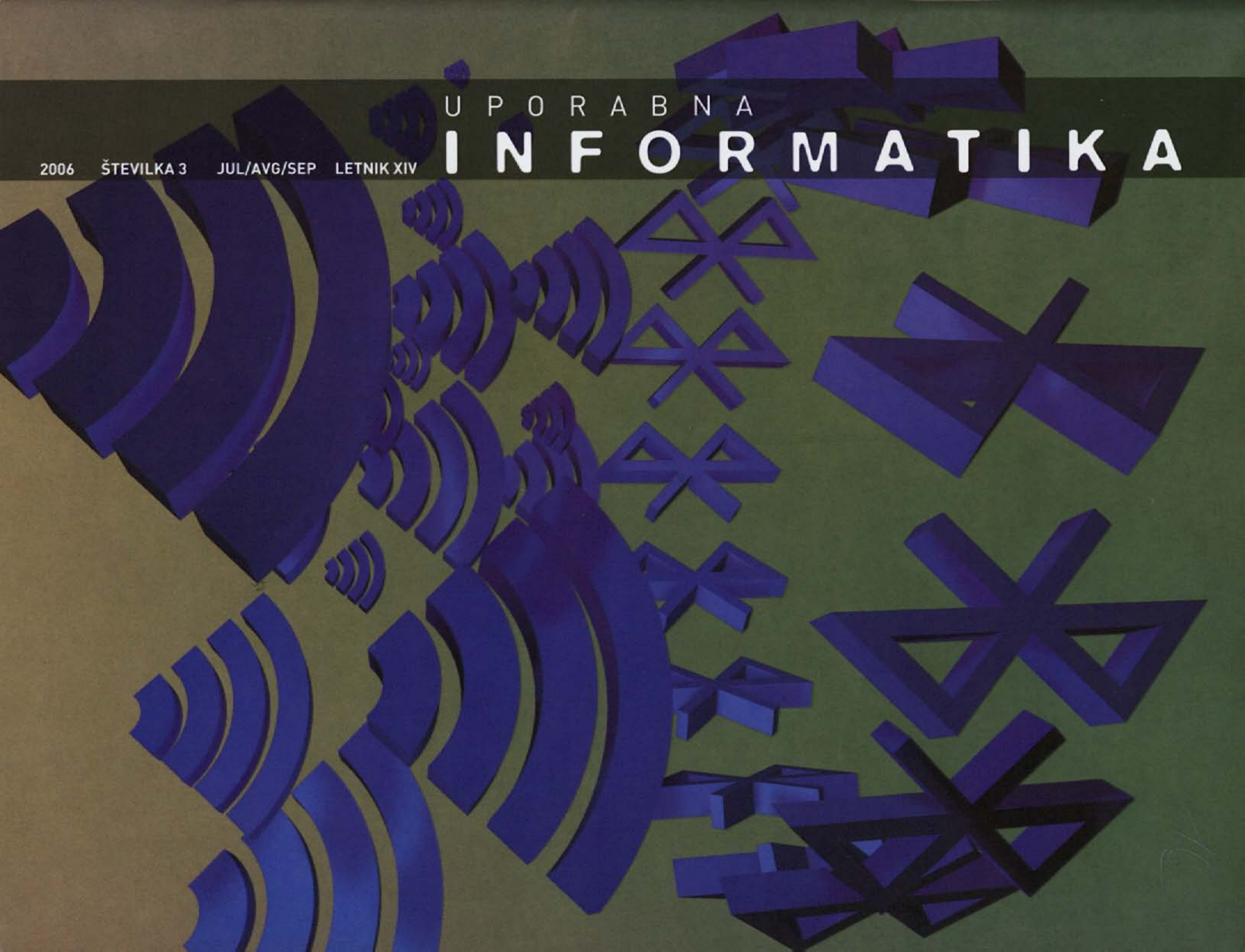
2006 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XIV

