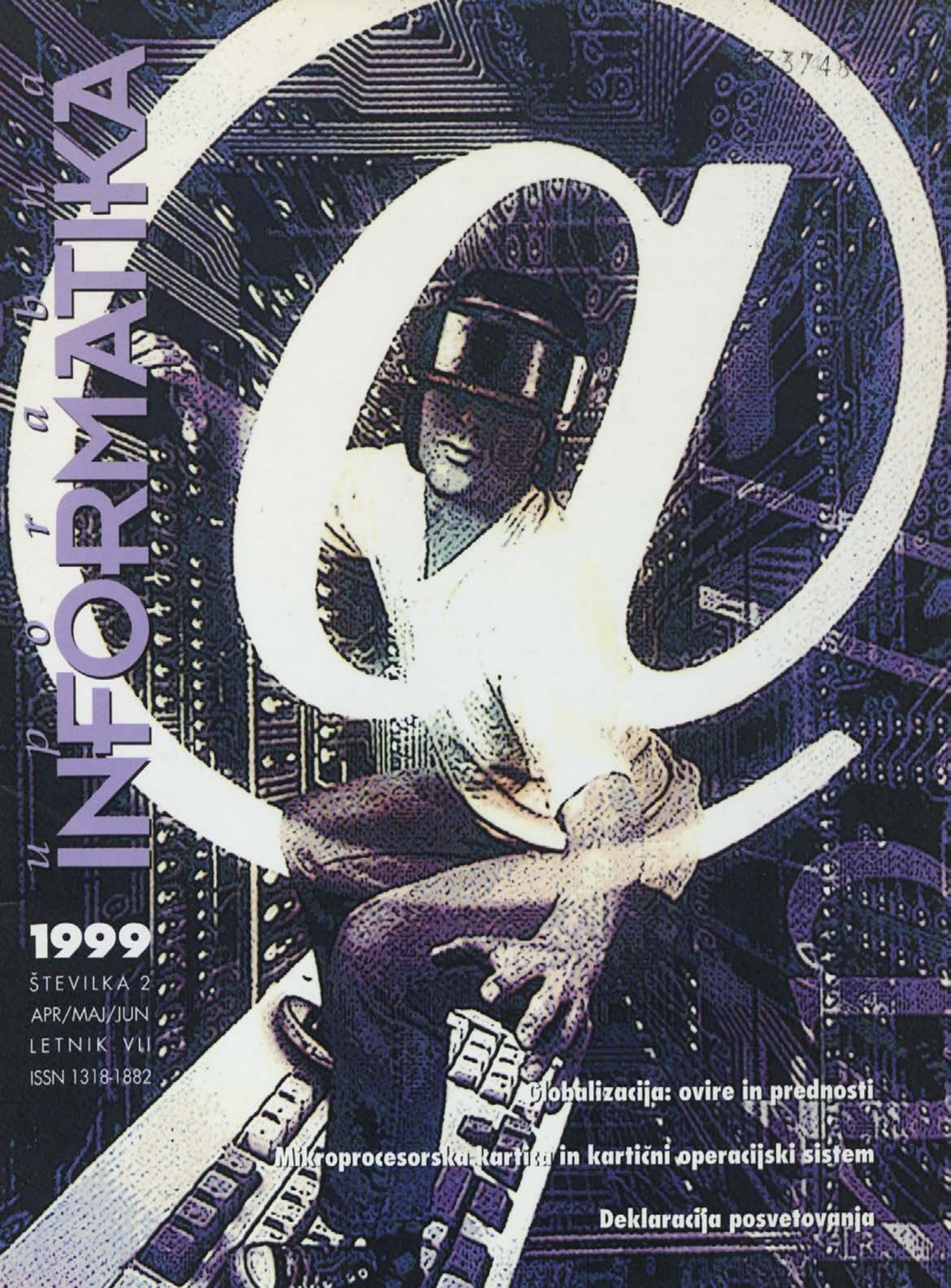
Uporabna
INFORMATIKA

1999
ŠTEVILKA 2
APR/MAJ/JUN
LETNIK VII
ISSN 1318-1882



Globalizacija: ovire in prednosti

Mikroprocesorska kartica in kartični operacijski sistem

Deklaracija posvetovanja

Spoštovane bralke in bralci,

ker je v tej številki govora o globalizaciji v luči prihajajoče informacijske družbe ter o njenem vplivu na naše majhno gospodarstvo, se mi zdi umestno odpreti razpravo o vlogi naše revije v tem procesu in s tem o njenem poslanstvu. Povodov za to je več. Eden je vezan na razprave v uredniškem odboru, glede uredniške politike, izbora prispevkov ter prednostnih tem, ki se zgostijo ob koncu vsakega leta. Drugi povod pa je razprava, objavljena v zadnji številki MIS Quarterly, ki načenja za našo revijo ter njene bralce zanimivo in pomembno temo o razmerju med relevantnostjo za prakso in znanstveno rigoroznostjo objavljenih del v revijah in zbornikih na temo poslovne informatike ter poslovnih informacijskih sistemov. Razprava, v sicer zelo ugledni in resni znanstveni reviji, izhaja iz ugotovitve, da relevantnost tem, ki se jih lotevajo avtorji v uglednih revijah in zbornikih posvetovanj, za prakso upada in da si praktiki z njimi pogosto nimajo kaj pomagati.

Ta razprava se mi zdi v tem trenutku aktualna iz več zornih kotov. Številni kazalci kažejo na to, da sta Slovenija in njeno gospodarstvo na globalizacijo trga in s tem povezanimi procesi na eni ter prilagajanje informacijski družbi na drugi strani, razmeroma slabo pripravljena (o tem si lahko preberete več v prispevku S. Dekleve v tej številki). Zaostajamo na vseh frontah, država ni opravila tistega dela, ki sodi v njeno pristojnost, to je vzpostavila sistemskih in infrastrukturnih elementov, ki so nujno potrebni za uspešno vključevanje gospodarskih subjektov v globalizacijske tokove, izobraževalni sistemi se s svojimi vsebinami in programi prepočasi prilagajajo potrebam po novih znanjih in tudi javni mediji, skupaj s strokovnimi publikacijami, kamor se prištevamo tudi mi, ne opravljajo svoje prosvetljevalne vloge v zadostni meri in ne osredotočajo svojih sporočil na spreminjanje razmer v konkretnih poslovnih okoljih.

Vrnimo se k ugotovitvam, ki jih navaja MIS Quarterly. Le-ta ugotavlja, da je z raziskovanjem poslovnih informacijskih sistemov nekaj narobe, saj analize kažejo, da praktiki in še posebej vodilni delavci, katerim so ugotovitve teh raziskav pogosto namenjene, le-teh ne berejo oziroma ne jemljejo kot nekaj pomembnega za svoje delo in sprejemanje poslovnih odločitev. Za primerjavo sta omenjeni dve drugi področji, kjer tega problema skorajda ne poznajo. Prvo je področje medicine, kjer je splošno znano, da praktiki, to je splošni pa tudi klinični zdravniki, praviloma zelo skrbno spremljajo najnovejše raziskovalne dosežke, jih štejejo kot pomembne za vsakodnevno prakso ter jih skušajo tudi čimprej upoštevati pri svojem delu. Drugo omenjeno področje pa je pravo, kjer prav tako pravniki na zahtevnejših mestih v praksi redno spremljajo razvoj pravne teorije ter nanj opirajo svoje vsakodnevno delo. Podobna zveza med raziskovanjem in razvojem poslovnih informacijskih sistemov, ki ga praktikom posredujejo znanstvene in strokovne revije, ter direktno uporabo ter znanj pri informatikih in vodilnih delavcih, odgovornih za informatizacijo svojih podjetij, kot kaže po ugotovitvah MQ, ne obstaja ali pa je bistveno šibkejša.

V razpravi se je izoblikovalo več, deloma nasprotujočih stališč, zakaj je prav področje, ki ga skuša pokrivati tudi naša revija, najbolj izpostavljeno temu problemu. Kje so vzroki? Razprava jih je nanizala kar nekaj. Večina drugih disciplin z daljšo tradicijo ima neko čvrsto jedro temeljnih znanj, zakonov in pravil, aksiomov, če hočete, ki služijo kot vodilo pri uvajanju znanstvenih dosežkov v praksi. Na področju poslovne informatike zaenkrat žal še ni tako. Celotno področje se še vedno zelo naglo razvija in še vedno nima neke čvrste temeljne teorije, ki bi služila kot jedro za nadgrajevanje z novimi spoznanji ter raziskovalnimi in razvojnimi dosežki. Vse doslej razvite metode in metodologije so še vedno zelo 'mehke' in ne nudijo praktikom jasnih in konkretnih napotkov za njihovo ravnanje.

Primanjkuje nam 'kumulativne tradicije' v raziskovanju pojavov na področju poslovne informatike, ki bi nam olajšala razvoj splošno uporabnih modelov za prakso. Skoraj na vseh področjih smo priča različnim teoretičnim modelom in pristopom, ki nadomeščajo neki skupen jezik ter nabor splošno uporabnih orodij, neodvisnih od problema, ki se ga lotevamo.

Vprašanja, ki smo jih nanizali, so še kako pomembna tudi v okviru razprav o poslanstvu naše revije. Že iz njenega naslova izhaja, da je naša želja, da bi bila njena vsebina uporabna v praksi. Gre za enega od temeljnih ciljev uredniške politike, ki pa ga ni tako lahko doseči. Večina prispevkov še vedno prihaja iz akademske sfere, ki zaradi želje po znanstveni prepričljivosti pogosto pozablja na uporabnost za prakso. Praktiki pri nas še vedno zelo neradi objavljajo svoja spoznanja in dosežke, saj očitno sodijo, da pisno komuniciranje s strokovno javnostjo ne njim in ne potencialnim bralcem ne prinaša nobenih koristi.

Pa smo spet pri globalizaciji. Če bomo hoteli preživeti v vedno bolj kompetitivnem okolju, v katerega vstopamo z veliko hitrostjo, potem bomo morali začeti svoje delo in znanje promovirati in to na način, ki bo v praksi zbudil interes potencialnih uporabnikov, kupcev, strank, strokovne javnosti itd. Če tega ne bomo storili mi, bo to storil nekdo drug namesto nas,

Mirko Vintar
Glavni in odgovorni urednik

UVODNIK

STROKOVNE RAZPRAVE

POROČILA

DOGODKI IN ODMEVI

OBVESTILA

KOLEDAR PRIREDITEV

To revijo sofinancira Ministrstvo za znanost in tehnologijo Republike Slovenije

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

INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET

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

http://www.drustvo-informatika.si

Za predloge in pripombe v zvezi z vsebino se priporočamo na naslov:

http://www.drustvo-informatika.si/posta

INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET ■ INTERNET

Navodila avtorjem

Prispevke pošiljajte v predpisani obliki na naslov Slovensko društvo Informatika, 1000 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. Na koncu dodajte kratek življenjepis.

Pošljite ga na disketi in odtisnjenega na papirju. Napisan naj bo v urejevalniku **WORD**. Na disketi označite ime datoteke. Datoteko imenujte s svojim priimkom, npr. Novak. doc ali Novak.txt.

Slike, grafikoni, organizacijske sheme itd. naj imajo belo podlago. Upoštevajte, da tiskamo v črno-beli tehniki s folije (ne s filma). Priložite jih na posebni datoteki.

Pišite v razmaku ene vrstice, 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, 1000 Ljubljana, Ulica Gubčeve brigade 120, tel.: 1271-579, elektronska pošta Katarina.Puc@drustvo-informatika.si.

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

GLOBALIZACIJA: OVIRE IN PREDNOSTI

Saša Dekleva

Povzetek

Razprava vsebuje dva glavna dela. V prvem odkriva priložnosti in predvsem ovire za vključitev Slovenije v tokove globalnega gospodarstva, ki jih lahko rešujemo le na nivoju cele države in v sodelovanju z mednarodnimi organizacijami. Drugi del opisuje ovire na nivoju posameznih organizacij. Pospešeni razvoj informacijske tehnologije omogoča nove organizacijske strukture in nas postavlja v trenutek, v katerem se lomijo poslovne strategije. Zato ugotavljamo, da sta učenje in raziskovanje novih gospodarskih okoliščin najtežje premagljivi oviri. Razprava vsebuje tudi primerjalno analizo pripravljenosti Slovenije na globalizacijo gospodarstva in navaja, katere informacijske tehnologije olajšujejo poslovanje globalnih organizacij.

Summary

This paper contains two main parts. It first presents those opportunities and particularly constraints for Slovenian integration into global economy that can be addressed only at the national level and in cooperation with the international institutions. Paper then presents the constraints internal to the individual companies. Excellerated evolution of information technology facilitates the implementation of new organizational structures and causes shifts in business strategies. Required eduction and research of new economic conditions are the most difficult hurdles. The paper also includes a comparative analysis of Slovenian readiness for global economy and identifies information technologies needed to support the companies operating globally.

■■■

S tem, da pomagamo digitalizirati poslovanje, globalizirati trgovino in razvneti kreativnost, vzpostavljamo novo obdobje gospodarskih priložnosti in napredka.
Al Gore

UVOD

To, da opazujem dogajanja v domovini od daleč - z druge strani luže - ima svojo dobro, a tudi slabo stran. Dobra je v tem, da mi omogoča videti celotno sliko brez vplivov podrobnosti in brez lokalnih stališč, pogosto čustveno obarvanih. Slaba stran pa je v tem, da dogajanj v Sloveniji ne poznam dovolj dobro in tako tvegam, da bom ponavljal že znano. Kljub temu zadržku pa verjamem, da je moje sporočilo zelo pomembno in se nadejam, da ne bo ostalo prezrto.

Globalizacija kot dolgoletni gospodarski trend ni nekaj novega. Nedavni tehnološki dosežki na področju računalništva in komunikacij pa ponujajo povsem nove priložnosti. Eksplozivna rast poslovne rabe Interneta daje globalizaciji posebno velik pospešek. Mnogi zanesenjaško govorijo o izničenju razdalj, o eni od najpomembnejših transformacij vseh časov [1], o spremembi gospodarskih in socialnih modelov, o diskontinuiteti poslovne strategije itd. Odvisno od izkušenj in interesov razpravljalcev imenujejo današnji čas in novi svet, v katerega vstopamo, globalizacija, omrežna ekonomija, kibernetski prostor in podobno, nove organizacijske oblike pa transnacionalne, globalne, ali virtualne organizacije. Za vsa ta razmišljanja je značilno, da povezujejo socialne, politične in gospodarske spremembe z uporabo novih tehnologij. Na to predpostavko se bomo oprli tudi v tem sestavku.

V nadaljevanju najprej preletimo obete gospodarske globalizacije. Za tem se malo pomudimo z opažanji političnih ekonomistov, ki se še vedno sprašujejo, ali je globalizacija v prid človeštvu in kateri del človeštva lahko ogrozi. Temu sledi podroben opis iniciativ, ki jih je v zadnjih letih sprejela ameriška vlada, s kratkim povzetkom najpomembnejšega dokumenta, ki ga je predsednik Clinton objavil sredi leta 1997. Temu so sledile bilateralne in druge mednarodne pobude, ki so tudi na kratko povzete v tem članku. Ovire pri globalizaciji gospodarstva, opisane v naslednjem poglavju, sledijo klasifikaciji Organizacije za gospodarsko sodelovanje in razvoj (Organization for Economic Cooperation and Development - OECD), ki je v mednarodnem merilu najaktivnejša pri določanju pravil igre omrežnega gospodarstva, a je vanjo

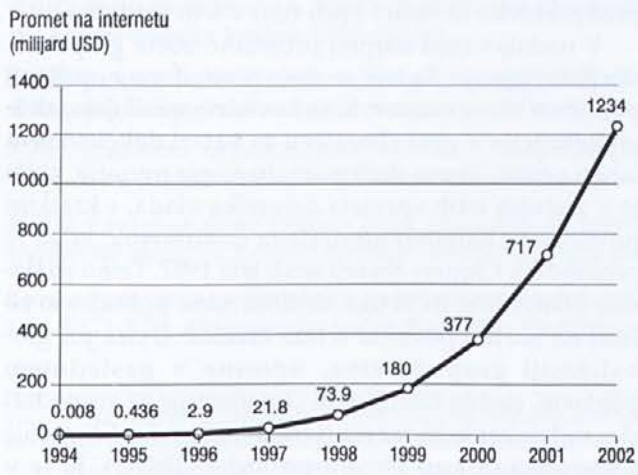
včlanjenih le 29 držav in Slovenije ni med njimi. Šesto poglavje najprej povzema nedavno analizo pripravljenosti članic EU za vključitev v globalno gospodarstvo, po tem pa skuša po istih kriterijih primerjati Slovenijo z izbranimi državami po svetu. Za primerjavo so večinoma izbrane države, ki so s Slovenijo primerljive po številu prebivalcev. Temu delu sledi kratek povzetek pripravljenosti Slovenije kot države na globalno gospodarstvo.

Poglavje osem je prvo od poglavij, posvečenih obravnavi ovir na nivoju posameznih organizacij. Opisuje posebej pomembne pogoje za vključitev v globalizacijo, predvsem učenje in širjenje znanja. Naslednje poglavje govori o potrebni informacijski tehnologiji. Na kratko opisuje primerne tehnologije in namene njihove uporabe. Referat zaključuje nekaj kratkih priporočil vodilnim kadrom.

2. PRILOŽNOSTI - ALI BOLJE - OBETI

Vsaj na površini ni težko zaznati priložnosti, ki jih prinaša globalizacija. Zdi se, da ima mali podjetnik prvič v zgodovini priložnost ponuditi svoje blago ali storitve po vsem svetu. Seveda velja tudi obratno - vsaka organizacija lahko nabavlja pri najugodnejšem ponudniku na svetu.

Toda spremembe so mnogo zapletenejše in presegajo okvir blagovne trgovine. Vemo, na primer, da največja ameriška knjižnica, The Library of Congress v Washingtonu, digitalizira na milijone knjig, fotografij, grafik, risb, rokopisov, redkih knjig, zemljevidov, zvočnih zapisov in filmov, tako kot knjižnice mnogih drugih držav in tudi naša Narodna in univerzitetna knjižnica. Te digitalizirane informacije so zaenkrat dosegljive brezplačno po celem svetu. Ali torej še velja, da "znanje" predstavlja moč, če je dostopno vsakomur? [2] Ali je zaradi enostavnega pristopa do potrebnih informacij naposled mogoče uresničiti samoupravljano, socialistično družbo? [3]. Že kratko razmišljanje o priložnostih, ki jih prinaša globalizacija, nas privede do križpotij brez potokazov.



Slika 1. Eksplozija poslovne rabe Interneta
Vir: ActivMedia, www.activmedia.com

Hitro spoznamo, da so priložnosti globalizacije tudi same vsaj načelno brez fizičnih meja. To pomeni, da jih bodo nekatere organizacije in celo države po vsej priliki izkoristile bolje kot druge. Ali bodo revne in zaostale države zaostale še bolj? Kakšna je cena zamude priložnosti? Kako naj se država organizira, da lahko kar najbolje izkoristi priložnosti? Lahka vprašanja, a zelo težka pot do odgovorov. Kot vedno seveda velja pri uvajanju novih tehnologij, da samo razvoj tehnoloških zmogljivosti, čeprav predpogoj, še daleč ne jamči uspeha. Družbene spremembe, potrebne za izrabo priložnosti, so mnogo, mnogo globlje.

Drugi zaključek, h kateremu vodim bralce, je ta, da je poslovno okolje za "omrežno gospodarstvo" še povsem nepripravljeno. Obenem pa vidimo, da ta neurejenost ne odvrača naprednih družb in malih ter velikih organizacij, da bi ne le plašno preizkušale nove priložnosti, ampak jih z veliko naglico in vnemo izkoriščale. Toda pravila nove igre določajo ravno te dni, zato za priključitev viharnim tokom globalizacije morda še ni prepozno. Slika 1 zgovorno kaže, zakaj se mnogi tako zanimajo za priključitev na drveči vlak. Najnovejše napovedi firme Forrester Research Inc. so, da se bo promet preko Interneta med poslovnimi organizacijami povečal od 48 milijard USD leta 1998 na 1,5 bilijard USD leta 2003, medtem ko bo prodaja potrošnikom poskočila v istem obdobju od 3,9 milijard USD na 108 milijard. [4]

3. POGLED S STRANI: POLITIČNA EKONOMIJA GLOBALIZACIJE

Politični ekonomisti soglašajo, da je globalizacija v tem času dominantno politično, socialno in gospodarsko vprašanje. Po njihovem se globalizacija nanaša na proces, v katerem je kapitalizem v vse večji meri zasnovan na mednarodni osnovi in to ne le na trgovanju s proizvodi in storitvami, ampak - še pomembneje - na pretoku kapitala in trgovanju z valutami in finančnimi instrumenti. Vodilni akterji globalizacije, to je nekaj sto največjih svetovnih privatnih organizacij, imajo v zadnjem desetletju proizvodnjo in trženje vse bolj povezano preko državnih mej.

Drugi opazovalci pa opozarjajo, da obsega globalizacije ne smemo precenjevati. Kljub trendu k vzpostavljanju velesilnih "brezdržavnih", transnacionalnih korporacij z investitorji, upravljalci in trgi po celem svetu, obstaja tudi opazno in rastoče rivalstvo med vodilnimi kapitalističnimi državami in regijami. Po mnenju teh se harmonično, integrirano svetovno tržišče ne bo razvilo prav kmalu, če se sploh kdaj bo.

Pravijo, da je to, kar pogosto imenujemo globalizacija, v resnici le vrsta neoliberalnih ekonomskih politik, ki smatrajo maksimiranje profita in prostega pretoka materiala in kapitala z minimalno vladno regulativo za osnovna načela učinkovitega in uspešnega gospodarstva.

V političnih krogih živahno diskutirajo, kako razvit je proces globalizacije, kam bo pripeljal in s kakšnimi političnimi posledicami. Večina kritikov globalizacije trdi, da ta favorizira velike korporacije in bogate ter krni možnost delavcev, zelenih, revnih in pravzaprav vseh drugih vplivati na svojo usodo. Pravijo, da spremlja globalizacijo protidemokratična usmeritev, ker prisiljuje državne uprave k podpiranju globalnih pretokov kapitala, sicer jim pretijo težave v gospodarstvu. Z drugo besedo, družbene odločitve so v vse večji meri odvisne od trga in vse manj od volje večine. Tretji spet trdijo, da je beseda globalizacija varljiva, da gre v resnici za razvoj kapitalizma in je globalizacija v zgodovinskem smislu precenjena. Ta vrsta razmišljanja vodi k razvrednotenju mistične "neizogibnosti", ki spremlja razprave o globalizaciji, posebej trditve, da niti države niti organizirani delavci ne morejo nasprotovati moči kapitala. Tisti, ki podpirajo globalizacijo, se pravzaprav s temi opažanji strinjajo, ob tem pa sodijo, da ni nobene druge poti ekonomskega razvoja in bodo previdne in gospodarstvu naklonjene državne intervencije skupaj s tržnimi zakonitostmi s časom ublažile trenutne tegobe [5]. Tako stališče drastično odstopa od odločnega klica tehnologov: "V omrežnem gospodarstvu nimajo hermetično zaprti sistemi nobene bodočnosti" [6].

Pomembnosti teh in nanje vezanih drugih vprašanj ni mogoče dovolj poudariti. Ali res ni druge poti kot plavati s tokom napredka, saj vse drugo vodi v gospodarsko pogubo? In če je tako, se je treba tega cilja bati ali pa si je treba na vso moč prizadevati, da ga čimprej dosežemo? Do kakšne mere lahko država, posebej majhna, vpliva na globalni razvoj in kako?

Poskus temeljite obravnave teh vprašanj bi nas potisnil daleč preko okvira tega sestavka. Zato predlagam, da se zaenkrat postavimo na stališče, da je trud za vključitev v globalno gospodarstvo v interesu družbe in večine njenih prebivalcev. Ob tem pa se zavedamo vročih razprav, kjer nekateri sodijo, da prinaša globalizacija že zaradi izničenja razdalj prvič priložnost za vključevanje v svetovne gospodarske tokove prav vsem. Drugi pa trdijo, da bodo nove tehnologije še močno povečale prepad med razvitimi, bogatimi in nerazvitimi, revnimi področji sveta. Ne smemo pozabiti, da imajo na primer v Afriki poprečno le 2,15 telefonski liniji na 100 prebivalcev (v Somaliji le 0,15; v Čadu 0,12; v Demokratični republiki Kongo pa le 0,04), v Evropi pa okoli 36 (v Sloveniji tudi 36; v Veliki Britaniji 54; v Nemčiji in Franciji 57; v Švici pa 66) [7]. Ali bo razvoj pustil države, ki ne izpolnjujejo pogojev, potrebnih za vključitev v vse bolj globalne in virtualne organizacije, ob strani? Se bo prepad med bogatimi in revnimi tako še povečal?

4. IZHODIŠČA ZA UREJANJE GLOBALNEGA ELEKTRONSKEGA POSLOVANJA

Razmišljanja o ovirah in prednostih globalizacije ni mogoče omejiti le na nivo posamezne organizacije. Prvi pogoj za njeno vključitev v svetovne gospodarske tokove je izpolnitev potrebnih pogojev na nivoju države. To zveni v protislovju s tezo, da postajajo mednarodne korporacije "brezdržavne", a le na videz. Razpredle bodo namreč mreže le preko tistih področij sveta, ki bodo pripravljena za tako sodelovanje. Torej se velja najprej posvetiti razpravi o ovirah in pogojih, ki jih lahko rešujemo le na nivoju države ali mednarodnih teles, potem pa lahko govorimo o tem, kakšne priložnosti in ovire prinaša globalizacija na nivoju posameznih organizacij.

Uvodoma velja omeniti, da smo šele na začetku ne le reševanja kompleksnih problemov, ampak celo na začetku njihovega zaznavanja. Kot primer lahko navedemo, da je predsednik Clinton nedavno naročil Nacionalnemu gospodarskemu svetu (National Economic Council), da v sodelovanju z raznimi agencijami analizira ekonomski vpliv Interneta in elektronskega poslovanja na ZDA in na svet v celoti in da naj pri tem razmišlja o novih indikatorjih za informacijsko gospodarstvo, o novih načinih zbiranja podatkov in novih raziskavah, ki naj jih izvajajo organizacije javnega in privatnega sektorja. S tem v zvezi je potekalo posvetovanje 25. in 26. maja 1999 na Ministrstvu za trgovino (Department of Commerce). [8]

ZDA so pospešeno in sistematično stopile na pot, ki vodi v globalizacijo, zasnovano na elektronskem poslovanju, 1. julija 1997, ko je predsednik Clinton objavil *Izhodišča globalnega elektronskega poslovanja* [9] (v nadaljevanju *Izhodišča*). Ta dokument, ki je definiral načela in odprta vprašanja, je služil kot izhodišče ne le za razprave in razvoj globalnega elektronskega poslovanja v ZDA, pač pa širom sveta in v organizacijah kot so Svetovna trgovinska organizacija (World Trade Organization - WTO), OECD, Evropska unija (European Union - EU) itd.

Pet načel, opisanih v tem dokumentu, naj bi služilo kot vodilo za vlogo vlade pri razvoju elektronskega poslovanja. Ta načela so:

1. **Pobudo naj ima privatni sektor.** Elektronsko poslovanje naj se razvije v areni tržnih sil in ne kot panoga, omejena s predpisi. Celo tam, kjer so državni ukrepi potrebni, naj vlade kjer je le mogoče spodbujajo svoboden razvoj elektronskega poslovanja in pobudo privatnega sektorja.

2. **Vlade naj ne sprejemajo neprimernih omejitev elektronskega poslovanja.** V splošnem naj bi poslovne stranke sklepale legitimna soglasja o prodaji in nakupu izdelkov in storitev preko Interneta z minimalnim sodelovanjem ali interveniranjem vlade. Vlade naj se vzdržijo sprejemanja novih in nepotrebnih zakonov, birokratskih postopkov ali novih taks in carinjenja poslovnih aktivnosti, ki se odvijajo preko Interneta.
3. **Kjer je vladno posredovanje potrebno, naj bo njegov namen podpreti in uveljaviti pričakovane, minimalne, konsistentne in enostavne pravne pogoje za poslovanje.** Vloga vlade, kjer je njeno posredovanje potrebno, naj bi bila v zagotovitvi svobodne konkurence, varovanju intelektualne lastnine in zasebnosti, preprečevanju prevar, pospeševanju jasnosti, v lajšanju reševanja sporov in ne v regulativi.
4. **Vlade naj spoznajo posebnosti Interneta.** Dokument pripisuje eksplozivni uspeh Interneta vsaj delno njegovi decentralizirani naravi in samoupravi in opozarja, da regulative, sprejete na področjih telekomunikacij, radija in televizije niso nujno primerne tudi za Internet. Zato naj bi obstoječe zakone prilagodili ali odpravili.
5. **Elektronsko poslovanje preko Interneta je treba pospeševati na globalni osnovi.** Internet je globalno tržišče. Pravna osnova poslovanja bi morala biti konsistentna in napovedljiva ne glede na sodno oblast, kjer je lociran določeni kupec ali prodajalec.

Gornje principe naj bi vodilo devet priporočil, tudi opisanih v *Izhodiščih*. Ta priporočila zadevajo carine in davke, elektronske plačilne sisteme, poenoteno poslovno zakonodajo elektronskega poslovanja, varovanje intelektualne lastnine, varovanje zasebnosti, varnost, telekomunikacijsko infrastrukturo ter informacijsko tehnologijo, primernost informacijske vsebine in tehnične standarde.

Novembra 1998 je Vladna delovna skupina za elektronsko poslovanje objavila *Prvo letno poročilo* [10], ki opisuje dogajanja po objavi *Izhodišč* in odkriva pet novo nastalih vprašanj, katerih rešitev naj bi omogočila uresničitev predsednikove inicijative do 1. januarja leta 2000.[1] Ta vprašanja zaslužijo po mnenju Vladne delovne skupine vso pozornost, zato so jih dodali k delovnemu načrtu in jih bodo letos reševali. To so:

1. **Zagotovitev primerne prepustnosti in dostopa.** Načela, ki jih je objavil podpredsednik Gore leta 1994, spodbujajo privatne investicije, pospeševanje konkurence, vzpostavljanje prilagodljivih zakonodajnih temeljev, odprt pristop do omrežja in zagotovitev univerzalnega dostopa do omrežja. Ta načela so vodila razvoj tako v ZDA kot po svetu. *Zakon o razvoju nove generacije Interneta* [11] iz leta 1998 nadaljuje pozitivno vlogo države pri podpiranju raziskav za povečanje kapacitete in uporabnosti Interneta.
2. **Zaščita potrošnikov.** Potrošniki na Internetu morajo imeti zaupanje, da bodo izdelki, storitve in digitalizirane informacije, ki jih ponujajo na spletu, verodostojno predstavljeni, da bodo potrošniki prejeli, kar so kupili ali pa bodo lahko reklamirali. Razumljivo je, da postaja tudi v globalni areni zaščita potrošnikov vse bolj pomembna. Zato se mora globalna družba spoprijeti z zapletenimi vprašanji, kot so izbira veljavnega prava in pravosodja, kako odločati o tem, kje je bila virtualna transakcija izvedena in kateri zakoni za zaščito potrošnika so veljavni.
3. **Internet in države v razvoju.** Internet je lahko močan vzvod ekonomskega razvoja, širjenja demokracije in pospeševanja mednarodnega komuniciranja in razumevanja. Lahko pa se zgodi, da bo informacijska revolucija obšla množice s sveta v razvoju.
4. **Razumevanje digitalnega gospodarstva.** V letu 1998 je vrsta poročil in srečanj osvetlila podobo o gospodarskem vplivu Interneta in obstoječega elektronskega poslovanja v ZDA.[2] *Prvo letno poročilo* navaja, da je ekonomski in socialni vpliv elektronskega poslovanja in informacijske tehnologije kompleksen, razprostranjen in se bo verjetno v prihodnosti še povečal. Avtorji priznavajo, da celotnega ekonomskega in socialnega vpliva še ne poznamo. Vladna delovna skupina je vzpostavila Delovno skupino za digitalno ekonomijo, ki jo vodi Nacionalni gospodarski odbor, sestavljajo pa predstavniki iz Ministrstva za trgovino (Department of Commerce), Ministrstva za finance (Department of Treasury), Ministrstva za delo (Department of Labor), Nacionalnega raziskovalnega sveta (National Science Foundation), Urada Bele hiše za znanstveno in tehnološko politiko (White House Office of Science and Technology Policy) in Sveta gospodarskih svetovalcev (Council of Economic Advisers). Tu

---

[1] *Težko je spregledati naglico in vnemo, s katero vlada ZDA odpravlja pregrade za razcvet elektronskega poslovanja.*

[2] *Posebno pomembna poročila so:*
"The Emerging Digital Economy", Online. Secretariat for Electronic Commerce, U.S. Department of Commerce, Nov. 1998. Dosegljivo na: **www.ecommerce.gov/emerging.htm.**
"Economic and Social Significance of Information Technologies", Online. National Science Foundation, Feb. 1998. Dosegljivo na: **www.nsf.gov/sbe/srs/seind98/frames.htm**, *kot poglavje v* "Science & Engineering Indicators 1998", *Online. Dosegljivo na:* **www.nsf.gov/sbe/srs/seind98/frames.htm.** *6. april 1999*
"A Borderless World - Realising the Potential for Global Electronic Commerce", Online. OECD, april 1999. Dosegljivo na: **www.oecd.org//dsti/sti/it/ec/news/ottawa.htm**. *7. marec 1999.*

vidimo še en dokaz, da vlada ZDA pripisuje globalizaciji in digitalni ekonomiji izredno velik pomen in se hitro organizira, da bi priložnost kar najbolje izkoristila.

