namernim in nenamernim. Klasična teorija o varnostnem sistemu obravnava samo eno vrsto groženj; to so namerne grožnje, ki so ali vohunjenje ali pa sabotaza. Vohunjenje vključuje vse pasivne namerne grožnje kot so pridobivanje neavtoriziranega vedenja o zaupnih informacijah. Sabotaza vključuje vse aktivne namerne grožnje, to je vse vrste neavtoriziranega ravnanja s po-

datki, dostop do resorjev v komunikacijskem sistemu itd.

Druge možne nezgode, ki so prav tako pomembne za varnost komunikacijskih mrež, so naključne grožnje, npr.: slabo vzdrževanje vodi do prekinitve mrežnega servisa. S stališča uporabnikov je vseeno, če je to storjeno iz škodoželjnosti ali pa iz nesposobnosti administratorja oziroma operaterja.

Različne grožnje in napadi v odprtih okoljih so klasificirani v okvirnih dokumentih ISO. Dokument ISO-7498 PART 2 opredeljuje pet različnih napadov na odprt komunikacijski sistem:

- pretvarjanje,
- tajenje akcije ali servisa,
- zanikanje servisa,
- prestreženje podatkov,
- manipulacija s podatki.

V nadaljevanju podrobneje opisujemo vsako izmed teh dejanj:

- a) Do pretvarjanja lahko pride pri medsebojnem overjanju oddajnikov in prejemnikov sporočila (Message Transfer Agent - MTA je procedura, ki prenese ali izmenja sporočila v servisu elektronske pošte) z zamenjavo MTA v tekstu. Nepoznan MTA se lahko (na primer v testni proceduri) poveže z nekim delujočim MTA, tako da pošlje enega od znanih imen. To je tipično pretvarjanje identitete z namenom kraje delovnih virov ali informacij. Pretvarjanje uporabnikove identitete je prav tako mogoče s spretno uporabo usmerjevalno orientiranih naslovov.
- b) Tajenje akcije ali servisa. V primeru pogodb ali drugih poslovnih dokumentov je tajenje izvora, predlogov ali dostave zelo boleče. Kako zaupati ponudbi, sprejeti z EDI servisom, če ni zagotovljen dokaz o identiteti pošiljatelja?
- c) Zanikanje servisa. Zanikanje servisa se lahko zgodi zaradi naključne prekinitve, ki jo povzročijo lokalne sistemske napake ali pa neprilagojene komponente v sodelujočih sistemih kot npr. napačen vnos pri usmerjanju naslovov ali tabelah preslikav. Namerne prekinitve so za vzdrževalne namene normalne.
- d) Prestrežanje podatkov. Prekinitve zaupnosti je najobičajnejši napad v obstoječih mrežah. S pomočjo sistemskega administratorja ni mogoče uganiti števila namernih vohunjenj ali vdorov drugih nepooblaščenih oseb, ki so sposobne čitati podatke na svojih ali pa tujih sistemih. Podatki so lahko prav tako prestreženi nenamerno, npr. pri napačno usmerjenih sporočilih itd.
- e) Manipulacija s podatki. Manipulacija s podatki je kakršnakoli sprememba podatkov, ki oskruni njihovo integriteto. Upravljanje z naslovi elektronske pošte je v nekem smislu prav tako oskrnitev integritete, ki je povzročena pomotoma zaradi slabega vzdrževanja. Jasen primer je tudi procesiranje v pretvor-

nikih (gateway), kjer se sporočilo odreže ali pa se iz sporočila izgubi del telesa. Taka vrsta ranljivosti komunikacijskega sistema vključuje tudi manipulacijo z vsebino sporočila v izvornem lokalnem pomnilniku po nezavrženem predlogu ali manipulacijo z vsebino sporočila v pomnilniku prejemnika po nezavrženem dostavi sporočila.

3. VARNOSTNE FUNKCIJE IN SERVISI

Varnostno ogrodje se ukvarja z uporabo varnostnih servisov v okoljih odprtih sistemov (Open System Environment), kjer izraz "odprti sistemi" vključuje področja kot so: podatkovne baze, distribuirane rešitve, obdelava pisarniške dokumentacije in komunikacijske mreže. To ogrodje definira načine, kako zagotoviti zaščito sistemom in objektom znotraj komunikacijskega sistema ter interakcijo med sistemi. Ukvarja se z informacijo in zaporedjem operacij, ki se uporabljajo za zagotovitev specifičnih varnostnih servisov. Ti varnostni servisi se lahko uporabljajo v komunikacijskih sistemih kakor tudi pri izmenjavi informacij med sistemi in pri lokalnih virih oziroma podatkovno manipulativnih sistemih. Izraz "varnost" je v ISO dokumentih definiran kot "način za minimiziranje ranljivosti sistema in njegovih virov". Varnost torej razumemo kot sistem, ki preprečuje napade in ščiti samo vrednost sistema pred grožnjami z varnostnimi servisi, ki se uporabljajo na različnih nivojih omrežja.

Varnostni servisi temeljijo na uporabi varnostnih mehanizmov. Nekateri mehanizmi ščitijo pred napadi, drugi napade odkrivajo, nekateri izmed njih pa kasneje obnovijo prvotno stanje. Ti mehanizmi so:

- a) Overjanje. Mnoge uporabniške rešitve odprtih sistemov imajo varnostne zahteve, ki so odvisne od pravilnega identificiranja vključenih oseb. Take zahteve lahko vsebujejo zaščito sistema in virov pred neavtoriziranim dostopom, za katerega mora biti uporabljen na identiteti osnovan mehanizem za kontrolo dostopa, oziroma za namene zaračunavanja/tarifiranja. Postopek potrjevanja identitete imenujemo overjanje.
- b) Kontrola dostopa. Mnoge uporabniške rešitve v odprtih sistemih vsebujejo varnostne zahteve, da se viri sistema lahko uporabljajo le v soglasju z dogovorjeno varnostno politiko. Proces dovoljevanja uporabe virov posameznim osebam znotraj okolja odprtega sistema in posledično zaščito pred takšno uporabo imenujemo kontrola dostopa.
- c) Preprečitev tajejanja. Servis za preprečitev tajejanja zagotavlja ustrezno zbirko informacij, ki so sestavljene iz podatkov o izvoru ali dostavi, z namenom, da zaščiti pošiljatelja pred neresničnim zanikanjem prejemnika, da je podatke sprejel, ali pa z namenom, da zaščiti prejemnika pred neresničnim zanikan-

jem pošiljatelja, da je podatke poslal. Servis te podatke hrani in vzdržuje.

- d) Integriteta podatkov. Vrednost podatkov v komunikacijah je dejansko njihova integriteta oziroma zagotovljena nespremenljivost podatka pri komunikaciji. Mnogo uporabniških rešitev v odprtih sistemih postavlja varnostne zahteve, ki so odvisne od integritete informacij, s katerimi te aplikacije poslujejo. Take zahteve lahko vključujejo zaščito informacij, ki se uporabljajo kot podpora drugim varnostnim servisom kot so: overjanje, kontrola dostopa, zaupnost, preverjanje in preprečitev tajejanja. Če napadalec spremeni te informacije, lahko omeji ali izniči učinkovitost omenjenih servisov.
- e) Zaupnost podatkov. Pogosto se pojavljajo zahteve po tajnosti podatkov. Take zahteve lahko vključujejo zaščito informacij, ki se uporabljajo kot podpora drugim varnostnim servisom kot so overjanje, kontrola dostopa ali integriteta. Če napadalec pozna te informacije, lahko omeji ali izniči učinkovitost omenjenih servisov. Vzdrževanje tajnosti podatkov imenujemo zaupnost podatkov.
- f) Preverjanje. Varnostno preverjanje je neodvisen pregled in preizkus sistemskih zapisov in aktivnosti. Namen varnostnega preverjanja je neodvisen pregled in preizkus sistemskih zapisov in aktivnosti. Varnostno preverjanje testira ustreznost sistema nadzora, potrjuje njegovo skladnost z varnostno politiko, svetuje spremembe v nadzoru, politiki in procedurah, pomaga pri analizi napadov na sisteme in priporoča procedure za nadzor škode. Varnostno preverjanje zahteva zbiranje in zapisovanje podatkov, ki se na poti varnostnega preverjanja nanašajo na varnost. Varnostno preverjanje samo pa vključuje analize in poročanje o informacijah, zbranih na poti varnostnega preverjanja.
- g) Upravljanje s ključi. V komunikacijskih in informacijskih sistemih obstaja vse večja potreba po podatkih, ki bi bili zaščiteni pred neavtoriziranimi razkritji ali manipulacijami. Varnost in zanesljivost takih mehanizmov je direktno odvisna od zaščite, ki jo dosežemo z varnostnimi parametri, imenovanimi "ključ". Namen upravljanja ključev je zagotoviti procedure za upravljanje s kriptografskimi ključi, ki se uporabljajo v simetričnih ali nesimetričnih kriptografskih mehanizmi. Upravljanje ključev vključuje: generiranje, distribucijo, instalacijo ključev ter shranjevanje in uničevanje ključev. Osnovni problem upravljanja s ključi je pripraviti šifrirni material, čigar izvor, integriteto in, v primeru tajnih ključev, zaupnost lahko garantiramo.

Namestitev posamezne varnostne funkcije v odprti arhitekturi ni natančno določena. Varnostni servisi ali funkcije so lahko zagotovljeni na različnih nivojih in z različnimi

protokoli, odvisno od zahtev uporabnikov in programskih rešitev. Nekatere rešitve so bolj, druge manj ranljive. Njihova zaščita je prav tako odvisna od prevzete varnostne politike in od uporabljene tehnologije. Lahko rečemo, da univerzalen model ne obstaja ter da se namestitev posameznih funkcij izbira po definiranju značilnosti in zahtev dane rešitve v zvezi z varnostjo in po pragmatičnem razmisleku.

V primerih nepovezanih protokolov, kot je primer IP, se uporablja tehnika označevanja, znana kot IPSO (IP Security Option). Oznake kot so npr. "občutljivo", "nerazporejeno", "stroga tajnost" navadno spremljajo prikriti podatke. Če so podatki poslani zanesljivemu komunikacijskem sistemu (dostava podatkov avtoriziranemu lokalnemu sistemu je garantirana) so take oznake lahko zadovoljiva zaščita, v primeru nepreizkušenih mrež kot so npr. javne podatkovne mreže pa so paketi podatkov prekriti in taka zaščita ne zadostuje.

Namestitev funkcij overjanja, integritete in zaupnosti v višje nivoje ali direktno v proces (npr. elektronska pošta) je jasna in pragmatična rešitev, ni pa optimalna. Namestitev varnostnih funkcij za vsako aplikacijo posebej (npr. za virtualni terminal, prenos datotek, servise direktorija) zahteva veliko razvojnega dela in podvajanje funkcionalnosti. Tak pristop prav tako nasprotuje principu, po katerem naj bi bila varnost integralen del celotnega komunikacijskega sistema in servisov, ki jih ta zagotavlja. Praksa je pokazala, da je tak pristop dandanes uporabnejši le zaradi kompleksnosti medsebojno povezanih mrež in različnih varnostnih zahtev v različnih rešitvah globalnih mrež kot je Internet.

4. VARNOSTNI MEHANIZMI

Mehanizme in algoritme, ki zagotavljajo različne varnostne funkcije in servise, imenujemo varnostne mehanizme. Ti mehanizmi dejansko oblikujejo hierarhijo in so lahko:

- mehanizmi višjih nivojev, kot so varnostni protokoli in semantična vsebina sporočil,
- mehanizmi nižjih nivojev, kot so kriptosistemi za formiranje zgoraj omenjenih mehanizmov višjih nivojev,
- fizični mehanizmi, kot so integrirana vezja za kripto zaščito in deli programske kode, ki uporabljajo zgoraj omenjene mehanizme.

Uporaba teh mehanizmov je odvisna predvsem od zahtevanih varnostnih funkcij in celovitosti sistema, ki ga želimo zaščititi. Varnost lokalnih sistemov je lahko v večji meri zagotovljena s fizičnimi varnostnimi ukrepi. V odprtih globalnih mrežah pa je zagotovitev varnosti komunikacij v smislu fizične varnosti nemogoča, zato se najpogosteje uporabljajo kriptografske tehnike.

Kriptografija je že dolgo znan način, s katerim lahko obdržimo informacijo tajno. Dandanes so kriptografski mehanizmi posebej razviti in se uporabljajo za zaščito prenosa podatkov in informacij. Obstaja mnogo kriptografskih mehanizmov, omenili bomo le osnovne, ki se uporabljajo v globalno povezanih mrežah: šifriranje in tehnike za zagotavljanje integritete in overjanja sporočil. Za podrobnosti glej(8,9).