5. **Drobno gospodarstvo in Internet.** Majhne firme imajo z Internetom globalen doseg, tako kot so ga do sedaj imele le velike korporacije. Kljub temu pa mnoge majhne organizacije ne izkoriščajo prednosti, ki jim jih nudi Internet. Ne razumejo potencialnih koristi, ne znajo razviti elektronskega poslovanja in ne vedo, kako naj se spoprimejo s kompliciranimi pravili, ki vplivajo na elektronsko poslovanje. Poleg tega mnogi nimajo tehničnih kadrov, ki bi jim lahko pomagali uresničiti poslovni model elektronskega poslovanja. Mnogim takim malim podjetjem sedaj pomagajo programi, ki jih sponzorirata vlada in Ministrstvo za trgovino in Ministrstvo za drobno gospodarstvo (Small Business Administration).

Kot rečeno, je imelo poročilo *Izhodišča globalnega elektronskega poslovanja* velik vpliv tako v ZDA kot v svetu. Kongres je uzakonil štiri pomembne pravne cilje: *Zakon o oprostitvi davkov na Internetu, Digitalni tisočletni zakon o založniških pravicah, Zakon o odpravljanju papirne dokumentacije v vladi* in *Zakon o varovanju zasebnosti otrok na spletu.*

V mednarodnem okviru so tudi sprejeli vrsto sporazumov, ki bolj ali manj podpirajo načela iz *Izhodišč.* WTO je na srečanju maja 1998, ki so se ga udeležili ministri iz 132 včlanjenih držav, dosegla soglasje med članicami o nadaljevanju prakse o oprostitvi carin za elektronsko poslovanje. OECD in razne industrijske grupacije so oktobra 1998 na ministrskem zasedanju o Globalnem elektronskem poslovanju (znanem kot Ottawška konferenca) izdale skupno deklaracijo s katero podpirajo davčne principe predstavljene v *Izhodiščih* in nasprotujejo diskriminatornim obdavčitvam Interneta in elektronskega poslovanja. Na Ottawški konferenci so sklenili priporočiti vladam, naj odstranijo ovire, vezane na uporabo papirnih dokumentov, in naj zagotovijo, da bodo privatne iniciative izbrale tehnologijo in poslovne metode za overjanje transakcij. V deklaraciji so tudi opozorili na pomembnost uvajanja politik, ki so tehnološko nevtralne, ki ne diskriminirajo in temeljijo na tržnih pristopih k overjanju.

Baselski odbor za bančni nadzor je s podporo vodilnih centralnih bank izdal marca 1998 poročilo, v katerem podpira sisteme elektronskih plačil brez regulative, kot je opisano v *Izhodiščih.* Globalno posvetovanje o standardih v Brusselu oktobra 1997 je tudi podprlo stališče, naj privatni sektor vodi razvoj Internetovih tehničnih standardov. Ameriški pristop k elektronskemu poslovanju je podprla vrsta drugih mednarodnih poslovnih skupin, kot so Transatlantski poslovni dialog (Transatlantic Business Dialogue), Poslovni odbor ZDA - Japonska (U.S./Japan Business Council), Mednarodna gospodarska zbornica (International Chamber of Commerce), Odbor za globalno informacijsko infrastrukturo (Global Information Infrastructure Council) ter Svetovno združenje za informacijsko tehnologijo in storitve (World Information Technology and Services Alliance).

Poleg tega so ZDA sprejele vrsto bilateralnih sporazumov, s katerimi so dosegle pomembne cilje pri elektronskem poslovanju. Maja 1998 sta predsednik Clinton in japonski ministrski predsednik Hashimoto v imenu svojih vlad izjavila, da državi ne bosta regulirali elektronskega poslovanja in bosta sodelovali v mednarodnih iniciativah pri odpravljanju ovir za elektronsko poslovanje. Junija 1998 sta podpredsednik Gore in francoski ministrski predsednik Jospin podobno podprla princip odprtega pristopa do informacij in prostega toka vsebinsko in jezikovno raznovrstne vsebine. Septembra 1998 sta predsednik Clinton in Taioseach Ahern iz Irske podpisala prvi medvladni sporazum, ki vsebuje digitalne podpise. Decembra pa sta predsednik Clinton in predsednik EU Santer izjavila, da bosta njuni vladi sledili principom, podobnim onim iz *Izhodišč* in nadaljevali z razpravami o elektronskem poslovanju, pa tudi z novoustanovljenim Transatlantskim gospodarskim partnerstvom (Transatlantic Economic Partnership).

ZDA so medtem napredovale pri izvajanju predsednikovih priporočil za privatno iniciativo in elektronsko poslovanje brez regulative. Julija 1998 je skupina firm, ki so med glavnimi uporabniki internetnih komunikacij, sklenila uresničiti varstvo zasebnosti skladno s predsednikovimi načeli v prvem kvartalu leta 1999 (pri tem ne le kasnijo, ampak so v hudem nesoglasju z EU). Za dosego tega cilja so ustanovili neodvisno nadzorno organizacijo. Vlada ZDA je podobno ustanovila novo privatno, neprofitno in uporabniško usmerjeno organizacijo, ki je prevzela tehnično upravljanje sistema za imena domen na Internetu. Razne skupine iz privatnega sektorja so dosegle precejšen napredek pri razvoju filtrirnih in rangirnih sistemov, ki naj bi otrokom onemogočali dostop do neprimernih naslovov in vsebine urejali v kategorije. Podobno so dosegli napredek pri pripravi kakovostnih vsebin za mladino.

5. OVIRE PRI GLOBALIZACIJI DIGITALNEGA GOSPODARSTVA

Plan akcije, ki ga navaja poročilo ministrske konference OECD o elektronskem poslovanju, [12] razvršča potrebne aktivnosti v štiri glavne kategorije:

1. Graditi zaupanje pri uporabnikih in potrošnikih
2. Postaviti osnovna pravila za digitalno tržišče

3. Izboljšati informacijsko infrastrukturo za elektronsko poslovanje
4. Optimizirati koristi od elektronskega poslovanja

Bralcem tega plana postane jasno, da so akcije namenjene odpravljanju ovir, zato lahko ta razvrstitev pomaga tudi pri razmišljanju o ovirah za globalizacijo gospodarstva. Te štiri skupine ovir lahko dalje delimo na podskupine. V prvo skupino - zaupanje uporabnikov in potrošnikov - sodijo naslednje zadeve:

1.1 Zaščita zasebnosti in osebnih podatkov
1.2 Varna infrastruktura in tehnologija, overjanje in preverjanje
1.3 Zaščita potrošnikov

Druga kategorija - osnovna pravila digitalnega tržišča - vključuje naslednje zadeve:

2.1 Poslovno pravo
2.2 Davki
2.3 Finančne zadeve, elektronska plačilna sredstva in transport blaga
2.4 Poslovna pravila in dostop do tržišča
2.5 Intelektualna lastnina

V tretjo kategorijo - informacijska infrastruktura - lahko uvrstimo:

3.1 Pristop do infrastrukture in njena uporaba
3.2 Upravljanje Interneta in sistema imen domen
3.3 Tehnične zadeve, protokol in standardi

V četrto skupino - optimiranje koristi - pa lahko uvrstimo naslednje zadeve:

4.1 Ekonomski in socialni vplivi
4.2 Poslovne strukture in aktivnosti
4.3 Drobno gospodarstvo in srednje velike organizacije
4.4 Razvijanje sposobnosti, učenje
4.5 Globalna zagotovitev sodelovanja

Podrobna razprava o vseh teh zadevah in ovirah bi spet presegla okvir tega prispevka. Zainteresirani bralci lahko najdejo posameznosti v referencah, ki so dosegljive na Intenetu.

6. EVROPA ZAOSTAJA

Analitiki *Forbes*a [13] ocenjujejo, da je izven Severne Amerike največ potenciala za investicije v razvoj Interneta v Evropi, a obenem ugotavljajo, da Evropa znatno zaostaja in da so razlike v zaostanku znotraj Evrope zelo velike. Evropa je razcepljena na gospodarsko zreli in tehnično sposobni sever in na gospodarsko ter tehnično zaostali jug. Do teh zaključkov so prišli na osnovi kvantitativnih podatkov, kot so:

- razširjenost tehnologije (uporaba računalnikov in Interneta, telefonske linije in kakovost omrežja)
- gospodarsko stanje (BDP na prebivalca, letni razpoložljivi dohodek, obrestna mera, stopnja nezaposlenosti)
- poslovno okolje (davčna stopnja, delovna sila, zakonodaja)

Poleg teh so upoštevali še druge faktorje, ki bodo po njihovem vplivali na razvoj Interneta in elektronskega poslovanja, kot so stroški priključitve in raba kreditnih kartic. Tem so dodali tudi kakovostne kriterije, kot so vladne politike o informacijski tehnologiji, razpoložljivost kapitala za novo nastala podjetja, uporaba Interneta v šolskem sistemu, konkurenca na trgu komunikacij, članstvo v evropski monetarni skupnosti in nacionalne posebnosti, kot npr. Minitel v Franciji.

Kako bi se odrezala Slovenija, če bi jo vključili v analizo in poročilo? Na osnovi podatkov [7, 14], ki so resda nekoliko stari, a po vsej priliki še vedno uporabni, lahko zaključimo naslednje:

- števili računalnikov in internetnih strežnikov sta nizki v primerjavi z najrazvitejšimi državami Evrope
- števili telefonskih linij in prenosnih telefonov sta tudi nizki
- cena telefonskega klica iz Slovenije v ZDA je bila leta 1996 okoli dvakrat dražja kot v razvitih državah Evrope
- števili televizorjev in kabelskih priključkov sta primerljivi z najrazvitejšimi
- kupna moč Slovencev raste, a seveda še zaostaja za najrazvitejšimi državami
- po izobraženosti se Slovenci kosajo z najrazvitejšimi
- blagovna izmenjava s tujino in njena rast kažeta na visoko stopnjo povezanosti Slovenije s svetom
- Slovenija močno zaostaja pri pretoku kapitala in bruto tujih investicijah, kar je pomembno merilo za globalno gospodarsko povezanost
- po številu znanstvenikov in raziskovalcev je Slovenija prav blizu vrha med najrazvitejšimi, po deležu visoke tehnologije v industrijskem izvozu pa ne[3].

7. TOREJ?

Vsi ti in drugi indikatorji vodijo k zaključku, da se Slovenija uspešno transformira in koraka po poti vključevanja v svetovno gospodarstvo, da pa pri tem še zaostaja za najrazvitejšemi državami Evrope. Kot smo videli v opisu dogajanj po svetu, se ZDA, Evropska unija in druge države predvsem v okviru OECD zelo hitro organizirajo za izrabo prednosti globalnega omrežnega gospodarstva. Pomembne iniciative imajo roke izpolnitve še v tem ali v prihodnjem letu. Čas na Internetu posebno hitro teče. Kaže, da je Slovenija po tehnični plati in po tehnološkem znanju dobro pripravljena. Ker igra državna uprava

[3] *Slikovni prikazi, ki ilustrirajo ta opažanja, so dosegljivi online na* **http://accountancy.depaul.edu/sdekleva/Priloga2.ppt.**

pomembno vlogo pri globalizaciji, se mora kar najbolj podvizati z ustvarjanjem potrebnih pogojev. Vloga države je pomembna na mnogih področjih, kot na primer pri izobraževanju gospodarstvenikov, posebno iz drobnega gospodarstva, pri prilagajanju gospodarske zakonodaje, financiranju raziskovalnih projektov, zagotavljanju odprtega pristopa do omrežja, zaščiti potrošnikov in intelektualne lastnine, sprejemanju standardov itd.

8. OVIRE NA NIVOJU POSAMEZNIH ORGANIZACIJ

Raziskovalci s področja globalizacije in nanjo vezanih preizkušenj so se zbrali novembra 1998 pod okriljem inštituta Cato pri Univerzi v severni Karolini in identificirali posebej ključne in pomembne zadeve [15]. Uvodoma so ugotovili, da se svet spreminja hitreje kot miselnost direktorjev. Tako pridemo do prve in izredno težke ovire. V enem od referatov s tega srečanja beremo, da tvegajo direktorji, ki se učijo počasi, da bodo izločeni in bodo propadli zaradi vedno zahtevnejšega in neodpustljivega konkurenčnega okolja. Da bi bile stvari še bolj zapletene, tudi tempo raziskav globalne konkurence zaostaja za hitrostjo spreminjanja poslovnega sveta. Tako lahko postrežemo s prvim nasvetom: menedžerji in firme se morajo učiti o spreminjanju globalne konkurence in o vplivih teh sprememb na poslovanje organizacij in celo na njihovo preživetje.

Eno od najpomembnejših vprašanj je, kdo pravzaprav so konkurenti? Kot primer lahko pomislimo na ustaljeno gospodarsko skupino, osredotočeno na domače in stabilno tržišče, na katero nenadno prodre tekmec z druge strani sveta. Pri tem ima nova firma lahko še dodatne prednosti, saj ni obremenjena z neamortiziranimi nepremičninami in obstoječimi poslovnimi aranžmaji. Izbere si lahko nove poslovne partnerje in si privošči nastop z nižjo ceno, ker lahko dlje čaka na ustvaritev dobička.

Naslednja pomembna zadeva je "organizacija kot komuna", kjer sodelovanje med navdušenimi in predanimi posamezniki razvname celotno skupino in spodbudi njeno bogastvo intelekta in znanja. Raba besede "posamezniki" pade v oči in sugerira delo v virtualnih ali kibernetskih skupinah in napoveduje, da bo klasično hierarhično organizacijsko strukturo zamenjalo delo v projektnih skupinah. Člani takih začasnih skupin složno prevzamejo odgovornosti za rezultate skupnega dela in igrajo zdaj vlogo vodij, zdaj vlogo vodenih.

Udeleženci posvetovanja so soglašali, da je pridobivanje znanja v organizaciji tudi ena od najpomembnejših zadev, vezana na vprašanji: Ali se firme učijo? Kako? S tem v zvezi domnevajo, da pestrost delovnih skupin in njihova gibljivost pospešujeta učenje. Ugotovili so tudi, da "mora biti v obdobjih dinamičnih sprememb, ki povzročajo strateške premike, tudi učenje nelinearno" [16]. Globalizacija je ena od takih sprememb, zato bi se morali v tem času še bolj posvetiti učenju. Ena od zadev v tem okviru je domneva, da postanejo v času takih tektonskih prelomov prejšnje temeljne sposobnosti organizacije nepomembne, zato jih morajo biti organizacije sposobne zamenjati z novimi. Eden od načinov učenja organizacij je prav sodelovanje v kooperaciji, kar nas spet privede h globalizaciji.

Med najpomembnejšimi vprašanji je tudi, kako postanejo menedžerji globalni? S tem v zvezi ugotavljajo, da so direktorji, ki govorijo več jezikov in se brez zadreg premikajo iz enega kontinenta na drugega, zelo redki in približno trikrat bolje plačani od lokalnih kadrov. Zato predlagajo, naj več menedžerjev s pomočjo tehnologije koordinira svoje aktivnosti in tako deluje globalno. Te tehnologije pa so tako nove, da premalo vemo, kaj lahko z njimi dosežemo in še manj, kakšne probleme lahko povzročijo.

9. O INFORMACIJSKI TEHNOLOGIJI (KONČNO!)

Po pričakovanju so na omenjeni konferenci med najpomembnejša uvrstili tudi nekaj na informacijsko tehnologijo vezanih vprašanj. Tako tudi že omenjeno vprašanje, kakšne probleme lahko povzroči računalniško podprto komuniciranje. Drugo vprašanje je, v kakšni meri lahko informacijska tehnologija prinese dolgotrajne prednosti za razliko od le začasnih.

Boudreau in njeni sodelavci menijo, da je osnovni problem najti organizacijsko obliko, katere lastnosti so učinkovitost in odzivnost na lokalne značilnosti in ki obenem omogoča prenos znanja med lokacijami [17]. Za globalno (avtorji jo imenujejo virtualno transnacionalno) organizacijo je značilna njena odvisnost od poslovnih povezav in partnerstev z drugimi organizacijami. Taka organizacija deluje kot skupnost organizacij, povezanih med seboj s pogodbami in z drugimi načini, kot so solastniški aranžmaji. To so lahko skupna vlaganja, strateške povezave, investicije v manjšinske deleže, konzorcijske pogodbe, koalicije, zunanje izvajanje in franšize. Pravijo na primer, da je razvoj bombnika B-1 zahteval sodelovanje skupin iz kar 2000 organizacij.

Cilj virtualne organizacije je izvleči kar največjo vrednost od partnerjev z minimalnimi investicijami v stalno zaposlene, v trajna sredstva in obratni kapital. To dosežejo tako, da odredijo svojim partnerjem največje mogoče število funkcij z izjemo osnovnih strateških funkcij, ki jih konkurenti težko povzamejo in ki omogočajo organizaciji ohraniti dolgoročno konkurenčno prednost.

Da bi pa virtualne organizacije dosegle svoje cilje, morajo premagati svojo najhujšo preizkušnjo - težavno koordinacijo. Koordiniranje je v globalnih organizacijah dražje zaradi številnih zunanjih in mednarodnih povezav, ki jih morajo voditi neodvisno od časa in prostora. Pri tem seveda pomaga informacijska tehnologija. Ta v resnici omogoča dramatične organizacijske spremembe. Tabela 1 opisuje značilne tehnologije in aplikacije, ki pomagajo globalni organizaciji pri učinkovitosti, odzivnosti na lokalne pogoje in pri sposobnosti učenja.

Računalniška izmenjava podatkov (RIP) poveča učinkovitost v maloprodaji do take mere, da računajo, da bo polovica maloprodajnih trgovin propadla do leta 2001 [18]. Močno poveča tudi odzivnost. V tekstilni industriji so izmerili, da potrebujejo firme, ki uporabljajo RIP, za izpolnitev naročila poprečno deset dni, medtem ko druge potrebujejo 125 dni.

Interorganizacijski sistemi omogočajo izvajanje poslovnih dogodkov med organizacijami, kar spet poveča njihovo učinkovitost in odzivnost. Taki sistemi se odlikujejo po zanesljivosti, varovanju podatkov, zagotavljanju zaupnosti uporabnikov in celovitosti. Klasična primera sta sistem razvit v American Hospital Supply in Singapurski TradeNet.[4] Slednji povezuje trgovske predstavnike, vladne agencije, luške oblasti, dostavljalce blaga, transportne firme, banke in zavarovalnice s strankami in carinskimi uradniki.

Poleg tega, da omogoča Internet poceni nastop na globalnem tržišču, lahko poveča razumevanje značilnosti posameznih strank, zaznavanje njihovega razvoja in lahko prelevi statistične podatke o potrošnikih v dolgotrajne in tesne odnose s njimi. V tem času se npr. bančna industrija temeljito spreminja. Računajo, da je banki šestkrat ceneje obdelati elektronsko transakcijo z izvorom kjerkoli na svetu kot obdelati lokalni ček.

Programe za prevajanje iz enega v drug jezik lahko uporabljamo za pospeševanje poslovanja in povečanje lokalne odzivnosti. Organizacija, ki lahko hitro prenese znanje iz obrata v Švedski na novo lokacijo v Slovenijo brez jezikovne pregrade, doseže prednost v primerjavi z lokalnimi in drugimi mednarodnimi organizacijami.

Tehnologija za individualizacijo serijske proizvodnje omogoča oblikovanje izdelkov ali storitev skladno s posebnostmi lokalnih zahtev ali posamičnih strank. Ključna pri tem je uporaba informacijske tehnologije za organizirano uvajanje posebnih značilnosti v procesu proizvodnje.

Ekstranet je aplikacija internetne tehnologije, ki omogoča izbranim zunanjim partnerjem dostop do informacij korporacije. Najpogosteje lahko stranke in partnerji preko ekstraneta dostopajo do podatkov o kontih in koordinirajo dobave artiklov. Uporaba te tehnologije omogoča npr. sledenje pošiljk v industriji dostavljanja paketov, kot sta Federal Express in DHL.

Največja težava pri globalnem delu v skupinah je v premagovanju razdalj in časovnih razlik, da bi lahko ljudje iz različnih okolij uspešno sodelovali. Uporaba tehnologije za podporo dela v skupinah je del rešitve. Ta tehnologija ne služi le izmenjavi sporočil, ampak omogoča tudi uporabo skupinskega zaslona, terminiranje skupinskega dela, podporo sestankov, skupinskega pisanja in druge aplikacije. Te zmogljivosti podpirajo pri delu vodje skupin, pospešujejo skupinske procese in povečujejo tehnične in upravljalne

4 *Omenjena sistema sta med drugim opisana v Harvardskih prigodkih: Marshall, C. L., Konsynski, B. in Sviokla, J.*, Baxter International: On-Call as Soon as Possible? *Prigodek št. 9-195-103. Boston: Harvard Business School Publishing, 1995.*
King, J. in Konsynski, B., Singapore TradeNet: A Tale of One City. *Prigodek št. 9-191-009. Boston: Harvard Business School Publishing, 1995.*

Tabela 1. **Tehnologije in aplikacije v podporo učinkovitosti, odzivnosti in učenju**

Informacijske tehnologije in aplikacije	Učinkovitost	Odzivnost	Učenje
Računalniška izmenjava podatkov	*	*	
Interorganizacijski sistemi	*	*	
Elektronsko poslovanje preko Interneta	*	*	*
Prevajanje iz enega v drugi jezik		*	
Tehnologija za individualizacijo serijske proizvodnje		*	
Ekstranet		*	*
Oprema za skupinsko delo (groupware)	*		*
Intranet	*		*
Sistemi za organizacijsko pomnenje		*	*

sposobnosti skupin. Dober primer take opreme je IBM-ov Lotus Notes.

Učenje je mogoče pospešiti tudi z intraneti, izoliranimi mrežami, ki pa omogočajo uslužbencem globalni pristop do novic, kadrovskih informacij, koledarja dogodkov, podatkov o zalogah izdelkov, prostih delovnih mestih itd. Včasih je v intranet vključena tudi elektronska pošta, da je tako zaščitena pred nepooblaščenimi.

V informacijske sisteme do nedavnega nismo vgrajevali funkcij za organizacijsko učenje in pomnenje. Sedaj pa organizacije uvajajo aplikacije za hranjenje tako numeričnih kot tekstovnih in drugih nekonvencionalnih oblik informacij. Taki sistemi združujejo in avtomatizirajo zbiranje, hranjenje, vzdrževanje, iskanje in dostop do multimedijskih informacij in tako pomagajo širiti izkušnje med uporabniki. Sisteme te vrste uporabljajo vse velike mednarodne svetovalne organizacije. Znani so tudi primeri uporabe te tehnologije pri proizvodnji programske opreme.

10. NASVETI VODILNIM

Organizacija, ki osvaja globalno strategijo, mora dobiti podporo zanjo na najvišji ravni organizacije. Posamične enote je ne morejo uresničiti, ker tako poslovanje vpliva prav na vse. Vodilne je treba izobraziti o osnovnih strategijah globalnih organizacij, vse druge zaposlene pa seznaniti o načinih poslovanja, skladnih z globalno strategijo.

Vodilni morajo podpirati iniciative, ki slonijo na informacijski tehnologiji. Globalna organizacija ni samo krik mode. Ker so take organizacije odvisne od informacijske tehnologije, ki se še naprej hitro razvija, bodo globalne organizacije kot organizacijska oblika ostale globoko v 21. stoletju. Glede na sedanji nivo zmogljivosti za podporo učinkovitosti, odzivnosti in učenja, se bodo morali vodilni usmeriti na tiste tehnologije, ki bodo organizaciji pomagale premostiti njene pomanjkljivosti. Če na primer organizacija nima sistemov za pomoč pri učenju, so primerne investicije v intranet in organizacijsko pomnenje. Uporaba tehnologij v skladu s potrebami organizacije lahko pomembno poveča njeno globalno konkurenčnost.

Reference

[1] Zahra, S. A., "Competitiveness and Global Leadership in the 21st Century", *Academy of Management Executive*, 12 (4), 1998, pp. 10-12.

[2] "Workshop Report", NSF Workshop Research Priorities in Electronic Commerce, september 1998. Dosegljivo na: http://cism.bus.utexas.edu/workshop/ecdraft.html. 14. april 1999.

[3] Pollack, A., "Information Technology and Socialist Self-management", v *Capitalism and the Information Age*, New York: Monthly Review Press, 1998.

[4] Lohr, S., "Computer Age Gains Respect Of Economists", *The New York Times*, 14. april 1999.

[5] McChesney, R.W., "The Political Economy of Global Communication", v *Capitalism and the Information Age*, New York: Monthly Review Press, 1998.

[6] Kelly, K., "New Rules for the New Economy: Twelve dependable principles for thriving in a turbulent world", *Wired*, september 1997. Dosegljivo na: www.wired.com/wired/5.09/newrules.html. 12. april 1999.

[7] *Telecommunications Industry at a Glance*. Online. International Telecommunications Union, 1998. Dosegljivo na: www.itu.int/ti/industryoverview/at_glance/basic98.pdf. 1. april 1999.

[8] "Understanding the Digital Economy: Data, Tools and Research", Online. U.S. Department of Commerce, International Trade Administration, 1999. Dosegljivo na: www.ita.doc.gov/industry/otea/utde/related.htm. 1. april 1999.

[9] Clinton, W.J. in Gore, A., Jr. "A Framework for Global Electronic Commerce", Online. Information Infrastructure Task Force, 1997. Dosegljivo na: www.iitf.nist.gov/eleccomm/ecomm.htm. 2. april 1999.

[10] "First Annual Report", Online. U.S. Government Working Group on Electronic Commerce, Nov. 1998. Dosegljivo na: www.doc.gov/ecommerce/E-comm.pdf. 3. april 1999.

[11] "Next Generation Internet Research Act of 1998", Online. National Coordination Office for Computing, Information, and Communications. Dosegljivo na: http://www.ccic.gov/legislation/pl_h_105-305.html. 15. april 1999.

[12] "OECD Action Plan for Electronic Commerce", Online. OECD, 22. dec. 1998. Dosegljivo na: www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final.

[13] Meland, M., "Europe: The next frontier: How does Europe stack up on the Internet? A country by country ranking". Online. *Forbes DigitalTool*, 2. april 1999. Dosegljivo na: www.forbes.com/tool/html/99/mar/0329/feat.htm. 12. april 1999.

[14] "1998 World Development Indicators", Washington D.C.: The World Bank, 1998.

[15] Zahra, S. A. in O'Neill, H. M., "Charting the landscape of global competition: Reflections on emerging organizational challenges and their implications for senior executives", *Academy of Management Executive*, 12 (4), 1998, pp. 13-21.

[16] Hitt, M. A., Keats, B. W. in DeMarie, S. M., "Navigating in the new competitive landscape: Building strategic flexibility and competitive advantage in the 21th century", *Academy of Management Executive*, 12 (4), 1998, pp. 22-42.

[17] Boudreau, M.-C., in drugi, "Going Global: Using information technology to advance the competitiveness of the virtual transnational organization", *Academy of Management Executive*, 12 (4), 1998, pp. 120-128.

[18] Keen, P. G. W., *Every Manager's Guide to Information Technology*, Boston: Harvard Business School Press, 1995.

◆

Prof. Saša Dekleva je vodja programov informatike na "Kellstadt Graduate School of Business" na "DePaul University" v Chicagu, kjer predava vrsto predmetov, med njimi tudi Elektronsko poslovanje in Management informacijske tehnologije. Dr. Dekleva, ki je pred odhodom v Ameriko deset let delal v industriji v Sloveniji in predaval na Fakulteti za organizacijske vede, je objavil več kot 50 člankov v revijah kot so "Communications of the ACM", "Data Base", "MIS Quarterly", "Information Systems Research" in "Information & Management". Prof. Dekleva sedaj raziskuje med drugim tudi elektronsko poslovanje in programsko inženirstvo.

MIKROPROCESORSKA KARTICA IN KARTIČNI OPERACIJSKI SISTEM

Peter Pehani

Povzetek

Uporaba mikroprocesorskih oz. pametnih kartic (angl. smart cards) se intenzivno širi na mnoga področja človekovega delovanja. Pametna kartica je kartica z mikroračunalnikom, ki ga nadzira kartični operacijski sistem. Kartični operacijski sistem je trajno shranjen v pomnilniku ROM. Njegovi prioriteti sta varno izvajanje ukazov, ki prihajajo v mikroračunalnik od zunaj, ter nadzor dostopa do podatkov, ki so shranjeni v kartičnem pomnilniku EEPROM.
Kartični operacijski sistemi prihodnosti, ki so v povojih, bodo omogočali sožitje več aplikacij na isti kartici, večjo prilagodljivost kartice za kasnejše spremembe, ipd.

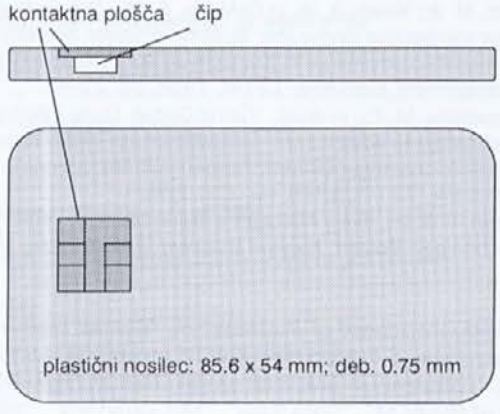
Abstract

Use of microprocessor cards - or smart cards - is spreading intensively on many fields of human activity. Smart card is a card with a microcomputer that is controlled by a card operating system. Card operating system is loaded permamently into ROM. Its priorities are secure execution of commands that enter into the microcomputer from outside world, and control of access to the data that are stored in the EEPROM.
Future card operation systems will enable sharing of more applications on a single card, greater flexibility of the card for possible changes, and so on.

1. UVOD

Kartice so hitro razvijajoča se veja informacijske tehnologije. Medtem, ko so koncem osemdesetih let svoj pohod začele *magnetne kartice*, so jim v devetdesetih sledile najprej *pomnilniške kartice* in nato še *mikroprocesorske kartice*.

Vsaka kartica je sestavljena iz nosilca standardnih dimenzij, na katerega je pritrjen pomnilniški medij. Našteti trije tipi kartic se razlikujejo po tem, kateri medij služi za shranjevanje podatkov: pri magnetnih karticah je to magnetni trak, pri pomnilniških pomnilniški čip, pri mikroprocesorskih pa mikroračunalnik z mikroprocesorjem. Tipični primeri za magnetne kartice so bančne in kreditne kartice, za pomnilniške telefonska kartica, za mikroprocesorske pa kartica zdravstvenega zavarovanja (pri nas v uvajanju). Obstaja še en tip kartic - *optične kartice*, pri katerih se informacija shranjuje na plasti, občutljivi za laserske žarke. Zaradi tehnologije, ki je draga in ki zaenkrat omogoča le enkraten zapis na neko lokacijo, te kartice še niso doživele široke uporabe.



Slika 1: Mikroprocesorsko kartico sestavljajo: nosilec, kontaktna plošča in mikroprocesorski čip.

Uporabljata se tudi imeni *čipne kartice* oz. *kartice z integrirnim vezjem*; to so pomnilniške in mikroprocesorske kartice, ker je v njih vstavljen čip. Glavna razlika med pomnilniškimi in mikroprocesorskimi karticami je v tem, da ima pomnilniška kartica v osnovi le preprosto varnostno logiko s kontrolo dostopa do pomnilnika pri branju in pisanju. V mikroprocesorsko kartico pa je vgrajen mikroračunalnik, ki ga je prek kartičnega operacijskega sistema mogoče programirati. Mikroprocesorska kartica ima visoke zmogljivosti pomnilnika, podatki so varno in dolgotrajno shranjeni, možno je izvajati razne kriptografske funkcije in druge algoritme. Tudi zato mikroprocesorske kartice večkrat imenujemo *pametne kartice* (angl. *smart cards*). Raba imena pa ni dosledna; včasih se uporablja le za mikroprocesorske kartice, včasih pa za mikroprocesorske in pomnilniške kartice skupaj. V članku uporabljamo naziv pametne kartice v ožjem smislu samo za mikroprocesorske kartice.

Čipne kartice se najbolj široko uporabljajo pri telekomunikacijah (80 % vseh v uporabi), kot telefonske in GSM kartice. Uporaba čipnih kartic se širi na področja bančništva, prometa, kontrole dostopa, zdravstva in trgovine. Kartica bo kmalu postala redni spremljevalec osebnega računalnika in bo uporabniku omogočala varen in zanesljiv vstop v informacijska omrežja.