Šifrirni mehanizem se uporablja za pretvorbo čistih tekstovnih sporočil v šifrirana sporočila, kriptograme. Šifrirni mehanizem je osnovan na javno poznanih algoritmih in najmanj enem ključu, ki je naključno izbran iz velike množice možnih ključev.

Mehanizmi za integriteto podatkov zagotavljajo tehnike, ki omogočajo, da zaporedja sporočil ostanejo nedotaknjena. To pomeni, da nobeno sporočilo ne ostane neodkrito, prezrto ali podvojeno in je ostala ohranjena originalna razvrstitev sporočil. Integriteta podatkov zagotavlja odkrivanje sprememb na prenesenih podatkih, če do njih pride, lahko pa tudi odpravljanje sprememb oziroma generiranje sporočil, kadar odpravljanje sprememb ni mogoče.

Navadno se za odkrivanje sprememb v podatkovnem nizu uporablja tehnika preverjanje vsote (checksum), ali pa bolj zaželeno preverjanje s ciklično redundanco (cyclic redundancy check).

Overjanje se dandanes izvaja z uporabo gesel (password). Ta metoda je zelo ranljiva, tako overjanje pa je znano kot šibko overjanje. Močno overjanje (strong authentication) je osnovano na simetrični ali javni kripti zaščiti. Procedura močnega overjanja in izmenjava ključev sta opisani v CCITT priporočilih X.509 ali pa v ISO 9594.

V simetričnih kriptosistemi je za močno overjanje med katerikoli parom strank A in B uporabljen ustrezen varnostni kontekst, ki mu pripada paroma medsebojno usklajen ključ. V asimetričnih šifrirnih mehanizmih je ključ razdeljen na dva dela: šifrirni ključ in dešifrirni ključ. Prejemnik sporočila ima ključ, s katerim lahko dešifrira, pošiljatelj pa uporablja različne ključe za šifriranje. Sistem zagotavlja varno komunikacijo samo v eni smeri in je poznan kot asimetrični ali javni šifrirni mehanizem. Le-ta zagotavlja popolno zaupnost, ne pa tudi overjanja pošiljatelja; če uporabimo tehniko digitalnega podpisa, lahko zagotovimo tudi overjanje.

Javni mehanizmi za šifrirani podpis imajo za overjanje več prednosti pred simetričnimi kriptosistemi. Upravljanje s ključi zelo poenostavi dejstvo, da se delijo javne šifre samo v parih in da je za vsako stranko potreben samo en par ključev.

Hitro se razširja področje tako imenovanih tehnik ničelnega znanja (zero-knowledge technique). V teh tehnikah igra varnostno overjanje informacij vsake stranke zelo dobro enako vlogo kot varnostni ključ v javnih šifrirnih kriptografskih sistemih, vendar le-to ne sme biti uporabljeno za šifriranje podatkov, temveč le za over-

janje podatkov in morda digitalnega podpisa. Nekaj obstoječih tehnik ničelnega znanja nudi zelo preprosto upravljanje s ključi, ki v celoti odpravijo potrebo po od uporabnika odvisnih javnih ključev. Šibka lastnost teh tehnik pa je, da je za generiranje varnostnih ključev potrebna tretja stranka in da ne morejo biti uporabljene za zagotovitev zaupnosti.

5. VARNOSTNA POLITIKA

Varnostna politika je politika zagotovitve varnostnih storitev v mrežah. Je integralni del odprtega modela, ki ga za lastne potrebe izvaja določena organizacija. Varnostna politika je množica pravil, ki določa eno ali več množic varnostno pomembnih aktivnosti iz ene ali več znanih množic varnostnih elementov. Ni nujno, da se ta politika uporablja pri vseh aktivnostih in elementih komunikacijskega sistema. To pomeni, da mora njena specifikacija vključevati specifikacije aktivnosti in elementov, na katere se politika nanaša. Pravila za vsak varnostni servis so izpeljana iz varnostne politike.

Navadno delimo varnostno politiko na politiko, osnovano na identiteti (identity-based), in politiko, osnovano na pravilih (rule-based). Prva je osnovana na ugodnostih ali možnostih, ki so dane uporabnikom oziroma na sezname oseb za nadzorovanje dostopa do relevantnih podatkov ali drugih virov. Druga varnostna politika pa določa, kaj je avtorizirano obnašanje posameznika. V sistemih, ki so osnovani na identiteti, se uporabniki praviloma predstavijo sistemu s prepustno besedo (password).

Uveljavljanje sprejete varnostne politike navadno poteka z informacijami o nadzoru varnosti. Ena izmed njih je varnostna oznaka. Varnostna oznaka je množica varnostnih atributov, ki so povezani z elementom, komunikacijskim kanalom ali podatki. Varnostna oznaka prav tako eksplicitno ali implicitno označuje organ, ki je odgovoren za kreiranje povezave in za varnostno politiko, ki izvaja z uporabo oznak. Primeri varnostnih oznak so: naznačitev občutljivosti (npr. nerazvrščeno, zaupno, itd.), naznačitev zaščite, odredba in druge zahteve v zvezi z rokovanjem in delom z določenimi podatki ali informacijami.

Druga zelo pomembna varnostna nadzorna informacija (Security Control Information - SCI) je potrdilo. Potrdilo vsebuje SCI, ki se nanaša na enega ali več varnostnih servisov. Potrdilo izda organ za potrdila. Uporablja se za pošiljanje SCI od organa do teles, ki to informacijo zahtevajo, da bi izvršili varnostno funkcijo. V splošnem lahko potrdilo vsebuje SCI za vse varnostne funkcije. V zgornjem poglavju opisani varnostni mehanizem vključuje izmenjavo SCI in sicer ali med dvema komunicirajočima strankama ali pa med varnostnim organom in sodelujočima strankama.

V opisanih mehanizmi se uporabljata dve obliki zaščitene varnostnih informacij. Prva se imenuje varnostni žeton in se uporablja za zaščito varnostnih informacij, ki se prenašajo med sodelujočima strankama. Druga se imenuje varnostno potrdilo, uporablja pa se za zaščito varnostnih informacij, ki jih pridobimo prek organa, za uporabo pri eni ali pa več sodelujočih strankah.

Varnostno ogrodje ne definira metod in postopkov za uvajanje varnostne politike in pripadajočih SCI. To je prepuščeno razvoju posameznih organizacij in sistemov.

6. ZAKLJUČEK

Varnost je ključnega pomena pri razvoju mrež z dodano vrednostjo. Varnostni servisi in funkcije so potrebni za zaščito infrastrukture komunikacijskih in lokalnih sistemov, kakor tudi za zagotovitev zaupanja bodočih uporabnikov in zagotavljanje varnega transporta občutljivih in pomembnih informacij. Na srečo današnji hitri napredek tehničnega razvoja rapidno izboljšuje varnost mrež, istočasno pa zagotavlja še njihovo odprtost in povezanost.

7. REFERENCE

1. R.Reardon (ed.) Future Networks, Blenheim Online, London 1989
2. Internet: Getting started, SRI International, Menlo Park, CA, 1992
3. ISO, Information Processing Systems, Open System Interconnection Reference Model, Part:1 Security Architecture, ISO 7498-2, Geneva 1988
4. R.Grimm, Security on Networks: Do WE Really Need it?, Comp.Networks and ISDN Systems, Vol.17, No 4&5, October 1989, p.315-321
5. A.T.Karila, Open System Security - an Architectural Framework, Espoo 1991, Helsinki
6. D.W.Davies and W.L.Price, Security for Computer Networks, Sc.ed., J.Willey and Sons, Chichester, 1989
7. S.Muftic, (ed.) Security Mechanisms for Computer Networks, Ellis Horwood Ltd, Chichester, 1989
8. C.Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, Vol.28, 1949, p.656-715
9. ISO, Information Technology, Security Techniques, A Data Integrity Mechanism, ISO DP 9797, Geneva 1990
10. S.Walker, Network security: The parts of the Sum, Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy, Oakland 1989, p.2-9
11. The Directory - Overview of Concepts, Models and Services, CCITT Recommendation X.500, Melbourne 1988, and The Directory, Part 8: Authentication Framework, CCITT Recommendation X.509 (Melbourne 1989.)
12. ISO 9594, Information Processing Systems, OSI - The Directory, 9594 through parts 1 - 8, Geneva 1989
13. ISO 10181, Information Technology, OSI Security Model, Part 1 Security Framework, Part 2, Authentication framework A.Shamir, Identity-Based Cryptosystem and Signature Scheme, Advances in Cryptology: Proceedings of Crypto 84, Springer, Berlin, 1985, pp.47-53

ALGORITMI ZA REŠEVANJE SPLOŠNEGA PROBLEMA TRGOVSKEGA POTNIKA

Vladimir Batagelj
Oddelek za Matematiko, Univerza v Ljubljani

Povzetek

Problem trgovskega potnika (PTP) spada med osnovne probleme kombinatorične optimizacije. V članku je podanih nekaj osnovnih dejstev o PTP in pregled pomembnejših algoritmičnih pristopov k njegovemu reševanju.

Abstract

The Traveling Salesman Problem (TSP) is one among the basic problems of combinatorial optimization. In the paper some basic facts about TSP are given, followed by an overview of the main algorithmic approaches for solving TSP.



Članek je nastal na osnovi gradiva za 2. seminar Izbrana poglavja iz računalništva na FNT, Oddelek za matematiko in mehaniko, Ljubljana v decembru 1992. Glavni cilj sestavka je bralca seznaniti s problemom trgovskega potnika (PTP) in s pomembnejšimi pristopi k njegovemu reševanju. Pri tem se ne spuščamo v podrobnosti, temveč bralca, ki bi želel izvedeti več, napotimo na ustrezne vire. Prav tako so iz pregleda izpuščeni algoritmi za posamezne posebne vrste PTP (na primer Evklidski) [10].

1. OSNOVE

1.1 Optimizacijske naloge

Naj bo na množici Φ dana funkcija

$$P : \Phi \rightarrow \mathbb{R}^*$$

kjer je $\mathbb{R}^* = \mathbb{R} \cup \{+\infty, -\infty\}$. Množici Φ bomo rekli *množica dopustnih rešitev*, funkciji P pa *namenska ali kriterijska funkcija*.

Pogosto pri določitvi množice dopustnih rešitev Φ izhajamo iz širše *množice rešitev* Ω , ki jo je enostavneje opisati. Množico dopustnih rešitev Φ tedaj sestavljajo tiste rešitve $X \in \Omega$, ki zadoščajo predikatu *dopustnosti* ali *omejitvam* $\Phi(X)$

$$\Phi = (\Omega, \Phi) = \{X \in \Omega : \Phi(X)\}$$

Postavimo

$$\text{Min}(\Phi, P) = \{X \in \Omega : \forall Y \in \Phi : P(Y) \geq P(X)\}$$

Vsi elementi množice $\text{Min}(\Phi, P)$, če je ta neprazna, imajo isto vrednost kriterijske funkcije P . Označimo jo z $\min(\Phi, P)$ in jo razširimo na primer, ko je množica $\text{Min}(\Phi, P)$ prazna, s predpisom:

$$\min(\Phi, P) = \begin{cases} \inf_{X \in \Phi} P(X) & \Phi \neq \emptyset \\ \infty & \Phi = \emptyset \end{cases}$$

Tedaj lahko zapišemo tudi

$$\text{Min}(\Phi, P) = \{X \in \Phi : P(X) = \min(\Phi, P)\}$$

Na podoben način lahko vpeljemo tudi $\text{Max}(\Phi, P)$ in $\max(\Phi, P)$; ali pa z uporabo zvez:

$$\begin{aligned} \text{Ext.1} \quad \text{Max}(\Phi, P) &= \text{Min}(\Phi, -P) \\ \text{Ext.2} \quad \max(\Phi, P) &= -\min(\Phi, -P) \end{aligned}$$

Ti dve zvezi nam omogočata, da se omejimo samo na Min in \min .

Optimizacijsko nalogo ali nalogo (matematičnega) programiranja dobimo, če dodamo dvojici (Φ, P) , glede na značilnosti naloge, vsaj eno od naslednjih, ali njim podobnih, zahtev:

- P1. določi $\text{Min}(\Phi, P)$
- P2. določi $X \in \text{Min}(\Phi, P)$
- P3. določi $\min(\Phi, P)$

- P4. določi zaporedje $(X_i : X_i \in \Phi, i \in \mathbb{N})$, tako da velja $\lim_{i \rightarrow \infty} P(X_i) = \min(\Phi, P)$
- P5. določi $X \in \Phi$, tako da bo (z dano verjetnostjo) razlika $P(X) - \min(\Phi, P)$ zadosti majhna.
- P6. določi $X \in \Phi$.

Tako zastavljene naloge bi pravzaprav morali označiti (Φ, P, \min) , kajti za vsako obstaja tudi naloga (Φ, P, \max) , ki se od nje razlikuje le po tem, da so v pogojih minimumi zamenjani z maksimumi.