Zavod za zdravstveno zavarovanje Slovenije (ZZZS) bo obstoječo zdravstveno izkaznico zamenjal s *kartico zdravstvenega zavarovanja* (KZZ). Za KZZ je bila izbrana mikroprocesorska kartica, ker nudi od vseh kartic najbolj varno okolje za shranjevanje občutljivih zavarovalniških in medicinskih podatkov.

2. MIKRORAČUNALNIK V MIKROPROCESORSKI KARTICI

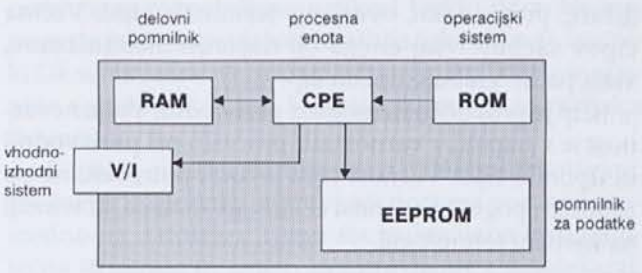
2.1. Mikroračunalniški čip

Čip, ki je vgrajen v mikroprocesorsko kartico, je kot majhen računalnik. Vsebuje naslednje komponente (glej sliko 3) [3, 4, 5, 6]:

- *Centralno mikroprocesorsko enoto* (CPE); CPE večinoma temeljijo na Motoroli 6805 in Intelu 8051; hitrosti do 5 MHz; večinoma so 8-bitne, modernejše pa so 16-bitne.
- Tri vrste pomnilnikov:
  - *RAM - delovni pomnilnik* (angl. Random Access Memory). Shranjuje začasne informacije med delovanjem procesorja. Za svoje delovanje rabi zunanji vir napetosti. Običajne velikosti so med 128 in 512 bajtov. Hitrost pisanja je velikostnega reda 10 ns.
  - *ROM - trajni pomnilnik* (angl. Read Only Memory). Vanj je tovarniško trajno naložen kartični operacijski sistem ali drugo programje za stalne funkcije (angl. *mask*). Ni ga možno naknadno spreminjati.
  - *EEPROM - bralno-pisalni pomnilnik* (angl. Electronically Erasable Programmable Read Only Memory). Služi za shranjevanje uporabnikovih podatkov. Opravlja podobno funkcijo, kot jo ima trdi disk na PC-ju. Navadno zavzema največ prostora v čipu, je največji porabnik energije ter tudi najdražji od vseh pomnilnikov. Prenese med 10.000 in 500.000 ciklov pisanja. Obstojnost podatkov je navadno 10 let. Hitrost pisanja je velikostnega reda 1 ms.
    EEPROM se lahko uporabi tudi za shranitev dopolnilnega kartičnega operacijskega sistema. Začasno se ga lahko uporablja tudi kot dopolnitev RAM-a, z 10^6-krat počasnejšim dostopom.
    Namesto EEPROM-a se lahko uporabita še pomnilnika Flash ali FERAM, ki porabita manj prostora glede na EEPROM in sta precej hitrejša (hitrost pisanja je pribl. 10 ms oz. 100 ns), vendar zaradi različnih vzrokov še nista dosegla tako široke uporabe.

Nobeden od naštetih pomnilnikov ni dostopen neposredno. Vsak zunanji dostop gre preko procesne enote ter varnostne logike.

- *vhodno-izhodni sistem*; dvosmerni serijski vmesnik.



Slika 3: Arhitektura mikroračunalnika v mikroprocesorski kartici.

	magnetna kartica	čipna kartica		optična kartica
		pomnilniška k.	mikroproc. k.	
pomnilniški medij	magnetni trak	pomnilniški čip	mikroračunalnik	optično občutljiva plast
pomnilniška kapaciteta	< 1 kB	0.256 - 2 kB	1 - 64 kB	1000 - 16000 kB
večkratno zapisovanje	DA	DA	DA	NE
varnost proti ponarejanju	majhna	srednja	zelo velika	velika
zaščita proti kopiranju	majhna	srednja	zelo velika	majhna
stopnja standardizacije	do detajlov	delno	delno	v povojih
primer	bančne kartice, kreditne kartice	telefonske kartice	k. zdravstvenega zavarovanja, k. za mobilni telefon	

Slika 2: Primerjava različnih tipov kartic [4].

Čip mikroprocesorske kartice lahko vsebuje dodatne strojne elemente kot so *kontrolne enote* za nadzor napetosti, ure in strojne varnostne logike (dostopanje do pomnilnikov, ipd, *generator naključnih števil* za izvajanje obojestranskega overjanja ter *matematični koprocesor* za izvajanje raznih kriptografskih algoritmov.

Velikosti vseh treh pomnilnikov v čipu mikroprocesorske kartice so relativno majhne v primerjavi z drugimi mikroprocesorji, ker morajo biti izredno majhni. Debelina mikroprocesorske kartice je 0.75 mm. Čipi mikroprocesorskih kartic so redko večji od standardiziranih 25 mm^2, saj pri večjih čipih obstaja nevarnost zloma. V borbi za več pomnilnika gre razvoj v izboljšavanje natančnosti tehnologije, ki je trenutno okoli 0.5 mm in napreduje v skladu z Moorovim zakonom.

Čip je na razne načine zaščiten pred zunanjimi vdori in poskusi analiz od zunaj. Vdori so lahko bolj strojne narave, npr. mikroskopski pregled čipa, ali bolj programsko-procesne narave, npr. analize odzivov na nizke frekvence, odzivnih časov, induciranih napak izven delovnega območja (temperatura, obsevanje). Proti prvim se uporabljajo naslednji obrambni mehanizmi: mešanje vodil, mešanje naslovov pomnilniških celic oz. navidez naključno nelogično razporejanje elementov po plasteh, varnostne prevleke plasti čipa, zavajujoče prazne komponente, ipd. Proti drugim pa: detekcija nizkih in visokih frekvenc, detekcija temperature, prazni takti, overjanje terminala., ipd. Večina čipov vsebuje vsaj enega od naštetih mehanizmov, vseh pa ne vsebuje noben čip.

Čip je praktično nemogoče ponarediti. Večja nevarnost je v napaki v varnostnih procesih pri proizvodnji in uporabi čipa. Varnost čipa je torej potreben, ne pa zadosten pogoj za varnost celotnega sistema, ki temelji na kartični tehnologiji.

2.2. Kontaktne in brezkontaktne mikroprocesorske kartice

Vmesnik med čipom in zunanjim svetom je kontaktna plošča s šest ali osem kontakti, ki prekriva čip. Kontaktna plošča je najbolj izpostavljen del celotnega tokokroga, izpostavljena obrabi, mehanskim poškodbam, pa tudi zlorabi. Komunikacija prek kontaktne plošče je običajen in najbolj razširjen način komunikacije z zunanjim svetom. Mikroprocesorske kartice s kontaktno ploščo imenujemo tudi *kontaktne*.

Mikroprocesorski čip pa lahko komunicira z zunanjim svetom še na en način: prek antene s pomočjo radijskih valov. Take kartice imenujemo *brezkontaktne kartice*. Antena zbira tudi energijo, potrebno za delovanje mikroračunalnika. Razdalja komunikacije je velikostnega reda 1 m in je prvenstveno odvisna od čitalnika (njegove frekvence). Brezkontaktne kartice so zelo primerne za uporabo v transportu in kontroli dostopa, manj pa za prenos zaupnih podatkov. Zaradi kompleksnejše strukture so dražje od kontaktnih, tehnologija še ni tako dognana.

2.3. Standardi

Kartice določajo standardi mednarodnih organizacij za standardizacijo ISO/IEC, CEN, ETSI, ipd, po posameznih industrijskih panogah pa jih dopolnjujejo industrijski standardi, ki jih določajo konzorciji največjih svetovnih proizvajalcev.

Od mednarodnih standardov je za kontaktne mikroprocesorske kartice najvažnejši ISO/IEC 7816 [7]. Gre pravzaprav za množico standardov - do sedaj je sprejetih že 10 delov - ki že več kot 10 let sledi razvoju tehnologije mikroprocesorskih kartic. Standard ISO/IEC 7816 določa fizične karakteristike kartic, dimenzije kartic, lokacije kontaktov, tipe označevanja, protokole komunikacije s svetom, priporočila za kartični operacijski sistem, nabor ukazov kartičnega operacijskega sistema, organizacijo podatkov na karticah, varnostne mehanizme, ipd.

Najpomembnejše industrijske standarde po panogah pripravljajo naslednje skupine:

- EMV (Europay, Mastercard, Visa): specifikacije funkcij kartic v bančništvu;
- ETSI (European Telecommunication Standards Institute): standardi za kartice v navadni in mobilni telefoniji;
- OpenCard Framework: vključitev mikroprocesorskih kartic v omrežja,
- SC/PC (Smart Card Personal Computer): vključitev mikroprocesorskih kartic v osebni računalnik.

3. KARTIČNI OPERACIJSKI SISTEM

Operacijski sistem je nekak posrednik med strojno opremo in aplikacijskim programjem. Gre za skupino sistemskih programov in nanje navezanih ukazov. Z ukazi zunanji svet (uporabnik) komunicira z računalnikom, ne da bi mu bilo treba poznati strojno opremo. *Kartični operacijski sistem* (angl. *COS - card operating system*) se ne more primerjati z obširnimi večopravilnimi sistemi na večjih računalnikih (npr. nima dela z zunanjimi napravami za komunikacijo z uporabnikom, vedno komunicira z računalnikom), kljub temu pa opraviči svoje ime. Prioriteti kartičnega operacijskega sistema sta varno izvajanje programov ter nadzor dostopa do podatkov.

Količina programske kode je zelo majhna, velikostnega reda 10 kB. Praviloma je koda spravljena v ROM-u. Tja se trajno shrani že med proizvodnjo čipa. Kasnejše spremembe niso možne, verjetnost za načrtno ali nenamerno spremembo vsebine ROM-a je praktično ničelna. Prav zato mora biti operacijski sistem, preden se vloži v ROM, celovit in praktično brez napak. Mnogo časa se posveča testiraju in odpravi napak. Zaradi

majhne procesorske moči in omejenih pomnilniških kapacitet pa mora ustrezati še naslednjim zahtevam: mora biti hiter pri izračunih, optimiziran glede porabe pomnilnika, robusten in zanesljiv, zaupen in vedno na razpolago.

Vsi operacijski sistemi dopuščajo, da se posamezne njegove funcije naložijo v EEPROM, ki sicer služi za shranjevanje podatkov.

Glavne naloge operacijskega sistema so:

- prenos podatkov na kartico in obratno;
- nadzor nad izvajanjem ukazov, časovno usklajevanje, notranja kontrola ukazov;
- ravnanje s podatki oz. z datotekami v EEPROM-u, s poudarkom na varnosti;
- ravnanje s kriptografskimi funkcijami in njihovo izvajanje;
- polnitev kartice z osebnimi podatki in kontrola življenjskega cikla kartice;
- pogosto: izvajanje aplikacijskih funkcij ali aplikacijske kontrolne logike (npr.: zmanjšanje vrednosti v elektronski denarnici, ipd.).

Proizvajalci procesorjev opremijo čip z okleščenim operacijskim sistemom z minimalnim naborom ukazov in funkcij, potrebnih za upravljanje z mikroračunalnikom. Nabor ukazov, ki jih mora kartični operacijski sistem podpirati, sestavljajo: ukazi za delo z aplikacijami in njihovimi podatki (branje, pisanje/obnavljanje, izbiranje), razni varnostni ukazi (izmenjava naključnih števil, preverjanje gesel in ključev, zapiranje dostopa), ipd.

Nabor s standardom predpisanih ukazov v praksi je le osnovni nabor ukazov. Ta nabor proizvajalci kartic razširijo z lastnimi ukazi, ki jih je pogosto še enkrat toliko kot osnovnih. Za množične aplikacije razvijejo proizvajalci kartic svoje kartične operacijske sisteme, ki jih vgradijo v čip ob proizvodnji. Iz enakega čipa tako nastane več različnih kartic, vsaka opremljena z drugačnim operacijskim sistemom. Proizvajalčevi specifični ukazi so dodatni ukazi za zagotavljanje varnosti (preverjanje elektronskega podpisa, obojestranske identitete, ...), ukazi za ravnanje z datotekami (ustvarjanje in brisanje datotek), ipd.

Operacijski sistemi različnih proizvajalcev niso kompatibilni. Razvoj aplikacij za vsak operacijski sistem zato zahteva natančno poznavanje tega sistema. Razloga za nekompatibilnost sta vsaj dva: odprtost standardov za različice in modifikacije operacijskih sistemov (standardi premalo strogi, preveč odprti) ter dodajanje novih funkcionalnosti, ki niso definirane v standardih. Poleg tega tehnologija in raba prehitevata standarde. Večina kartic, ki so sedaj v uporabi, je bila načrtovana pred objavo standardov.

Podrobnosti operacijskih sistemov so skrbno varovane skrivnosti. Opisovanje kartičnega operacijskega sistema je možno le fenomenološko, na splošnem nivoju. Uveljavljeni kartični operacijski sistemi se naslanjajo na standard ISO 7816-4, ki temelji na datotečni organizaciji podatkov v EEPROM-u.

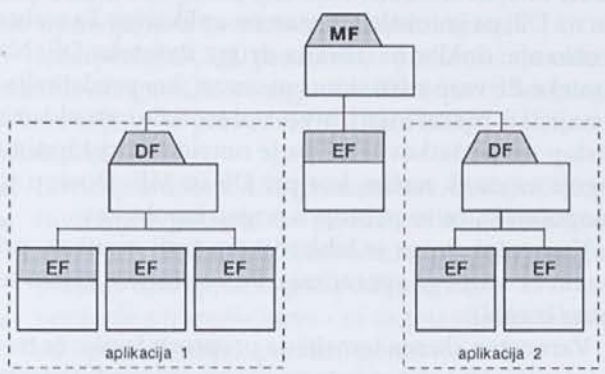
3.1. Datoteke, ki jih podpira kartični operacijski sistem

Strukturo datotek v EEPROM-u, ki jo podpirajo kartični operacijski sistemi, določa standard ISO 7816-4. Struktura je hierarhična, drevesna, povsem podobna DOS-ovi strukturi. Sestavljajo jo naslednji *tipi* datotek:

- *MF* - glavna datoteka oz. glavni imenik (angl. *Master File*): vsebuje vse druge datoteke in imenike. Obsega ves razpoložljivi prostor za datoteke.
- *DF* - namenska datoteka (angl. *Dedicated File*) je datoteka v vlogi imenika; je nekakšna višja organizacijska enota; vanjo so naložene sorodne elementarne datoteke ali imeniki, ki pripadajo skupni aplikaciji.
- *EF* - elementarna datoteka (angl. *Elementary File*) je datoteka s podatki. Postavljena je pod MF ali DF. Datoteka EF ima lahko različno *strukturo*, glede na organizacijo zapisov. Strukture so: trasparentna - EF brez notranje stukture; linearna fiksna - sestavlja jo več enako dolgih nizov; spremenljiva fiksna - sestavljajo jo nizi različnih dolžin; linearna ciklična - enako dolgi nizi, ki se polnijo v cikličnem zaporedju. Izbira strukture EF je pogojena s podatki.

Število nivojev v datototečnem drevesu je poljubno, omejuje ga razpoložljiva velikost EEPROM-a. Najbolj pogosta je trostopenjska hierarhija (glej sliko 4). Imeniki DF so navadno vezani na *aplikacijo*. Aplikacija je skupina sorodnih datotek, ki imajo skupnega upravljalca (lastnika).

Kartični operacijski sistemi so objektno orientirani, pri čemer so podatki o pravicah dostopa vezani neposredno na datoteko. Temu sta prilagojena tudi datotečna struktura in sistem za upravljanje z datotekami. Vsako datoteko sestavljata dva dela: glava (angl. header, file descriptor) in telo (angl. body). Navadno sta fizično na ločenih lokacijah. Glavo datoteke trajno določimo ob vzpostavljanju datoteke. Glava vsebuje



Slika 4: Drevesna struktura datotek v EEPROM-u z vsemi tremi tipi datotek: MF, DF in EF. Struktura predstavlja dvo-aplikacijsko kartico; vsaka aplikacija je na svojem imeniku DF.

lastnosti datoteke: ime, tip, struktura, velikost, lega v drevesu, varnostni atributi (npr.: pristopni pogoji) in drugi atributi. Telo datoteke vsebuje spremenljive uporabnikove podatke, ki jih je mogoče večrat brati in pisati. Izbira datotek poteka na osnovi logičnih naslovov. Te mora poznati terminal, ki pošilja ukaze na kartico.

3.2. Varnostna shema kartičnega operacijskega sistema

Varnostna shema, ki jo podpira kartični operacijski sistem, vsebuje: pristopne mehanizme, pristopne pogoje in varnostni status.

Pristopni mehanizmi so ukazi ali kombinacije ukazov, ki spreminjajo varnostni status in s tem omogočajo delo z datotekami. To so naslednji mehanizmi:

- identifikacija lastnika: preverjanje, ali je kartica v pravih - t.j. lastnikovih - rokah prek poznavanja gesla oz. osebne kode PIN (angl. personal identification number);
- overjanje zunanjega okolja: preverjanje, ali kartico bere pravo okolje; okolje dokaže poznavanje šifrirnega ključa;
- overjanje kartice: obratno - okolje preveri, ali kartica pozna šifrirni ključ.

Pristopni pogoji do posamezne datoteke določajo predpogoje, ki morajo biti izpolnjeni, preden se lahko nad datoteko izvedejo ukazi. Pristopni pogoji se za vsako datoteko v EEPROM-u določijo ob izgradnji datoteke. Zapisani so v glavi datoteke in so trajni. Odvisni so od tipa datoteke ter od zaupnosti podatkov v datoteki. Do datotek dostopamo z različnimi zunanjimi ukazi, ki so bralno-zapisovalni ali administrativni (npr.: branje, pisanje, iskanje, onemogočanje, zaklepanje, brisanje, dodajanje, ...). Pristopni pogoji so definirani za vsak ukaz posebej. Dostop do datoteke s posameznim ukazom je lahko prost, omejen s pristopnim mehanizmom (geslom ali ključem), ali pa prepovedan.

Varnostni status predstavlja stanje po izvedenem pristopnem mehanizmu. Status je vezan na datoteke MF in DF. Status, vezan na MF, je celovit. Status, vezan na DF, pa je lokalen, vezan na aplikacijo. Ta status se ohranja, dokler ni izbrana druga datoteka DF. Na datoteke EF varnostni status ni vezan, ker predstavljajo najnižji hierarhični nivo v datotečni strukturi. Dostop do podatkov v EF pa je omejen s pristopnimi pogoji na enak način, kot pri DF in MF. Dostop je omogočen le, če so pristopni pogoji izpolnjeni.

Varnostni status je lahko vezan tudi na ukaz, pri ukazih t.i. varnega sporočanja. Po končanem ukazu se status izgubi.

Varnostna shema temelji na preprosti logiki: če trenutni varnostni status ustreza zahtevanim pristopnim pogojem, je omogočen dostop do datotek in izvedba nadaljnjih ukazov, kot so branje, pisanje, prehod v nižji hierarhični nivo po datotečnem drevesu. Niže gremo lahko le, ko zadovoljimo pogoje na višjem nivoju.

V varnostno shemo sodita še dva varnostna mehanizma, ki ne spreminjata varnostnega statusa, služita pa za varen prenos podatkov. To sta:

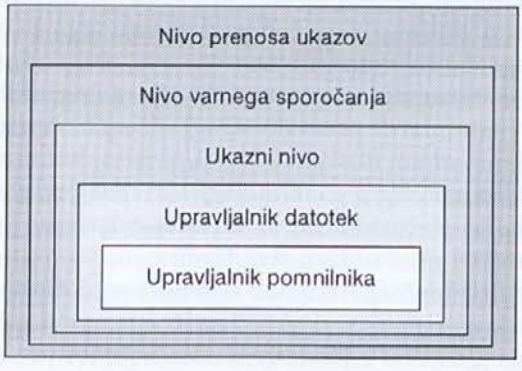
- zagotavljanje celovitosti podatkov: preverjanje, ali se je kak del podatkov pri prenosu izgubil ali je bil "ukraden"; prek šifrirne kode MAC (angl. massage authentication code);
- zagotavljanje zaupnosti podatkov: preprečevanje branja podatkov tretji osebi se zagotovi s šifriranjem s simetričnim ali asimetričnim algoritmom.

3.3. Izvajanje ukazov v kartičnem operacijskem sistemu

Izvajanje ukazov, ki pridejo od zunaj, poteka v več nivojih, ki jih podpira kartični operacijski sistem. To zagotavlja večjo varnost.

Ukaz pride iz zunanjega sveta preko vhodno-izhodnega sistema. Najvišji nivo (angl. transport manager) nadzoruje prenos podatkov s standardnimi protokoli, poleg tega pa nadzira pravilnost prenosa ukazov. Nivo t.i. varnega sporočanja (angl. secure messaging manager) opravi zahtevane kontrole in dešifriranja. Če niso zahtevane, je ta nivo povsem transparenten.

Sledi ukazni nivo (angl. command handling), ki izvaja ukaze in nadzira njihovo izvajanje. Ta nivo prepozna ukaz, opravi kontrolo pravilnosti zaporedja ukazov ter izvede ukaz, če je v trenutnem stanju dovoljen. Zaporedje ukazov se lahko definira vnaprej. Predpisano zaporedje nadzoruje avtomatski nadzor ukazov, ki je postavljen med prepoznavo ukazov in med izvedbo ukazov. Avtomatski nadzor ukazov je paralelna zaščita, ki dopolnjuje zaščito s pravicami dostopa do posameznih datotek. Gre za nekakšno vgrajeno kontrolo izvajanja zaporedja ukazov. Običajno se ta kontrola definira za kratka, a pomembna zaporedja ukazov. Pogost primer so overjanja, kjer morajo ukazi prihajati točno v določenem vrstnem redu. V primeru napačnega vrstnega reda ukazov ali napačnih parametrov overjanje ne uspe in avtomatski nadzor ukazov vzpostavi predhodno stanje.



Slika 5: Nivojska struktura kartičnega operacijskega sistema

Datotečni nivo (angl. file manager) zagotavlja podporo in upravlja z različnimi tipi datotek EF in DF. Če ukaz zahteva dostopanje do datotek, ta nivo prevede logične naslove datotek v fizične. Nadzira tudi pravice dostopa do datotek. Pomnilni nivo (angl. memory manager) skrbi za kontrolo dostopanja do posameznih delov pomnilnika, ureja prosti pomnilnik, izvaja kontrole na nivoju pomnilnika.

Sestavljanje odgovorov je naloga centralnega upravljalnika odgovorov (angl. central return code manager). Upravljalnik pripravlja in razpošilja odgovore tako za notranje nivoje kot za zunanji svet v vseh fazah izvajanja ukaza.

Komunikacija med čitalnikom in kartico poteka po enem samem kanalu, v t.i. polodupleks (angl. half duplex) načinu. Terminal igra vlogo strežnika, ki pošlje ukaz. Kartica pa igra vlogo uporabnika, ki ukaz izvede in vrne odgovor. Vsa komunikacija poteka po sistemu ukaz - odgovor. Nikdar ne pride pobuda s kartične strani.

4. KARTICE PRIHODNOSTI

Daljnoročni cilj razvijalcev mikroprocesorskih kartic je, da bi lastnik z eno kartico lahko opravil več storitev. Poplava vsemogočih kartic za različne namene ta logični razvojni premik že implicitno zahteva: prehod od posamezne kartice za vsako *aplikacijo* na t.i. *večaplikacijsko kartico* (angl. multiapplication card), ki vsebuje več aplikacij in pokriva funkcionalnost več kartic. Pojem "aplikacija" predstavlja skupek funkcij, ki pripadajo istemu poslovnemu subjektu (podjetju, organizaciji, državni službi, javni službi, ...). Večaplikacijska kartica pomeni deljeno lastništvo in odgovornost med več poslovnih subjektov, kar skriva zapleteno shemo poslovnih, organizacijskih, finančnih, tehnoloških in varnostnih vprašanj.

Večaplikacijske kartice ne gre mešati z *večfunkcionalno kartico*. Večfunkcionalna kartica je opremljena z aplikacijo, katere lastnik in izdajatelj je en sam poslovni subjekt. Aplikacija na njej lahko opravlja različne *funkcije*, vendar vse v službi istega lastnika, zato je njen razvoj razmeroma preprost. Primer je večfunkcionalna kartica večjega podjetja, opremljena z aplikacijo, ki opravlja naslednje funkcije: kontrola prihodov-odhodov, kontrola dostopa do varovanih objektov, mesečna karta za mestni avtobus, plačevanje malice v menzi.

Večaplikacijske kartice bi potrebovale operacijski sistem, podoben klasičnim operacijskim sistemom, z naslednjimi zahtevami:

- Podpora več-aplikativnosti: uporabnik ima le eno kartico, ki gosti aplikacije različnih lastnikov z različnih področij življenja (plačilni promet, zdravstveno in socialno varstvo, transport, vladni in splošni dokumenti, elektronsko poslovanje, telekomunikacije).
- Varnost: soobstoj več aplikacij, pogosti prenosi podatkov ter izguba kartice so veliki riziki. Nujni so dodatni mehanizmi, ki omogočajo souporabo delov podatkov in programja med aplikacijami, po drugi strani pa varnostni mehanizmi pri razmejevanju dostopov med zaupnimi podatki posameznih aplikacij. Druge nujne dopolnitve: kompleksen sistem upravljanja s ključi; poostrene sheme overjanja terminala, kartice in aplikacije.
- Interoperabilnost kartice na vseh dostopnih točkah, ki se doseže s skladnostjo z vsemi mogočimi standardi ter obsega kompatibilnost med posameznimi tipi kartic, operacijskimi sistemi in spremljevalnimi orodji (čitalniki kartic).
- Prilagodljivost in odprtost: operacijski sistem naj omogoča dinamično dopolnjevanje funkcionalnosti; standardizirano nalaganje novih aplikacij na kartice v obtoku na varen in zanesljiv način; sistem upravljanja z aplikacijami, ki ji kartica vsebuje, in njihovimi verzijami.

Narejenih je bilo že nekaj poskusov, približati se takemu odprtemu operacijskemu sistemu:

- operacijski sistem za podporo bazam podatkov po standardu ISO 7816-7
- modularni interpreterji, npr. Java
- večaplikacijski operacijski sistemi, npr. MULTOS

4.1 Kartice s podporo bazam podatkov

Kartice s podporo bazam podatkov slonijo na že sprejetem standardu ISO 7816-7. Standard predpisuje objekte baze podatkov na kartici, uporabniške profile ter ukaze jezika SCQL (angl. smart card query language), ki služi kot interpreter za običajni jezik SQL.

Objekti baze SCQL so podobni objektom v običajnih bazah podatkov: tabele, pogledi (podmnožice tabel), sistemske tabele (objekti, uporabniki, dostopne pravice). Uporabniški profili so hierarhično strukturirani v tri razrede: lastnik baze podatkov, lastnik posameznega objekta v bazi, uporabnik. Uporabniški razredi določajo pravice uporabnikov. Višji razredi dopuščajo več pravic pri upravljanju z objekti tabele, ter upravljanje z hierarhično nižjimi razredi.

Interpreter SCQL predstavlja podmnožico ukazov standardnega SQL-a (angl. standard query language). Ukazi SQL-a se prevedejo v ukaze SCQL-a. Ukazi so naslednji:

- ravnanje z uporabniki (predstavitev, dodaj/odvzemi),
- ravnanje s podatki oz. podatkovnimi objekti (ustvari bazo, dodaj/odvzemi tabelo, pogled, omogoči/prekliči dostop, briši/piši podatek, ...),
- ravnanje s transakcijami - za zagotavljanje celovitosti operacij (začni, prekini, ponovi).

V nasprotju z uveljavljenimi operacijskimi sistemi, ki temeljijo na standardu ISO 7816-4, je baza podatkov SCQL precej bolj fleksibilna in omogoča:

- enostavno spreminjanje dostopnih pravic;
- dinamično ravnanje s pomnilnikom (glede na zasedenost in dolžino podatkov);
- različna overjanja, ki jih je možno kombinirati v poljubni kombinaciji;
- kontrolo celovitosti procesov pri transakcijah;
- iskanje po bazi.

4.2. Java kartice, MULTOS kartice

Java je programski jezik, ki teče na številnih mikroprocesorskih platformah. Je popolnoma objekten jezik z dobrimi varnostnimi mehanizmi, zato je primeren tudi za uporabo na mikroprocesorskih karticah.

Java kartica temelji na modularnem sistemu. Interpreter je naravna rešitev, saj je pri kartici včasih težko ločiti strojni del od programskega; sta zelo prepletena. Ideja je naslednja: aplikacijo napišemo na PC-ju z Javo. Na kartici je poseben interpreter te Java kode JVM (angl. Java Virtual Machine), ki razume programsko kodo. Funkcionalnost JVM je neodvisna od procesorja. Kot vmesnik med procesorjem in JVM delujejo programske knjižnice Java API, ki komunicirajo s poljubnim kartičnim operacijskim sistemom. Trenutno so kartični procesorji prešibki za celotno prevajanje Java kode. Zato je JVM dvodelna: en del je na PC-ju in z njim se opravi predprevajanje. Drugi del pa je na kartici in prevaja to predpripravljeno kodo.

Slika 6: Arhitektura Java kartice.

Java kartica bo zaživela ob zmogljivejših kartičnih mikroprocesorjih. Že zdaj napoveduje lažji razvoj novih aplikacij in možnost elegantne večaplikativne kartice. Prvi primerki Java kartic so že na testiranjih.

MULTOS kartica (angl. Multiapplication Operating system): MULTOS predstavlja prvi poizkus za izdelavo pravega večaplikacijskega operacijskega sistema. Arhitektura aplikacije z MULTOS-om je večnivojska, podobna kot pri Java kartici: aplikacijo se napiše v C-ju, prek C-prevajalnika prevede v interpretativni jezik MEL (angl. MULTOS Executable Language). Tako prevedena koda prek API-jev komunicira z operacijskim sistemom MULTOS.

5. ZAKLJUČEK

Čipne kartice se širijo na mnoga področja našega življenja. Z nekaterimi modernimi produkti, kot npr. mobilni telefon, so praktično zrasle skupaj. Zaenkrat ni videti meja razvoja. Letna proizvodnja čipnih kartic že presega 1000 milj. in nezadržno raste. Od tega odpade večina (80 %) na pomnilniške kartice, slabih 20 % pa na mikroprocesorske, ki se uporabljajo za aplikacije, zahtevne s tehnološkega vidika ali zaščite podatkov. Zaenkrat je uporaba bolj domena Evrope (90 %). Potencialno tržišče bo v letu 2000 blizu 3000 milj. čipnih kartic, od tega okoli 50 % telefonskih.

Že od nastanka je spremljalo mikroprocesorske kartice pomanjkanje široko sprejetih standardov, predvsem za operacijske sisteme. Proizvajalci so razvijali svoje rešitve, standardi pa so capljali za njimi. Problem postaja z željami po večaplikacijski kartici vedno bolj pereč. V boj za operacijski sistem, ki bo prevladal nad ostalimi in postal de-facto standard, se je z letošnjim letom vključil tudi Microsoft. To pa pomeni velik pritisk na vse ostale proizvajalce. Ni nujno, da bo zmagala kvaliteta, lahko da bo tržna prodornost.

6. REFERENCE

[1] ADAMS, Jane: "*More Brain Power for Smart Cards*", Card Technology, January 1999, pp. 54-57
[2] BALABAN, Dan: "*Stepping into the spotlight*", Card Technology, January 1999, pp 20-24
[3] HENDRY, Mark: *Smart Cards - Security and Applications*, Artech House, Norwood 1997
[4] LENDER, Friedwart: *Hybrid cards*, Tutorial at the International Health Card Conference, Heidelberg 1995
[5] RANKL, Wolfgang, in EFFING, Wolfgang: *Smart Card Handbook*, John Wiley & Sons, Chichester 1997
[6] VEDDER, Klaus, in WEIKMANN, Franz: *Smart Cards - Requirements, Properties and Applications*, Giesecke & Devrient, 1998
[7] ISO/IEC 7816, *Information technology - Identification cards - Integrated circuit(s) cards with contacts.*
Part 1: 1987, Physical characteristics
Part 2: 1988, Dimensions and location of the contacts
Part 3: 1989, Electronic signals and transmission protocols
Part 4: 1993-95, Interindustry commands for interchange
Part 5: 1994, Numbering system and registration procedure for application identifiers
Part 6: 1994, Interindustry data elements
Part 7: 1997, Interindustry commands for Structured Card Query Language (SCQL)
Part 8: 1998, Security related interindustry commands
Part 9: v branju, Enhanced interindustry commands
Part 11: v branju, Security architecturedržavljane Slovenije.