Optimizacijski nalogi (Φ, P, \min) in (Ψ, Q, \min) sta *enakovredni*, če iz rešitev ene dobimo rešitve druge in obratno. Relacijo enakovrednosti označimo z \cong . Zaradi zvez Ext.1 in Ext.2 je naloga (Φ, P, \max) enakovredna nalogi $(\Phi, -P, \min)$. Zato se lahko v nadaljnjem omejimo samo na naloge minimizacije.

Množica optimizacijskih nalog sestavlja *optimizacijski problem*. Običajno združimo v optimizacijski problem med seboj podobne naloge, ki imajo enako obliko in se razlikujejo le po podatkih. Nalogi, ki pripada optimizacijskemu problemu, pravimo tudi *primerek problema*.

1.1.1. Naloga o prirejanju

n ljudi mora opraviti n opravil. Stroški, ki jih imamo, če človek i opravi opravilo j naj bodo a_{ij} . Ljudem moramo prirediti vsakemu po eno opravilo, tako da bodo skupni stroški najmanjši, pri čemer pa morajo biti opravljena vsa opravila. Zastavljeni problem lahko prevedemo na optimizacijsko nalogo (S_n, P, \min) , kjer je S_n množica vseh permutacij števil od 1 do n in

$$P(\pi) = \sum_{i=1}^n a_{i, \pi(i)}$$

V linearni algebri ponavadi permutacijo π podamo z dvojniško matriko X , določeno s predpisom

$$x_{ij} = \begin{cases} 1 & j = \pi(i) \\ 0 & \text{sicer} \end{cases}$$

nalogo o prirejanju pa oblečemo takole: (Φ, P, \min) , kjer je $I = 1..n$,

$$\Phi = \{X \in \{0,1\}^{n^2} : \forall i \in I : \sum_{j \in I} x_{ij} = 1, \forall j \in I : \sum_{i \in I} x_{ij} = 1\}$$

in

$$P(X) = \sum_{(i,j) \in I \times I} a_{ij} x_{ij}$$

Pogoji v opisu množice Φ zagotavljajo, da je X matrika neke permutacije. Iz tega zapisa naloge o prirejanju vidimo, da sodi med naloge (celoštevilskega) linearnega programiranja.

1.1.2. Naloga o trgovskem potniku

Trговец se je namenil, da bo obšel n mest tako, da se bo v vsakem mudil samo enkrat. Znane so razdalje d_{ij} med posameznimi mesti. Kako naj trgovec potuje, da bo opravil čim krajšo pot?

Pri formalizaciji problema nadomestimo zemljevid z grafom povezanosti mest $G = (V, E)$. Točke tega grafa so mesta, povezave pa predstavljajo prometne zveze med mesti. Vsaki povezavi je pripisana še pripadajoča razdalja.

Vsakemu trgovčevemu potovanju ustreza Hamiltonov cikel po grafu G . Tega lahko popišemo z urejeno n -terko točk π , sestavljeno po pravilu

$$j = \pi(i) \quad \text{- točka } j \text{ je v ciklu naslednik točke } i$$

Če naj π popisuje Hamiltonov cikel, mora biti ciklična permutacija. Tako dobimo nalogo (Γ_n, P, \min) , kjer je Γ_n množica cikličnih permutacij števil od 1 do n in

$$P(\pi) = \sum_{i \in I} d_{i, \pi(i)}$$

Najbrž ni potrebno posebej opozarjati na podobnost problema o trgovskem potniku s problemom o prirejanju. Žal je podobnost le površinska - za problem o prirejanju obstajajo učinkoviti algoritmi; problem trgovskega potnika pa je NP-težek, kar med drugim pomeni, da imajo vsi znani (točni) algoritmi zanj eksponentno zahtevnost. Je pa ta podobnost s pridom izkoriščena v nekaterih algoritmih za reševanje problema trgovskega potnika.

1.2. Grafi in problem trgovskega potnika

Naj bo $G = (V, A)$ končen enostaven usmerjen graf z množico točk V in množico povezav $A \subseteq V \times V$.

Končno zaporedje točk $\gamma = (v_0, v_1, v_2, \dots, v_d)$, ki zadošča pogoju

$$\forall i \in 1..d : (v_{i-1}, v_i) \in A$$

imenujemo *sprehod po* G ; d je dolžina sprehoda γ . Če je $v_0 = v_d$, je sprehod *sklenjen* ali *obhod*. Sprehod je *osnoven* ali *pot*, če gre skozi posamezno točko grafa največ enkrat. Osnovnemu obhodu rečemo *krajše cikel*. Sprehod je *poln*, če gre skozi vse točke grafa. Polnemu ciklu pravimo tudi *Hamiltonov cikel*.

Če je $A = V \times V$, je graf G *poln*. V polnem grafu ustrezajo Hamiltonovim ciklom natanko vse ciklične permutacije (z začetno točko).

Urejeno trojico $G = (V, A, c)$, kjer je (V, A) graf in $c : A \rightarrow \mathbb{R}$ cena povezav, imenujemo *graf z vrednostmi na povezavah*. V nadaljnjem bomo predpostavljali, da je cena nenegativna $c : A \rightarrow \mathbb{R}_0^+$.

Cena c zadošča *trikotniški neenakosti*, če zanjo velja

$$\forall x, y, z \in V : c(x, z) + c(z, y) \geq c(x, y)$$

Če ima poleg tega še lastnost $\forall v \in V : c(v,v) = 0$, ji bomo rekli *oddaljenost*. Pozor, oddaljenost ni nujno simetrična $\forall x,y \in V : c(x,y) = c(y,x)$. V primeru, ko lahko točke grafa predstavimo kot točke v \mathbb{R}^k in je cena povezave enaka kar Evklidski razdalji med njenima krajiščema, govorimo o *Evklidski nalogi TP*. Pogosto se pri predstavitvi omejimo na ravnino \mathbb{R}^2 .

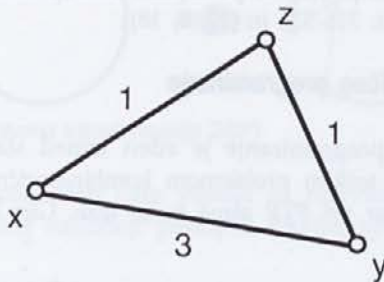
Ceno lahko razširimo s povezav na sprehode s predpisom

$$c(\gamma) = \sum_{i=1}^d c(v_{i-1}, v_i)$$

Morda pa bi lahko trgovski potnik opravil svoje potovanje ceneje, če bi kakšno od mest obiskal večkrat. To je res v primeru na sliki 1, za katerega velja:

$$c((x,z,y,z,x)) = 4 \quad \text{in} \quad c((x,y,z,x)) = 5.$$

Torej minimalne rešitve naloge TP niso vselej Hamiltonovi cikli, temveč jih moramo iskati med polnimi obhodi.



Slika 1: Minimalne rešitve naloge TP niso vselej Hamiltonovi cikli

Naj bo $\Gamma(A)$ množica vseh polnih obhodov grafa G . Tedaj lahko *nalogo trgovskega potnika* zapišemo kot optimizacijsko nalogo

$$TP = (\Gamma(A), c, \min)$$

Množica vseh nalog trgovskega potnika sestavlja *problem trgovskega potnika*.

Dano ceno \hat{c} razširimo na množico $V \times V$ s predpisom

$$\hat{c}(u,v) = \begin{cases} c(u,v) & (u,v) \in A \\ \infty & \text{sicer} \end{cases}$$

Tedaj velja

Izrek 1. *Naloga TP $(\Gamma(A), c, \min)$ je enakovredna nalogi $(\Gamma(V \times V), \hat{c}, \min)$.*

Množico Hamiltonovih ciklov grafa G označimo s $H(A)$. Nalogo $(H(A), c, \min)$ imenujemo *naloga o najcenejšem Hamiltonovem ciklu*.

Čeprav v splošnem rešitev NTP ni vedno Hamiltonov cikel, pa velja:

Izrek 2. *Če v grafu z vrednostmi na povezavah $(V,V \times V, c)$ velja za ceno c trikotniška neenakost, obstaja Hamiltonov obhod $\gamma \in \text{Min}(\Gamma(V \times V), c)$.*

Grafu $G = (V,A,c)$ lahko vselej priredimo nov graf $H = (V,V \times V, d)$ takole: Naj bo za $u, v \in V$ $\langle u,v \rangle$ najcenejši sprehod (ali eden izmed njih, če jih je več) iz u v v po G . Tedaj postavimo:

$$d(u,v) = \sum_{(i,j) \in \langle u,v \rangle} c_{ij}$$

Nova cena d zadošča trikotniški neenakosti.

Izrek 3. *Naloga TP $(\Gamma(A), c, \min)$ po G je enakovredna nalogi $(H(V \times V), d, \min)$ najcenejšega Hamiltonovega cikla v H .*

Torej je vsaka naloga TP prevedljiva na enakovredno nalogo iskanja najcenejšega Hamiltonovega cikla v grafu s ceno, ki zadošča trikotniški neenakosti.

2. ALGORITMI

Problem trgovskega potnika (potujočega trgovca, kramarja) ima svoje začetke v zabavnih (matematičnih) nalogah [1] kot sta *naloga o požrešnem šahovskem konjičku* (Euler, 1759; Vandermonde, 1771) in *dvajsetiška igra* (Sir William Rowan Hamilton, 1856). Prvi je obravnaval splošni problem obstoja Hamiltonovih ciklov Kirkman 1855.

Pravi problem trgovskega potnika je obravnavan v knjigi nasvetov za trgovske potnike, ki je izšla v Nemčiji leta 1832.

V matematične kroge je PTP zašel v tridesetih letih tega stoletja (Menger, Whitney H., Tucker A.W., Flood M.). Okrog leta 1948 je RAND corporation, kjer je bilo takrat središče operacijskih raziskav, razpisal nagrado za pomemben izrek o PTP.

Leta 1954 so Dantzig, Fulkerson in Johnson objavili prvo rešitev obsežne NTP - 49 mest ZDA; 48 velikih mest v zveznih ameriških državah in Washington D.C. Rešitev so določili z nitko na modelu. Optimalnost pa so dokazali z uporabo linerne programiranja, pri katerem so z *metodo odsekov* (dodatne omejitve) zagotovili cikličnost in celoštevilskost rešitve. Zadostovalo je 25 dodatnih omejitev. Pri pripravi rešitve so uporabili tudi osnovne zamisli *metode razveji in omeji*. Uporabo odsekov pri reševanju nalog celoštevilskega linearnega programiranja je naprej razvijal Gomory.

V tistih časih, začetek petdesetih, so se pojavili prvi pomembnejši rezultati v kombinatorični optimizaciji (linearno programiranje, prirejanje, pretoki, razporejanje poslov, ...). Zato je trdovratnost PTP privlačila posebno pozornost.

Leta 1963 so Little, Murty, Sweeney in Karel objavili postopek razveji in omeji za reševanje PTP in prvi uporabili termin *branch & bound*. Postopka razveji in omeji sta za reševanje PTP predlagala že leta 1958 tudi Eastman in Croes. Leta 1970 sta Held in Karp predložila za ocenjevanje mej uporabo *Lagrangeovske relaksacije*.

Mesto PTP so v svojih člankih o zahtevnosti problemov razjasnili Cook (1971), Karp (1972) in Levin (1973). PTP je NP-težek; prav tako tudi večina podproblemov (npr. Evklidski). Ti rezultati nas vodijo v dve smeri:

- za točno reševanje PTP se najbolje obnesejo izpeljane metode razveji in omeji. Pri tem je prava umetnost razvoj čim boljnih ocen mej. Leta 1980 sta Crowder in Padberg rešila NTP na 318 točkah, ki je bila do 1987, najobsežnejša naloga z dokazano optimalno rešitvijo. Leta 1987 sta Padberg in Rinaldi objavila optimalne rešitve nalog velikosti 532, 1002 in 2392; leta 1988 pa Grötschel in Holland 666 in 1000 [13, 7].
- če je naloga preobsežna ali imamo omejene vire, se moramo zadovoljiti s približnimi rešitvami. Do teh lahko pridemo z različnimi *heuristicami*, kakršna je na primer *najbližji sosed* (Menger, 1930), ali pa s *postopki lokalne optimizacije*.

Poglejmo si posamezne pristope:

2.1 Prebor vseh možnosti

Najpreprostejši točen postopek je prebor vseh možnosti - vseh $(n-1)!$ cikličnih permutacij.

```

CONST nmax = 20;
TYPE vector = ARRAY [1..nmax] OF integer;
      matrix = ARRAY [1..nmax, 1..nmax] OF integer;
.....
VAR q, route : vector;
    w : matrix;
.....
PROCEDURE perm(k:integer);
  VAR i, t: integer;
BEGIN
  IF k<=2 THEN BEGIN
    c := c+1; ts := w[q[n],q[1]]; write(1st,c:8,' > ');
    FOR i := 1 TO n DO write(1st,q[i]:3);
    FOR i:=1 TO n-1 DO ts := ts + w[q[i],q[i+1]];
    write(1st,ts:8);
    IF ts < bts THEN BEGIN bts := ts; route := q END;
  END ELSE BEGIN
    perm(k-1);
    FOR i:= 2 TO k-1 DO BEGIN
      t := q[i]; q[i] := q[k]; q[k] := t;
      perm(k-1);
      t := q[i]; q[i] := q[k]; q[k] := t
    END;
  END;
END {perm};
BEGIN
.....
  FOR i := 1 TO n DO q[i] := i;
  c := 0; bts := maxint;
  perm(n);
.....
END.
```

Žal je ta postopek uporaben le za zelo majhne naloge. Pri polnem preboru rešitev moramo pregledati $(n-1)!$ permutacij.

n	(n-1)!	n	(n-1)!
10	362880	16	1307674368000
11	3628800	17	20922789888000
12	39916800	18	355687428096000
13	479001600	20	121645100408832000
14	6227020800	25	620448401733239439360000
15	87178291200	30	8841761993739701954543616000000

Recimo, da program pri polnem preboru (na superračunalniku) pregleda milijon rešitev na sekundo. Tedaj bi pri $n=15$ tekel 24.2 ur; pri $n=18$ pa že 11.3 let in pri $n=30$ kar $2.8 \cdot 10^{17}$ let.

2.2. Razveji in omeji

Postopek polnega prebora lahko izboljšamo tako, da s kleščanjem slabih vej, omejimo pregledovanje na obetavne veje. To je osnova postopkov razveji in omeji. Glej Kozak [9], str. 316-324 in [12, 8, 18].

2.3. Dinamično programiranje

Dinamično programiranje je eden izmed standardnih pristopov k težkim problemom kombinatorične optimizacije; vendar pri PTP nima večje teže. Glej Kozak [9], str. 269-271.

2.4. Monte Carlo – naključne permutacije

Pri zelo obsežnih problemih bi lahko dani obhod naključno določili in izračunali njegovo vrednost

```

FOR i := n DOWNTO 2 DO BEGIN
  j := 1 + trunc(i*random);
  t := route[i]; route[i] := route[j]; route[j] := t;
END;
ts := w[route[n],route[1]];
FOR i:=1 TO n-1 DO ts := ts + w[route[i],route[i+1]];
.....
```

To bi velikokrat ponovili in obdržali najboljšo dobljeno rešitev.

Ta zamisel ne vodi do zadovoljivih rezultatov. Uporabili pa jo bomo za določanje naključnih začetnih rešitev pri postopkih lokalne optimizacije.

2.5. Lokalna optimizacija

2.5.1. Globalni in lokalni minimumi

Pogosto lahko v dani množici Ω definiramo relacijo *sosebnosti* rešitev $S \subseteq \Omega \times \Omega$, za katero zahtevamo le refleksivnost.

Pri diskretnih optimizacijskih problemih običajno definiramo sosebnost z *lokalnimi transformacijami*, ki prevedejo eno rešitev v drugo.

Element $x \in \Phi$ je lokalni minimum glede na S natanko takrat, ko je $x \in \text{Min}(\Phi \cap S(x), P)$; ali drugače povedano, ko

$$\forall y \in \Phi \cap S(x) : P(x) \leq P(y)$$

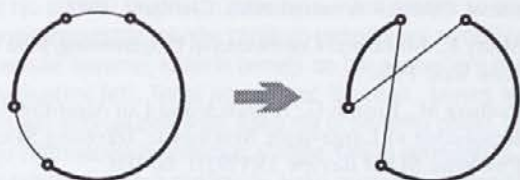
Množico vseh lokalnih minimumov naloge (Φ, P, min) glede na sosednost S označimo $\text{LocMin}(\Phi, P, S)$.

Zato, da bi poudarili razliko, pravimo elementom množice $\text{Min}(\Phi, P)$ tudi *globalni minimumi*. Očitno je vsak globalni minimum tudi lokalni. Poleg tega velja še:

Izrek 4. Za vsako sosednost S je

$$\text{LocMin}(\Phi, P, \Phi \times \Phi) = \text{Min}(\Phi, P) \subseteq \text{LocMin}(\Phi, P, S)$$

in, če je $\emptyset \subset Q \subset S$, tudi $\text{LocMin}(\Phi, P, S) \subseteq \text{LocMin}(\Phi, P, Q)$.

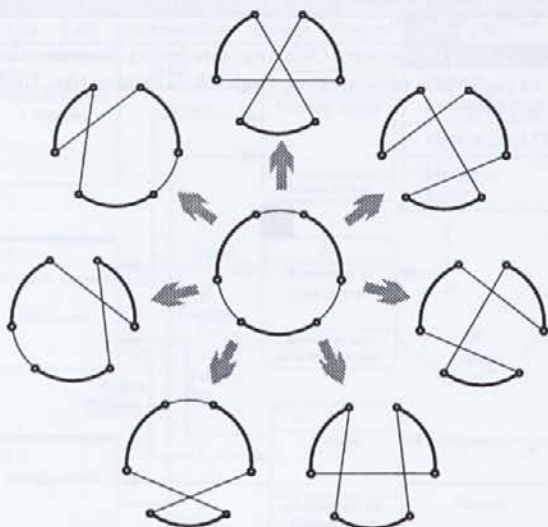


Slika 2. Lokalna transformacija 2-OPT

Relacija sosednosti nam ponuja za reševanje optimizacijskih nalog naslednji postopek lokalne optimizacije:

```
izberi  $x \in \Phi$  ;
while  $\exists y \in S(x) \cap \Phi : P(y) < P(x)$  do  $x := y$  ;
```

Če se postopek izteče v končno korakih, konča v lokalnem minimumu.



Slika 3. Lokalne transformacije 3-OPT

Pri problemu trgovskega potnika se najpogosteje uporabljajo sosednosti r -OPT, pri katerih so sosednje rešitve določene tako, da iz tekočega cikla odstranimo r povezav in jih nadomestimo z novimi, ki zopet sestavljajo cikel. Na slikah 2 in 3 sta prikazani sosednosti 2-OPT in 3-OPT. Lin je s poskusi pokazal, da je sosednost 3-OPT veliko boljša kot sosednost 2-OPT, učinek sosednosti višjih redov pa ne upravičuje povečane porabe časa [14, 18].

2.5.2. Ohlajanje

Ohlajanje (simulated annealing) je izpeljanka postopka lokalne optimizacije, ki se poskuša s posnemanjem gibanja delcev plina izogniti lokalnim minimumom. Prvi ga je okrog leta 1953 predlagal Metropolis s sodelavci; zelo priljubljen pa je postal v zadnjem desetletju. Postopek lokalne optimizacije z ohlajanjem za PTP najdemo v [15] str. 328-334.

Podrobneje je uporaba ohlajanja pri PTP obdelana v [19].

2.5.3. Prepovedane smeri

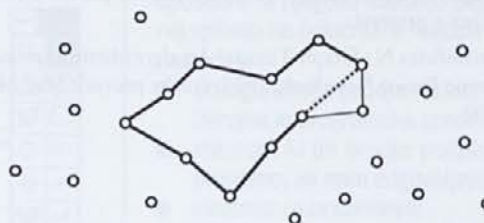
Zadnjih nekaj let se uveljavlja druga izboljšava postopkov lokalne optimizacije - uporaba *prepovedanih smeri* (Tabu search) [6]. Pri teh postopkih se vselej premaknemo v sosednjo dovoljeno rešitev z najmanjšo vrednostjo, pri čemer lahko nekatere premike prepovemo. To nam omogoča, da se skobacamo iz lokalnih minimumov in da upoštevamo nabrano informacijo o prostoru rešitev.

Po poročilih v člankih se pri PTP ti postopki izjemno dobro obnesejo.

2.5.4. Genetski algoritmi

Eden izmed obetajočih pristopov k (približnemu) reševanju kombinatoričnih optimizacijskih problemov so tudi *genetski algoritmi*, pri katerih poskušamo s posnemanjem razvoja (reprodukcija, križanje, mutacije) množice rešitev vzgojiti čim boljše rešitve [4].

2.6. APROKSIMACIJSKI ALGORITMI



Slika 4. Širjenje delnega cikla

Hevristični algoritmi pogosto temeljijo na načelu *požrešnosti*. Pri PTP lahko zgradimo take postopke tako, da zaporedoma dodajamo točke delnemu ciklu. Postopki se med seboj ločijo po odločitvah: *katero* točko dodati in *kam*.

Pri zelo velikih nalogah lahko poskušamo priti do dobrih rešitev tudi tako, da v postopkih razveji in omeji obdržimo le najbolj obetavne veje.

Označimo $c^* = \min(H(V \times V), c)$ in s $c(A)$ ceno rešitve, ki jo vrne dani aproksimacijski algoritem A. Zanima nas, ali obstaja taka konstanta α , da velja

$$1 \leq \frac{c(A)}{c^*} \leq \alpha$$

Za algoritem *najbližji sosed* je mogoče pokazati, da velja

$$\alpha = \frac{1}{2} (\lceil \ln n \rceil + 1)$$

Sahni in Gonzales sta leta 1976 pokazala, da je tudi problem aproksimacije za splošni PTP NP-težek.

Dobro aproksimacijo, $\alpha < \frac{3}{2}$, lahko zagotovimo v primeru, ko je cena c razdalja. Kako to storimo je opisano v [11].

3. ZAKLJUČEK

Povzemimo: čeprav je PTP NP-težek problem, ni treba takoj vreči puške v koruzo. Če narava naše naloge ne zahteva točne rešitve, lahko pridemo razmeroma hitro do precej dobrih rešitev, tudi za naloge z več tisoč točkami, z uporabo postopkov lokalne optimizacije ali njihovih izboljšav. Te postopke je razmeroma enostavno sprogramirati. Za naloge TP, pri katerih je zahtevana točna rešitev, je doseg najboljših postopkov okrog 2000 točk. Ti postopki zahtevajo za svoj razvoj veliko znanja in časa. V našem prostoru (vsaj kolikor je avtorju sestavka znano) še niso dostopni.

LITERATURA

1. Batagelj V.: Hamiltonova naloga za grafe. 8. seminar iz matematike: Zanimiva matematika, DMFA SRS, Ljubljana, 1980, 13-25; Presek 11(1983-84)1, 4-16.
2. Batagelj V.: Optimizacijske metode. Zapiski predavanj na FER, skripta v pripravi.
3. Christofides N.: Graph Theory; An algorithmic approach. Academic Press, New York, 1975. (ruski prevod: Mir, Moskva, 1978)

4. Filipič B.: Primerjava genetskih algoritmov na problemu trgovskega potnika. Zbornik XXXV ETAN, Ohrid 1991, 257-264.
5. Gibbons A.: Algorithmic Graph Theory. Cambridge University Press, Cambridge, 1985.
6. Glover F.: Tabu search. ORSA Journal on Computing, Part I: 1(1989)3, 190-206; Part II: 2(1990)1, 4-32.
7. Grötschel M., Holland O.: Solution of large-scale symmetric traveling salesman problems. Mathematical Programming 51(1991), 141-202.
8. Horowitz E., Sahni S.: Fundamentals of Computer Algorithms. Computer Science Press, Rockville, 1978.
9. Kozak J.: Podatkovne strukture in algoritmi. DMFA SRS, Ljubljana, 1986.
10. Lawler E.L., Lenstra J.K., Rinnooy Kan A.H.G., Shmoys D.B.: The Traveling Salesman Problem; A guided tour of combinatorial optimization. John Wiley, New York, 1986.
11. Mohar B.: Aproksimacijski postopki za problem trgovskega potnika. Gradivo za 2. seminar: Izbrana poglavja iz računalništva, Oddelek za matematiko, Ljubljana, 1992.
12. Murty K.: Linear and Combinatorial Programming. John Wiley, New York, 1976.
13. Padberg M., Rinaldi G.: A Branch-and-Cut Algorithm for the Resolution of Large-scale Symmetric Traveling Salesman Problems. SIAM Review 33(1991)1, 60-100.
14. Papadimitriou C.H., Steiglitz K.: Combinatorial Optimization: Algorithms and Complexity. Prentice-Hall, Englewood Cliffs, NJ, 1982.
15. Press W.H., Flannery B.P., Teukolsky S.A., Vetterling W.T.: Numerical Recipes; The art of scientific computing. Cambridge University Press, Cambridge, 1986.
16. Reingold E.M., Nievergelt J., Deo N.: Combinatorial Algorithms; Theory and practice. Prentice-Hall, Englewood Cliffs, NJ, 1977. (ruski prevod: Mir, Moskva, 1980)
17. Sakovič V.A.: Issledovanie operacij. Višejšaja škola, Minsk, 1985.
18. Syslo M.M., Deo N., Kowalik J.S.: Discrete Optimization Algorithms; with pascal programs. Prentice-Hall, Englewood Cliffs, NJ, 1983.
19. Žerovnik J.: Algoritem Ohlajanje. Gradivo za 2. seminar: Izbrana poglavja iz računalništva, Oddelek za matematiko, Ljubljana, 1992.