◆

Peter Pehani je diplomiral na Fakulteti za fiziko in matematiko, Oddelku za fiziko. Zaposlen je na Zavodu za zdravstveno zavarovanje Slovenije, *za tehnično podporo projektu "Kartice zdravstvenega zavarovanja" področje: kartica in kartična tehnologija, personalizacija, čitalniki. Projekt je v zaključni fazi - pred uvedbo sistema kartice zdravstvenega zavarovanja, z 2 milijona karticami za vse državljane Slovenije.*

KRIPTOGRAFSKI SISTEMI

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

Povzetek

Zagotavljanje tajnosti sporočil brez kriptografskih sistemov je za področje računalniških komunikacij nemogoča naloga, saj so metode prisluškovanja tako enostavne, da jih obvlada vsak povprečen programer. V prispevku bodo opisani koncepti različnih kriptografskih sistemov, ki jih uporabljamo predvsem na področju računalniških komunikacij.

Abstract

Computer network eavesdropping is a very easy task for an average programmer. It is almost impossible to assure confidentiality of information without using cryptographic systems. Various concepts of cryptographic systems that are currently used in the computer networks will be briefly presented.

1. Uvod

Z razvojem računalniških omrežij se je izredno povečal tudi pretok informacij. V začetnem obdobju Interneta je elektronska pošta omogočala samo prenos besedil, današnji protokoli pa omogočajo prenos poljubnih datotek. Sistem za prenos podatkov naj zagotavlja predvsem:

- *zasebnost (tajnost)*: prenašano sporočilo naj bo razumljivo le avtorizirani osebi to je osebi, ki je upravičena oziroma pooblaščena za to, da ga sme npr. prebrati, tiskati in prikazovati.
- *verodostojnost - avtentičnost*: pošiljatelj sporočila naj bo pravilno identificiran oziroma, njegova identifikacija ne sme biti lažna.
- *celovitost:* sprejeta sporočila morajo biti prav takšna kot smo jih poslali, t.j. nespremenjena. Pod spreminjanjem razumemo: pisanje, brisanje, zakasnitev ali ponavljanje sporočila.
- *preprečitev zanikanja:* niti pošiljatelj niti prejemnik ne moreta zanikati poslanega ali prejetega sporočila.
- *dostopnost:* pravico dostopa do sporočila mora imeti le verodostojna oseba t.j. oseba s pravilno identifikacijo.

V tem prispevku se bomo omejili le na zagotavljanje zasebnosti. Razlaga bo temeljila na preprostem modelu, ki je sestavljen iz izvora in ponora sporočil ter informacijskega kanala. Ker je informacijski kanal medij za prenos sporočil oziroma informacij, ki ga velikokrat ni mogoče fizično zaščititi, je po njem prenašano sporočilo izpostavljeno raznovrstnim *napadom*. Ti so zasnovani tako, da skušajo onemogočiti eno ali več zahtev, ki smo jih postavili glede prenosa podatkov. Proti napadom se lahko borimo z oviranjem (npr. šifriranje) in alarmiranjem (detekcija napada). Zasebnost lahko zagotavljamo s *šifrirno napravo*, ki jo vstavimo med izvor sporočila in informacijski kanal. Šifrirna naprava napadov ne more preprečiti, ampak jih lahko samo v večji ali manjši meri ovira. Šifrirna naprava, ki izvorno sporočilo *šifrira* t.j. pretvori v nerazumljivo obliko, poskrbi v prvi vrsti za zasebnost sporočila, hkrati pa lahko v kombinaciji z drugimi podsistemi zagotovi tudi verodostojnost, celovitost in prepreči možnost zanikanja. Onemogočanje ali kršenje zasebnosti sporočil imenujemo *kriptografski napad*.

Namen tega prispevka je prikaz raznih kriptografskih sistemov, ki se najpogosteje uporabljajo v računalniških omrežjih.

2. Kriptografski sistemi

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

Šifriranje je uporabljal že Julij Cezar pred več kot 2000 leti, ko je pošiljal pošto Ciceru. Uporabljal je zelo enostaven postopek šifriranja. Vse črke v besedilu je zamenjal s črkami, ki so bile za tri mesta naprej v latinski abecedi. Beseda CESARUS je bila na ta način šifrirana v FHVDUAV. Cezar je uporabljal isti postopek tudi, ko si je dopisoval z drugimi prijatelji. Ker so morali vsi poznati postopek, da so lahko prebrali svojo pošto, jim je to omogočalo, da so prebrali tudi pošto namenjeno Ciceru. Nekdo, ki se danes ukvarja s šifriranjem, bi tak postopek z lahkoto razvozlal že na osnovi dveh do treh

šifriranih stavkov. Kljub tej enostavnosti je v tem postopku skrita osnovna ideja šifriranja.

Šifrirati je mogoče klasična in elektronska sporočila. Šifriranje in dešifriranje elektronskih sporočil je preprostejše, saj ta dva postopka opravi računalnik. Veda, ki se ukvarja s šifranjem sporočil (*kriptografija*) in z razkrivanjem šifriranih podatkov (*kriptoanaliza*) se imenuje *kriptologija*. Beseda izhaja iz grških izrazov: *kryptos logos* kar pomeni skrita beseda. Oglejmo si najprej nekatere osnovne pojme v kriptografiji.

2.1 Osnovni pojmi v kriptografiji

Namen kriptografije je načrtovanje šifrirnih in dešifrirnih algoritmov, s pomočjo katerih je mogoče zagotoviti osnovne lastnosti sporočil: zasebnost, verodostojnost, celovitost in preprečitev zanikanja.

Pri šifriranju (slika 1) gre za transformacijo *odprtega sporočila*[1] ali *čistopisa* (angl.plaintext) v nerazumljivo *šifrirano sporočilo* ali *tajnopis* (angl. ciphertext). Tovrstna transformacija, ki se običajno izvaja kar z računalnikom, poteka v skladu s *transformacijskimi tabelami* ali *šifrirnimi algoritmi* (angl. cipher). Šifrirni postopek mora biti reverzibilen, saj je le v tem primeru tajnopis mogoče dešifrirati oziroma transformirati nazaj v originalno odprto sporočilo.

Šifriranje in dešifriranje vhodnega sporočila poteka na osnovi *ključa*, ki mora biti tajen, kar pomeni, da ga sme poznati samo pošiljatelj sporočila in tisti, ki mu je sporočilo namenjeno. Ključ, ki mora biti povsem neodvisen od odprtega sporočila, tvorijo izbrane vrednosti parametrov šifrirnega oziroma *dešifrirnega algoritma* (angl. decipher).

2.2 Splošna klasifikacija kriptografskih sistemov

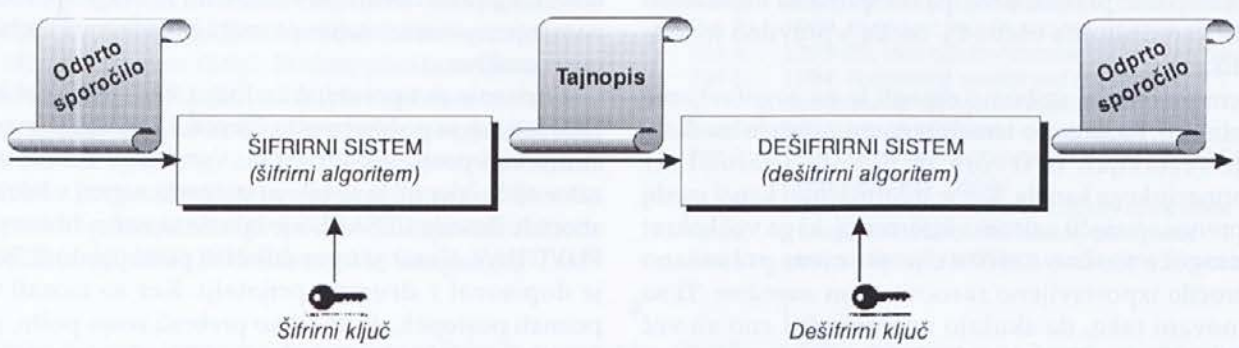
Kriptografske sisteme lahko klasificiramo (slika 2) po treh kriterijih [2]:

1. ***Število uporabljenih ključev.*** V primeru, da pošiljatelj in prejemnik uporabljata en sam ključ, govorimo o *simetričnem, enoključnem* ali *konvencionalnem šifriranju* (angl. symetric, single-key, secret key - conventional cipher), če pa uporabljata dva različna ključa, gre za *asimetrično, dvoključno šifriranje* ali *šifriranje z javnim ključem* (angl. asymetric, two-key, public key cipher).
2. ***Metoda šifriranja.*** Šifriranje sporočil se izvaja z različnimi metodami. Medtem, ko sta pri simetričnih sistemih uveljavljena predvsem principa *zamenjave* in *premeščanja*, se v asimetričnih sistemih šifriranje izvaja s posebnimi matematičnimi transformacijami. Pri zamenjavi se vsak element (bit, znak, skupina bitov ali znakov) v odprtem sporočilu preslika v drugi element, pri premeščanju pa se elementi odprtega sporočila prerazporejajo. Večina sistemov vsebuje več stopenj zamenjave in premeščanj.
3. **Velikost vhodnega bloka, ki ga uporablja šifrirna metoda.** Kriptografski sistem lahko šifrira ali dešifrira odprto sporočilo po blokih določene dolžine - v tem primeru govorimo o blokovnih šifrirnih sistemih (angl. Block cipher), obstajajo pa sistemi, ki odprto sporočilo šifrirajo ali dešifrirajo bit za bitom - tokovni šifrirni sistemi (angl. Stream cipher). Tovrstni shemi zasledimo v primeru simetričnih kriptografskih sistemov.

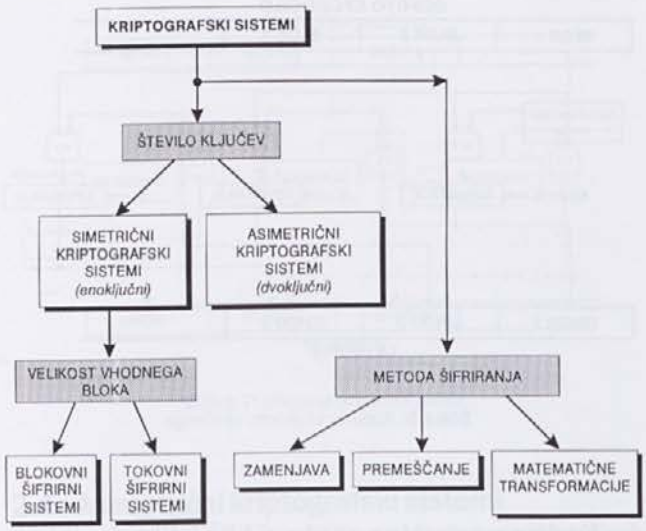
2.3 Simetrični kriptografski sistemi

Slika 3 prikazuje preprost model simetričnega kriptografskega sistema. Proces šifriranja poteka na osnovi šifrirnega algoritma in enega samega *tajnega ključa* (angl. Secret key). Izhod šifrirnega algoritma - tajnopis je po sprejemu potrebno transformirati nazaj v originalno odprto sporočilo, kar se izvede z dešifrirnim algoritmom in enakim ključem, kot je bil uporabljen pri šifriranju.

1 *Uporabljajo se tudi izrazi prikrito sporočilo, šifropis, ali kriptogram.*



Slika 1:
Kriptografski sistem sestavljata šifrirni in dešifrirni sistem. Tajnopis je mogoče uspešno dešifrirati samo v primeru poznanega dešifrirnega ključa.

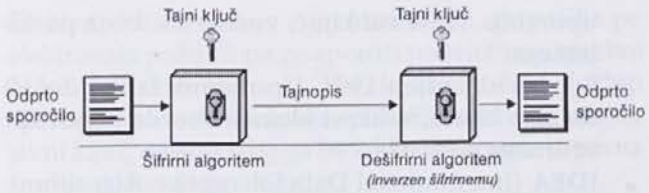


Slika 2: Splošna klasifikacija kriptografskih sistemov

Šifriranje in dešifriranje s simetričnimi algoritmi je običajno hitro, pojavi pa se problem varne izmenjave ključa med pošiljateljem in prejemnikom.

Oglejmo si pomembne elemente simetričnih kriptografskih sistemov nekoliko natančneje (slika 4). Šifrirni algoritem ima dva vhoda. Prvi je povezan z izvorom, ki tvori odprto sporočilo M, sestavljeno iz končne množice znakov - abecede[2]. Na drugem vhodu je ključ K, ki ga je potrebno po varnem kanalu distribuirati na ciljno stran - ponor. Za varno distribucijo ključa poskrbi pošiljatelj, obstaja pa možnost, da ključ izdela tretja oseba in ga pošlje na obe strani - izvor in ponor.

[2] *Danes se najpogosteje uporablja binarna abeceda [0, 1]*



Slika 3: Preprost model simetričnega kriptografskega sistema

Na osnovi odprtega sporočila M in tajnega ključa K šifrirni algoritem E tvori tajnopis C:

$$C = E(M, K). \tag{1}$$

Tajnopis se po šifriranju odpošlje. Njegov prejemnik ga nato, s pomočjo dešifrirnega algoritma D, pretvori nazaj v odprto sporočilo M:

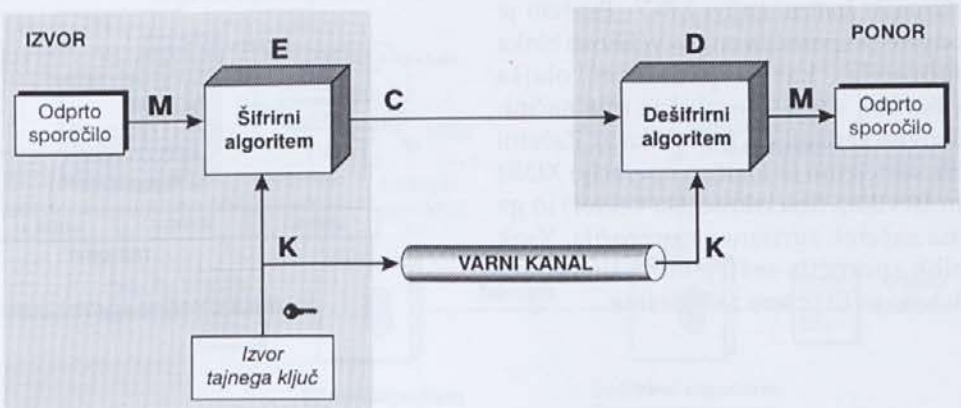
$$M = D(C, K) = D(E(M, K), K) \tag{2}$$

Najbolj znani simetrični kriptografski sistemi so [4]:

- **DES (Data Encryption Standard)** ali DEA (Data Encryption Algorithm), ki sta ga razvila NIST (National Institute of Standards and Technology) ter IBM.
- **RC2, RC4, RC5** - je razvil Ronald Rivest.

RC2 se vgrajuje v nekatere programe (npr. Outlook Express), namenjene za delo z elektronsko pošto. Uporabljamo lahko ključe dolžine 1 do 2048 bitov razen za verzije, ki so namenjene uporabnikom zunaj ZDA. Za te verzije je ameriška vlada izdala zakon, s katerim je omejila ključ na največ 40 bitov.

RC4 je tekoč šifrirni algoritem z spremenljivo dolžino ključa do 2048 bitov. Vgrajen je v Netscape-ov brkljalnik kot del protokola SSL. Ameriška verzija



Slika 4: Podrobnejši model simetričnega kriptografskega sistema

uporablja 128-bitni ključ, verzija za izvoz pa 40-bitnega.

RC5 je bil objavljen 1994. Uporabnik lahko določi dolžino ključa, velikost bloka in število ponovitev šifrirnega postopka.

- **IDEA** (International Data Encryption Algorithm): razvila sta ga James L.Massey in Xuejia Lai v Zürichu in objavila leta 1990. Uporablja 128 bitov dolg ključ na 64 bitov dolgih blokih. Patent zanj ima Ascom-Tech iz Švice. Izven ZDA ga lahko uporabljamo brez plačila licenčnine. Če DES uporabljamo s trojnim ključem, je počasnejši od IDEA.
- **Skipjack:** algoritem, ki ga je razvila NSA (National Security Agency), je strogo zaščiten. Uporabljen je v šifrirnem čipu Clipper. Ključ je 80-biten. Vsak čip ima svoj ključ, katerega polovici sta shranjeni v različnih agencijah (key escrow agency).

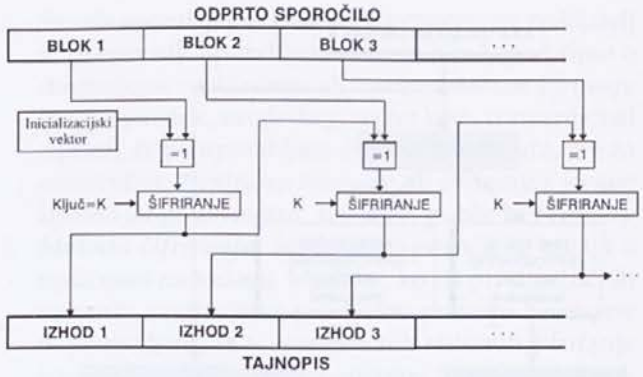
2.3.1 Tokovni in blokovni simetrični šifrirni sistemi

Pri *tokovnem* načinu šifriranja se sporočilo šifrira bit za bitom tako, da se kombinira bit ključa in bit sporočila - običajno je to kar logična operacija XOR. Če je uporabljen kratek, ponavljajoči ključ, postopek ni varen - s kombiniranjem šifriranega sporočila je razmeroma lahko ugotoviti najprej dolžino ključa, potem vrednost ključa in nato sporočilo dešifrirati. Nasprotno pa je sistem kriptografsko zelo robusten, če se ključ ne ponavlja in je povsem naključen niz bitov.

Večina algoritmov, ki se danes uporabljajo v civilnih organizacijah, je *blokovnih*: sporočilo se razbije na tako dolge bloke, kot zahteva algoritem, nato pa se vsak blok preoblikuje in kombinira s ključem. Permutacije, substitucije in kombinacije s ključem (npr. DES) morajo zagotoviti, da so v izhodnem bloku zabrisani vsi vzorci iz vhodnega bloka - skratka, da izgleda kot naključen niz bitov. Za vse simetrične algoritme velja, da se šifriranega sporočila ne da zgostiti za več kot nekaj odstotkov.

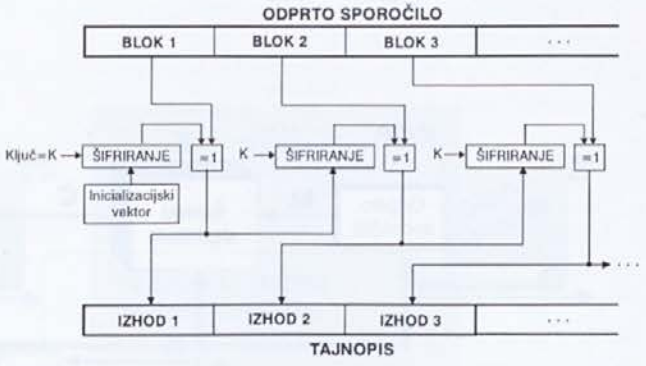
Pri blokovnih algoritmih je pomemben tudi način povezovanje blokov [5]. Če se šifrira vsak blok posebej, govorimo o *elektronski kodirni knjigi EBC*[3]. Pri tem je velikost bloka odprtega sporočila enaka velikosti bloka šifriranega sporočila, kar napadalcem olajša dešifriranje. Veliko bolj varni so naslednji trije načini:

- **Kodirno blokovno veriženje CBC**[4] (slika 5): Začetni blok sporočila seštejemo (z logično operacijo XOR) z naključnim številom (inicializacijski vektor) in ga postavimo na začetek šifriranega sporočila. Vsak naslednji blok sporočila seštejemo s šifriranim prejšnjim blokom in to potem zašifriramo.



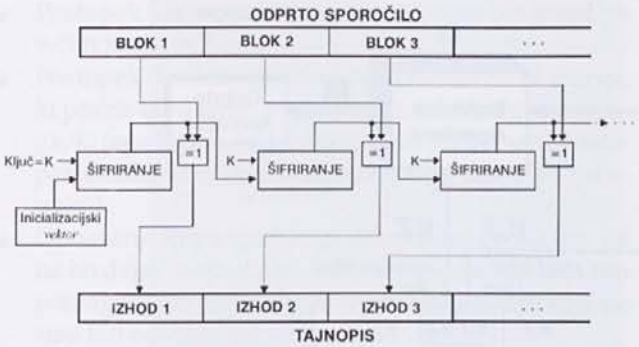
Slika 5: Kodirno blokovno veriženje

- **Kodirna povratna zanka CFB**[5] (slika 6): inicializacijski vektor zašifriramo s ključem in rezultat seštejemo (z logično operacijo XOR) s prvim blokom sporočila. Tako dobimo prvi šifrirani blok. To vsoto zašifriramo s ključem in tako dobimo začasni ključ. Temu prištejemo drugi blok sporočila... Vidimo, da pri tem načinu s šifriranjem pravzaprav spreminjamo ključ.
- **Izhodna povratna zanka OFB**[6] (slika 7): šifriranje je podobno prejšnjemu načinu. Inicializacijski vektor zašifriramo s ključem. Ta rezultat (recimo mu R1) seštejemo (z logično operacijo XOR) s prvim blokom sporočila in to je prvi šifrirani blok sporočila. Potem dobimo ključ za šifriranje naslednjega bloka tako, da R1 zašifriramo s prvotnim ključem... Od prejšnjega načina se razlikuje v tem, da začasni ključ, tvorjen s šifriranjem predhodnega ključa, ni odvisen od sporočila.



Slika 6: Kodirna povratna zanka

3 *Angl. Electronic Code Book*
4 *Angl. Cipher Block Chaining*
5 *Angl. Cipher Feedback*
6 *Angl. Output Feedback*



Slika 7: Izhodna povratna zanka

2.4 Asimetrični kriptografski sistemi

Problem varne izmenjave tajnega ključa pri simetričnih kriptografskih sistemih so rešili šele z uvedbo *asimetričnih kriptografskih sistemov* oziroma *kriptografskih sistemov z javnim*. Njihova prva predstavitev[7] leta 1976 je povzročila radikalne spremembe v dotedanjih kriptografskih sistemih. Za razliko od simetričnih sistemov, pri katerih se šifriranje/dešifriranje izvaja na osnovi zamenjav in transpozicij, temeljijo asimetrični sistemi na posebnih matematičnih funkcijah. Njihovo delovanje ni vezano le na enega, temveč na dva ločena ključa, s pomočjo katerih je mogoče zagotoviti ne le zasebnosti sporočil[8] temveč tudi verodostojnost in celovitost.

Pri kriptografskih sistemih z javnim ključem uporabnik kreira na svojem računalniku dva ključa: *zasebnega*[9] in *javnega*[10]. Javni ključ javno objavi na katerem od strežnikov z javnimi ključi, ga pošilja po elektronski pošti ali pa ga sporoči po telefonu, zasebni ključ pa drži v tajnosti. Vsi, ki mu hočejo poslati sporočilo, bodo za šifriranje sporočila uporabili njegov javni ključ, dešifriral pa ga bo lahko le on sam, ki pozna še svoj skriti zasebni ključ.

Na sliki 8 je prikazan preprost model kriptografskega sistema z javnim ključem, kjer pošiljatelj pošilja sporočilo prejemniku - Andreju. Sporočilo šifrira z Andrejevim javnim ključem, ki je v prostem dostopu na strežniku z javnimi ključi. Odposlan tajnopis bo lahko dešifriral samo Andrej, ki pozna svoj zasebni ključ.

S pomočjo slike 9 si oglejmo nekatere podrobnosti. Ponor B tvori par ključev: javnega *KJ* in zasebnega *KZ*. Medtem, ko je zasebni ključ *KZ* znan samo ponoru B, je ključ *KJ* javno objavljen kar pomeni, da je dostopen tudi izvoru A. Izvor A, ki namerava šifrirati odprto sporočilo *M* in ga poslati ponoru B, uporabi za šifriranje javni ključ *KJ* in šifrirni algoritem *E*. Odprto sporočilo *M* tako pretvori v tajnopis *C*:

$$C = E(M, KJ) \tag{3}$$

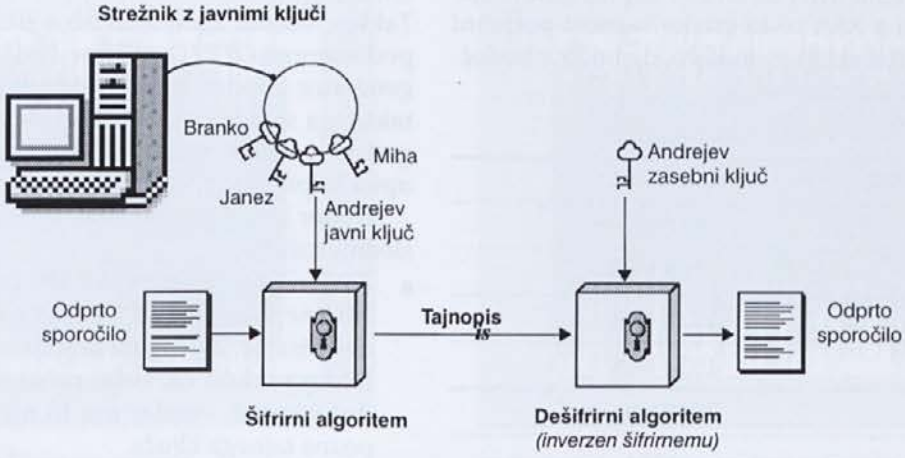
Ponor B tajnopis sprejme in ga s pomočjo dešifrirnega algoritma *D* in zasebnega ključa *KZ* pretvori nazaj v odprto sporočilo *M*:

$$M = D(C, KZ) = D(E(M, KJ), KZ) \tag{4}$$

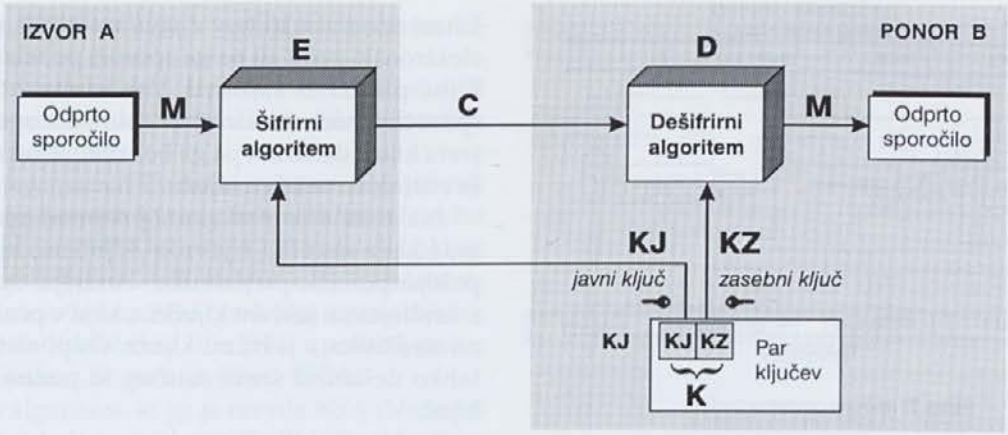
Šifrirni in dešifrirni algoritmi temeljijo na uporabi *navideznih enosmernih funkcij*[11], t.j. *enosmernih funkcij z vgrajeno pastjo*, za katere je značilno:

1. posamezna funkcijska vrednost $C=f(M,K)$ ima unikatni inverz $M=f^{-1}(C, K)$;
2. izračun funkcijske vrednosti $C=f(M,K)$ je enostaven, če sta *M* in *K* znana;

[7] *Predstavila sta ga W. Diffie in M. Hellman.*
[8] *Simetrični kriptografski sistemi v splošnem poskrbijo le za zasebnost sporočil.*
[9] *Angl. Private key*
[10] *Angl. Public key*
[11] *Angl. Trap-door one-way function.*



Slika 8: Preprost model asimetričnega kriptografskega sistema



Slika 9: Podrobnejši model asimetričnega kriptografskega sistema

3. izračun inverzne vrednosti $M=f^{-1}(C, K)$ je enostaven, če sta C in K znana;
4. inverzno vrednost $M=f^{-1}(C, K)$ je nemogoče izračunati, če je C in K neznan, kar pomeni, da enosmerne pasti ne moremo odpreti brez poznavanja ključa K.

Najbolj znana algoritma z javnim ključem sta [4]:

- algoritem **RSA**, poimenovan po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman) in patentiran v ZDA. Metoda temelji na zahtevni nalogi faktorizacije števila, ki je zmnožek dveh velikih praštevil.

  Na voljo je veliko komercialnih izvedb RSA (tako programskih kot strojnih). Uporabljajo se ključi daljši od 512 bitov. Za ameriške firme velja omejitev za izvoz: dobiti morajo dovoljenje vlade, ta pa običajno ne dovoli izvoziti programa, ki uporablja daljši ključ od 512 bitov. RSA Laboratories priporoča ključ 768 bitov za osebno uporabo, 1024 bitov za uporabo v organizacijah in 2048 bitov za ključe v izredno pomembnih operacijah.
- **ECC** (Elliptic Curve Cryptosystems) je algoritem, katerega matematična osnova so eliptične funkcije. V primerjavi z RSA so za enako varnost potrebni krajši ključi (tabela 1), zato kaže, da bodo v bodočnosti ti algoritmi prevladali.

dolžina ključa ECC	dolžina ključa RSA
106 bitov	512 bitov
132 bitov	768 bitov
160 bitov	1024 bitov
191 bitov	1536 bitov
211 bitov	2048 bitov

Tabela 1: Primerjava med dolžinami ključev, potrebnih za enako stopnjo varnosti pri RSA in ECC [4].

Leta 1990 so se razširile govorice, da ameriška vlada na predlog FBI in NSA pripravlja zakon, ki bo zelo omejil uporabo kriptografskih algoritmov [4]. Phil Zimmermann[12], računalniški strokovnjak, je kot odgovor na to napisal programski paket **PGP (Pretty Good Privacy)**, ki je brezplačen in uporablja simetrične in asimetrične algoritme, zgostitvene funkcije in vse, kar je potrebno za pošiljanje šifriranih sporočil po elektronski pošti. Poleg avtorja so ga dopolnjevali uporabniki po vsem svetu. Od verzije 5 naprej je možno izbirati med algoritmi RSA, Diffie-Hellman, IDEA in drugimi simetričnimi algoritmi.

2.5 Splošne lastnosti kriptografskih sistemov

Namen načrtovalcev kriptografskih sistemov je izdelati dober oziroma kakovosten kriptografski sistem. Kakovost se ocenjuje na osnovi njegovih lastnosti, ki so: varnost, hitrost, zanesljivost, enostavnost, cenenost, vzdrževalnost.

Ena izmed najpomembnejših lastnosti kriptografskih sistemov je njihova varnost. O popolni varnosti bi lahko govorili samo v primeru, če bi razpolagali z vsaj toliko ključi, kolikor odprtih sporočil želimo šifrirati [1]. Takšen, vendar zgolj teoretičen šifrirni sistem, je znan pod imenom *OTP* (One-Time-Pad). Njegova osnova je generator popolnoma naključnih števil. Ker v praksi takšnega sistema ni mogoče realizirati, velja kriptografski sistem za varnega, če se že dolgo časa uspešno upira kriptoanalizi svetovne strokovne javnosti.

Dober kriptografski sistem mora izpolnjevati naslednje zahteve:

- Zasebnost sporočil ne sme sloneti na tajnosti samega šifrirnega postopka temveč na tajnosti ključa za dešifriranje. Z drugimi besedami to pomeni, da ima lahko vsakdo na voljo računalniški program za dešifriranje, vendar mu to nič ne pomaga, če ne pozna tajnega ključa.

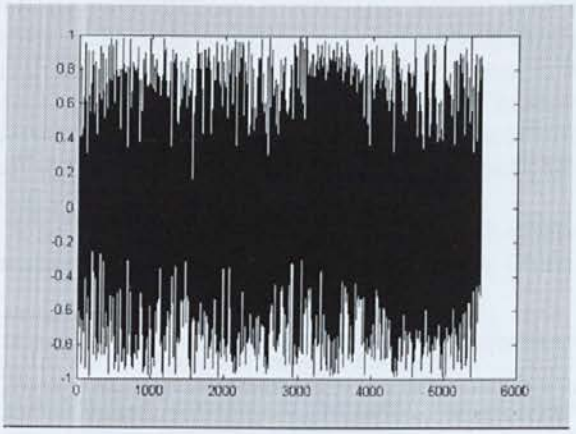
[12] *http://www.nai.com/products/security/phil/phil.asp*

- Postopek šifriranja in dešifriranja mora biti izvedljiv v čim krajšem času.
- Postopek dešifriranja mora biti enostaven za tistega, ki pozna tajni ključ, in praktično neizvedljiv za tistega, ki tega ključa ne pozna, četudi pozna sam postopek dešifriranja in ima na razpolago zmogljiv računalnik.
- Obnašanje kriptografskega sistema naj bo takšno, da ne bo dajalo napadalcu nobenih informacij, ki bi mu pomagale pri dešifriranju (npr. hitrost šifriranja ne sme biti odvisna od velikosti ključa).
- Vsi tajnopisi, ki jih tvori kripografski sistem, morajo imeti enake statistične lastnosti. Samo zamenjava vrstnega reda črk v tekstu temu ne ustreza, saj lahko napadalec s statistično analizo ugotovi, da je znak, ki se najbolj pogosto pojavlja, črka E (velja za slovenščino). Slika 10 prikazuje rezultate šifriranja dveh različnih tipov odprtih sporočil s kaotičnim kriptografskim sistemom, ki uporablja kaotično digitalno sito [6]. Izgled tajnopisov kaže, da se njune statistične lastnosti nekoliko razlikujejo.

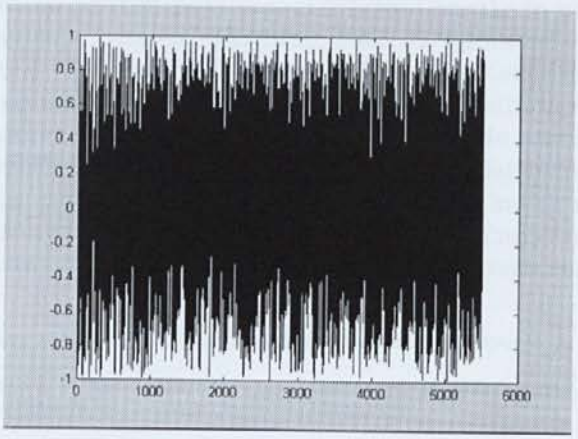
Na varnost kriptografskih sistemov vplivajo:

- *časovna zahtevnost šifrirnih in dešifrirnih algoritmov*: zasnova sodobnih kriptografskih sistemov je takšna, da prevede dešifriranje tajnopisa brez poznavanja ključa na zelo zahtevno računsko nalogo, ki zahteva za svoje reševanje zelo veliko časa. Zahtevnost algoritmov za šifriranje in dešifriranje je povezana z računsko zahtevnostjo [1], ki se ovrednoti glede na število osnovnih računskih operacij kot so npr. seštevanje, odštevanje, množenje, deljenje, primerjanje, itd.
  Problem, ki ga rešuje algoritem, je preprost, če je rešljiv v *polinomskem času* kar pomeni, da je pri n-bitnem vhodu v algoritem, čas za izračun izhodne vrednosti proporcionalen vrednosti n^a, pri čemer je a konstanta [2]. Za takšne algoritme pravimo, da pripadajo razredu **P** - *polinomski*. Obstajajo pa še varnejši algoritmi, ki so povezani s precej zahtevnejšimi koncepti. To so algoritmi, ki pripadajo razredu **NP** - *nedeterministični polinomski razred* in se vgrajujejo v sodobne kriptografske sisteme (RSA). Njihova časovna zahtevnost je sorazmerna vrednosti c^n, kjer je c pozitivna konstanta, n pa število bitov vhoda.
- *zasnova - struktura*: Stuktura blokovnih sistemov, ki uporablja dodatne načine povezovanja blokov (CBC, CFB ali OFB), se izkaže za precej varnejšo kot navadna struktura, ki šifrira vsak blok posebej (EBC). Struktura RSA sistema temelji na računsko zelo zahtevni operaciji faktoriziranja števil. Za tovrstno operacijo je bilo predstavljenih precej različnih algoritmov, za katere je značilno, da so izredno dolgotrajni. Razbijanje takšnih sistemov je zaradi tega zelo naporno oziroma nesmiselno.
- *dolžina uporabljenega ključa* in njegovo *distribuiranje*: daljši ključ pomeni večjo varnost. V mnogih primerih se z dolžino ključa veča tudi čas šifriranja in dešifriranja. Distribucija tajnega ključa med pošiljateljem in prejemnikom mora biti varna.
- *kakovost implementacije*: pomembno je, da so kriptografski sistemi pravilno implementirani z neokrnjenimi in kriptografsko analiziranimi verzijami šifrirnih in dešifrirnih algoritmov. Še tako dober algoritem ni varen, če ni pravilno implementiran.

Tudi hitrost šifriranja in dešifriranja vpliva na kakovost kriptografskega sistema. Delovanje kriptografskega sistema v realnem času v večini primerov zahteva aparaturno izvedbo. Primerjava hitrosti asimetričnih in simetričnih algoritmov kaže, da so asimetrični algoritmi neuporabni za masovno šifriranje podatkov, saj so precej počasnejši od simetričnih. Algoritem RSA je namreč 1000-5000 krat počasnejši od algoritma DES.



a) Šifriran sinusni signal



b) Šifrirana tekstovna datoteka

Slika 10: Primer šifriranja sinusnega signala in datoteke z istim ključem. Statistične lastnosti obeh tajnopisov niso povsem enake.

Vzdrževalnost kriptografskega sistema je odvisna od njegove zasnove in implementacije. Zelo priporočljivo je, da obstaja možnost enostavne spremembe:

- ključa in njegove dolžine
- dolžine vhodnih blokov (odprto sporočilo)
- šifrirnega in dešifrirnega algoritma (v primeru kasneje odkritih pomanjkljivosti).

Tovrstne spremembe naj ne bodo pogojene z zahtevnimi posegi v strojno opremo ali celo načrtovanjem nove, pač pa naj bo omogočeno programsko spreminjanje.

3. Zaključek

Kriptografski sistemi so imeli že v preteklosti pomembno vlogo, ki pa je bila omejena predvsem na vojaško področje. Ker je v računalniških omrežjih relativno enostavno prisluškovati, se je že zelo zgodaj pojavila potreba po kriptografskih sistemih. V prispevku smo prikazali koncepte najpomembnejših kriptograskih sistemov, ki se uporabljajo predvsem na področju računalniških komunikacij.

Noben kriptografski sistem ne zagotavlja popolne zasebnosti. Njihova kakovost je odvisna od vrste algoritma in kakovostne implementacije. Vsak napadalec se za napad odloči šele takrat, ko se stroški (napor) vloženi v napad povrnejo z vrednostjo prebrane informacije. Na podlagi te ugotovitve so zasnovani vsi kriptografski sistemi.

Literatura

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

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

[3] S. Tomažič, M. Umek : *Varne komunikacije preko Interneta*, Zbornik posvetovanja Dnevi slovenske informatike, Portorož, 17.-20. april 1996. - Ljubljana: Slovensko društvo Informatika, 1996 - str. 214-222.

[4] Center vlade za informatiko: *http://www.sigov.si/tecaj/kripto/index.htm*, marec 1999.

[5] Eli Biham, Lars R. Knudsen, RSA Laboratories' CryptoBytes: *DES, Triple-DES and AES*, vol. 4, Number 1, Summer 1998.

[6] M. Šalamon, T. Dogša: *Kaos v digitalnem situ drugega reda*, Zbornik sedme Elektrotehniške in računalniške konference ERK '98, 24. - 26. september 1998, Portorož, - Ljubljana, Zv. A, str. 65-68.

◆

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

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

◆

MERJENJE ELEKTRONSKEGA POSLOVANJA S POMOČJO VZORČNIH ANKET

Vasja Vehovar[1], Fakulteta za družbene vede, Univerza v Ljubljani

Povzetek

V prispevku so sistematično obravnavana vprašanja, ki nastajajo pri spremljanju elektronskega poslovanja z metodo vzorčnih anket. Posebna pozornost je posvečena težavam definicij in vzorčenja, kar povzroča pri tovrstnem merjenju največja razhajanja. Problematika je umeščena tudi v širši kontekst merjenja informacijske družbe. Podane so ilustracije iz anket podjetij in gospodinjstev, ki potekajo v okviru projekta RIS (Raba Interneta v Sloveniji).

Abstract

The paper systematically discusses issues in survey measurement of electronic commerce. In particular, problems of definitions and sampling are addressed. The methodological problems are discussed also from a broader prospective of information society measurements. Empirical examples are presented from surveys performed within the project RIS (Research on Internet in Slovenia) 1996-1999.

1. Uvod

Standardizirane oblike elektronske izmenjave dokumentov so desetletja potekale prek zasebnih omrežij, predvsem v bančništvu in večjih korporacijah, vendar je šele z Internetom in vključitvijo končnih potrošnikov elektronsko poslovanje (e-poslovanje) pokazalo svoj resnični domet. Živimo v dobi, ko se poslovne transakcije postopno prenašajo iz papirnatih v elektronske forme, kar velja tako za odnos občan-država, za interakcijo potrošnik-ponudnik, predvsem pa za izmenjavo poslovnih dokumentov in plačil med organizacijami. V naslednjih letih torej pričakujemo radikalno in obsežno transformacijo večine poslovnih transakcij. Zaradi obsega in dinamike navedenega prehoda pa je njegovo spremljanje nadvse težavno. Velika razhajanja opazimo celo pri najbolj elementarnih kategorijah, kot je npr. število[2] uporabnikov Interneta (NUA) ali število internetnih "hostov"[3] (Network Wizzard, RIPE). Prav tako se soočamo z nadvse različnimi ocenami obsega e-poslovanja, saj se nahajajo[4] celo v razponu 1:100.

V nadaljevanju se bomo najprej dotaknili splošnih vprašanj merjenja informacijske družbe (2) in e-poslovanja (3). Slednje bomo obravnavali predvsem v kontekstu anketnega zbiranja podatkov (4), kjer bomo prikazali običajne metodološke probleme na tem področju kot tudi nekatere specifičnosti. Problematiko bomo ilustrirali s primeri iz raziskave Raba Interneta v Sloveniji RIS 1996-1999.

2. Spremljanje informacijske družbe

Merjenje e-poslovanja lahko umestimo v širša prizadevanja za spremljanje fenomenov informacijske družbe. Pojem informacijske družbe pravzaprav ni posebej nov, saj so se tovrstna vprašanja pojavljala že v prvih desetletjih tega stoletja, v drugi polovici tega stoletja pa nastanejo tudi eksplicitne oznake in prva merjenja "znanja" (Machlup, 1962) in "informacijskih storitev" (Porat, 1972; Rubin&Huber, 1986; Katz, 1986). Napori so usmerjeni predvsem k izračunavanju deležev teh sektorjev v družbenem proizvodu oziroma zaposlenosti, zato nove metode zbiranja podatkov niso bile potrebne. Izkazalo pa se je, da merjenje informacijske družbe presega golo preračunavanje obstoječih podatkov. Na tem mestu velja navesti znani

1 *Dr. Vasja Vehovar je docent za statistiko na Fakulteti za družbene vede, Univerza v Ljubljani. Ukvarja se z vzorčenjem, anketno metodologijo, že štiri leta pa vodi tudi projekt Raba Interneta v Sloveniji (RIS).*

2 *Znana je bila razprava Donne Hoffman v okviru Projekta 2000 o definiciji in številu ameriških uporabnikov izpred nekaj let* ***(http://www2000.ogsm.vanderbilt.edu/dhvita.html)****. Prav tako lahko prikažemo razhajanja kot jih navaja Clemente (1998:152).*

3 *Število strežnikov povezanih v omrežje Internet.*

4 *Tipična ocena obsega e-poslovanja v letih 1995 do 1997 je bila v razponu med 475 milijoni (EITO) in 8000 milijoni USD (Forrester), lahko pa celo 70 milijonov USD (INPUT) (The Economic and Social Impacts of Electronic Commerce, OECD, 1998: 27 - http://www.oecd.org/dsti/sti/it/ec/index.htm). Razlike v napovedanem obsegu e-poslovanja pa so običajno še veliko večje.*

paradoks (Hayes&Erikson, 1982; Braumstein, 1985) o investicijah v infrastrukturo informacijske družbe, predvsem v pisarniško opremo, kjer z obstoječimi metodami ne moremo izmeriti učinka teh vlaganj.

Posebej pereč problem nastaja pri mednarodnih primerjavah, ki so na tem področju vitalnega pomena, saj informacijsko družbo najbolje označuje prav globalizacija. Izkušnje iz mednarodnih projektov namreč govorijo, da je oblikovanje mednarodno usklajene metodologije zahteven in dolgotrajen proces. Tako npr. so metode za merjenje delovne sile potrebovale desetletja velikih metodoloških naporov in usklajevanj. Podobno velja za merjenje znanosti in tehnologije, kjer je revizija metodologije Frascati potekala skozi nadvse težavna in dolgotrajna usklajevanja.

Dinamika tehnoloških sprememb je probleme bistveno zaostrila, saj pojavi nastajajo in izginjajo tako hitro, da ni časa za običajne postopke standardizacije in harmonizacije[5]. V razvitem svetu sicer obstaja vrsta pobud in aktivnosti resornih organizacij (US Department of Commerce, OECD, UNESCO, Eurostat, pisarna ISPO, projekt ESIS) za spremljanje tega področja, vendar glavnino najbolj aktualnih podatkov prispevajo komercialni viri. Procese, ki so potrebni za izvedbo globalnih meritev na tem področju, je namreč potrebno upravljati izredno hitro, kar je pogosto prezahtevno za koordinacijo med neodvisnimi predstavniki držav.

Sodobni trendi so torej merjenje informacijske družbe – in še posebej e-poslovanja – prenesli v zasebne korporacije, ki se ukvarjajo z globalnim spremljanjem fenomenov na tem področju. Pri tem je dejstvo, da je opredelitev informacijske družbe nedorečena - ali v najboljšem primeru ohlapna - povsem nepomembno. Navedene korporacije pač izvajajo raziskave, ki jih je mogoče prodajati, naj bodo to analiza novih medijev (Nielsen NetRatings), spremljanje računalniške industrije (Gartner, IDC) ali mnenjske raziskave (Gallup, HarrisBlack). Nastopila so tudi nova podjetja, ki se specializirajo prav za merjenje (MIDS, MediaMatrix) in diseminacijo teh podatkov (NUA). Videti je torej, da so uradne statistike na tem področju povsem marginalizirane, saj se npr. vsi pomembni dokumenti, ki obravnavajo tovrstno problematiko, skoraj v celoti sklicujejo na komercialne vire informacij. Slednji imajo seveda tudi prenekatero slabost. Tako so metodologije pogosto vprašljive, nejasne, ali pa vanje ni mogoče dobiti javnega vpogleda[6].

Že uvodoma velja poudariti dve ključni značilnosti sodobnih merjenj na področju informacijske družbe:

a) Problemi definicij, terminologije, mednarodnih primerjav in standardiziranih metodologij so postali skoraj nerešljivi, saj hitre in dramatične spremembe preprečujejo usklajevanje. Tako se npr. lahko Internet izredno hitro spremeni (združevanje s telefonom, televizijo in videom), čemur mora z enako hitrostjo slediti tudi merjenje. Enako velja za e-poslovanje, kjer se pojavljajo novi in novi načini poslovanja in plačevanja.

b) Mnenjske spremenljivke imajo vse pomembnejšo vlogo pri tovrstnih merjenjih. Kot primer lahko navedemo nedavni Eurobarometer 50.1, ki je v celoti posvečen merjenju informacijske družbe ter uporabi e-poslovanja v gospodinjstvih znotraj držav Evropski uniji[7] - glavnina vprašanj pa se osredotoča predvsem na stališča. Podobno npr. dejstvo, da je tretjina aktivne populacije v Sloveniji že uporabila Internet, pove verjetno manj kot pa dejstvo, da ga 60% sploh ne namerava uporabiti. Informacija, da skoraj polovica srednjih in velikih podjetij uporablja Internet za vpogled v žiro račun, pa je verjetno enako pomembna, kot dejstvo, da ima tovrstne načrte samo še slaba petina teh podjetij. Da bi torej razumeli sodobne procese je torej potrebno vse več "mehkega" merjenja stališča ter kvalitativnega raziskovanja.

3. Merjenje e-poslovanja

Merjenje e-poslovanja lahko opazujemo v naslednjih kategorijah:

3.1 Merjenje komunikacije med računalniki ("computer-to-computer")

V tem okviru analiziramo "log" datoteke, odzive ("ping") ter druge zapise in dogodke komunikacij med računalniki. V nasprotju z merjenjem obiskanosti strani na svetovnem spletu, kjer tovrstne analize nudijo le omejen vpogled v problematiko, daje beleženje komunikacij med računalniki popolno sliko o vsaki elektronski transakciji.

3.2 Standardni ekonomsko-finančni indikatorji

Finančni indikatorji so gonilna sila razvoja e-poslovanja. V nasprotju s prejšnjim primerom gre tu za običajne, standardizirane in lahko razumljive kazalce. Informacije o borznem poslovanju, finančni vidiki transakcij, ki jih opravimo v različnih oblikah e-poslovanja, prodajne statistike - so tipični indikatorji v tej skupini.

---

[5] *Npr. http://www.internetindicators.com/*

[6] *IDC v publikaciji EITO (1999) za Slovenijo ocenjuje in javno predstavlja vse najpomembnejše indikatorje informacijske družbe (vlaganja, število novih PC-jev, število uporabnikov Interneta ipd), vendar metodologija ni javno dostopna (povzetek teh ocen je na http://www.ris.org/si/ris99/eito.html).*

[7] *http://www.ispo.cec.be/polls/EB98.htm.*

3.3 Anketno raziskovanje

Zgornja dva načina sodita v uporabo "trdih statističnih" podatkov, saj gre za merjenja na standardiziranih (največkrat razmernostnih) merskih lestvicah, ki se kažejo v kvantitativnih kazalcih, zbranih za celotno populacijo. Pri anketnem raziskovanju pa raziskave večinoma temeljijo na vzorcu, merski instrument pa na ordinalnih lestvicah. Seveda so vzorčne ankete pogosto tudi edini način za oceno kvantitativnih agregatov kot npr. za izdatke potrošnikov za nakupe prek Interneta ali za delež podjetij, ki uporablja e-poslovanje.

3.4 Kvalitativno merjenje

Posebej velja ločevati kvalitativne metode, ki rezultatov ne posplošujejo na celotno populacijo in pogosto ne dajejo niti kvantitativnih informacij, ampak le osvetljujejo odnose med koncepti. Na tem področju obstaja vrsta najrazličnejših metod, od fokusnih skupin do raziskav primerov, kar vse lahko privede do globljega vpogleda v kompleksne značilnosti procesov e-poslovanja.

V naslednjem razdelku se bomo osredotočili na metodološke vidike anketnih raziskav s področja e-poslovanja. Predstavili bomo splošni pregled, kritična vprašanja in ilustrirali problematiko z empiričnimi primeri.

4. Problemi anketnega raziskovanje e-poslovanja

Problematiko anketnega merjenja e-poslovanja bomo obravnavali z vidika izkušenj pri raziskovanju e-poslovanja med gospodinjstvi in podjetji v projektu Raba Interneta v Sloveniji (RIS). V nadaljevanju so sistematično urejeni tipični problemi, ki se pojavljajo pri oblikovanju vprašanj, pri kontaktu z respondenti ter problemi statističnega sklepanja in kvalitete podatkov.

4.1 Terminologija in prevod pojma

Angleški pojem "electronic commerce" vsekakor zožuje razumevanje v smer "elektronske prodaje". Prevodi v druge jezike lahko sledijo temu zgledu, ali pa, kot je to v primeru slovenščine, pomen prenesejo bliže dejanski vsebini, to je pojmu "elektronskega posla" (ang. "electronic business"). V vsakem primeru pa lahko angleški izvirnik privede do resnih težav anketnega merjenja.

4.2 Definicija e-poslovanja

V uporabi obstaja množica definicij. Že preprosto iskanje pod ključnimi besedami "electronic commerce" v spletnih iskalnikih nam prinese na tisoče strani, med katerimi desetine ponujajo tudi definicije tega pojma, vendar pa se nobena sklicuje na nek standardni vir. Poleg tega so definicije pogosto ohlapne, saj zajemajo pojme kot "vsako uveljavljanje elektronskih poslov" ali "vsako poslovno transakcijo, ki poteka preko omrežij". Podobno velja za definicije v nekaterih pomembnih dokumentih[8], strokovnih priročnikih in strokovnih člankih.

Poudariti velja, da se vse opredelitve praviloma strinjajo, da e-poslovanje vključuje tudi transakcije dokumentov in ne samo aplikacije neposredno vezane na nakup, prodajo in finančne transakcije. Nobena od teh definicij pa ni povsem izdelana, kar se najlepše pokaže, ko je treba pojem operacionalizirati za potrebe anketnega merjenja. Predstavljamo dva tipična primera vprašanj v raziskavah podjetij:

a) *E-poslovanje je komercialna aktivnost, ki se izvaja prek elektronskih omrežij, pogosto preko Interneta, in vodi k nakupu ali prodaji dobrin ali storitev* (EITO, 1999:169).
b) *S pojmom e-poslovanje razumemo vsak prenos poslovnih dokumentov (naročila, plačila, potrdila...) prek računalniških omrežij.* (RIS, 1999).

Vsekakor zgornji definiciji sprožata vprašanje veljavnosti – ali res merimo tisto, kar želimo meriti? Če za določene aktivnosti ni jasno ali sodijo v navedene opredelitve, potem merimo le respondentovo razumevanje nejasnega pojma. Obstaja tudi problem zanesljivosti – določena oseba znotraj podjetja ima lahko drugačno razumevanje in pri ponovitvi merjenja bi prejeli drugačen odgovor. Prav tako nastajajo tudi problemi primerjav med ponavljajočimi raziskavami in še posebej med različnimi raziskavami.

V Tabeli 1 so prikazani odgovori velikih in srednjih podjetij na navedeni vprašanji, česar zaradi možnih razlik v razumevanju vprašanja v resnici **ni mogoče primerjati.** Problemi bi lahko obstajali celo v primeru povsem enakih vprašanj. Zaradi razlik v prevodu in razumevanju se seveda tudi odgovori 15 držav EU lahko razlikujejo v percepciji e-poslovanja.

Po drugi strani pa lahko ilustriramo *elektronsko podporo poprodajnih aktivnosti* kot dovolj dobro opredeljen pojem, ki omogoča enako razumevanje in s tem tudi primerjavo.

Tabela 1: Odstotek podjetij, ki uporablja e-poslovanje (EITO, RIS)

	EU	Slovenija
Uporablja e-poslovanje	*61*	*49*
Načrtuje uporabo e-poslovanja	*19*	*20*
E-poslovanje v poprodajnih aktivnostih	16	5
Načrtovana uporaba v poprodajnih aktivnostih	29	9

Seveda obstajajo še druge ovire za pravilno primerjavo, kot so recimo problemi vzorčenja[9], o katerih bomo govorili kasneje.

[8] *Dokumenti, ki so bili napisani znotraj organizacij, kot so OECD, Evropska unija, UNESCO itd., imajo določeno regulativno funkcijo.*

[9] *Slovenska podjetja so bila izbrana tako, da se ujemajo z prevladujočim izborom velikih podjetij v raziskavi EITO.*

4.3 Komponente e-poslovanja

Kot smo že omenili, je pojem e-poslovanja razmeroma ohlapen. Kot primer lahko navedemo vprašanje iz raziskave RIS 1999, ko je večina podjetij, ki so trdila, da uporabljajo e-poslovanje, na vprašanje o številu poslovnih partnerjev, s katerimi si izmenjujejo naročila in plačila, navedla, da takih partnerjev nimajo. Natančna podvprašanja so torej najboljša strategija za opredelitev, ali podjetje uporablja e-poslovanje ali ne. V EITO raziskavi je bilo tako eksplicitno navedenih 16 aktivnosti, ki so tudi omogočila natančno sklepanje, ali podjetje uporablja e-poslovanje.

Podoben pristop je običajen tudi na drugih področjih, kjer merimo kompleksne pojave. Tipičen primer je vprašanje zaposlitvenega statusa v raziskavah delovne sile, saj je status brezposelnosti funkcija odgovorov štirih natančnih podvprašanj. Neposredno vprašanje, ali je oseba brezposelna, bi dalo le subjektivno percepcijo respondenta, zato se takega vprašanja sploh ne postavlja.

4.4 Ločevanje e-poslovanja od drugih kategorij

Ob pripravi vprašalnika, ki obravnava e-poslovanje, se običajno pojavijo naslednje dileme:

a) **E- poslovanje in internetno poslovanje.** Jasno je treba ločiti e-poslovanje od ostalih ekonomskih aktivnosti kot npr. internetnega poslovanja ("Internet commerce") ali internetna ekonomija ("Internet economy"). E-poslovanje je namreč le majhen poslovnih aktivnosti, vezanih na Internet[10], zato potrebujemo ostro linijo razločevanje, posebej npr. od internetnega oglaševanja.

b) **E-poslovanje in elektronska pošta.** Ali e-poslovanje vključuje preprosto elektronsko sporočilo (poizvedba, ponudba, komunikacija)? Velika večina opredelitev e-poslovanja bi temu pritrdila, kar pomeni, da praktično vsako podjetje z dostopom do Interneta uporablja tudi e-poslovanje, kar pa morda le ni povsem sprejemljivo.

c) **E-poslovanje in EDI (RIP-računalniška izmenjava podatkov).** EDI ("electronic data interchange") se pogosto obravnava kot jedro e-poslovanja. Z novimi načini, ki omogočajo varne in standardizirane oblike izmenjavanja podatkov prek Interneta, pa se stvari zapletajo. Podjetja namreč danes pospešeno zamenjujejo standardne načine EDI (RIP) z aplikacijami e-poslovanja[11] na Internetu. Posebej težavna so podjetja, ki specifičnega pojma EDI (RIP) ne poznajo, prevod "računalniška izmenjav a podatkov" pa poljudno razlagajo kot vsako izmenjavo podatkov prek omrežij - slednje navaja tretjina slovenskih podjetij. Seveda pa v teh primerih ne gre za formalni proces EDI. Očitno je torej, da bi za jasnejšo razmejitev morali dodati še vrsto dodatnih vprašanj.

d) **E-poslovanje in elektronske finančne transakcije.** Del e-poslovanja, ki je vezan na elektronske finančne transakcije, je posebej občutljiv za tovrstno merjenje, saj se transakcije raztezajo od bančnih ali borznih operacij do številnih oblik elektronskih plačil končnih potrošnikov. V praksi se sicer najpogosteje obravnava prodaja končnim potrošnikom, kar je vsekakor treba ločevati od poslovanja med podjetji ("business-to-business"), ki obsega veliko večino elektronskih transakcij. V tem pogledu je nadvse ilustrativen slovenski primer, kjer tretjina finančnih transakcij med podjetji poteka prek Agencije za plačilni promet (APP) v elektronski obliki na Internetu. Lahko bi torej rekli, da je e-poslovanje že v letu 1998 obsegalo 30 milijard USD. Po drugi strani pa je "resnični" obseg elektronske prodaje končnim kupcem le v rangu nekaj milijonov USD, prav tako pa je majhen tudi "resnični" obseg take prodaje med podjetji.

e) **E-poslovanje: domače ali tuje?** Lokacija telektronskega nakupa je posebej problematična za majhne države. Ko poročamo o končni elektronski prodaji, je zato pomembno razločevati, ali vključuje domače in tudi tuje spletne strani. V Sloveniji je namreč 80% vrednosti takih nakupov izvedenih na tujih spletnih straneh in Amazon.com je npr. imel med slovenskim uporabniki podoben elektronski promet kot vse slovenske knjigarne skupaj.

f) **E-poslovanje in elektronski nakup.** Slovenske banke v letu 1998 niso omogočale elektronskega overovljanja kreditnih kartic, zato "pravih" elektronskih nakupov v letu 1998 ni bilo. Seveda pa respondenti v anketah zagotavljajo, da so v Sloveniji opravili elektronski nakup. V veliki večini gre za naročilo, plačilo po povzetju ali druge načine overovitve kreditne kartice. Pogosto je namreč mogoče prek aplikacije na spletu posredovati kreditno kartico brez varnega strežnika in brez elektronske overovitve. Če pa z elektronskim nakupom razumemo le nakup, ki ga spremlja takojšen in varen prenos ter overovitev - in tako razumevanje je nadvse pogosto - je obseg takih nakupov seveda bistveno zmanjšan.

4.5 Problemi vzorčenja

Pri verjetnostnih in znanstvenih vzorcih lahko kvantificiramo tveganje posploševanja iz vzorca na populacijo. Seveda pa teorija vzorčenja odpove pri neustreznih vzorčnih okvirih, pri veliki stopnji neodgovorov in vselej, ko verjetnosti vključitve v vzorec

[10] *Gre za hardver, softver, aplikacije in številne storitve, ki so povezane z Internetom, npr. (npr. http://www.internetindicators.com/)*

[11] *Med večjimi podjetji v evropskih državah raba EDI še vedno prevladuje nad rabo Interneta, vendar tretjina EDI uporabnikov že zamenjuje EDI z aplikacijami, ki temeljijo na Internetu (EITO, 1999:186).*

niso znane vnaprej. Posebno kritično je to pri anketah, kjer se respondenti v anketo izberejo sami. Tovrstne težave so v sodobnih anketah običajne, zato ne preseneča, da se tudi pri raziskavah o e-poslovanju metodološke podrobnosti redko navajajo. Kadar pa so navedene, pa je pogosto očitno, da visoke stopnje neodgovorov postavljajo pod vprašaj večino ugotovitev (Clemente, 1998).

Napako, ki jo zagrešimo, kadar sklepamo samo na razpoložljivih podatkih, je mogoče povsem enostavno izraziti (Cochran, 1978: 123):

$$D_Y = W_{manjkajoči}(Y_{opazovani} - Y_{manjkajoči}),$$

kjer $W_{manjkajoči}$ predstavlja delež populacije, ki manjka (zaradi nepokritja vzorčnega okvira ali neodgovorov), $Y_{opazovani}$ predstavlja parameter v populaciji, ki se lahko pojavi v našem vzorcu, $Y_{manjkajoči}$ pa predstavlja vrednost parametra med manjkajočimi enotami. Zgornja enačba povsem jasno pokaže, da se npr. pri 40% enot vključenih v vzorec ($W_{manjakjoči} = 0.6$) glavnina razlike med opazovanimi in manjkajočimi podatki prenese v končno napako D_Y.

Kadar ni razlik ($Y_{opazovani} - Y_{manjkajoči}$), je spremenljivka Y robustna in pri takem sklepanju imamo pač srečno naključje, kar pa ne more biti osnova za statistično sklepanje. Obstajajo številni primeri, kjer so razlike med razpoložljivimi in manjkajočimi enotami dramatično velike.

Spomnimo se zgoraj omenjene EITO raziskave, ki je bila izvedena med evropskimi podjetji. Če vseh 70% manjkajočih podjetij (nerespondenti)[12] sploh ne uporablja e-poslovanja, uporablja pa ga 60% anketiranih podjetij (respondentov), je resnični delež samo 18% in ne 60%. Napaka torej znaša $D_y = 60\%-18\% = 42\% = 0.70*(60\%-0\%)$. To je seveda nesprejemljivo in nizka stopnja odgovorov bi resno ogrozila raziskavo. V resnici torej le krhka, tiha, implicitna in nepreverjena predpostavka - namreč, da se nerespondenti ne razlikujejo od respondentov - ohranja zaupanja, da je delež uporabnikov e-poslovanja v resnici 60%.

V anketah o Internetu in e-poslovanju vsekakor lahko pričakujemo, da bodo podjetja, ki uporabljajo tovrstne storitve, pogosteje sodelovala. V letih 1996, 1997 in 1998 smo navedeni problem podrobno opazovali tudi v anketah RIS med podjetji. Nadvse presenetljivo pa se je izkazalo, da se podjetja, ki težje sodelujejo v anketi, bistveno ne razlikujejo od ostalih (Vehovar, Lozar, 1998).

a) V pisemskih anketah RIS-podjetja v letih 1996 in 1997 (n=3.500, standardni TDM postopek s štirimi kontakti) se je odstotek podjetij, ki so imela dostop do Interneta, ustalil že po dveh kontaktih. Razširjena analiza neodgovorov, vključno z primerjavami števila kontaktov in stroškov, pa je pokazala, da sta optimalna dva kontakta.
b) Podobni rezultati izhajajo v letu 1998 v telefonski raziskavi RIS-podjetja (n=1700) z več kot 12 poskusi kontakta[13]. Podjetja, ki so odgovorila po petem poskusu kontaktiranja, se niso v ničemer razlikovala od ostalih. Napake neodgovorov torej za ta pojav niso pomembne. Seveda pa velja upoštevati, da je bila v vseh zgornjih primerih stopnja odgovorov 80% za velika podjetja in 50% za najmanjša. Povsem mogoče je, da bi v primeru nižjih stopenj nastopile večje težave.
c) V letu 1998 smo opazovali tudi razlike pri anketnem merjenju deleža podjetij, ki uporabljajo elektronske transakcije prek Agencije za plačilni promet (APP):

Ali uporabljate elektronske plačilne naloge?
Ali uporabljate Internet za elektronski vpogled v žiro račun?