Kam gre razvoj orodij CASE?

Uroš Ponikvar

V prvi številki te publikacije so orodja CASE omenjali kar trije članki. Nobeden jih ni opisal podrobneje, kar me je spodbudilo, da napišem prispevek na to temo. CASE, po slovensko računalniško podprto programsko inženirstvo, je programska oprema, s katero si sistemski analitiki in načrtovalci informacijskih sistemov pomagajo pri svojem delu. Prav čudno je, da so strokovnjaki z drugih področij veliko prej ugotovili, da jim računalnik pri delu lahko izdatno pomaga. Matematiki, fiziki, kemiki, strojniki, arhitekti, ekonomisti ... Informatiki smo se tega zavedeli prav med zadnjimi, oziroma se tega še vedno premalo zavedamo.

Neke vrste namenska programska oprema torej. Kaj pa je moč z njo početi? Preprosto povedano, v teh orodjih so bile uporabljane raznovrstne tehnike različnih metodologij za načrtovanje programske opreme, katerih temelji so bili postavljeni pred več kot dvajsetimi leti. Tedaj so namreč Yourdon, James Martin, Finkelstein in drugi definirali, kako naj bi se temu poslu, namreč razvoju informacijskih sistemov, streglo. Gre za definicijo t.i. strukturnih tehnik, oziroma predpisov, kako predstavimo posamezen koncept. Primer take tehnike je diagram toka podatkov (DFD, Data Flow Diagram). Primer DFD kaže slika 1. V bolj ali manj prilagojeni obliki se take tehnike uporabljajo še danes. V orodjih CASE pa najdemo prijazen delovni prostor, ki omogoča manipulacijo z različnimi diagrami (modeli), bogato in pregledno dokumentacijo ter povezavo med različnimi istovrstnimi ali raznovrstnimi diagrami in modeli. Nekatera orodja CASE podpirajo tudi prototipni pristop in generiranje izvorne kode oziroma uporabniških rešitev..

Spodnji in zgornji razred orodij CASE, I-CASE

Orodja CASE delimo na več razredov. V zgornji razred (Upper

CASE, Front-End CASE) štejemo orodja, s katerimi si pomagamo pri planiranju, analizi in načrtovanju na logičnem nivoju, simulaciji in izdelavi prototipov. V spodnji razred orodij CASE sodijo tista, ki jih uporabljamo pri uvajanju uporabniških rešitev: generiranju kode, prevajanju, testiranju in integraciji. Integrirana orodja CASE (I-CASE) kombinirajo lastnosti orodij iz obeh opisanih razredov, poleg tega pa vključujejo tudi spremljanje razvojnih aktivnosti na projektnem nivoju. Vsako orodje CASE ima (vsaj) podatkovni slovar, to je skladišče podatkov, ki opisujejo attribute, spremenljivke, ključe, formate itd. Integrirano orodje CASE vsebuje poleg podatkovnega slovarja še dodatne metapodatke, ki omogočajo spremljanje razvoja na projektnem nivoju. Tako skladišče imenujemo repozitorij.

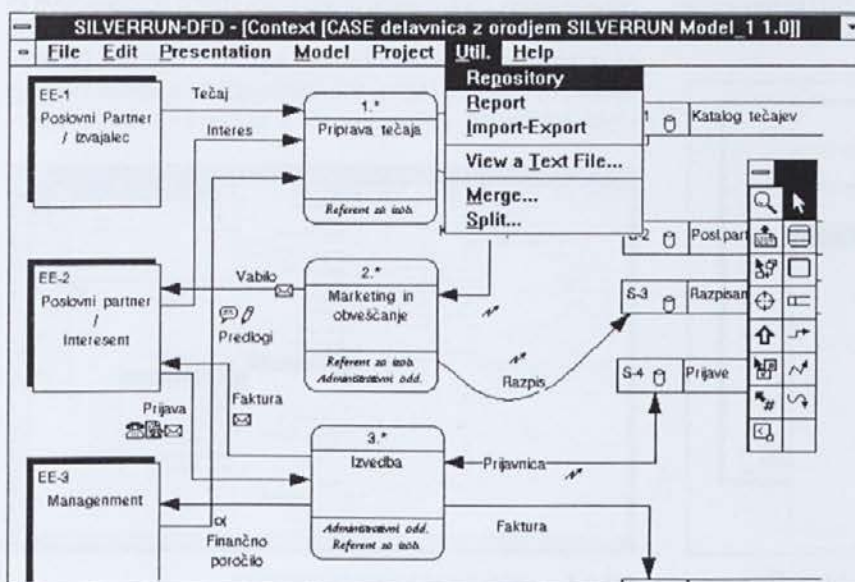
Uspešnost uporabe orodij CASE

Do sedaj je izkušenj pri uporabi orodij CASE že kar nekaj. Precej jih je zelo pozitivnih, kar nekaj pa je tudi "neuspešnih zgodb". Orodje CASE samo namreč ne naredi (skoraj) ničesar. Uporabnik mora svoje orodje obvladati tako tehnološko, kot tudi metodološko. Tehnološko pomeni, da zna uporabljati vsaj osnovne funkcije orodja. Metodološko obvladovanje pomeni, da v določenem kontekstu uporabi te funkcije pomensko pravilno in v skladu z uporabljeno metodo. Preprosto povedano: znati je treba priti do enakega rezultata tudi "peš" - brez podpore orodja. Le-to predstavlja zgolj bližnjico do cilja. Skrbi za preverjanje konsistentnosti ter standardno dokumentacijo. Omogoča tudi lažje (in cenejše) vzdrževanje, ponovno (večkratno) uporabo specifikacij. Morda najpomembnejša pridobitev, ki jo nudi uporaba orodij CASE, pa je, da se zelo zmanjša čas, porabljen za nekreativna opravila. Več časa posvetimo bistvenim problemom (vsebini), manj časa pa nebitnim (zunanemu videzu, večkratnem vnosu podatkov...)

Po drugi strani imajo orodja CASE razmeroma visoko ceno. Razvoj tovrstne programske opreme je zahteven, tržišče pa majhno, še posebej, če ga primerjamo npr. s tržiščem urejevalnikov besedil. Investicija v nakup ustreznega števila licenc za orodje CASE je le del stroškov, ki jih zahteva uvedba orodja. Tudi izobraževanje kadrov, brez katerega pač ne gre, predstavlja znaten strošek. Upoštevati je treba, da je to dolgotrajen proces (od nekaj mesecev, do enega leta!).

Preden se odločimo za investicijo v orodje CASE, sami pri sebi preverimo, ali smo metodološko in organizacijsko sposobni za njegovo uvedbo. Dejavniki, ki naj vplivajo na odločitev o nakupu naj bodo naslednji:

- prilagojenost orodja našemu okolju (strojna in programska oprema);
- metode, ki jih orodje podpira (ali jih poznamo, ali nam odgovarjajo);
- možnost izobraževanja;
- preverimo reference (če kdo orodje že ima, ga povprašajmo po izkušnjah);
- možnost nadgradnje (napovedani razvoj, združljivost s prihajajočimi programskimi produkti npr. DBMS, operacijskimi sistemi, itd);
- možnost povezave z drugimi orodji, okolji, operacijskimi sistemi.



Slika 1. Diagram toka podatkov v orodju SILVERRUN-DFD (CSAR)

Trendi razvoja orodij CASE

Pri prva orodja CASE so pripadala bodisi zgornjemu, bodisi spodnjemu razredu. Pri prvih predstavlja problem sama uvedba po definicijah, zapisanih v slovarju ali repozitoriju. Največkrat so bile rezultati orodja CASE globalno opisane zahteve, dokaj ohlapne specifikacije za pisanje programske kode, DDL definicije za ciljni DBMS. To seveda ni malo, če upoštevamo, da so vsi naštetih rezultati standardno dokumentirani. Vendar pa uporaba tovrstnih orodij CASE ne predstavlja bistvenega časovnega prihranka pri razvoju aplikacij.

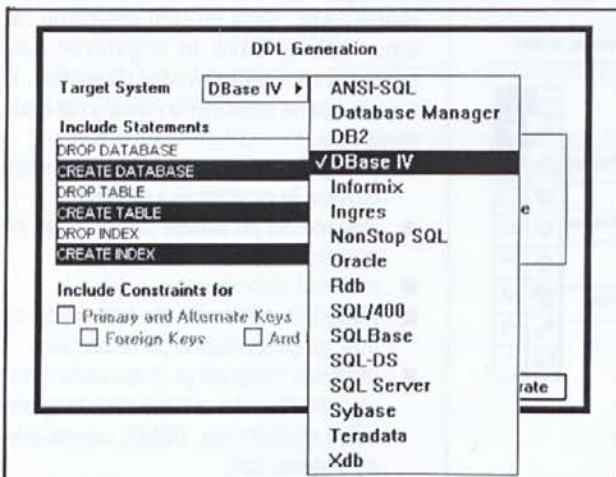
Po drugi strani orodja iz spodnjega razreda omogočajo hiter razvoj programov, njihovo testiranje in preverjanje. Orodja iz spodnjega razreda do neke mere odpravljajo hibo orodij iz gornjega razreda. Pri njihovi uporabi pa nimamo pregleda nad celotno aplikacijo, ki jo razvijamo, kar največkrat vodi k odmiku od bistva problema. Dobimo torej na kupe lepe in strukturirane kode, ki pa ne dela tistega, kar bi morala.

Rešitev se torej ponuja sama po sebi: I-CASE. V enem združimo orodja zgornjega in spodnjega razreda, pa smo na konju! Obstajajo integrirana orodja CASE, ki so vezana na eno okolje (npr. ORACLE CASE), kar je seveda ugodno za uporabnike tega okolja. Le-ti si z njim lahko učinkovito pomagajo, za druge pa stvari niso tako enostavne. Pomagajo si z drugim načinom združevanja orodij, z uporabo vmesnikov. Le-teh je zelo veliko in povezujejo najrazličnejša orodja iz različnih razredov. Po podatkih, ki so mi dostopni, bi sklepal, da je največ vmesnikov postavljenih v smeri orodja IEW™ oz. ADW™ (I-CASE, Knowledgeware™). Upoštevati je treba, da povezovanje ni vedno enostavno, saj je konceptom posameznih orodij medsebojno včasih težko poiskati skupni imenovalec. Obstajajo pa seveda prave "simbioze" med orodji. Primer za to sta SILVERRUN™ in SYNON™.

Vse kaže, da se orodja CASE razvijajo v smeri podpore "tovarnam programske opreme", kjer je mogoče z uporabo okolja za razvoj aplikacij (v bistvu spet I-CASE) hitro proizvesti raznovrstne rešitve za različne ravni in okolja.

Primer razvoja - orodje SILVERRUN

Dober primer takšnega razvoja je SILVERRUN, s katerim delam poldrugo leto. SILVERRUN je produkt firme CSA Research iz Kanade (Quebec). Na začetku je bilo to orodje DFD za modeliranje procesov za računalnike Macintosh. Kmalu so ga razširili še v



Slika 2. Sistemi za upravljanje s podatkovno bazo, za katere SILVERRUN-RDM generira DDL definicije

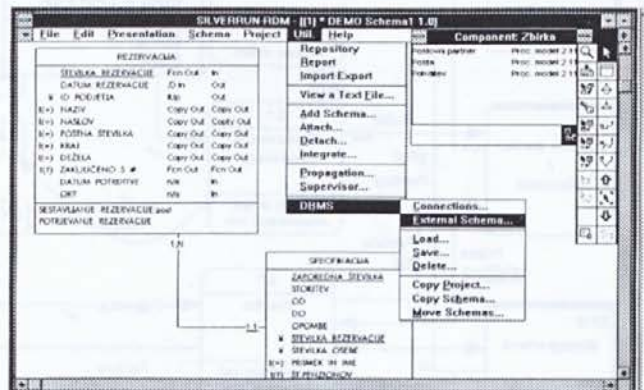
smeri modeliranja podatkov. Dodali so še modula ERX (Entity Relationship eXpert) za delo s konceptualnimi podatkovnimi modeli in z ERX povezani RDM (Relational Data Modeler) za modeliranje na logičnem nivoju. Zaradi potreb trga so področje uporabe zelo hitro razširili še za operacijska sistema OS/2™ in Microsoft Windows™. Pred slabim letom so dodali še modul za delo s projektnim repozitorijem WRM (Workgroup Repository Manager). Tako je nastal zelo soliden produkt, ki ga je moč šteti v gornji razred orodij CASE. CSA razvija ali že zagotavlja še nekaj vmesnikov za okolja. Možne so povezave z: IEW/ADW, INFORMIX, INGRES, ORACLE, PROGRESS, SYBASE/SQL Serv., SYNON/2E (ESF). Cela vrsta vmesnikov je v razvoju. SILVERRUN-RDM "pozna" in generira DDL definicije za 16 SQL sistemov za upravljanje z podatkovno bazo (DBMS) (Slika 2). Na voljo je tudi funkcija Import/Export, kjer lahko uporabnik sam definira obliko vhodno/izhodne datoteke. Uporabnik poljubno oblikuje tudi vsebino in izgled poročil.