Tabela 2: Odstotek podjetij, ki uporabljajo e-poslovanje z APP

E-poslovanje,	Anketa RIS, (Dec, 98)		Administrativni podatki (Maj, 99)
Vpogled v račune	Uporabljajo	Nameravajo v roku 12 mesecev	Uporabljajo
Velika podjetja	45	16	44
Srednja podjetja	31	19	35
Mala podjetja	22	12	16
Elektronske transakcije			
Velika podjetja	27	29	31
Srednja podjetja	19	26	25
Mala podjetja	16	13	8

Primerjava je sicer otežena z različnimi problemi[14], kljub temu lahko razberemo osnovno sporočilo: pri velikih in srednjih podjetjih je bilo precenjevanje v decembrski anketi RIS minimalno, čeprav je nedvomno obstajalo. Večje so težave pri majhnih podjetjih. Dodati velja, da je med velikimi[15] podjetji odgovorilo 80% enot (srednja 70%, mala 55%). Z naraščanjem števila manjkajočih enot torej narašča tudi napaka. Domnevamo lahko, da raziskave s stopnjo odgovorov, ki je več kot polovico manjša od zgornje raziskave[16] - kar je za večino komercialnih raziskav povsem običajno - pomenijo potencialno nevarnost za precenjevanje pojavov s področja e-poslovanja.

[12] *Število neodgovorov je težko natančno izračunati zaradi uporabe kvot, vendar je od 3241 enot odgovorilo le 570.*
[13] *Celotno poročilo RIS98-podjetja je na Internetu - http://www.ris.org/ris98/podjetja/.*
[14] *Podatki APP so na nivoju Slovenije agregirani za vsa podjetja, po velikostni strukturi pa razpolagamo le s podatki za ljubljansko podružnico. Na osnovi razmerij v anketi RIS 98 in RIS97 pa so bile izdelane ocene tudi za celo Slovenijo.*

Po drugi strani pa zgornji rezultati kažejo na določeno robustnost pojavov e-poslovanja za problem manjkajočih odgovorov, vsaj med večjimi podjetji, kjer je delež manjkajočih enot manjši od 30%.

4.6 Učinki načina raziskovanja

Spremljanje e-poslovanja lahko izvajamo tudi v samoizbranih anketah, ki potekajo preko svetovnega spleta (WWW). Le-te so posebej občutljive na proces samoizbire, saj delež manjkajočih enot običajno presega W = 0.9. Kljub temu najnovejše raziskave[17] kažejo, da so - z izjemo nekaterih redkih vsebin - razlike med respondenti in nerespondenti majhne.

V telefonski anketi med uporabniki Interneta (RIS98) ter v anketi po svetovnem spletu, obe sta potekali v obdobju julij – september, smo postavili vprašanje o obsegu elektronske potrošnje v zadnjih 12 mesecih. Rezultati v tem pogledu ne kažejo (Tabela 3) razlik med telefonsko in anketo po WWW, kažejo pa na razhajanja v oceni deleža uporabnikov, ki so tak nakup opravili. Razlike so pričakovane in nastajajo zaradi večje intenzivnosti uporabe Interneta med respondenti v WWW anketi. Razlika torej izhaja iz izbora vzorca in ne zaradi načina anketiranja.

Tabela 3: Primerjava rezultatov telefonske in WWW ankete (RIS, 1998).

	Telefonska anketa	WWW anketa
Nakup prek Interneta	10 %	20 %
Povprečna porabljena vsota	150 US$	155 US$

Podobna zakonitost se kaže tudi pri drugih spremenljivkah, zato lahko povzamemo, da so ankete po WWW primerne za analizo značilnosti in odnosov znotraj e-poslovanja, niso pa primerne za oceno populacijskih agregatov.

5. Zaključek

E-poslovanje je za moderne družbe izjemno pomembno, saj transformacija administrativnih in finančnih transakcij v poslovanje brez papirjev napreduje z velikimi koraki. Zaradi dinamičnosti, kompleksnosti in raznolikosti teh procesov bo anketno in kvalitativno merjenje postajalo na tem področju vse bolj pomembno.

Povzamemo lahko tudi naslednje:

- Merjenje informacijske družbe postaja vedno bolj zapleteno, kar velja tudi za e-poslovanje. Zaradi hitrosti nastajanja pojavov in zaradi dinamike njihovega spreminjanja se vloga uradnih statistik na tem področju hitro manjša. Namesto njih vstopajo globalne korporacije, ki pa kvalitete in poslanstva uradnih statistik ne morejo nadomestiti. Potreba po izrazitejši mednarodni koordinaciji vladnih organizacij je zato vse bolj opazna.
- Pri merjenju e-poslovanja je posebej pomemben problem enotnih opredelitev. Ne obstaja samo potreba po standardiziranih definicijah, ampak predvsem po permanentnem mehanizmu, ki bo vzpostavljal in posredoval enotne usmeritve pri razumevanju temeljnih pojmov na tem področju.
- Obstoječi metodološki standardi anketnega raziskovanja se morajo upoštevati tudi na področju e-poslovanja. Pogosto to ni izvedljivo zaradi kratkega časa, ki je na voljo za izvedbo raziskave, ali zaradi same narave teh raziskav. V takem primeru so rezultati seveda nadvse vprašljivi.
- Empirični rezultati kažejo, da so spremenljivke povezane z e-poslovanjem razmeroma neobčutljive za manjkajoče podatke, vsaj pri proučevanju značilnosti podskupin, in celo pri ocenjevanju agregatov, kadar delež manjkajočih podatkov ne presega tretjine enot.

6. Literatura

Braunstein, Y.M. (1985): Information as a Factor of Production: Substituability and Productivity. The *Information Society 3(3): 261-273.*

Clemente P. (1998): The state of the net. New York: McGraw-Hill.

Cochran (1978): Sampling techniques. New York: Wiley.

EITO (1999), European Information Technology Outlook. Manheim: EITO.

Gartner, http://ww w.gartnergroup.com.

Gričar Jože (1998): Electronic Commerce Implementation in a Country Developing a Market Economy - http://ecom.fov.uni-mb.si/predstavitve/IST98-ok.doc.

Hayes, R.M. & T.Erickson (1982): Added Value As a Function of Purchases of Information Services. *The Information Society 1:307-338.*

IDC, http://www.idc.com.

ISPO, http://www.ispo.cec.be.

Network Wizzard, http://www.ne.com.

NUA, http://www.nua.ie.

Katz, R. L. (1986): Measurement and Cross National Comparisons of the Information Work Force. *The Information Society 4(4):231-277.*

Machlup, F. (1962). *The Production and Distribution of Knowledge in the United States.* New Jersey: Princeton University Press.

MIDS, http://www.mids.org.

Porat, M.U. (1977): *The Information Economy: Definition and Measurement.* US Office of Technology Special Publication 77-12(1). Washington, DC: Department of Commerce.

RIPE, http://www.ripe.net/.

RIS, http://www.ris.org.

Rubin, M.R., Huber, M.T. (1986). *The Knowledge Industry in the United States 1960-1980.* New Jersey: Princeton University Press.

Vehovar, V., Lozar, K. (1998): How many mailings are enough? In Koch, Achim and Porst Rolf (eds.). *Nonresponse in survey research,* (Nachrichten spezial, No. 4). Mannheim, Germany: Zentrum für Umfragen, Methoden und Analysen.

---

[15] *Odgovorilo je 316 enot med velikimi podjetji (več kot 250 zaposlenih), 542 med srednjimi podjetji (50 – 250 zaposlenih) in 867 med majhnimi podjetji (pod 50 zaposlenih).*

[16] *V raziskavi RIS so bili izvedeni posebni napori, da bi dobili visoko stopnjo sodelovanja: osebna pisemska vabila, več kot 12 ponovnih klicev, javna objava rezultatov, pošiljanje rezultatov prejšnjih raziskav.*

[17] *Značilno je, da tovrstne raziskave potekajo predvsem med marketinškimi organizacijami, npr.* ***http://www.ama.org/conf/artforum/99/)***

REVIZIJA INFORMACIJSKIH SISTEMOV, KOT PRISPEVEK K NJIHOVI USPEŠNOSTI IN UČINKOVITOSTI

Boža Javornik, CISA, Nova Ljubljanska banka d.d.

V vedno hitreje se spreminjajočem okolju finančnih storitev ima informacijska tehnologija vedno večjo vlogo. Velika in pomembna tveganja povezana z njeno uporabo morajo iskati ravnotežje z izjemnimi priložnostmi.

V sedanjem času sta pomembna ključna faktorja uspeha podjetij dostop do kapitala in trgov. Uspešnosti pri tem ni mogoče zagotavljati brez ustrezne izrabe informacijske tehnologije. Razpoložljivost in transparentnost informacij omogočata potencialnim investitorjem oceniti podjetje in ustrezno varno naložiti svoje viške sredstev, potencialnim poslovnim partnerjem transparentna informacija zagotavlja jamstvo dolgoročne uspešnosti poslovnih povezav. Vsako spreminjanje informacij in podatkov v smislu sprememb pričakovanih velikosti in odnosov, ki pomenijo osnovo vrednotenja podjetja za investitorje in poslovne partnerje, lahko pomeni vzrok za pomembno poslabšanje dostopnosti kapitala in stabilnosti odnosov z dobavitelji in kupci.

Upravljanje poslovnih sistemov postopoma postaja sistem spreminjajočega se okvira pravil, ki v določenem smislu pomeni načine obnašanja in reagiranja na spremembe v okolju in sistemu samem. Informacijski sistemi že dlje časa izgubljajo svojo zgolj evidenčno funkcijo in njihova vrednost postaja v sposobnosti zgodnjega odkrivanja indikatorjev neprijetnih dogodkov in njihove predstavitve. Tradicionalni mehanizmi kontroliranja aktivnosti v smislu preprečevanja "neprijetnih posledic" neustreznega ali celo nezakonitega delovanja niso več aktualni. Pritiski na zniževanje stroškov administriranja, kamor sodijo stroški kontroliranja, hoteli ali ne, so prisilili snovalce informacijskih sistemov, da kontrole avtomatizirajo, neprimerne za avtomatizacijo pa so lahko celo izginile. Avtomatizirane oblike kontrol so z integracijo posamičnih poslovnih aplikacij v "integrirane informacijske sisteme" izgubile prvotno obliko, njihova transformacija je bila povezana z (ne)združljivostjo z informacijsko tehnologijo in načinom njene izrabe. Redko je bilo pri transformaciji obravnavano tveganje, ki naj bi ga kontrola v osnovi preprečevala ali minimizirala posledice neprijetnih dogodkov v povezavi z njim. Razvoj družbenih odnosov je v upravljanje poslovnih sistemov prinesel še dejstvo, da ni potrebno poslovati zgolj uspešno in učinkovito. Upravljanje s poslovnimi sistemi zahteva, da so upoštevana etična načela nekega okolja ali celo širše skupnosti. Baselska načela varnega poslovanja bank v svoji osnovi ne pomenijo drugega kot prisilo ali vsakodnevni opomin bančnikom, da ne pozabijo skrbno ravnati s prihranki posameznikov, ki so jih jim zaupali.

Upravljalci poslovnih sistemov se vedno bolj zavedajo odvisnosti uspešnosti in učinkovitosti od razpoložljivosti informacijskega sistema. Male nočne more postajajo zgodbe, ki so se zgodile drugim: požar v računskem centru, izguba podatkov zaradi tehnične okvare, nočni klici izsiljevanja povezani z izgubo podatkov ali razkritjem skrivnosti, milijoni dolarjev vloženi v razvojne projekte v povezavi z informacijsko tehnologijo brez pravega jamstva, da bodo pričakovani učinki prihrankov oz. zaslužkov ob novih priložnostih dejansko doseženi, ali pa vsa vlaganja morda pomenijo le preživetje. Ravnateljstva morajo prepričati delničarje in poslovne partnerje, da obvladujejo poslovanje in to ne le danes ampak tudi za prihodnost. Podjetje obvladuje informacijski sistem, če uspe iz podatkov pridobiti kvalitetnejša znanja hitreje kot konkurenca. Izvršni vodje morajo imeti na razpolago podatke za načrtovanje poslovanja in ukrepanja ob spremljajočih se pogojih v okolju.

Jasno je, da kontroliranje informacijskih sistemov že dolgo ne pomeni več zagotavljanje varnosti procesiranja in zaščite pred razkritjem, vedno večji del kontrol je usmerjen k razpoložljivosti sistema, njegovi učinkovitosti in uspešnosti. Način poslovanja v smislu odvisnosti od uporabe informacijske tehnologije vedno bolj zahteva, da se informacijski sistem obravnava kot osnovna in ne podporna dejavnost. Cilji poslovanja so vedno pogosteje lahko doseženi le, če so podprti z uspešnim in učinkovitim informacijskim sistemom. Avtomatizacija poslovnih procesov in elektronsko izmenjavanje podatkov imata za posledico, da je analiziranje poslovnih procesov vedno težje, vedno manj je možnosti, da bi brez informacijskega znanja bilo mogoče razumeti, kako so oblikovane kontrole, še težje pa je preverjati, ali delujejo. Tveganja povezana s poslovanjem morajo biti jasno opredeljena v smislu materializiranih posledic neprijetnih dogodkov, da je mogoče pri oblikovanju rešitev informacijskega sistema oceniti, katere kontrole so potrebne in zadostne, da so tveganja minizirana na še sprejemljivi nivo. Poslovni

sistemi si preprosto ne morejo privoščiti preveč oz. prekrivajočih se kontrol.

Odgovornosti nadzornih svetov, uprav, izvršnih direktorjev so se zaostrile, zato so njihove zahteve do revizorjev računovodskih izkazov in notranjih revizorjev bolj določene v smislu večje zanesljivosti trditev, zahtevajo visok nivo profesionalnega ocenjevanja. Zaradi kompleksnosti vprašanja varnega ravnanja z informacijskim sistemom, njegovo uspešnostjo in učinkovitostjo, zagotavljanjem zakonitosti in preprečevanjem prevar, je potreba po profesionalni oceni kontrolnih sistemov in rešitev informacijskega sistema na sploh, vedno bolj izoblikovala vlogo revizorja informacijskih sistemov pri tem. Omenjeni proces je na drugi strani izoblikoval širino znanj, ki jih revizor informacijskih sistemov potrebuje, kot tudi potrebo po izdelavi primerjalnega okvira dobrega obvladovanja informacijskega sistema.

Mednarodna organizacija revizorjev informacijskih sistemov (Information System Audit and Control Association - ISACA) se tega že dlje časa zaveda. V sredini 90-tih let je raziskovalna organizacija tega združenja pričela z izdelavo okvira kontroliranja informacijskih sistemov. V letu 1996 je bila tako izdana prva, v letu 1998 pa že druga izpopolnjena izdaja COBIT-a (Governance, Control and Audit for Information and Related Technology). Namen izdelave serije petih priročnikov Cobit-a je bil raziskati, razviti, dokumentirati in promovirati mednarodno priznan, kvaliteten, z zadnjimi dosežki izpopolnjen in široko sprejemljiv okvir kontroliranja informacijske tehnologije, namenjen tako upravljalcem poslovnih procesov kot profesionalcem s področja informatike in revizorjem. Pristopi kontroliranja so v priročnikih predstavljeni nivojsko, glede na ciljno skupino bralcev: od ravnateljev do odgovornih za varno ravnanje s posameznimi elementi informacijskih sistemov. Na osnovi tveganj, ki so povezana z uporabo informacijske tehnologije, je grobo predstavljena dobra praksa varnega ravnanja in pa napotki, kako naj revizor to preveri.

Revizorji informacijskih sistemov, kot odgovorni za informacijske sisteme v velikih poslovnih sistemih, so priročnike ugodno sprejeli in tako z njihovimi prizadevanji nastajajo še podrobnejši in bolj praktični okviri obvladovanja posameznih tehnologij (strežnik - odjemalec, obvladovanje reševanja skladnosti za leto 2000 za menedžerje, Y2K - načrtovanje dela brez prekinitve ..).

Drugo dejstvo, ki kaže na to, da potreba po reviziji informacijskih sistemov narašča, je, da se pomembno spreminjajo vsebine znanj, ki bi jih morali obvladati revizorji računovodskih izkazov in računovodski ter finančni strokovnjaki na sploh. Podobno velja za interne revizorje. Da se je obseg revidiranja informacijskih sistemov močno povečal, kaže tudi dejstvo, da je inciativa za prenovo standardov revidiranja informacijskih sistemov pokazala ne le, da je potrebno standarde prenoviti, temveč, da je potrebno izdelati nekatere nove standarde, kot tudi, da je za posamične segmente tehnologij potrebno izdelati smernice revidiranja. Da spremembe standardov niso le kozmetične narave, kaže tudi dejstvo, da je npr. besedilo smernice Vplivi revizorjevega vključevanja v pridobivanje in uvajanje po prvi objavi za obravnavo pri članstvu narastlo za 6 krat. Trenutno je dokončanih, v javni obravnavi ali pa so še v strokovni dodelavi več kot 30 smernic.

Revizija informacijskih sistemov obsega tako revizijo splošnih kontrol varnega ravnanja s podatki, kot tudi revizijo uspešnosti in učinkovitosti posameznih rešitev podpor poslovnih sistemov. V sklopu preverjanja delovanja splošnih kontrol je mogoče kot primerjalni okvir upoštevati Slovenski standard varnega ravnanja s podatki (prevod angleškega standarda BS 7799) ali COBIT. Preverjanje varnih, uspešnih in učinkovitih uporab informacijske tehnologije v poslovnih procesih pa zahteva ustrezno razumevanje in poznavanje tveganj poslovanja, metod prepoznavanja in zgodnjega odkrivanja indikatorjev prisotnosti tveganj in v povezavi s tem sposobnosti presojanja, kaj je priporočljiva dobra praksa pri uporabi informacijske tehnologije in kako so oblikovane uspešne in učinkovite kontrole za omejevanje posledic tveganj pri poslovanju.

Rešitve v posameznih poslovnih procesih niso enake, za nekatere velja, da je ključno, da so sistemi na razpolago brez časovnih zakasnitev, drugje je spet pomembno, da je zagotovljeno vse, da ni mogoče nepooblaščeno pridobiti podatkov in jih razkriti, pri nekaterih sistemih je pomembno, da so postavljeni tako, da omejujejo prevare. Od računovodskih sistemov zahtevamo njihovo preglednost, sledljivost sprememb, popolnost in točnost podatkov in pa zagotavljanje varnosti pred izgubo podatkov; uporaba prekrivanja vrednosti podatkov je najstrožje prepovedana.

Revizija informacijskih sistemov ni oblika kontrole kakovosti v smislu ocenjevanja dobrih računalniških rešitev (certificiranja). Posamezno rešitev obravnava v okolju poslovanja, zato je isto programsko rešitev mogoče nekje oceniti kot ne tvegano, v drugem okolju pa kot izjemno tvegano, pač odvisno kolikšen vpliv na poslovanje (zagotavljanja finančnega rezultata ali zakonitosti poslovanja) ima del poslovanja, ki jo rešitev podpira. Pristopi pri revidiranju se razlikujejo tudi od okolja: manjši poslovni sistemi imajo lahko enostavnejše rešitve, ki jih obvladuje peščica posameznikov in je seveda lahko ekonomsko neopravičljivo vztrajanje na določenih standardih dobre prakse; drugačne so rešitve povezane z varnim ravnanjem s podatki v primerih servisnih storitev; najzahtevnejši in najkompleksnejši pa so sistemi kontrol obvladovanja tveganj pri velikih

poslovnih sistemih z najraznovrstnejšo uporabljeno informacijsko tehnologijo in visokimi zahtevami razpoložljivosti informacijskega sistema.

Kako lahko ravnateljstvom pomaga revizija informacijskih sistemov?

Nezadostno razumevanje možnosti in načinov uporabe informacijske tehnologije ne omogoča enostavnega odgovora, ali se naložbe v informacijsko tehnologijo vračajo z rezultati poslovanja. Ravnateljstva si zastavljajo vprašanja, ali morda ni nevarnosti, da nekega lepega jutra sistem preprosto ne bo deloval in ga ne bo mogoče vzpostaviti dlje časa in ali sploh podjetje zmore poslovati brez informacijske podpore, oz. so posledice tega lahko omejene. Na podobna vprašanja jim lahko pomagajo najti odgovor revizorji informacijskih sistemov. Res je, lahko bi jim dali odgovor tudi odgovorni sodelavci v organizacijskih enotah informatike - računskih centrih, obstajata le vprašanji: ali se more in ali se je modro zanesti na tak odgovor. V primeru računovodskih izkazov bi bila dilema lahko podobna - mnenje o računodskih izkazih bi podali računovodje, vendar sta se lastnik in v določenem smislu tudi država odločila drugače. ■

EVROPSKI IN DOMAČI VIDIKI ELEKTRONSKEGA POSLOVANJA

Aljoša Domijan

Okrogle mize na temo elektronskega poslovanja na DSI 99 so se udeležili Aaron Marko, direktor Microsoft d.o.o, kot predstavnik ponudnika programske opreme za izvedbo elektronske trgovine, Zoran Thaler, direktor EON d.o.o., kot predstavnik ponudnika varnega poslovanja na Internetu, dr. Dušan Caf kot predstavnik GZS ter Aljoša Domijan, direktor Gambit trade d.o.o., kot vodja okrogle mize in predstavnik sistemske hiše, ki ponuja izdelavo zasnove, izvedbo in vzdrževanje elektronskih trgovin.

Letos smo med publiko prvič zasledili tudi predstavnike podjetij, ki so z odprtjem elektronskih trgovin razširila svojo ponudbo in se približala tudi kupcem na svetovnem spletu. V razpravi smo se osredotočili predvsem na izvedbeni del in delitev nalog med ponudniki komunikacijske infrastrukture, ponudniki varnih transakcij, bankami, trgovci in nenazadnje kupci. Ugotovili smo, da je Slovenija tik pred tem, da elektronsko trgovanje postane del našega vsakdana, saj smo bili v primerjavi z DSI 98, ko so referenti govorili predvsem o varnosti in teoriji elektronskega poslovanja, letos zelo konkretni. Na DSI 2000 pa bomo zagotovo že govorili o izkušnjah in razlogih za uspeh najuspešnejših domačih e-trgovcev.

1. UVOD

Pred leti se je Jeff Bezos, ustanovitelj podjetja Amazon.com uprl takratni splošni prodajni logiki, ki je govorila, da je pot do uspešne elektronske prodaje v ponujanju kvalitetnih produktov z visoko vrednostjo, in pričel s prodajo knjig na internetu. Takrat je bila večina ljudi mnenja, da je cena edino, kar je pomembno. A Buzon je menil drugače. Razmišljal je v smeri, da je uspeh prodaje preko interneta v informiranosti potencialnih kupcev. Najrevolucionarnejši vidik prodaje preko interneta je bil in je še vedno ta, da potencialni kupec, ki se "oglasi" v virtualni trgovini, najde nekaj zase. Le tako bo ponudnik produkt oz. storitev tudi prodal.

Jeff Bezos je danes lastnik najbolj znane trgovine na internetu s ponudbo več kot 3 milijone naslovov knjig in pol milijarde dolarjev prometa, s podružnico v Evropi in z izredno hitro rastjo vrednosti delnic. Jeff Bezos je seveda Američan. Zdi se, da v Evropi ne bi mel nobenih možnosti, da Slovenije niti ne omenjamo. In vendarle, Bezos ni odkril ničesar novega! Ista tehnologija je na voljo tudi v Sloveniji in Evropi. In čeprav Evropejci preko svetovnega spleta kupujejo vse več in večino denarja potrošijo na spletnih straneh ameriških podjetij, se zdi, da Evropa še vedno ni našla pravega odgovora. Ali ga sploh lahko?

2. EVROPSKE ZAVORE

Ko primerjamo trgovanje preko interneta v Ameriki in Evropi, ne moremo mimo dejstva, da je ameriški trg večji. Izreden uspeh Amazon.com, kateremu nikakor ne gre oporekati, je v veliki meri tudi posledica velikega trga. Dosežki drugih dveh uspešnih ameriških podjetij s svojima elektronskima trgovinama Gap.com (oblačila) in Dell.com (računalniki) kažejo, da gre kljub

velikim vsotam le za nekaj odsotkov njune »klasične« prodaje. In te vsote postanejo majhne celo v Evropski skupnosti kot enotnem trgu, kaj šele v posameznih državah.

Pri prodaji preko interneta vidimo cel svet kot enotno tržišče. Vendar pa je v resnici trg poln ovir imenovanih carine in davki. Američani imajo državni davčni sistem, ki je zelo podoben trenutno veljavnemu pri nas, Evropa pa DDV. In prav DDV ni primeren za trgovanje po internetu. Pripada namreč državi v kateri je registriran sedež prodajalca in ne državi v kateri je trenutno kupec ali prodajni strežnik. Večina trgovin je zato trenutno v ZDA, ki imajo primernejši sistem obdavčevanja. EU tako izgublja posel in denar. Zato se tudi želi dogovarjati! Američanom se seveda ne mudi, saj se medtem, ko se politiki pogovarjajo, vse več evropskih podjetij s svojimi elektronskimi trgovinami seli v ZDA. V EU se tega zavedajo in že iščejo rešitve oziroma izhodišča za boljšo pogajalsko pozicijo z Američani. Trenutno predvsem v smeri iskanja možnosti hitrejšega vračanja obračunanih davkov za na internetu kupljeno in izvoženo blago.

Dejstvo je, da je elektronsko trgovanje tudi v svetovnih razmerah šele na začetku. Američani so se odločili za liberalen pristop in nameravajo zakonodajo prilagoditi razmeram. Ena izmed posledic takega pristopa je tudi sodni spopad med Microsoft Internet Explorerjem in Netscape Navigatorjem. Evropa se želi izogniti sprotnemu reševanju težav in predhodno določiti ustrezno zakonodajo za področje elektronskega podpisa, elektronskega ključa, elektronskega notarijata, zaščite podatkov, varovanja osebnih podatkov ter podpisati ustrezne meddržavne pogodbe, ki bodo urejale trgovanje preko interneta. Svoj strokovni prispevek k izboljšanju razmer na internetu vidi EU predvsem v izdelavi ustreznih matematičnih algoritmov za kodiranje podatkov.

3. E-SLOVENIJA

Kljub izredno dobro razširjeni uporabi interneta je pregled .si domačih strani konec februarja 1999 pokazal, da ne premoremo niti ene prave elektronske trgovine. No, pico lahko naročimo na dom. Na svetovnem spletu se predstavljamo s predstavitvenimi stranmi in nekaj možnostmi naročanja predstavljenega blaga. Prave elektronske trgovine, v kateri blago izbereš, varno plačaš s kreditno kartico in nato samo še počakaš, da ti ga dostavijo na dom, pri nas še ni.

Zakonodaje, ki bi urejala elektronsko trgovanje, nimamo. Elektronski podpis ni pravno veljaven. Prav tako nimamo strežnikov za identifikacijo uporabnikov in strežnikov za potrjevanje plačila s kreditnimi karticami. Medbančni promet ni urejen. Poleg navedb, da je slovenski trg majhen in je število uporabnikov interneta pri nas majhno, so to najpogostejši vzroki, katere podjetniki navajajo kot razlog, zakaj se ne odločijo za prodajo preko interneta. Ali je to res?

Trditev: »*Uvedba elektronskega trgovanja v podjetje je poseg v organizacijsko strukturo podjetja, v logistiko podjetja in spreminja način razmišljanja podjetja kot organizacije. Povzroča velike premike, tako pri izrabi poslovnih možnosti kot pri racionalizaciji poslovanja in relativnem nižanju stroškov*«, zagotovo drži in v sebi skriva nekaj osnovnih razlogov naše zadržanosti pred elektronskim poslovanjem.

Pri prodaji preko elektronske trgovine je potrebno dobro poznati kupce, njihove potrebe in navade. Čeprav namreč ponudimo blago naprodaj le slovenskim sprehajalcem po svetovnem spletu, je doseg naše ponudbe s trenutkom objave precej večji kot pa doseg klasične trgovine. Ker pa kupci na svetovnem spletu pričakujejo hitro dobavo, morajo biti že ob objavi na voljo ustrezne zaloge. Elektronsko trgovino, ki ima zamude z dostavo blaga, bomo kmalu zaprli. V primeru viškov zalog pa nas čakajo poslovne težave. Rizik za domače podjetnike je očitno prevelik, sredstev za predhodno strokovno analizo trga pa premalo.

Seveda ni dovolj, da imamo blago le na zalogi. Potrebno ga je tudi dostaviti. V ZDA je ponudba izvajalcev izredno pestra, ponudniki pa so zelo zanesljivi in prilagodljivi. Delajo 24 ur na dan. Ne zamujajo in so pripravljeni plačati ustrezne pogodbene kazni za vsako zamudo. Nezadovoljen kupec je pač v državi, ki skrbi za potrošnika, draga stvar. Ponudba podjetij za dostavo pri nas zagotavlja dostavo na dom v 24 urah v normalnih pogojih. Kaj pa v primeru, ko se število naročil v času Božiča izredno poveča.

Odločitev za prodajo preko meje se bo zagotovo ustavila na naši meji. Še nikoli se namreč ni zgodilo, da bi nekdo iz Slovenije prodal večjo količino izdelkov množici različnih kupcev po svetu. Carina tako preprosto ni pripravljena na tak dogodek in vsak, ki bi se tega podviga rad lotil, se bo moral najprej dogovoriti z ustreznimi predstavniki državne administracije in si izposlovati nekaj ugodnosti. Sicer se bo moral sprijazniti z zamudami pri carinjenju.

Stroški kršitve pogodbe o poslovnem sodelovanju pri nas so praviloma nizki. Razširjeno je mnenje, da jih ni potrebno plačevati, saj naj bi bile kršitve v večini primerov posledica nepredvidenih vzrokov. Uspeh na sodišču je nepredvidljiv. Tako ostane celoten rizik na ponudniku elektronske trgovine. Le tega trgovec vračuna v ceno izdelka in nakup postane zaradi previsoke cene nezanimiv. Zveni znano?

Tudi prodajalec mora blago kupiti. Tako postane odvisen od svojega dobavitelja. Dobavitelj mora zagotoviti sprotne dobave, najugodnejše cene in vse

potrebne informacije kot pomoč pri prodaji. Trgovca mora obveščati o vseh spremembah, predvsem pa o ukinitvi in uvajanju novih prodajnih programov. V nasprotnem primeru bo končnemu uporabniku na voljo napačna informacija, ponudniku pa ostane le še spor z dobaviteljem. In z razgovori na sodišču zagotovo ne bosta prišla do uspešne prodaje.

Potrebujemo tudi ustrezno informacijsko podporo. Večina dogodkov v elektronski trgovini poteka avtomatično. Vsi dokumenti so v elektronski obliki in jih izdelajo računalniki. Veliko število kupcev, artiklov in dobaviteljev obenem z velikim številom poslovnih dogodkov zahteva vnaprej pripravljeno organizacijsko shemo podjetja, določene procese v podjetju, urejen pretok dokumentov in arhiviranje vseh zapisov o poslovnih dogodkih. Investicija v informacijsko opremo je neizogibna in sorazmerno visoka.

In nenazadnje potrebujemo tudi ustrezno omrežje, ki omogoča hiter in cenen prenos podatkov. V ZDA so tudi na tem področju daleč pred Evropo. Slovenci kljub vsemu raje lovimo Evropo, tako s številom hitrih ISDN priključkov kot s ceno. Državna administracija pa nič, kot bi se ne zavedala, da je prav široka dostopnost javnega komunikacijskega omrežja predpogoj za razvoj elektronskega trgovanja.

4. ZAKLJUČEK

EU je sprožila široko akcijo za popularizacijo uporabe informacijske tehnologije v malih in srednje velikih podjetjih, kot okoljih, ki s svojo pestrostjo in prilagodljivostjo edina lahko pospešijo zbliževanje z ZDA. Obenem je s spremembo zakonodaje omogočila privatizacijo sicer državnih telekomunikacijskih ponudnikov in dovolila tujim podjetjem ponudnikom internet in telekomunikacijskih storitev vstop na svoj trg.

Tudi pri nas je tako dela za podjetnike, ponudnike internetnih storitev in državno administracijo več kot dovolj. Ali lahko v naslednjem letu pričakujemo, da bodo vsak zase opravili svojo nalogo in Slovenijo zapisali med države z okoljem, naklonjenim elektronskemu trgovanju. Mogoče pa bi bila za druga evropska podjetja končnica .si lahko zanimivejša kot .com. ■

NAJBOLJŠE PROGRAMSKE REŠITVE IN PRAVI IZVAJALCI ?