Repozitorij

Zanimiva je razdelitev na interni in projektni repozitorij, na kakršno naletimo v SILVERRUN-u. Oba sta objektno usmerjena. V projektnem repozitoriju so koncepti, ki so skupni vsem trem, ki jih podpira SILVERRUN: model E-R, relacijska shema, diagram toka podatkov. To so t.i. skupni gradniki, podatkovne strukture, domene, osnovni podatkovni tipi ter podatki o različnih reprezentacijah in njihovih komponentah v okviru enega projekta. To pomeni, da vsebino ene relacijske sheme (SILVERRUN-RDM) lahko uporabimo v drugi relacijski shemi, ali v nekem diagramu toka podatkov (SILVERRUN-DFD), ali v konceptualnem modelu (SILVERRUN-ERX). Z orodjem SILVERRUN-WRM podatke iz repozitorija lahko dodeljemo posameznikom, ki delajo na (pod)projektu. Le-ti vračajo nove informacije, ki jih potem hranimo v globalnem repozitoriju za več (pod)projektov skupaj. WRM omogoča tudi prenos podatkov med različnimi (pod)projekti (med več projektnimi repozitoriji).

SILVERRUN-RDM 2.2

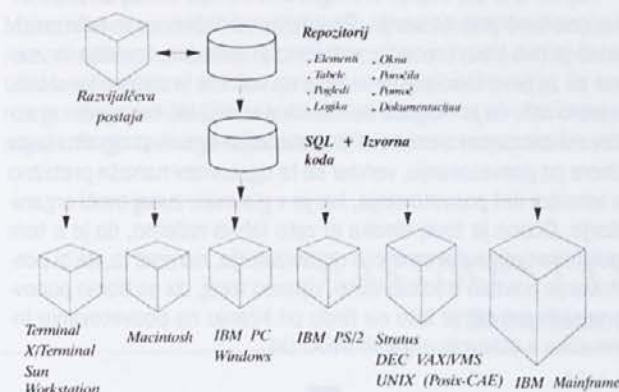
Korak naprej je prav gotovo nova verzija RDM 2.2. (drugi moduli so še vedno verzija 2.1.1). Le-ta podpira pojem podsheme, torej relacijske sheme, ki je vezana na neko nadrejeno shemo (podobno kot proces in podrejeni nivo v DFD). Podsheme lahko združujemo, pridružujemo drugo drugo, vršimo propagacijo in integracijo. S hierarhijo shem dosežemo predstavitev podrobnosti na različnih nivojih: konceptualnem, logičnem, fizičnem. Opišemo lahko podrobnosti logike posameznega dela uporabniškega vmesnika (zaslona, izpisa) v povezavi s tabelami v podatkovni bazi.



Slika 3. Primer načrtovanega vmesnika

SILVERRUN-ADE

Razvoj SILVERRUN-RDM 2.2 je bil kot kaže korak, ki je manjkal do povezave v celotno okolje za razvoj aplikacij. Tako se namreč imenuje produkt SILVERRUN-ADE (Application Development Environment). Izpustitev oznake CASE je najbrž bolj marketinškega pomena, dejansko pa je to orodje I-CASE, ki vključuje že omenjene module SILVERRUN-ERX, SILVERRUN-RDM, SILVERRUN-DFD in SILVERRUN-WRM z SILVERRUN-ADC (Application Development Center). ADC omogoča oblikovanje uporabniškega vmesnika ter generiranje kode C za različna okolja (slika 4). Dostop do podatkovne baze je v kodi realiziran z uporabo jezika SQL[®] oziroma t.i. vstavljenega SQL (embedded SQL). Vse skupaj se dogaja na grafični delovni postaji (Macintosh[™], OS/2[™], Windows[™]) ali v



Slika 4. SILVERRUN-ADE

Opomba

SILVERRUN-ADE je že v fazi alfa testa in bo na voljo spomladi.

mreži delovnih postaj. Repozičtorij je v zasnovi enak, kot je že obstoječi SILVERRUN-ov repozičtorij. Ker je že v osnovi definiran objektno; ga pač ni bilo težko razširiti.

S pomočjo SILVERRUN-ADE lahko razvijamo aplikacije tipa odjemalec-strežnik, za delo v omrežju ali za samostojen računalnik. Uporabljamo iste specifikacije, le generirana koda je prilagojena. Enako velja tudi, če izdelamo najprej aplikacijo za lokalno omrežje, potem pa še za samostojno delovno postajo.

Zaključek

V času, ko tempo poslovanja vrtoglavo narašča, ko smo dobesedno zasuti z novimi dosežki informacijske tehnologije, ko uporabniki postajajo vse bolj osveščeni in zahtevnejši, najbrž ne bomo kos svojim nalogam brez ustreznih orodij. Orodje, kot je SILVERRUN-ADE, je primerno za razvoj poslovnih programskih rešitev v različnih okoljih in za ali zelo velikega in zahtevnega naročnika, ali pa za veliko število naročnikov. Prav gotovo bodo šla orodja CASE v tej smeri, namreč v integracijo in možnost generiranja programskih rešitev za različna okolja, ki bodo predvsem izkoriščala prednosti, ki jih prinaša nova tehnologija.

Jasno je, da si vsi ne bodo mogli privoščiti najsodobnejših razvojnih orodij, pač pa bodo to storile velike programske hiše in organizacije. Le-te si bodo namreč edine lahko privoščile strošek uvajanja takšnega orodja. Drugim se to ne bo izplačalo. Aplikacije, razvite na ta način bodo lahko cenejše od lastnega razvoja. Oblikovale se bodo že omenjene tovarne programske opreme, ki bodo sposobne izdelovati poceni "konfekcijske" aplikacije in aplikacije po naročilu. No, na srečo pa bo tudi ta način dela zahteval ljudi iz naše stroke. Za nas dela (še) ne bo zmanjkalo, le prilagoditi se bomo morali.

INFORMATIKA V DRŽAVNIH ORGANIH

Poročilo o posvetovanju INDO'93

Niko Schlamberger

V dneh 16 in 17 septembra 1993 je bilo na Brdu pri Kranju organizirano posvetovanje o informatiki v državnih organih. Posvetovanje je organiziral Center vlade za informatiko kot srečanje informatikov, ki delajo v državnih organih. Zamisel za strokovno srečanje je zorela dlje časa. Začetek sega v februar leta 1992, ko je tedanji Republiški zavod za informatiko s soorganizatorjem Fakulteto za organizacijske vede iz Kranja priredil v Ljubljani posvetovanje o računalniškem izmenjavanju podatkov v javni upravi. Teža posvetovanja se je udeležilo precej informatikov iz državnih organov in splošno mnenje teh strokovnjakov je bilo, da bi kazalo organizirati bolj specializirano prireditev, ki bi bila po vsebini lahko širša, vendar bi bila prvenstveno namenjena izmenjavi njihovih izkušenj.

Razlogov za organizacijo takega posvetovanja je seveda več. Naj navedemo le nekaj pglavitnih. Informatika je stroka, ki v nekem smislu povezuje vse državne organe, saj si je nemogoče predstavljati, da bi bile njihove odločitve lahko kvalitetne brez razpolaganja z relevantnimi podatki in informacijami. Na področju informatike država relativno veliko investira. Velikostni red proračunske postavke Centra vlade za informatiko, ki je zadolžen za pridobivanje naprav, programov in storitev informacijske tehnologije za večino državnih organov, znaša v letu 1993 milijardo tolarjev. Poleg tega so v državnih organih praktično povsod zapos-

eni informatiki različnih profilov, katerih delo in prizadevanja morajo biti usklajeni, če naj imajo investicije v informacijsko tehnologijo za državo pozitivne učinke. Zaradi narave dela in organizacije državnih organov so strokovni stiki pogosto omejeni na realizacijo projektov in srečanje take vrste lahko pripomore k temu, da se informacije o dosežkih in problemih izmenjajo v širokem strokovnem krogu, s čemer pridobijo vsi, ki se ga udeležijo, organizator pa je imel možnost preveriti svoje usmeritve in načrte za prihodnost.

Posvetovanje, na katerega je prišlo preko sto udeležencev, je

bilo organizirano v štirih vsebinskih sklopih: informacijska tehnologija, informatika v pravosodnih organih, informatika v državnem zboru in informatika v izvršilni oblasti. Kot častni pokrovitelj posvetovanja posvetovanja se je tej prošnji prijazno odzval finančni minister g. Mitja Gaspari, za kar se mu tudi na tem mestu zahvaljujemo. K aktivnemu sodelovanju na posvetovanju so bili povabljeni vsi državni organi, kar pomeni, da se je od vseh pričakoval referat, ki bi po presoji avtorja ali državnega organa prispeval h kakovosti in ciljem posvetovanja. Obžalujemo lahko, da se vabilu k sodelovanju niso odzvala ministrstva, ki bi kot državni organ imela kaj povedati predvsem o usmeritvah in dosežkih informacijske tehnologije. S tem bi se še dvignila kvaliteta vsebine posvetovanja, hkrati pa bi lahko zainteresirana ministrstva na nevsiljiv način na marsikaj opozorila. Naj ostane ta ugotovitev zapisana kot izziv in vabilo za prihodnje posvetovanje.

Poleg teh štirih sklopov sta bila ob posvetovanju organizirana še dva dogodka. Prvi je bil predstavitev naprav in programskih produktov različnih podjetij, ki poslovno sodelujejo z državnimi organi, drugi pa okrogla miza po posvetovanju. Le-ta je bila namenjena poglobljenim diskusijam na katerokoli od tem, za katere je zmanjkalo časa po predstavitvi prispevka in je bil zanj še vedno interes, ali pa temi, ki kot referat ni bila predstavljena na posvetovanju, je pa udeleženec presodil, da je dovolj zanimiva in aktualna za obravnavo v javnosti.

Organizator je bil nad odzivom podjetij prijetno presenečen, ker je sprva kazalo, da bo bolj skromen. Zdi pa se, da so podjetja le razumela nastop na posvetovanju kot poslovno priložnost in dogodek, na katerega jim publike ni treba posebej povabiti. Prijetno presenečenje je bila tudi okrogla miza, ki je bila organizirana

na po koncu vsebinskega dela na drugi dan posvetovanja - v petek popoldne, vendar dvorana le ni ostala prazna.

Vsi referati, ki so bili predstavljeni na posvetovanju, so natisnjeni v zborniku referatov z naslovom Informatika v državnih organih. V okviru tega poročila ni mogoče in tudi ni smiselno, da bi povzeli vsebino vseh prispevkov. Naj vendarle navedemo, da jih je bilo osemindvajset, pri čemer niso bili objavljeni vsi, ki so bili predloženi. Programski odbor je zavzel stališče, da so dobrodošli vsi prispevki, ki osvetljujejo problematiko, tehnologijo ali opisujejo dosežke, da pa ne morejo biti sprejeti prispevki, ki so pretežno reklamne narave. Po zborniku je mogoče presoditi, ali je bila odločitev pravilna in izbor ustrezen v smislu strokovne kvalitete posvetovanja.

Naj končno še, čeprav bi mogoče lahko kdo očital, da pristransko, ocenimo posvetovanje. Po odzivu udeležencev in referentov sodeč je bilo tako srečanje potrebno in koristno, izvedba in vsebina pa za prvo tako posvetovanje na več kot le zadovoljivi višini. Verjetno drži, da je mogoče še marsikaj izboljšati, kar je bila ugotovitev na skupnem sestanku organizacijskega in programskega odbora po posvetovanju, vendar se ta ugotovitev nanaša pretežno na tehnični del posvetovanja, kar je v glavnem zunaj moči organizatorja. Ocena je torej visoka in zato lahko rečemo, da je s tem izpolnjena tudi skrita ambicija organizatorja, namreč ta, da bi posvetovanje postalo tradicionalno. Upamo torej, da se bomo ponovno sestali prihodnje leto na Brdu pri Kranju na posvetovanju Informatika v državnih organih INDO'94.



POROČILO O II. POSVETOVANJU

"KAKOVOST V PROGRAMSKEM INŽENIRSTVU"

RADENCI, 23. IN 24. SEPTEMBRA 1993

Marjan Pivka

Društvo ekonomistov Maribor, sekcija za informatiko, je organiziralo že drugo posvetovanje na temo kakovost v programskem inženirstvu. Tokrat je bilo posvetovanje v Radencih, trajalo je dva dni, udeležilo pa se ga je blizu 80 strokovnjakov iz Slovenije.

Program posvetovanja je bil razdeljen na naslednje tri tematske sklope:

- temeljna izhodišča obravnave kakovosti,
- kakovost procesa gradnje programske opreme
- in kakovost programskih izdelkov.

V prvem delu je treba poudariti referata, ki sta obravnavala vprašanja inovacij, povezanostjo inovacij s programsko opremo ter odgovornost managementa za dosego primerljive odličnosti.

V drugem, najboljše delu posvetovanja, je bilo predstavljenih kar 10 referatov, zato je zaradi omejitve prostora težko izločiti in poudariti najpomembnejše. Obravnavane so bile naslednje teme, ki se neposredno nanašajo na kakovost procesa: obvladovanje kakovosti, nadzor razvojnega postopka, ekspertni sistemi, preverjanje, testiranje in vrednotenje ter certificiranje procesov. Poleg teh pa so bile podane tudi nekatere teme, ki so se nanašale na programska orodja in objektivno orientirane pristope.

V tretjem delu so bila obravnavana nekatera vprašanja kakovosti programskih izdelkov. To področje je bilo v Sloveniji v zadnjih treh letih velikokrat obravnavano, zato ne preseneča manjše število referatov.

Organizirana je bila tudi okrogla miza, ki je dodobra razburkala tako poslušalce kot moderatorje. Nekateri domači proizvajalci so namreč predstavili svoje poglede na kakovost v programskem inženirstvu, ki pa se niso vedno skladali s teoretičnimi spoznanji raziskovalcev. Prevladalo je prepričanje, da je v zvezi s kakovostjo treba prestopiti obstoječi prag, poti pa so lahko različne.

Iz vsebine in števila referatov izhaja, da se postopoma širi število raziskovalcev in razvijalcev iz prakse, ki se ukvarjajo z vprašanjem kakovosti v programskem inženirstvu. To je izredno pomembno, saj se bo v Sloveniji le na ta način razvilo dovolj znanja na strani raziskovalcev, kar bo posredno generiralo nove potrebe pri uporabnikih.

Vsi referati (skupaj jih je 17) so natisnjeni v tehnično in oblikovno lepo urejenem zborniku. Nekaj števil zbornika je še na razpolago v tajništvu društva.

Udeleženci posvetovanja so se oba dneva aktivno vključevali

v potek posvetovanja. Problemi, vprašanja in dileme, ki so jih udeleženci odpirali, so bili kritični in hkrati sodelovalni.

Posebej lahko izpostavimo naslednje probleme in dileme udeležencev:

1. Večina slovenskih programskih hiš je še vedno na začetni ravni razvoja. Tisti, ki se tega zavedajo in se zavedajo potrebe po zorenju, imajo težave z lastnim znanjem, nerazumevanjem managementa in lastnimi organizacijsko psihološkimi pregradami.
2. Jasno je bila vidna tesna povezanost med kakovostjo izdelka in kakovostjo procesa.
3. Izpostavljena je bila dilema o zaupanju v certifikacijski postopek.
4. Izpostavljeno je bilo vprašanje stroškov preskušanja in certificiranja.

Ministrstvo za znanost in tehnologijo, Urad za standardizacijo in meroslovje, je predstavilo predvideno shemo preskušanja in certificiranja izdelkov, storitev, procesov in ljudi v Sloveniji. Ta shema je integralni del Zakona o standardizaciji, ki je v fazi sprejemanja. Predstavitev je lepo popestrila posvetovanje in prikazala,

kako se prizadevanja za dvig kakovosti v programskem inženirstvu odražajo v infrastrukturi države.

Posvetovanje so omogočile naslednje firme: Marand d.o.o. Ljubljana, Aster d.o.o. Ljubljana, Pro Bit Slovenske Konjice, Liko Pris Vrhnika, Razvojni center IRC Celje, Tip Pri d.o.o. Maribor in Marles Maribor.

Sponzorjem je bil na voljo razstavni prostor, na katerem so lahko predstavili svoje izdelke in storitve. Brez njih bi bila izvedba posvetovanja vprašljiva.

Organizatorje posvetovanja so zavzetost in število udeležencev ter visok nivo večine referatov prepričali, da je treba s posvetovanji nadaljevati tudi naslednja leta. Nekateri so predlagali, da posežemo v mednarodni prostor. Organizatorjem je to dobrodošel izziv. Potrudili se bomo, da bomo naslednje posvetovanje organizirali že v mednarodni zasedbi.



EAST/WEST COMMUNICATION

3. mednarodni simpozij o EDI

Niko Schlamberger

Dne 28. in 29. oktobra letos sta Gospodarska zbornica Avstrije in Austriapro, združenje za pospeševanje računalniškega izmenjavanja podatkov, organizirala na Dunaju tretje mednarodno posvetovanje o računalniškem izmenjavanju podatkov pod imenom East/West Telecommunication. Na posvetovanje je bilo povabljenih več strokovnjakov iz držav centralne in vzhodne Evrope, ki imajo interes za to področje informatike in ki lahko hkrati prispevajo k izmenjavi izkušenj in dosežkov. Zastopane so bile Avstrija, Nemčija, Češka, Slovaška, Hrvaška, Madžarska, pa tudi Bolgarija, Makedonija, Romunija, Poljska, Rusija in Ukrajina. Slovenija je bila zastopana z udeleženci posvetovanja in tudi z referenti, ki jih je povabil prireditelj. Posvetovanju, je predsedoval Helge Schoener, direktor združenja Austriapro.

Naj v nadaljevanju povzamemo potek posvetovanja in slovensko udeležbo na njem. Za začetek je zanimivo navesti, kdo je pozdravil okoli sto tiriideset udeležencev posvetovanja. Prvi nagovor je imela dr. Helga Koch, podpredsednica avstrijske zvezne gospodarske zbornice. Pozdravu je sledil nagovor dr. Roberta Launškega-Tiefenthala, predsednika združenja Austriapro. Sledili so prispevki referentov, med katerimi naj posebej navedemo H. A. Hansella, člana sekretariata UN/ECE, ter T. Blomfeldta, predsednika delovne skupine UN/ECE Trade WP.4. Ta imena in tudi podatek, da je udeležba kotizacije prosta, so vredna omembe predvsem zato, da bi bilo kar se da nazorno, kakšen pomen dajeta področju izmenjavanja podatkov avstrijska gospodarska zbornica in država ter da sta pripravljena v to kar nekaj investirati. V nadaljevanju so bili prikazani dosežki in pristopi računalniškega izmenjavanja podatkov iz različnih področij gospodarstva, med drugim bančništva, transporta, gradbeništva, avtomobilske industrije in komunikacij.

Na posvetovanju je bila Slovenija aktivno zastopana in sicer

so bili povabljeni referenti M. Dobravc, ki je podala splošen pregled stanja v Sloveniji, N. Schlamberger, ki je prikazal razvoj računalniškega izmenjavanja podatkov v državnih organih, R. Novak s predstavitevjo združenja SLOdette in M. Damjan, ki je bila povabljen kot predsednica društva EDI Slovenija. Lahko rečemo, da so bili slovenski prispevki deležni pozornosti predvsem iz razloga, ker so za večino udeležencev iz držav bivše vzhodne Evrope pokazali pristop k uporabi računalniškega izmenjavanja podatkov in mogoče usmeritve na tem področju za razliko od tistih, ki so korak pred nami in so prikazovali že konkretne delujoče rešitve. Pri tem pa se ne smemo spozabiti, da bi tiste, ki zanje verjamo, da lahko od slovenskih zgledov pridobijo, podcenjevali. Na Poljskem na primer deluje združenje EDIPOL Ltd. in predsednik tega združenja je prikazal implementacijo EDIFACT v transportu; podpredsednik češkega podjetja CS FITPRO je podal pregled uporabe UN/EDIFACT na češkem in stanje v državah vzhodne Evrope; udeleženec iz Madžarske je prikazal prizadevanja v svoji državi. Posebne omembe sta vredna dva prispevka udeležencev posvetovanja iz Romunije: ena je podala pregled računalniškega izmenjavanja podatkov v Romuniji, druga pa predstavila projekt uvedbe računalniškega izmenjavanja podatkov v romunski carini (!), ki je že v teku (!).

Posvetovanje so spremljali nastopi podjetij iz različnih držav - zdi se, da so postali del železnega repertoarja posvetovanj - ki so prikazala svoje dosežke in rešitve, reči moramo, da na prijazen in nevsiljiv način in v posebni dvorani. Podjetja so navedena v dokončnem programu posvetovanja - v tej zvezi pa še ena prijetna in ena manj razveseljiva informacija. Med predstavitelji je napovedano podjetje EDIpro iz Slovenije (pohvalno), ki pa se na Dunaju žal ni pojavilo (žal).

NAČRTOVANJE IN GRADNJA INFORMACIJSKIH SISTEMOV

- Povzetek recenzijskih poročil -

Pred izidom knjige "Načrtovanje in gradnja informacijskih sistemov", katere avtorja sta dr. Andrej Kovačič in dr. Mirko Vintar, podajava recenzenta povzetek recenzijskih poročil, ki so nastala ob pregledu rokopisa.

Knjigo sta avtorja razdelila v tri dele. Prvi del opredeljuje podjetniški vidik informatike kot infrastrukture sodobne organizacije in metodološke pristope ter metode in tehnike modeliranja podatkov in postopkov. Drugi del ob primeru iz vsakdanje prakse utemeljuje celovit, sodoben metodološki pristop, ki se je dokazal tudi v našem okolju in zajema tako faze načrtovanja informatike kot tudi same gradnje baze podatkov in programskih rešitev. V tretjem delu pa avtorja podajata tehnološka, organizacijska in kadrovska izhodišča, ki ob upoštevanju ustreznih standardov zagotavljajo uspešno načrtovanje, gradnjo in uporabo informacijskih sistemov.

Knjiga je po obsegu, vsebini in zgradbi namenjena

širokemu krogu bralcev, ki se srečujejo z obravnavano problematiko. Namenjena je študentom, saj je v prvem delu napisana kot učbenik, ki zajema študijski program informatike večine šol in fakultet. Drugi in tretji del pa sta zasnovana tako, da predstavljata nepogrešljiv pripomoček vodstvenim delavcem, načrtovalcem informatike in drugim razvijalcem informacijskih sistemov ter članom projektnih timov v organizacijah.

Do sedaj pri nas nismo izdali domačega dela, ki bi tako celovito zajelo obravnavano problematiko. Knjiga bo nedvomno zapolnila določeno vrzel v slovenski strokovni literaturi s tega področja. Zato meniva, da bo delo vzbudilo zanimanje širšega kroga ljudi.

Knjiga bo izšla v začetku januarja 1994 v obsegu 316 strani pri Državni založbi Slovenije.

Recenzenta

prof. dr. Janez Grad

prof. dr. Ferdinand Marn

GOSPODARSKA ZBORNICA SLOVENIJE
SLOVENSKO DRUŠTVO INFORMATIKA
DRUŠTVO EKONOMISTOV LJUBLJANA

organizirajo 1. posvetovanje

DNEVI SLOVENSKE INFORMATIKE
PORTOROŽ 94

(Portorož 13-15 april 1994)

POVABILO K SODELOVANJU
(Prva objava)

Namen in cilji posvetovanja

V svetu, pa tudi pri nas, vse bolj prevladuje drugačen pogled na uporabo informacijske tehnologije, kot smo bili priča v preteklosti. Ob ugotovitvi, da je uporaba informacijske tehnologije nujna za preživetje in uspešno delovanje organizacije na trgu, se vse bolj uveljavlja naložbeni vidik uporabe. Le-ta je usmerjen v ugotavljanje priložnosti uporabe informacijske tehnologije, s stališča povrnitve naložbenega vložka in pridobitve konkurenčne prednosti pred ostalimi organizacijami.

Ob tem ugotavljamo, da je informacijska tehnologija dobila v sodobnih družbah infrastrukturni značaj, zato je število ljudi, ki se tako ali drugače srečujejo z njo, iz dneva v dan večje. Pri tem so vloge pravzaprav razdeljene na uporabnike in na načrtovalce njene uporabe. Enim in drugim je sprotno spremljanje razvoja tega področja nujno za uspešno delo v stroki.