(Teze in ugotovitve okrogle mize)

Andrej Kovačič, Ekonomska fakulteta, Ljubljana

UVOD

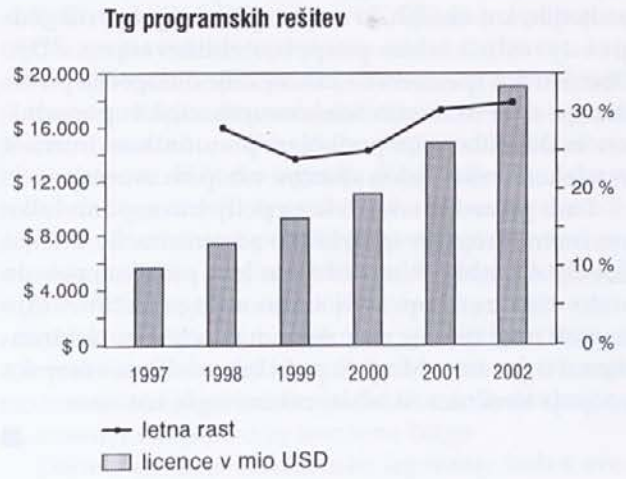
Okrogla miza z naslovom "Izbira najboljšega ali pravega izvajalca", ki se je odvijala v okviru posvetovanja Dnevi slovenske informatike – Portorož '99, je načela in obravnavala niz problemov, s katerimi se spopadajo organizacije ob uporabi sodobne informacijske tehnologije in prehodu na nove celovite programske rešitve. Svoje poglede na obravnavano problematiko so poleg vodje okrogle mize (dr. Andrej Kovačič) podali tudi drugi panelisti. Njihova stališča so bila seveda po pričakovanjih v veliki meri različna, saj so zastopali poglede uporabnikov rešitev oziroma naročnikov (g. Denis Stepančič, Gradbeno podjetje Grosuplje), domačih razvijalcev in ponudnikov (dr. Ivan Vezočnik, Razvojni center Celje) ter ponudnikov tujih rešitev (g. Stanislav Klešnik, Intertrade ITS, ki zastopa firmo Baan).

Udeleženci so se strinjali z večino tez, ki so bile kot izhodišče razprave predhodno izoblikovane in predstavljene, izoblikovali pa so tudi svoja stališča in razmišljanja o problematiki, ki je v našem okolju še zlasti pereča in vse bolj prisotna. Ugotovili so, da v začetni fazi, ko obravnavamo možne scenarije in dileme prehoda, naletimo na eni strani na potrebo po presoji odločitev o razvoju ali nakupu oziroma primernosti razpoložljivih programskih rešitev, na drugi strani pa o primernosti razvijalcev ali uvajalcev teh rešitev.

1. IZHODIŠČA

Mnogi ocenjujejo, da prehajamo v obdobje, ki ga bo zaznamoval trg celovitih programskih rešitev in nanje vezanih storitev uvajanja, vzdrževanja in nadgrajevanja. V letu 1997 je bil na tem trgu ustvarjen promet v višini 300 milijard ameriških dolarjev. Brez posebnih špekulacij ocenjujemo, da se bo ta obseg v letu 2002 podvojil [1]. Prihodki od prodanih licenc programskih

rešitev in nanje vezanih rešitev skokovito naraščajo (slika 1, vir: GartnerGroup, 1998). Velike svetovalne hiše, ki se brez izjeme vse bolj uveljavljajo tudi kot neodvisni sistemski integratorji, ugotavljajo naraščanje deleža prihodka, ki ga ustvarijo z uvajanjem rešitev. Le-ta v večini primerov znaša med 20 in 30 odstotkov celotnega prihodka.



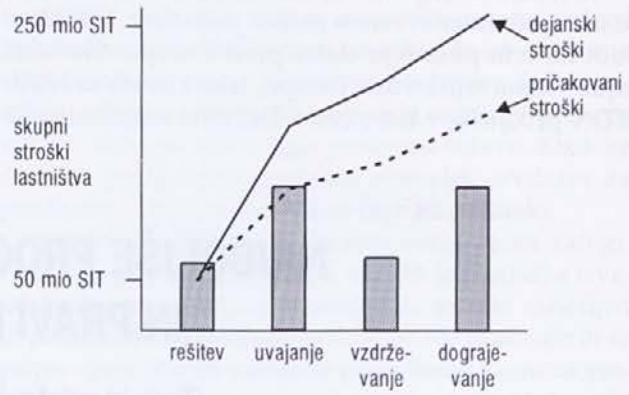
Slika 1: Trg programskih rešitev

Dilema o nakupu ali lastnem razvoju programske rešitve ostaja. Prednosti in slabosti nakupa že izdelanih rešitev so znane v literaturi in vsakdanji praksi [2]. Velja, da z nakupom lahko močno skrajšamo čas razvoja in znižamo nivo tveganja o ustreznosti končnega rezultata, ki smo mu priča pri lastnem razvoju. Pridobimo tudi morebitna tuja (praktična) znanja z obravnavanega poslovnega področja, ki jih vsebujejo kakovostne uporabniške programske rešitve. Slabosti nakupa se kažejo v relativno visoki ceni nakupa in osnovnega prilagajanja rešitev. Še bolj pa se poudarijo skozi problematiko uvajanja oziroma prilagajanja informacijskim potrebam uporabnikov in prenosu vseh znanj, potrebnih za vzdrževanje in nadaljni razvoj, na informatike v podjetju. Vseeno nekateri napovedujejo, da se bo delež "doma razvitih" rešitev na svetovni ravni znižal s sedanjih 33 % na 25 % v letu 2002.

Odločitev o nakupu rešitev se lahko izvede le na osnovi podrobno opredeljenih ter z modelom podatkov formaliziranih in prikazanih informacijskih potreb izvajanja postopkov znotraj poslovnega procesa. Velja pravilo, da je ob normalnih tržnih pogojih smotrna odločitev o nakupu v primeru, da aplikativna rešitev pokriva vsaj 80% informacijskih potreb obravnavanega področja. Z normalnimi pogoji mislimo, ob ustrezni ceni tudi razpoložljivost ustreznih rešitev v izvorni obliki in pripravljenost ponudnika za sodelovanje pri uvedbi in prilagajanju rešitve.

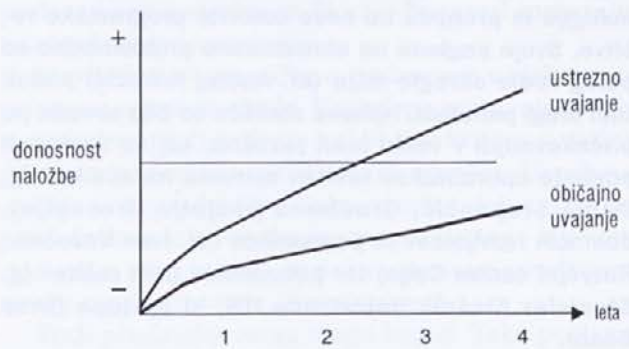
2. VZROKI IN POSLEDICE NEUSTREZNEGA UVAJANJA PROGRAMSKIH PROIZVODOV

Ocena o ustreznosti odločitve o nakupu programske rešitve nikakor ni enostavna. Nikakor je ne smemo prepustiti le bodočim uporabnikom. V primeru, da gre za obsežnejši sklop poslovno pomembnih rešitev, je smotrno takšno ocenjevanje prepustiti neodvisni instituciji ali svetovalcu. Le-ta mora v ta namen predhodno analizirati informacijske potrebe podjetja na obravnavanem področju, jih formalizirati z modelom izvajanja postopkov in podatkov in ugotovitve primerjati z možnostmi ponujene programske rešitve. Na ta način se lahko približamo izhodiščem, ki jih prikazuje slika 2, ter izognemo razočaranju in nepričakovanim stroškom.



Slika 2: Skupni stroški lastništva rešitev v srednje velikem slovenskem podjetju

Slika 2 prikazuje skupne stroške lastništva programskih rešitev, ki jih ob ustreznem pristopu k uvajanju doseže morebiti eno od petih večjih slovenskih podjetij. V vseh ostalih pa so ti stroški nekajkrat prekoračeni ali pa projekt ni doživel uspešnega konca. Slika 3 prikazuje posledice takšnih pristopov (prirejeno po GartnerGroup).



Slika 3: Vpliv ustreznosti uvajanja programske rešitve na donosnost naložbe v informatizacijo poslovanja

Seveda obstaja kar nekaj objektivnih vzrokov, ki pogojujejo takšno stanje. Med njimi izstopajo zgoraj prikazane ugotovitve o hitro se razvijajočem trgu programskih rešitev ob kroničnem pomanjkanju ustreznih kadrov ponudnikov teh rešitev na eni strani, na drugi strani pa hitro naraščajoče ter slabo opredeljene poslovne in informacijske potrebe uporabnikov oziroma kupcev proizvodov in naročnikov teh storitev.

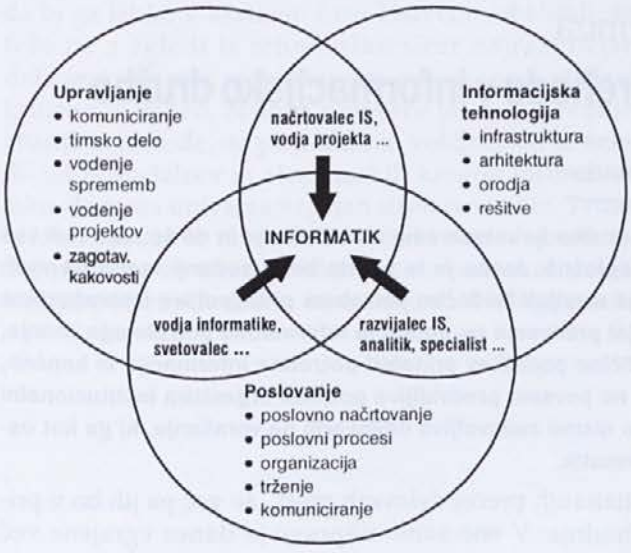
V obeh primerih gre za problematiko potrebnih znanj, ki naj bi jih zagotavljali informatiki ponudnika in obvladovali informatiki in uporabniki naročnika v širšem smislu. Možnosti, ki jih nudi uporaba sodobne informacijske tehnologije, postavljajo pred informatike potrebo po drugačnih, predvsem pa širših znanjih, kot smo jim bili priča v preteklosti (slika 4) [3].

Informatiki morajo biti tako ob prehodu v informacijsko družbo oboroženi z interdisciplinarnimi znanji s področij upravljanja, poslovanja in uporabe same informacijske tehnologije. To so pravzaprav interdisciplinarno znanje s področij upravljanja, informacijske tehnologije ter poslovna, organizacijska in komunikacijska znanja.

3. IZHODIŠČNE TEZE

Teze kot izhodišča za razpravo na okrogli mizi lahko strnemo v naslednjih vrsticah:

- delež doma (v hiši) razvitih celovitih programskih rešitev se bo tudi pri nas še naprej zmanjševal
- kadrom domačih in tujih ponudnikov, ki izvajajo projekte informatizacije, večinoma primanjkujejo predvsem poslovna znanja, veščine poslovnega modeliranja in prenove poslovnih procesov ter vodenja projektov in sprememb;



Slika 4: Znanja, ki jih potrebuje informatik

- profil sodobnega informatika v našem okolju še vedno ni splošno razpoznaven, njihovo pomanjkanje je izredno, izobraževalne institucije ne "proizvedejo" zadostnega števila takšnih kadrov ali pa jih ne opremijo s celotno paleto potrebnih znanj;
- večina domačih programskih rešitev, kljub primerljivi tehnološki ravni, konceptualno ni ustrezno zasnovana v primerjavi s tujmi rešitvami (npr.: Baan, SAP ...) in pomanjkljivo dokumentirana
  - običajno tuje rešitve celovito podpirajo poslovne procese (procesna zasnova), večina domačih pa vztraja na paketni zasnovi
  - večina tujih rešitev ima dokumentirane referenčne procesne modele in podatkovne modele, pri domačih je to redkost;
- ponudniki tujih rešitev se običajno sklicujejo na "najboljšo prakso" oziroma uveljavljenost njihovih rešitev v razvitih okoljih, pri tem pa vsebino in tehnološke možnosti samih rešitev in specifiko domačega okolja poznajo bistveno slabše od domačih ponudnikov;
- postopek ugotavljanja informacijskih potreb uporabnikov in samega uvajanja pri ponudnikih tujih rešitev ne poteka skladno z metodološkimi pristopi in možnostmi, ki jih zagotavlja proizvajalec rešitve. Rešitve se največkrat uvajajo paketno (po poslovnih funkcijah) ali pa informatizirajo poslovne procese takšne kot so (brez predhodne preureditve);
- v našem okolju še posebej malo projektov informatizacije uspe povrniti naložbene vložke v trajanju tehnološke dobe uporabe rešitev. Ti vložki so običajno, zaradi konjukturnosti in "modnosti" takšnega (celovitega, v nekritičen nakup rešitev usmerjenega) pristopa k informatizaciji, preobsežni in neopravičljivi;
- v primeru, da ponudnik oziroma izvajalec nove rešitve tega ne nudi ali ne zaupamo v njegovo strokovnost, je smotrno ocenjevanje primernosti rešitve prepustiti neodvisni instituciji ali svetovalcu. Le-ta mora v ta namen predhodno analizirati informacijske potrebe podjetja na obravnavanem področju, jih formalizirati z modelom izvajanja postopkov in podatkov in ugotovitve primerjati z možnostmi ponujene programske rešitve;
- pri nas neprimerno uvajanje ali uvajanje in dograjevanje neprimerne rešitve, če sploh uspe, predstavlja običajno nekajkrat, v posameznih primerih pa tudi nekaj desetkrat višje stroške od stroškov, povezanih s samim nakupom rešitve.

4. UGOTOVITVE

Udeleženci okrogle mize so sprejeli in v obravnavi tudi potrdili ugotovitve, ki izhajajo iz gornjih tez. Temeljna in največkrat izpostavljena ugotovitev okrogle mize je,

da **naročniki** na eni strani največkrat niso sposobni opredeliti in v razumljivi obliki izvajalcu predstaviti svojih informacijskih potreb, na drugi strani pa **izvajalci** oziroma ponudniki največkrat ne izražajo želja ali zahtev po ugotavljanju teh potreb in zagovarjajo "najboljšo prakso", ki je zajeta v njihovih rešitvah.

Tako eni kupijo "mačka v žaklju", drugi pa se v nadaljevanju ubadajo z "grdimi podrobnostmi", ki se izpostavijo skozi podrobno opredeljevanje informacijskih potreb ob uvajanju in prilagajanju programskih rešitev. Eni in drugi se tako sicer izognejo, v teoriji in praksi ugotovljeni, ključni fazi načrtovanja informatike in skušajo posledice takšnega početja prevaliti drug na drugega. Ob neposredno merljivih dodatnih stroških prilagajanja rešitev in oportunitetnih stroških, ki izhajajo iz časovnih kasnitev projektov, predstavlja ključni problem uporaba, s stališča izvajanja poslovnih procesov organizacije, neustreznih rešitev.

Prevladuje prepričanje, da pri nas pri uvajanju in prilagajanju programskih rešitev prevladujeta dve skrajnosti. Prva je značilna za projekte informatizacije, kjer se rešitve razvijajo "po meri" naročnika. V tem primeru se rešitve največkrat prilagajajo željam (ne pa informacijskim potrebam !) naročnika, takšno uvajanje in prilagajanje je dolgotrajno in dostikrat izčrpljujoče za obe strani (naročnika in izvajalca), spremljajoče z nekajkrat višjimi stroški od stroškov samega nakupa programske rešitve.

Drugačen pogled in pristop pomeni izhodišče izvajalca (ponudnika) rešitve, da sama rešitev z vgrajenim poslovnim in tehnološkim znanjem celovito pokriva informacijske potrebe naročnika. V tem primeru se od slednjega pričakuje, da bo izvajanje poslovnih procesov kar se da prilagodil rešitvi. Tedaj so stroški na področju uvajanja in prilagajanja lahko bistveno nižji. V prid takšne ugotovitve gredo podatki podjetja Intertrade ITS, ki uspeva uvesti in prilagoditi naročniku rešitve Baan s stroški, ki so nižji od stroškov nakupa licence same programske rešitve.

Kateri od teh dveh pristopov, če sploh, je pravilen oziroma priporočljiv v naših razmerah? Mogoče njuna kombinacija ali neka srednja rešitev? Resnica žal ni vedno nekje na sredini, temveč se optimalni pristop od primera do primera, v različnih organizacijah, različno približuje opisanim skrajnostim. Nedvomno pa lahko potrdimo, da tako kot ni smiselno informatizirati neustreznih obstoječih procesov, ne da bi jih predhodno ocenili in preuredili, tudi ni modro slepo in nekritično prilagajanje procesov rešitvam, ki so se morda nekje, nekoč, v nekem okolju pokazale kot uspešne. Ob tem tudi ugotavljamo, da naročniki največkrat, tudi v primerih, ko ne gre zgolj za prilagajanje novi programski rešitvi, niso pripravljeni prilagoditi svojih poslovnih procesov. Stopnja njihove pripravljenosti je, kar je naša značilnost, bistveno večja, ko gre za tuje rešitve.

5. UPORABLJENA LITERATURA

[1] Mirchandani V.: - SIS and Packaged Applications, - Packaged Application Implementations, Symposium ITxpo98, GartnerGroup, Florida, 1998

[2] Kovačič A.: Kakšne uporabniške programske rešitve potrebujemo?, Uporabna informatika, Slovensko društvo Informatika, Ljubljana, 1997

[3] Kovačič A.: Informatizacija poslovanja, Ekonomska fakulteta, Ljubljana, 1998

■

Okrogla miza

Znanja in poklic informatika na prehodu v informacijsko družbo

Niko Schlamberger

Osnovna ugotovitev okrogle mize je bila, da je informacijska družba še razmeroma nedefinirana in da so zato tudi vsa predvidevanja o potrebah na področju izobraževanja dokaj splošna. Jasno je le to, da bodo sedanji vzorci na vseh področjih vse manj uporabni. Glavna naloga izobraževalcev je razvijati bodočim potrebam prilagodljive izobraževalne sisteme. Vodja okrogle mize Franc Žerdin je diskusijo usmerjal predvsem na področje informatiku potrebnega znanja, kako ga pridobivati, kako iz eksponencialno naraščajoče količine podatkov pridobiti potrebne informacije in končno, kakšna naj se za delovanje v spreminjajočem se okolju in za ne povsem predvidljive potrebe organizira institucionalni izobraževalni sistem. Osnovna ugotovitev je bila, da še vedno nismo zadovoljivo odgovorili na vprašanje, ki ga kot osrednje vsebuje naslov okrogle mize in sicer kdo je sploh informatik.

Vprašanje je sorodno vprašanju opredelitve informatike kot stroke. Ker le-ta še ni vpisana v uradne klasifikacije, je posledično tudi poklic informatika opredeljen razmeroma mehko. Že danes je informatiziranih precej delovnih mest, še več pa jih bo v prihodnje. V eno samo napravo je danes vgrajene več procesne moči, kakor so je pred tremi desetletji premogli vsi računalniki v Sloveniji. Računalnik, ki upravlja

zapestno uro, bi moral še ne tako dolgo tega stati v kar velikem prostoru. Ali smo zato informatiki kar vsi? Glavna ugotovitev je bila, naj kot informatika ali splošneje kot poklice v informatiki upoštevamo tiste, katerih glavno področje dela je povezano z *omogočanjem* uporabe in upravljanja računalnikov in ne z njihovo uporabo za opravljanje neke druge dejavnosti ali aktivnosti.

Drugi sklop diskusije se je nanašal na vprašanja izobraževanja in usposabljanja informatikov. Informatika se razvija še vedno izjemo hitro kot tehnika, pa tudi kot teorija. Izobraževalne ustanove se po naravi tako hitrim spremembam težko prilagajajo, zato morajo upoštevati, da bodo ob razpolovni dobi znanja, ki znaša okoli štiri leta, informatiki, ki so se vpisali letos, morali posodobiti znanje že takoj po zaključeni šoli. Nekoliko poenostavljeno bi lahko povzeli, da mora šola učiti metodo in ne veščino. Ne more imeti ambicij, da bo usposobila za opravljanje poklica, temveč mora predvsem naučiti iskati in uporabljati vire za pridobivanje potrebnih informacij. Zato mora institucionalni izobraževalni sistem nujno upoštevati možnosti neinstitucionalnega usposabljanja, ki se odvija zunaj šol in univerz, ki pa praviloma posreduje res najnovejše dosežke na področju tehnike, pa tudi teorije. Primer, ki to dokazuje, je koncept podatkovnih skladišč, ki k nam ni prišel preko univerz, temveč mimo njih. Splošni očitek, da pridejo informatiki iz šole s premalo uporabniškega znanja, je neupravičen, saj je področij, kjer se bo lahko zaposlil, zelo veliko in nemogoče je informatika usposobiti za vsa ali celo vsaj za večino drugih področij.

Posebno vprašanje je prenos vsebin izobraževalnih programov iz tujih, predvsem ameriških univerz, v slovensko okolje. Upoštevati moramo, da je slovenski izobraževalni sistem del evropskega, ki se je razvijal in izpopolnjeval stoletja dolgo. Ne moremo pričakovati, da bi ga lahko v kratkem času bistveno izboljšali, še teže pa z zgledi iz tehnološko sicer najrazvitejše države, ki na svoj izobraževalni sistem sama gleda s kritično distanco. Naloga univerze je, da posreduje znanje in metode, ne pa prakso in veščine, kar je nekdo od poslušalcev iz akademskih krogov formuliral tako, da mora univerza vzgajati strokovno elito. Temu bi lahko dodali le to, da bodo tisti, ki obvladajo metodo, podatke že znali poiskati in se bodo tudi znali naučiti potrebnih veščin in spretnosti. Naloga predvsem univerze je, da bo izkušnje in primere tujih univerz obravnavala z nujno kritično distanco in prevzemala nove tehnike in vsebine s potrebno modrostjo.

Precej časa je bilo posvečenega diskusiji o potrebnih znanjih uporabnikov računalniških rešitev. Splošno mnenje je, da se uporabniki ne zanimajo dovolj za informatiko in da tovrstnemu usposabljanju ne namenjajo dovolj časa. Tako stališče ne upošteva dejstva, če si smemo spet dovoliti poenostavitev, da v vsakem primeru posebej obstajata dve množici znanja, znanje informatike in znanje stroke uporabnika. Upoštevati moramo, da je za uporabnika primarna zahteva obvladovanje njegove stroke, ker je to tudi pogoj za uspešno delovanje njegove organizacije in da mora znati informatike le toliko, da obvlada informatizirano delovno mesto ali informatiziran delovni proces. Analogno bi lahko ugotovili, da mora informatik razumeti uporabnikovo delo in stroko toliko, da lahko razvija funkcionalno ustrezne rešitve. Ključ do uspešnega sodelovanja torej ni v tem, da bi vsi znali vse, temveč *v maksimalnem funkcionalnem preseku obeh znanj*. Če pogledamo, koliko uporabnikov obiskuje seminarje s področja informatike in koliko informatikov se usposablja na neinformatičnih področjih, bi lahko sklenili, da so očitki o premajhnem interesu uporabnikov za informatiko pretežno neupravičeni, če ne kar krivični.

Sklepne ugotovitve bi lahko povzeli v naslednjih stavkih. Izobraževalne ustanove naj učijo predvsem to, kako znanje pridobivati in kako ga uporabljati. Ni mogoče izšolati informatka za delo v poljubnem okolju, zato je nujno povezati izobraževalni sistem z možnostmi usposabljanja zunaj rednega izobraževanja in predvsem po njem. V informacijski družbi bodo nastajali novi poklici in razvili se bodo novi vzorci delovanja in življenja nasploh, ki jih danes še ne poznamo in za katere tudi ne moremo zahtevati, da bi jih izobraževalni sistem že upošteval. En poklic za vse življenje je že danes redkost in učenje za prihodnost je skorajda stvar preteklosti. Vsi se bomo morali sprijazniti s konceptom permanentnega izobraževanja. Spoštovati moramo prizadevanja uporabnikov, da osvojijo potrebno znanje informatike, in informatikov, da se usposobijo na področju dela uporabnikov, pri čemer je treba zasledovati cilj, ki je potrebni presek obeh znanj. ■

GOVOR REKTORJA UNIVERZE V MARIBORU PROF. DR. LUDVIKA TOPLAKA

ob otvoritvi posvetovanja »Dnevi slovenske informatike v Portorožu '99« dne 21. 4. 1999

Spoštovano predsedstvo....

Ob letošnjem šestem posvetovanju »Dnevi slovenske informatike '99« organizatorjem iskreno čestitam, tako Združenju za računalništvo in informatiko in Slovenskemu društvu Informatika.

Letošnje posvetovanje informatike je posvečeno globalizaciji poslovanja. Informatika je postala infrastruktura vseh segmentov, posebej še univerze. Informatika je prodrla v vse pore našega življenja. Pred desetletji se je vodila samo evidenca registriranja avtomobilov in podobno, kasneje so se računale plače in pokojnine, danes pa postaja orodje inženirjev, ekonomistov, učiteljev, študentov in raziskovalcev ter postaja celo izrazno sredstvo umetnikov. Žal pa je informatika tudi orodje organiziranih mednarodnih in domačih kriminalnih združb.

Kot orodje ekonomistov je informatika postala tudi sredstvo pospešenega razvoja poslovanja, zlasti na mednarodnem nivoju. S tem pa je globalizaciji dan nov zagon. Globalizacija, ki pomeni poenotenje standardov v svetovnem merilu, je star proces. Latinski jezik, dekadni sistem, kulturni in verski tokovi, so nedvomno močno prispevali h globalizaciji, sodobna informatika pa je danes orodje in sredstvo globalizacije. Posebej Internet je dal novega zagona globalizaciji na vseh področjih, zlasti povečal storilnost učiteljev in učencev, raziskovalcev, inženirjev in trgovcev.

Zgodovinski proces globalizacije je večen, in spremlja istočasno proces diferenciacije. In prav sodobni proces razvoja informatike s tem ustvarja možnosti za poln razvoj posameznika, podjetij in drugih institucij ter narodov, s tem pa tudi zaščito malih pred presijo monopolistov. Prav sodobni razvoj informatike ustvarja nove možnosti razvoja kulturne identitete, tudi malih narodov. Uvodno sporočilo organizatorjev kaže na tankočutnost in smisel tega cenjenega zbora, prav do vprašanj vsestranskega kulturnega in znanstvenega razvoja Slovencev. Tudi »Dežmanov sindrom«, ki je večkrat zajel tudi zelo izobražene Slovence, je sindrom našega časa, kot posledica kompleksa malosti ali kompleksa manjvrednosti. In prav sodoben razvoj informatike osvobaja in ščiti male in tudi daje novega zagona razvoju kulturne identitete Slovencev.

V tej zvezi še nekaj. Zemlja je omejena dobrina, rudna bogastva so omejene dobrine, človekova domišljija in človekova pamet informacijsko podprta, nimata meja. Zavedamo se, da prihaja nov čas. T.i. postindustrijska revolucija je revolucija, ki se kaže na vseh področjih. Za nas Slovence je to nova zgodovinska priložnost. Organizatorjem tega posvetovanja zato posebna hvala.

Oba fenomena našega časa, informatika in globalizacija, se posebej močno odražata pri življenju in delu slovenske univerze. Univerza v Mariboru je v okviru Fakultete za elektrotehniko, računalništvo in informatiko zelo zgodaj razvila program računalništva in informatike. Gospod prof. dr. Ivan Rozman, ki aktivno dela tudi v okviru tega posvetovanja, bo najbolj avtentično predstavil prizadevanja univerze na področju razvoja informacijskih znanosti ter posebej pedagoški in izobraževalni program. Univerza v Mariboru se zaveda trojnega poslanstva: regionalnega, nacionalnega in mednarodnega. V okviru regionalnega poslanstva univerza sodeluje v povezavi z gospodarstvom. Znana so mednarodna posvetovanja, ki jih organizirajo fakultete Univerze v Mariboru, za današnji posvet pa so zanimive specializirane konference o elektronskem poslovanju.

Informatika pa postaja tudi infrastruktura celotne univerze, orodje profesorjev in študentov in zlasti izrazno sredstvo profesorjev in študentov informatike. Prav sodobni razvoj informatike in telekomunikacij omogoča učenje na daljavo. V svetu se učenje na daljavo uveljavlja kot poseben sistem izobraževanja, ki povečuje učinkovitost, zmanjšuje stroške in omogoča večjo izkoriščenost opreme. Znani so nacionalni programi učenja na daljavo v Turčiji in v Koloradu v ZDA. V Sloveniji se tega lotevamo z zaostankom in s preskromnimi ambicijami.

Slovenski univerzi si prizadevata, žal zaradi nesinhronizirane nacionalne politike, doma prepočasi. Univerza v Mariboru zato preko mednarodnih mrež oblikuje sistem učenja na daljavo v povezavi s programi Evropske unije, po vzgledu in izkušnjah v uspešnih državah. Po naši oceni razvit program učenja na daljavo bi lahko bil tudi tržni artikel, glede na izjemne priložnosti, ki jih univerza danes zaseda v evropskih združenjih univerz. Potrebna je seveda ustrezna podjetnost doma.

Informatika, kot sredstvo sodobnega in uspešnega poslovanja, je pomembna zaradi uvajanja novih tehnologij in s tem povečane konkurenčnosti v pogledu kvalitete in cen. Posebej pa v pogledu poslovanja, to je trgovine in financ.

Ob vseh teh spoznanjih pa se moramo zavedati, da najbolj donosna ekonomska dejavnost je razvoj in to razvoj informatike. Zato naša družba mora skrbeti, da ne bomo samo preprodajalci računalnikov in njihovi uporabniki, ampak zlasti tudi sooblikovalci. Univerza se tega zaveda, posebej z veseljem spremljamo tovrstno podporo Gospodarske zbornice in obeh drugih soorganizatorjev današnjega posvetovanja.

Spoznanje, da je investicija v razvoj najprogresivnejša gospodarska dejavnost, me je motiviralo, da sem se pred dvemi desetletji tudi sam priključil skupini mladih entuzijastov, med njimi so tudi soorganizatorji tega posvetovanja, posebej naj omenim prof. dr. Andreja Kovačiča.

Zavedam se, da pravni položaj informatike terja posebno ustrezno pravno ureditev, tako na področju avtorskih pravic, kot na področju davčne politike, ki bo vzpodbujala razvoj.

To isto spoznanje me vodi danes pri delu na univerzi in želim delo posvečati prav tem programom.

Na kraju organizatorjem posvetovanja še enkrat iskrene čestitke in zahvala za povabilo. Konferenci želim uspešno delo, udeležencem pa, da spoznanja tudi praktično ovrednotijo na delovnih mestih, v interesu celovitega razvoja naše družbe in kvalitete življenja.

■

ŠESTO POSVETOVANJE

DNEVI SLOVENSKE INFORMATIKE '99

GLOBALIZACIJA POSLOVANJA

KONGRESNI CENTER GRAND HOTEL EMONA, PORTOROŽ
21. do 24. april 1999

Na šesto posvetovanje z mednarodno udeležbo Dnevi slovenske informatike '99 sta prireditelja Slovensko društvo INFORMATIKA ter Gospodarska zbornica Slovenije - Združenje za računalništvo in informatiko zbrala preko štiri sto udeležencev. Aktualna rdeča nit posvetovanja je bila globalizacija poslovanja, o čemer so predavali vabljeni predavatelji, med njimi tudi ugledni strokovnjaki slovenskega rodu. Tema je aktualna prav v tem času, namen pa je opozoriti na možnosti delovanja v pogojih, ko bodo lokalni trgi stvar izbire in ne stvar usode. V štirih dneh se je zvrstilo več kot devetdeset referatov, ki so obravnavali aktualne teme informatike z različnih vidikov, tako znanstvenih kot strokovnih in poslovnih. Lahko rečemo, da je posvetovanje pregled stanja informatike v Sloveniji in tudi njenega vpliva na različna področja uporabe rešitev.

Posvetovanje se je začelo s predkonferenco Tehnologije prihodnosti, katere namen je bil prikazati, kaj je novega v razvojnih razmišljanjih vodilnih podjetij v informatiki. Nadaljevala se je s svečanim plenarnim delom, kjer so bili govorniki pomembni gostje posvetovanja in častni govornik rektor mariborske univerze dr. Ludvik Toplak. Drugi in tretji dan posvetovanja sta bila posvečena strokovnemu delu; leto je potekalo v treh vzporednih sekcijah, ki jih je bilo skupaj kar sedem: Metodologija informacijskih sistemov, Internet in informacijska infrastruktura, Prenova in informatizacija poslovnih procesov, Informacijske rešitve in orodja, Izobraževanje in usposabljanje v informatiki ter dve vsebinsko novi, Sociološki vidiki in Operacijske raziskave. Naj pripomnimo, da se je s tem posvetovanje razvilo v pravo multikonferenco, ki ne obravnava zgolj tehničnih, temveč tudi širše vidike prehoda v informacijsko družbo. Štiri okrogle mize so načele aktualna vprašanja informatike v Sloveniji, katerih vsako bi zaslužilo obravnavo v posebnem problemsko usmerjenem referatu v eni od plenarnih sekcij. To so bile Strategija informatike v Republiki Sloveniji, Evropski in domači vidiki elektronskega poslovanja, Izbira najboljšega (ali pravega) izvajalca in Znanja in poklic informatika na prehodu v informacijsko družbo.