DNEVI SLOVENSKE INFORMATIKE izhajajo iz tradicije portoroških srečanj ekonomistov na temo informatike, vendar menimo, da spremenjene razmere kličejo po širšem in interdisciplinarnem pristopu, ki bo zanimiv za najširši krog udeležencev.

Delo posvetovanja bo potekalo v več sekcijah, ki jih bo izoblikoval programski odbor na osnovi predloženih prispevkov.

V okviru prvega simpozija dajemo prednost naslednjim tematskim vprašanjem:

- poslovne priložnosti uporabe informacijske tehnologije,
- direktorski informacijski sistemi,
- odprti sistemi,
- reinženiring poslovnih postopkov,
- downsizing, outsourcing,
- procesiranje in arhiviranje elektronskih dokumentov in multimedija,
- CASE orodja,
- razvoj metodologij načrtovanja in gradnje informacijskih sistemov,
- informacijska orodja,
- avtomatizacija pisarn,
- računalniško integrirana proizvodnja,

- objektivni pristop,
- komunikacije in elektronska izmenjava podatkov,
- standardi,
- izobraževanje na področju informatike,
- javne baze podatkov,
- odprti sistemi,
- informatika v računovodstvu.

Prispevki izbranih avtorjev bodo razvrščeni v naslednje kategorije:

- strokovne razprave (v obsegu 5-8 strani),
- poročila (2-5 strani),
- prikazi rešitev itd (2-5 strani).

Vsi sprejeti prispevki bodo objavljeni v posebni številki revije Uporabna informatika.

Pomembni datumi:

- 31.12.1993 rok za oddajo prijav,
- 15.1.1994 obvestilo avtorjem o uvrstitvi prispevkov v program,
- 28.2.1994 rok za oddajo za tisk pripravljenih prispevkov.

Prijave naj vsebujejo:

- natančen naslov avtorja,
- naslov prispevka,
- povzetek prispevka v obsegu največ ene strani.

Naslov organizacijskega odbora :

*Gospodarska zbornica Slovenije, Ljubljana,
Slovenska 58, 61000 Ljubljana
(Za simpozij Dnevi slovenske informatike)*

Kontaktna oseba: Franci Žle

tel. : (061 317-287, 061 13-13-190)

fax. : (061 312-569)

VČLANITEV SLOVENIJE V MEDNARODNO ORGANIZACIJO IFIP

Večini slovenskih informatikov ime organizacije IFIP verjetno ni znano, vendar pa mnogi najbrž ne poznajo podrobneje njenega delovanja, aktivnosti ter organiziranosti. Zato jo bomo najprej na kratko predstavili.

IFIP (The International Federation for Information Processing) je največja mednarodna zveza profesionalnih in tehničnih orga-

nizacij (ali nacionalnih združenj), ki se ukvarjajo z obdelavo informacij oziroma informacijsko tehnologijo ali na kratko informatiko. Iz vsake države je lahko sprejeta v polnopravno članstvo le ena taka organizacija, ki mora biti predstavnica nacionalnih aktivnosti na področju informatike. Trenutno je zastopanih v IFIP-u, preko svojih nacionalnih združenj, blizu sedemdeset držav.

Glavni cilji naše svetovne stanovske organizacije so:

- pospeševanje razvoja, raziskav in uporabe informacijske tehnologije na najrazličnejših področjih ter mednarodnega sodelovanja pri teh aktivnostih,
- omogočanje izmenjave izkušenj med nacionalnimi združenji ter načrtovanja bodočih aktivnosti na področju informatike, ki so mednarodnega pomena,
- promocija profesionalnosti, standardov, etičnih norm itd na področju informatike,
- proučevanje socialnih in drugih družbenih posledic uvajanja in uporabe informacijske tehnologije ter zaščita ljudi pred njeno zlorabo.

Organizacija IFIP je bila ustanovljena leta 1960 pod pokroviteljstvom UNESCA. Danes se njene aktivnosti odvijajo v okviru štirinajstih tehničnih komitejev (TC- technical committees) ter petinšestdesetih delovnih skupin (WG- working groups), ki pokrivajo praktično vsa področja informatike. Tehnični komiteji in delovne skupine organizirajo različna srečanja in znanstvene konference za svoje člane in druge udeležence. Vsaka tri leta (od leta 1992 dalje pa vsaki dve leti) organizira IFIP svetovni kongres. Zadnji kongres je bil septembra 1992 v Madridu, naslednji pa bo od 28. avgusta do 2. septembra 1994 v Hamburgu.

Za vsako državo oziroma njeno nacionalno združenje informatikov, ki jo predstavlja, je čast postati oziroma biti član te organizacije. Sprejem v polnopravno članstvo je namreč povezan z dolgotrajno proceduro in je priznanje za delo in dosežke predstavnikov države članice na nacionalni in mednarodni ravni. Slovenski informatiki smo bili do razpada Jugoslavije včlanjeni v IFIP v okviru Jugoslavije. Lahko rečemo, da so slovenski predstavniki v preteklosti igrali vidno vlogo v tej razvejani organizaciji, saj smo leta 1971 organizirali v Ljubljani tudi enega prvih svetovnih kongresov. Z razpadom Jugoslavije in osamosvojitvijo Slovenije pa smo, po obrazložitvi IFIP-ove komisije za sprejem novih članic, izgubili tudi svoje članstvo v IFIP-u.

Zato je Slovensko društvo Informatika že lani začelo postopek za včlanitev Slovenije kot polnopravne članice v to organizacijo in upamo, da nam bo to v prihodnjem letu tudi uspelo.

M.V

PREDAVANJE

Slovensko društvo Informatika organizira predavanje dr. Roba Blokzijla iz Amsterdama, predsednika RIPE - evropskega dela mreže Internet, z naslovom:

Omrežje Internet in njegov evropski del

Predavanje bo v okviru prireditve **INFOS, 23. novembra 1993, ob 13 uri v Štihovi dvorani Cankarjevega doma.**

Prisrčno vabljeni!

The Fourth International Conference
INFORMATION SYSTEMS DEVELOPMENT - ISD '94, Methods & Tools, Theory and Practice,
20 - 22 September 1994, Bled,

Fakulteta za organizacijske vede, Univerza v Mariboru in Oddelek za informacijske sisteme, Univerza v Gdansk
(University of Maribor, School of Organizational Sciences and University of Gdansk,
Department of Information Systems)

Informacije: Jože Zupančič, tel. 064 222 804, 064 221 424



Revija Uporabna informatika bo brezplačno objavljala v rubriki Koledar prireditev datume strokovnih srečanj, posvetovanj in drugih prireditev s področja informatike. Obvestila pošljite v naslednji obliki: ime srečanja, datum in kraj prireditve, naziv organizatorja, ime in telefonska številka kontaktne osebe. Naš naslov: Slovensko društvo Informatika, za revijo Uporabna informatika, rubrika: Koledar prireditev, 61000 Ljubljana, Vožarski pot 12. Objavljali bomo vsa obvestila, ki bodo prispela 30 dni pred objavo revije.



Navodila avtorjem

Prispevke pošiljajte v predpisani obliki na naslov Slovensko društvo Informatika, 61000 Ljubljana, Vožarski pot 12, s pripisom za revijo Uporabna informatika. Če je možno, naj bo članek lektoriran. V uredništvu bomo opravili korekturo in se po presoji posvetovali z avtorjem, da članek tudi lektoriramo. Prispevek naj bo v obsegu največ avtorska pola (30.000 znakov) za strokovne članke in približno 2 do 3 tiskane strani za druge prispevke. Vsak strokovni članek naj ima na začetku povzetek v slovenskem in v angleškem jeziku. Pošljite ga na disketi in odtisnjene na papirju. Napisan je lahko v kateremkoli urejevalniku besedil, vendar naj bo na disketi tudi kopija v ASCII formatu. Na disketi označite, kateri urejevalnik ste uporabili, in ime datoteke. Datoteko imenujte s svojim priimkom, n. pr. Novak.doc ali Novak.txt. Slike, ki ste jih izdelali z grafičnim programom, označite podobno. Na natisnjem izvodu članka naj bo jasno vidno, kam sodi posamezna slika. Lahko priložite tudi originalne predloge, ki jih na hrbtni strani označite s številkami, tako kot v natisnjem besedilu. Pišite v razmaku vrstic 1, brez posebnih ali poudarjenih črk ali podčrtovanja, za ločilom na koncu stavka napravite samo en prazen prostor, ne uporabljajte zamika pri odstavkih.

Za vsa vprašanja se obračajte na tehnično urednico Katarino Puc, 61000 Ljubljana, Ulica Gubčeve brigade 120, tel. 1271-579

UPORABNA INFORMATIKA

Ustanovitelj in izdajatelj:

Slovensko društvo Informatika, 61000 Ljubljana, Vožarski pot 12

Glavni in odgovorni urednik:

Mirko Vintar

Svet revije:

Čiril Baskovič, Andrej Cetinski, Ljubica Djordjevič, Franc Križaj, Ivan Žerko

Uredniški odbor:

Tomaž Banovec (statistična in prostorska informatika),

Vladimir Batagelj (tehniška informatika),

Cene Bayec (informacijska infrastruktura),

Jože Gričar (računalniška izmenjava podatkov in medorganizacijski sistemi),

Janez Grad (operacijske raziskave),

Andrej Kovačič (poslovna informatika),

Marjan Pivka (kakovost in standardi),

Katarina Puc (informatika in okolje),

Vladislav Rajkovič (sistemi za podporo odločanju),

Ivan Rozman (informacijska tehnologija),

Niko Schlamberger (informatika v upravi),

Mirko Vintar (avtomatizacija pisarn).

Tehnična urednica: Katarina Puc

Oblikovanje: Zorja Vintar, Dušan Weiss

Tisk: Tiskarna Tone Tomšič

Naklada: 1.000 izvodov

Revija izhaja četrtletno. Cena posamezne številke je 980 SIT.

Letna naročnina za podjetja SIT 4.000, za vsak nadaljnji izvod SIT 2.400.

Letna naročnina za posameznika SIT 2.400, za študente SIT 1.200.

Po mnenju Urada vlade za informiranje Republike Slovenije z dne 1.6.1993 je revija Uporabna informatika proizvod informativnega značaja iz 13. točke tarifne številke 3 tarife prometnega davka, po kateri se plačuje davek od prometa proizvodov po stopnji 5%. Prometni davek je vračunan v ceno revije.

ZAVOD REPUBLIKE SLOVENIJE ZA STATISTIKO, Vožarski pot 12, 61000 LJUBLJANA

INDOK CENTER

Informacijsko dokumentacijski center

Telefon: 061 21-69-51, 061 125-53-22 int. 215

Telefax: 061 21-69-32

STORITVE

SPLOŠNE INFORMACIJE

- NAJNOVEJŠE INFORMACIJE (indeksi cen, plače)
- ZADNJI MESEČNI IN LETNI PODATKI
- VEČMESEČNE ALI LETNE SERIJE PODATKOV
- IZPOSOJA VSEH OBJAVLJENIH STATISTIČNIH PODATKOV V ČITALNICI
- v pregled ali prepis Vam nudimo vse objavljene statistične podatke, ki jih hranimo v Indok centru

IZPOSOJA NA DOM

- za določen čas posojamo publikacije in objavljene rezultate statističnih raziskovanj.

PRIPRAVA IN IZVEDBA NOVINARSKIH KONFERENC

- seznanjanje javnosti z aktualnimi, najnovejšimi podatki,
- informacije o socioekonomskih gibanjih v določenem obdobju,
- predstavitve in analiza dogajanj na posameznih področjih statistike.

POSLOVANJE

Informacije, izposoja, čitalnica:

ponedeljek - petek od 8.00 - 12.00 ure

sreda od 8.00 - 12.00 ure in od 14.00 - 16.00 ure

DOKUMENTACIJA

računalniško podprta bibliografska baza podatkov vsebuje:

- izdane publikacije Zavoda RS za statistiko in drugih mednarodnih državnih statističnih institucij,
- dokumentirana gradiva, prejeta od različnih mednarodnih institucij (ZN, OECD, FAO, ILO...)

KNJIŽNICA

- statistika kot veda (izdaje slovenskih in nekaterih tujih avtorjev s področja statistike)
- statistika - podatki (naše in tuje izdaje bibliografij, katalogov, almanahov...)
- publicistika drugih važnejših strokovnih področij (informacijske znanosti, matematika, upravljanje, vodenje, zakonodaja...)
- zborniki s posvetovanj (različnih strokovnih društev, npr.: statistikov, matematikov, ekonomistov)
- standardi - nomenklature (s statističnega in drugih področij)
- slovarji posameznih svetovnih jezikov
- domače in tuje revije, domači in tuji časopisi



ZAVOD REPUBLIKE SLOVENIJE ZA STATISTIKO