Posvetovanje so spremljali številnejši dogodki kakor prejšnja leta. Kot posebno vidno naj navedemo sejo upravnega odbora Gospodarske zbornice Slovenije, ki jo štejeta prireditelja kot priznanje, ki ga je na ta način gospodarstvo izkazalo informatiki, pa tudi kot zavedanje vodilnih gospodarstvenikov, da brez informatike ni uspešnega poslovanja niti doma, kaj šele v svetu. Na seji je Slovensko društvo INFORMATIKA (SDI) predstavilo izhodišča za dokument o Sloveniji kot družbi znanja, s katerim želi podati realno vizijo prehoda v informacijsko družbo. Pomemben dogodek je bil izredni občni zbor SDI, na katerem so bila sprejeta izhodišča dokumenta Slovenija kot družba znanja in določeno uredništvo. Na tem občnem zboru je bil sprejet kodeks poklicne etike informatikov, ki je pomemben korak pri razvijanju strokovne odličnosti. Praktično je bila ta volja in usmeritev izkazana s tem, da so bili ustanovni člani SDI sprejeti v častno članstvo, seveda pa tudi s tem, da so dr. Anton P. Železnikar, dr. Matjaž Gams in dr. Marjan Krisper na prvi dan posvetovanja prejeli priznanja SDI za vidne prispevke na področju informatike.

Dve delavnici sta prikazali programiranje v Javi in revidiranje informacijskih sistemov. Za obe je bilo zanimanje precejšnje, kar dokazuje primerno izbrano vsebino delavnic. Poslovni del je obsegal že tradicionalno priložnostno razstavo, katere del so bile z internetom povezane informacijske delovne postaje, kjer je bilo mogoče pristopiti do večine referatov. Vsi sprejeti referati so bili objavljeni tudi v Zborniku posvetovanja, ki je bil letos natisnjen na preko 800 straneh in v dveh zvezkih. Avtorji treh referattov, ki so jih udeleženci ocenili kot najboljše, so dobili posebna priznanja in nagrade. Reklamno usmerjeni prispevki so bili objavljeni v posebni številki revije Uporabna informatika. Seveda moramo omeniti tudi družabni del, ki je bil med drugim tudi priložnost za manj formalne stike in izmenjave mnenj.

Zadnji dan posvetovanja so bili na programu vabljeni predavatelji, okrogla miza ter slovesen zaključek posvetovanja. Udeležencem je bila predstavljena vsebina deklaracije posvetovanja, katere precejšnji del je namenjen možnemu načinu prehoda v informacijsko družbo. Deklaracija je bila sprejeta brez pridržkov s priporočilom, naj bo tudi javno objavljena[1]. Končno je bil predlagan in sprejet tudi termin za posvetovanje Dnevi slovenske informatike 2000 in sicer 19. do 23. april 2000.

Kljub mogočemu očitku, da ocena ne bo objektivna, naj jo vendarle izrečemo. Mnenja, medijska odmevnost in anketa udeležencev nas potrjujeta v mnenju, da je izbrana usmeritev posvetovanja pravilna. Poudarek je na strokovnosti prispevkov, na širini obravnavanja in na bogastvu tem, ki so jih našli avtorji referatov kot odgovor na vabilo k sodelovanju. Poleg širine posvetovanja je posebna odlika ohranjevanje stikov z vidnimi informatiki slovenskega rodu, ki delujejo na tujem. Za prav tako pomembno ocenjujemo, da je posvetovanje dostopno študentom brez plačila kotizacije in da je strokovnjakom možnost javnega nastopa in predstavitve svojih zamisli in dosežkov. Z vsem tem SDI izpolnjuje pomemben del svojega poslanstva. Seveda pa bi bilo ošabno misliti, da smo napravili že vse, kar se je dalo. Nobeno posvetovanje ni tako popolno, da se ga ne bi dalo še izboljšati in eno od možnosti vidimo v razširitvi strokovnih stikov s profesionalnimi društvi za informatiko v sosednjih državah ter z mednarodnimi organizacijami, katerih član je SDI. Vsekakor naj bo to naloga strokovnih in tehničnih teles bodočih posvetovanj.

Niko Schlamberger

1 *To obvezo izpolnjujemo v tej številki revije, objavljena pa bo tudi na domačih straneh SDI.*

Udeleženci posvetovanja Dnevi slovenske informatike 1999 (DSI'99) so v Portorožu v dneh od 21. do 24. aprila 1999 razpravljali o stanju na področju informatike v državi in v svetu in na zadnji dan posvetovanja sprejeli naslednjo

Deklaracijo posvetovanja Dnevi slovenske informatike '99 - Globalizacija poslovanja,

s katero želijo javnosti sporočiti ocene, spoznanja, ugotovitve in priporočila kot rezultate predstavitev in izmenjave informacij na posvetovanju.

1. Udeleženci ugotavljajo, da je posvetovanje Dnevi slovenske informatike verjetno najpomembnejše letno strokovno srečanje informatikov in uporabnikov informacijske tehnologije in tehničnih rešitev s tega področja. To dokazujejo strokovna širina posvetovanja, število nastopajočih referentov, razprave na okroglih mizah in udeležba na delavnicah, odmevnost posvetovanja v medijih, pa tudi število udeležencev posvetovanja in ugledni častni in vabljeni govorniki. Vodilna misel posvetovanja je bila globalizacija poslovanja, ki ob vstopanju v informacijsko družbo pogojuje razvijanje novih vzorcev obnašanja in delovanja vseh segmentov družbe.
2. Na predkonferenci so se udeleženci seznanili z razvojnimi cilji pomembnih svetovnih dobaviteljev informacijske tehnologije in z zadovoljstvom ugotavljajo, da nove tehnologije in informacije o njih prihajajo v Slovenijo praktično brez zakasnitev. Razprave, ki so potekale ob predstavitvah referatov, ob okroglih mizah in na delavnicah, so z različnih, ne samo tehnoloških vidikov obravnavale informatizacijo procesov in funkcij v kontekstu globalnega delovanja ter poglede javnega (posebej države in obeh slovenskih univerz) ter zasebnega sektorja, civilne družbe in gospodinjstev.
3. V uvodnem delu posvetovanja so bila podeljena priznanja Slovenskega društva INFORMATIKA za dosežke na področju informatike v bližnji preteklosti. Na izrednem občnem zboru društva, ki je bil eden od spremljajočih dogodkov posvetovanja, je bil sprejet kodeks poklicne etike informatikov. Oboje, priznanja in kodeks, razumejo udeleženci kot prispevek k povečevanju strokovne odličnosti informatikov in priporočajo, naj se ta usmeritev ohrani.
4. Pomemben vidik globalizacije poslovanja je elektronsko poslovanje in udeleženci ugotavljajo, da se morajo sami in njihove ustanove prilagajati organizacijsko, tehnološko in z novimi načini delovanja. Obenem opažajo, da pomembni pogoji za nove tehnike poslovanja še niso izpolnjeni, kakor bi bilo pričakovati. Pri tem mislijo deloma na pravne ureditve v zvezi z elektronskim poslovanjem, kot vsaj tako pomembne pa upoštevajo ovire zaradi preskromne in prepočasne demonopolizacije in deregulacije, pa tudi še vedno premajhne dostopnosti podatkov javnih podatkovnih zbirk. Posledica takega stanja je po oceni udeležencev prepočasno izpolnjevanje obvez in usmeritev, prevzetih s predpristopnim sporazumom.
5. Udeležencem so bila predstavljena izhodišča za dokument Slovenskega društva INFORMATIKA (SDI) o Sloveniji kot družbi znanja. Dokument je pogled društva na realno možnost načina prehoda Slovenije v informacijsko družbo. Predlagana pot upošteva zadevne evropske dokumente v tem, da priporoča liberalizacijo in deregulacijo, da vidi kot vodilne subjekte tiste iz zasebnega poslovnega sektorja, da pa upošteva specifične možnosti Slovenije in njen ekonomski in politični položaj. Osnovno izhodišče za pripravo takega dokumenta je, da Slovenija še nima splošnega konsenza o viziji razvoja informatike in zato si je SDI kot združenje strokovnjakov, ki delujejo na področju informatike, zadalo nalogo, da pripravi programski dokument, ki bo splošno sprejemljiv. Prepričan je, da je to sposoben narediti, saj s tem nadaljuje korake, ki jih je začel z javno predstavljeno in objavljeno *Deklaracijo o razvoju informacijske družbe in razvoju informatike v Sloveniji* na posvetovanju Dnevi slovenske informatike DSI '97. Pri tem upošteva tudi druge javno objavljene in dostopne slovenske dokumente in pobude.
6. Delovni naziv za dokument SDI je Modra knjiga o razvoju informatike v Sloveniji. Kot osnutek bo izdelana do konca maja 1999 in bo v razpravi znotraj društva in v Gospodarski zbornici Slovenije (GZS) kot ustanovi, ki je doslej pokazala največ pripravljenosti za partnerstvo, do septembra 1999. GZS in SDI imata ambicijo, da bi postala Modra knjiga strateški državni dokument za področje informatike. Javna razprava bo upoštevala internet poleg klasičnih komunikacijskih medijev. Predstavljen in sprejet je bil vsebinski koncept Modre knjige, ki je podan v nadaljevanju.
7. Modra knjiga bo obravnavala pet glavnih področij: odnos javnosti, infrastruktura, izobraževanje, zasebni sektor ter javni sektor (država, uprava in javne službe). Cilji po posameznih področjih so naslednji:

Odnos javnosti

Javnost se mora seznaniti z dejstvom, da bodo mehanizmi in načini delovanja vseh subjektov, ki so se razvijali v industrijski družbi, kmalu preseženi in neprimerni tudi v Sloveniji. Razumeti mora, da niti za preživetje, kaj šele za blagostanje v družbi novega tipa, obstoječi vzorci ne zadoščajo več. Po drugi strani mora vsa javnost sprejeti nove odnose ob prehodu v informacijsko družbo, zato je nujen najširši družbeni konsenz in temu je

namenjen prvi del Modre knjige. Doseganje konsenza vključuje zanimanje za priložnosti, ki jih ponujata življenje in delo v informacijski družbi, povečanje zaupanja v nove tehnologije ter oblike dela in poslovanja ob posebni pozornosti do interneta kot medija prihodnosti, obravnavanje varnosti prenosa podatkov in zaščite osebne identitete pri uporabi interneta. Pomemben del dokumenta naj bodo slovenske "Bangemannove" aplikacije, ki so aktualne za vse sektorje in zadevajo najširšo javnost.

Informacijska infrastruktura

Na področju informacijske infrastrukture so lahko zgled tehnološko najrazvitejše države sveta, posebej Združene države Amerike in države Evropske zveze. Zasebni sektor pričakuje in zahteva ne toliko direktna državna vlaganja v graditev in razvoj infrastrukture kot aktiven odnos do nosilnih infrastrukturnih projektov. Ob tem je treba ugotoviti, da prispevek države že doslej ni bil zanemarljiv. Za najpomembnejše infrastrukturne projekte bodo morali biti določeni cilji, predlagana strategija, nosilci ter opredeljene faze razvoja, za ugotavljanje rezultatov pa tudi še podrobneje opisno in številčno določene. Pri tem morata biti kar najbolj upoštevana naslednja dejavnika: (1) odprt trg, ki omogoča razvoj konkurence in tekmovalnost in (2) podpora vlaganjem v postavitev najhitrejših ter tehnično in cenovno vsem dostopnih omrežij.

Izobraževanje in usposabljanje

Temeljna usmeritev je, da bodi vsem državljanom ne glede na starost in izobrazbo omogočeno ustrezno izobraževanje in pridobivanje znanj, potrebnih za aktivno življenje skozi celotno življenjsko obdobje. Pri tem mora biti posebna pozornost namenjena doslej manj vidnim skupinam, kot so invalidne osebe, mladostniki in druge manjšinske skupine. Novi vlogi mora biti prilagojen institucionalni sistem izobraževanja, ki je doslej premalo upošteval možnosti sinergijskih učinkov pri sodelovanju z zunajinstitucionalnimi izobraževalnimi ustanovami. Izobraževalni sistem mora biti sposoben prilagajanja hitrim spremembam in vključevanja novih vsebin in novih načinov podajanja. Pred vse, ki odločajo o izobraževalnem sistemu ter ga izvajajo, bodo postavljene nove naloge usposobitve za potrebne določitve o spremembah in izvajanju programov. Povsem nov pogled je spodbujanje konkurenčnosti na področju znanosti, posebej pa moramo zahtevati podpiranje razvojnih in raziskovalnih programov s področja informatike, komunikacij ter življenja in dela v informacijski dobi.

Zasebni sektor

Zasebna podjetniška iniciativa mora videti poslovni interes v priložnostih za vlaganja v nove storitve na osnovi informacijske tehnologije ali v povezavi z njo. Evropski dokumenti, ki jih je sprejela tudi Slovenija in ki jih od vsega začetka stroka močno podpira, pričakujejo največje razvojne pobude od zasebnega poslovnega sektorja. Pri tem ugotavljamo, da so bile slovenske gospodarske družbe doslej premalo naravnane v enakopravno mednarodno trgovanje. Pretoki blaga in storitev so bili in so še pretežno enosmerni, kar je bilo sprejemljivo v okviru uveljavljenih vzorcev delovanja in v odnosu do vodilnih družb informacijske tehnologije. V pogojih globalnega poslovanja to ne bo več zadoščalo za svetovno konkurenčno sposobnost in verjetno ne bo omogočalo niti akumulacije znanja za uspešno delovanje doma. Da ne bi postali kolonija novega tipa, mora zasebni poslovni sektor razvijati lastno identiteto kot najpomembnejši element razpoznave na globalnem trgu. Ustvarjati mora pogoje za razvoj velikoserijske proizvodnje visoko kvalitetnih proizvodov, razvijati nove, predvsem storitvene dejavnosti, programske produkte in visoko specializirano informacijsko opremo, ki vsebuje visoko stopnjo dodane vrednosti, spodbujanje kreativnosti in uporabo znanja.

Javni sektor (državna uprava in javne službe)

Doslej je zlasti država posredno ali neposredno nastopala kot vodilna pri razvoju infrastrukturnih sistemov informatike, večino za to primernih delovnih mest je informatizirala in tudi investirala v pomembne razvojne projekte informacijske tehnologije. Slednja vloga ji ostane tudi v bodoče, več in kmalu pa bo moralo biti narejeno na področju vzpostavljanja ustreznega zakonskega okvira za nove načine in tehnike poslovanja, kjer je enakopraven subjekt tudi sama. Zaščita domače industrije visoke tehnologije se bo morala dogajati po evropsko sprejemljive načine - ne v obliki subvencij in protekcionistično, temveč v obliki razvojnih spodbud in udeležbe v razvojnih projektih. V tej obliki bo morala najti sredstva za pomoč pri vzpostavitvi domače industrije informacijske tehnologije in komunikacij s spodbujanjem vlaganj v informatiko in telekomunikacije, z davčnimi olajšavami ter promocijo. Na trgu storitev bo nastopila kot enakopraven ponudnik, njene storitve pa bodo morale biti ponujene na državljanu prijazen način. Izjemno pomembna vloga države je podporo promocije in aktivnosti v času prehoda v informacijsko družbo ter podpora projektom, ki naslavljajo kulturo. Cilj mora biti podpreti vsa področja in dejavnosti, ki utrjujejo kulturno identiteto ter njeno promocijo, razvijajo ustrezne znanosti in drugih, ki ustvarjajo pogoje za kvalitetnejše življenje in delo v informacijski družbi. Vse javne službe morajo upoštevati, da informacijske storitve niso mogoče brez odprtih in javno dostopnih podatkovnih zbirk, in jih temu primerno ponuditi vsem zainteresiranim pod enakimi, cenovno dostopnimi pogoji.

8. Udeleženci se strinjajo z ugotovitvijo, da se mora v državi ustanoviti nevtralno strokovno telo, ki bo dobilo vlogo usmerjevalnega in svetovalnega foruma za vse aktivnosti v zvezi s prehodom v informacijsko družbo in ki bo tudi sogovornik ustreznih mednarodnih, zlasti evropskih teles. Telo naj bo sestavljeno tako, da bodo v njem zastopani vsi institucionalni sektorji ne glede na vse druge usmeritve, glavno merilo za vstop posameznikov pa mora biti strokovnost. Udeleženci tudi ugotavljajo, da mora obstajati institucionalni okvir, ki bo telo imenoval in mu bo omogočal realne vire za izvajanje nalog in funkcij, ki in kakor bodo opredeljene in potrebne. Dokument, telo in ustanova so celota, ki lahko omogoči lažjo in čim bolj gladko realizacijo nalog in ciljev, določenih v Modri knjigi, in udeleženci posvetovanja podpirajo vse subjekte, ki so pripravljeni sodelovati in se povezovati za dosego tega cilja.
9. Končno udeleženci ugotavljajo, da ima posvetovanje Dnevi slovenske informatike izjemno pomembno vlogo pri (1) vzpostavljanju, ohranjevanju in poglabljanju stikov z vidnimi informatiki slovenskega rodu, ki delujejo na tujem, da ima (2) za nacionalno posvetovanje primerno udeležbo vidnih tujih informatikov, da (3) z možnostmi, ki jih daje domačim, še neuveljavljenim strokovnjakom za javno nastopanje in predstavitev lastnih dosežkov, vzpodbuja strokovno odličnost in s tem, da (4) subvencionira študentom udeležbo na posvetovanju, dopolnjuje segmente usposabljanja, ki še ne morejo biti vključeni v redno izobraževanje in torej SDI kot ustanova civilne družbe že deluje v smislu z Modro knjigo začrtanih usmeritev. Udeleženci priporočajo prirediteljem, naj se taka zasnova in usmeritev posvetovanja ohranita tudi v prihodnje.

Portorož, 24. april 1999

Na posvetovanju Dnevi slovenske informatike je Slovensko društvo INFORMATIKA podelilo naslednja priznanja:

Dr. Matjaž Gams: *za razvoj slovenskega izrazja informatike*
Dr. Matjaž Gams je dolgoletni sodelavec revije Informatica, kjer je kontaktni izvršni urednik. Redno je zaposlen na Inštitutu Jožef Stefan, dolga leta pa sodeluje z obema slovenskima univerzama. Je predsednik Slovenskega društva za umetno inteligenco in Društva za kognitivne znanosti; je tajnik Slovenskega akademijskega tehniško-naravoslovnega društva SATENA, ki ima v svoji sestavi tudi Inženirsko akademijo Slovenije, in član izvršnega odbora Slovenskega društva INFORMATIKA. Je podpredsednik za znanost pri sindikatu SVIZ. Njegova bibliografija zajema več sto objav v znanstvenih revijah, knjigah, zbornikih konferenc in tujih revijah s področja računalništva in informatike. Med praktičnimi dosežki je zadnji, ne pa edini zaposlovalni agent na internetu, ki nastaja tudi v okviru mednarodnega projekta in razume slovensko in angleško. Dr. Gams je sodeloval pri izdaji računalniškega slovarčka, leksikona "Računalništvo" in velikega leksikona Cankarjeve založbe ter tako sooblikoval temelje slovenskega računalniškega izrazoslovja na področju informatike in računalništva.

Dr. Marjan Krisper: *za dosežke v prenosu tehničnih spoznanj v poslovna okolja*
Dr. Marjan Krisper je med bolj izpostavljenimi, ko gre za prenos in uveljavitev sodobnih tehnoloških in poslovnih možnosti informatike v naše okolje. Pri tem ga vodijo izkušnje in prefinjen občutek ocene primernosti in praktične uporabnosti teoretično obetavnih tehnoloških usmeritev in pristopov. Tako je skozi pedagoško delo na Fakulteti za računalništvo in informatiko in usmerjanje projektov informatizacije v naših organizacijah usposobil plejado informatikov ter uveljavil načrten in urejen inženirski pristop k razvoju informatike. Projektni pristop in pomemben premik v kakovosti načrtovanja, vzpostavljanja in spremljanja informacijskih projektov je uveljavil tudi v državni upravi. Bil je soustanovitelj prve slovenske računalniške revije BIT in eden prvih pobudnikov združevanja gospodarskih subjektov s področja informatike, kar je pripomoglo k ustanovitvi Združenja za računalništvo in informatiko pri GZS. Je tudi član izvršnega odbora Slovenskega društva INFORMATIKA.

Dr. Anton P. Železnikar: *za mednarodno uveljavitev slovenskih dosežkov v informatiki*
Dr. A. P. Železnikar je v teku svoje bogate znanstvene in poslovne kariere izjemno veliko teoretično in praktično prispeval k razvoju informatike. Od sedemdesetih let dalje je usmerjal in vodil razvoj računalniških naprav in programskih produktov tedanje domače računalniške industrije. Poleg tega je bil vseskozi prisoten s prispevki na mednarodnih strokovnih in znanstvenih srečanjih, ki se jih še vedno udeležuje. Za vse dosežke ga je Slovensko društvo INFORMATIKA imenovalo za častnega predsednika. Dr. A. P. Železnikar je bil eden od ustanovnih članov društva in njegov prvi predsednik. Že leto dni po ustanovitvi je začel izdajati znanstveno revijo Informatica, ki je še danes edina znanstvena revija za področje informatike, ki izhaja v Sloveniji in ima mednarodno veljavo. Pojavlja se kot referenčna publikacija v mednarodnih navedbenih podatkovnih bazah SCI, SSCI in TCI. Glavno zaslugo za tak status revije ima dr. Železnikar, ki je njen sodelavec in glavni urednik vse od njene ustanovitve dalje. Njegova velika zasluga je, da je Slovenija na področju informatike mednarodno prepoznavna in je bilo tudi zato Slovensko društvo INFORMATIKA sprejeto v mednarodni združenji CEPIS in IFIP brez vsakega zadržka.

Na letošnjem posvetovanju Dnevi slovenske informatike so udeleženci podelili naslednja priznanja:

Najaktualnejši prispevek:
Miran Merčun: Vpeljava poslovnega informacijskega sistema v Telekomu Slovenije
Najzanimivejši prispevek:
Boris Benko, Viljem Žumer: Implementacija protokola za dodeljevanje in izmenjavo podatkov pri paralelnem procesiranju
Najbolje predstavljeni prispevek:
Metka Hajšek: Koliko naj danes izdelam?

IZ POROČILA NADZORNEGA ODBORA SLOVENSKEGA DRUŠTVA INFORMATIKA ZA LETO 1998

V letu 1998 je imel izvršni odbor SDI tri seje, eno korespondenčno sejo in en sestanek. Na sejah in sestanku izvršnega odbora SDI so obravnavane zadeve, ki izhajajo iz delovnega področja SDI, kot so:

- posvetovanje Dnevi slovenske informatike (o pripravah, organizaciji, izvedbi in rezultatih 1998 ter o pripravah posvetovanja v letu 1999)
- urejanje zadev v zvezi z uskladitvijo statuta SDI z Zakonom o društvih
- uskladitev uredništev Uporabne informatike in Informatice z določili statuta
- izobraževanje in usposabljanje na področju informatike v Sloveniji
- Modra knjiga o informatiki
- sodelovanje na domačih in mednarodnih strokovnih konferencah oziroma simpozijih
- mednarodno sodelovanje
- včlanitev v mednarodne asociacije s področja informatike (CEPIS, IFIP - o tem so bili prispevki že objavljeni v Uporabni informatiki; za CEPIS v številki 2/1998, za IFIP v številki 3/1998)
- domača stran SDI na internetu
- organiziranje posvetovanja Informacijske storitve za lokalno samoupravo.

Sklepi izvršnega odbora SDI na sejah in sestanku v letu 1998 so bili v skladu s statutom SDI.

Dne 24. 12. 1998 je Upravna enota Ljubljane, kot pristojni organ, izdala za SDI odločbo: »V Register društev, ki ga vodi Upravna enota Ljubljana, se pod zaporedno številko 1861 vpiše Slovensko društvo informatika, s sedežem v Ljubljani, Vožarski pot 12, dosedaj vpisano v Register društev pri Ministrstvu za notranje zadeve Republike Slovenije, pod zaporedno številko 109 ter pri tem društvu sprememba temeljnega akta. Kot zastopnik društva se vpiše Niko Schlamberger.«

Upravna enota Ljubljana je kot pristojni organ ugotovila, »da je temeljni akt, s sprejetimi spremembami in dopolnitvami v skladu z določbami Zakona o društvih, izpolnjeni pa so tudi drugi pogoji za registracijo sprememb temeljnega akta društva ter registracijo zastopnika društva«.

Z dnem, ko je pristojni organ registriral spremembe in dopolnitve temeljnega akta je stopil v veljavo »novi« statut SDI (50. člen Statuta SDI).

V poročilu nadzornega odbora za občni zbor leta 1997 so bili prikazani tudi podatki o finančnem poslovanju društva za obdobje od 1993 do 1996, niso pa bili prikazani rezultati finančnega poslovanja za leto 1997, ker še nismo imeli vseh podatkov. Zaradi kontinuitete o finančnem poslovanju SDI in boljše informiranosti vseh članov društva so v tem poročilu prikazani osnovni podatki o finančnem poslovanju SDI tudi za leto 1997.

V letu 1997 je društvo imelo skupaj:

- prihodke 26.706.631,02 SIT
- stroške 20.998.666,90 SIT

Presežek finančnega poslovanja pa je bil: 5.707.964,12 SIT

V letu 1998 je društvo imelo **skupaj:**

- prihodke 24.029.416,63 SIT
- stroške 21.211.256,73 SIT

Presežek finančnega poslovanja pa je bil: 2.818.159,90 SIT

Podatke o finančnem poslovanju SDI je prikazal in pregledal Nadzorni odbor na podlagi finančnega poročila ge. Milene Šercer in finančnih izpiskov s posameznimi podatki o prihodkih in stroških po sekcijah društva. Konec leta 1998 niso še bili plačani računi za Uporabno informatiko za leto 1997 in 1998 skupaj 448.980.00 SIT in tudi račun za DSI '97 v znesku 44.000,00 SIT.

Iz prikazanih podatkov je razvidno, da je bilo finančno poslovanje SDI bolj uspešno v letu 1997. Zato bo potrebno pri nekaterih sekcijah društva izvesti ustrezne aktivnosti, da se zmanjša primanjkljaj in s tem tudi omogoči nadaljnje uspešno delovanje društva.

Nadzorni odbor SDI predlaga, da se v bodoče, poleg zagotavljanja podatkov za letno poročilo, tudi sestavlja letno poročilo društva v skladu z določili Slovenskega računovodskega standarda 33 (1996), ki veljajo za društva.

Poročilo sta pripravila:

Ljubica DJORDJEVIĆ, predsednica Nadzornega odbora SDI in Zlatko RITLOP, član Nadzornega odbora SDI

Business Information Technology Management the global imperative	30. 6. - 2 . 7. 1999	Cape Town, South Africa	University of Western cape, Cape Town, South Africa	http://www.man-bus.mmu.ac.uk/confs/bitworld
19TH IFIP CONF. ON SYSTEM MODELLING & OPTIMISATION	12. - 16. 7. 1999	Cambridge, UK	IFIP TC7	m.j.d.powell@dampt.cam.ac.uk fax: + 44 122 3 337918
INTL. CONF. ON BUILDING UNIVERSITY ELECTRONIC EDUCATIONAL ENVIRONMENTS	3. - 6. 8. 1999	Irvine, CA, USA	IFIP WG3.2	ifipconf@uci.educi.edu http://www. eee.uci.edu/program/ifipwg32/
INFORMATION SYSTEMS DEVELOPMENT ISD '99	11. - 13. 8. 1999	Boise, Idaho, USA	Boise State University Univerza v Mariboru, FOV University of Gdansk	W.Gregor Wojtkovski ISD'99 ISD99@cobfac.idbsu.edu www.idbsu.edu/isd99
ISSC Conference: Citizen and Public Administration at the information Age	18. - 20. 8. 1999	Tampere, FI	ISSC	http://www.uta.fi/laitokset/hallinto/CIPA99/
IFIP WORLD COMPUTER CONGRESS 2000	21 - 25. 8. 1999	Beuing. PRC	IFIP	mqzhou@public.bta.net.cn fax: + 86106882 34 58
INTERACT '99 HUMAN COMPUTER INTERACTION	29. 8. - 3. 9. 1999	Edinburgh, UK	IFIP TC13	kilgour@bcs.org.uk, fax: +44 1314513327
THE 5TH INTERNATIONAL SYMPOSIUM ON OPERATIONAL RESEARCH SOR '99	30. 9. - 2. 10. 1999	Preddvor, Slovenija	Slovensko društvo INFORMATIKA, Sekcija za operacijske raziskave	Lidija Zadnik Stirn lidija.zadnik@uni-lj.si fax: + 386 61 271 169
3rd Intl. Symposium on Environmental Software Systems	30.8.-2.9.1999	Dunedin, NZ	IFIP WGS.I 1, CRLE Guelph, CA; Univ. of Otago, NZ.; Aust. Research Ctr., Seibersdorf, AT	ralf.denzer@eii.hd.shuttle.de, Fax: +49 6223 970236
IFIP WG9.4 Conf. on The Social Implications of Computers in Developing Countries	15. - 16. 9. 1999	Kuching, MY	IFIP WG9.4, Univ. Malaysia Sarawak	roger@fit.unimas.my, Fax: +82 672301
Work. Conf. on Information System Concepts: An Integrated Discipline Emerging	20. - 22. 9. 1999	Leiden, NL	IFIP WG8.1	alexander.verrynstuan~wxs.nl, http://www.wi.leidenuniv.nl/-verrynsdISC04-f.html, Fax: +31 71 5276985
7th International Conference on the Auditing and Control of Information Systems	22. - 24. 9. 1999	Otočec, Slovenija	Slovenski inštitut za revizijo, ISACA	www.si-revizija.si
20th Annual International Conference on IInformation Systems ICIS '99	12. - 15. 12. 1999	Charlotte, North Carolina	ICIS	http://www.uncc.edu/icis99/
HAWAI'I International Conference on System Sciences	4. - 7. 1. 2000	Maui, Hawaii	HICSS-33, University of Hawaii's College of Business Administration	hicss@hawaii.edu fax:1 808 956 57 59 http://www.hicss.hawai.edu
7th Int. IFIP Conf. on Women, Work and Computerisation	25. - 28. 5. 2000	Vancouver, BC, CA	IFIP WG9.1, WG on Women and Computing	ebalka@sfu.ca, Fax: +1 604 2914024
IFIP World Computer Congress 2000	21. - 25. 8. 2000	Beijing, CN	IFIP	mqzhou@public.bta.net.cn, http://www.cie- china.org/wcc2000.htm, Fax: +861 06828 3458
European Conference on Information Systems ECIS 2001 Global Co-operation in the New Millenium	27. - 29. 6. 2001	Bled, Slovenija	Univerza v Mariboru, FOV Kranj	http://ecis2001.fov.uni-mb.si fax: +386 64 374 299
7th IFIP World Computer Conf. on Computers in Education	29. 7. - 3. 8. 2001	Copenhagen, DK	IFIP TC3	tf@sek.ddf.dk, Fax: +45 33 931580
Symposium on Information Control Problems iin Manufacturing Technologies	24. -26. 9. 2001	Vienna, AT	FAC, IFIP TCS	e318@ihrtl.ihrt.tuwien.ac.at, Fax: +43 1 50418359

Pristopna izjava

Želim postati član Slovenskega društva Informatika

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

(ime in priimek, s tiskanimi črkami)

(poklic)

(domači naslov in telefon)

(službeni naslov in telefon)

(elektronska pošta)

Datum: Podpis:

Včlanite se v Slovensko društvo INFORMATIKA.

Članarina SIT 5.200,- (plačljiva v dveh obrokih) vključuje tudi naročnino za revijo Uporabna informatika.

Študenti imajo posebno ugodnost: plačujejo članarino SIT 2.400,- in za to prejemajo tudi revijo.

Izpolnjeno Naročilnico ali Pristopno izjavo pošljite na naslov:
Slovensko društvo INFORMATIKA, Vožarski pot 12, 1000 Ljubljana.

Naročilnica

Naročam(o) revijo UPORABNA INFORMATIKA

- ☐ s plačilom letne naročnine SIT 4.600
- ☐ ..... izvodov, po pogojih za podjetja SIT 8.900 za eno letno naročnino in SIT 8.000 za vsako nadaljnjo naročnino
- ☐ po pogojih za študente letno SIT 2.000

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

_____

(ime in priimek, s tiskanimi črkami)

_____

(podjetje)

_____

(ulica, hišna številka)

_____

(pošta)

Datum: Podpis:

■

UPORABNA INFORMATIKA
ISSN 1318-1882

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

Glavni in odgovorni urednik:
Mirko Vintar

Uredniški odbor:
Dušan Caf, Aljoša Domjan, Janez Grad, Andrej Kovačič, Tomaž Mohorič,
Katarina Puc, Vladislav Rajkovič, Ivan Rozman, Niko Schlamberger, Ivan Vezočnik, Mirko Vintar

Tehnična urednica: Katarina Puc

Oblikovanje: Zarja Vintar, Dušan Weiss, Ada Poklač
Naslovnica: Zarja Vintar

Tisk: Prograf
Naklada: 700 izvodov

Revija izhaja četrtletno. Cena posamezne številke je 2.500 SIT.

Letna naročnina za podjetja SIT 8.900, za vsak nadaljnji izvod SIT 8.000.
Letna naročnina za posameznika SIT 4.600, za študente SIT 2.000.

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 13 Zakona o prometnem davku, za katere se plačuje davek od prometa proizvodov po stopnji 5 %. Prometni davek je vračunan v ceno revije.