UPORABNA INFORMATIKA



Izpitni centri ECDL

ECDL (European Computer Driving License), ki ga v Sloveniji imenujemo evropsko računalniško spričevalo, je standardni program usposabljanja uporabnikov, ki da zaposlenim potrebno znanje za delo s standardnimi računalniškimi programi na informatiziranem delovnem mestu, delodajalcem pa pomeni dokazilo o usposobljenosti. V Evropi je za uvajanje, usposabljanje in nadzor izvajanja ECDL pooblaščena ustanova ECDL Foundation, v Sloveniji pa je kot član CEPIS (Council of European Professional Informatics Societies) to pravico pridobilo Slovensko društvo INFORMATIKA. V državah Evropske unije so pri uvajanju ECDL močno angažirane srednje in visoke šole, aktivni pa so tudi različni vladni resorji. Posebej pomembno je, da velja spričevalo v več 140-tih državah, ki so vključene v program ECDL. Doslej je bilo v svetu izdanih že več kot 5,5 milijonov indeksov, v Sloveniji okoli 4000 in več kot 2000 podeljenih spričeval. Za izpitne centre ECDL so se v Sloveniji usposobile organizacije, katerih logotipi so natisnjeni na tej strani.

AGORA ustvarjalne komunikacije

PECA ALP VIZIJA RAZVOJA

SOFT

IZOBRAŽEVANJE INFORMACIJSKE STORITVE

ELES - ICES

UNIVERZA V LJUBLJANI Fakulteta za pomorstvo in promet

ISA INFORMACIJSKE TEHNOLOGIJE

ISER

KOPA

LJUDSKA UNIVERZA KOPER UNIVERSITÀ POPOLARE CAPODISTRIA

LJUDSKA UNIVERZA CELJE

LJUDSKA UNIVERZA MURSKA SOBOTA

Micro Team

Much

SC Slovenske Konjice - Zreče

spin

SRCSI sistemske integracije

ŠOLSKI CENTER Novo mesto

ŠCV ŠOLSKI CENTER VELENJE

UPI LJUDSKA UNIVERZA ŽALEC šola prijaznih ljudi

vls computers

PRAH IZOBRAŽEVALNI CENTER Rogaška Slatina www.prah.si

LASER computer RAČUNALNIŠTVO RAZVOJ PROIZVODNJA TRGOVINA SERVIS IZOBRAŽEVANJE

Intereuropa it Informacijska tehnologija, d.o.o.

UPORABNA
INFORMATIKA
2006 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XIV ISSN 1318-1882

Uvodnik

Razprave

Izbrani prispevki DSI 2006

Poročila

Obvestila

Koledar prireditev

UPORABNA
INFORMATIKA

2006 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XIV ISSN 1318-1882

Ustanovitelj in izdajatelj
Slovensko društvo INFORMATIKA
Vožarski pot 12
1000 Ljubljana

Predstavnik
Niko Schlamberger

Odgovorni urednik
Andrej Kovačič

Tehnična urednica
Mira Turk Škraba

Oblikovanje
Bons

Prelom
Dušan Weiss, Ada Poklač

Tisk
Prograf

Naklada
700 izvodov

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

Revija izhaja četrtletno. Cena posamezne številke je 5.000 SIT (20,86 €). Letna naročnina za podjetja 20.000 SIT (83,45 €), za vsak nadaljnji izvod 14.000 SIT (58,48 €), za posameznike 8.000 SIT (33,81 €), za študente 3.500 SIT (14,61 €).
Cene v evrih so informativne; izračunane so po centralnem paritetnem tečaju 1 € = 239,640 SIT

Revijo sofinancira Ministrstvo za visoko šolstvo, znanost in tehnologijo.

Revija Uporabna informatika je od številke 4/VII vključena v mednarodno bazo INSPEC.

Revija Uporabna informatika je pod zaporedno številko 666 vpisana v razvid medijev, ki ga vodi Ministrstvo za kulturo.

Navodila avtorjem

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

Članke objavljamo praviloma v slovenščini, prispevke tujih avtorjev v angleščini.

Prispevki so obojestransko anonimno recenzirani. Vsak članek za rubriko Razprave mora za objavo prejeti dve pozitivni recenziji. O objavi samostojno odloča uredniški odbor.

Prispevki naj bodo lektorirani, v uredništvu opravljamo samo korekturo. Po presoji se bomo posvetovali z avtorjem in članek tudi lektorirali. Prispevki za rubriko Razprave naj imajo dolžino do 40.000, prispevki za rubrike Rešitve, Poročila do 30.000, Obvestila pa do 8.000 znakov.

Naslovu prispevka naj sledi ime in priimek avtorja, ustanova, kjer je zaposlen, in elektronski naslov. Članek naj ima v začetku do 10 vrstic dolg izvleček v slovenščini in angleščini, v katerem avtor opiše vsebino prispevka, dosežene rezultate raziskave. Abstract se začne s prevodom naslova v angleščino. Članku dodajte kratek avtorjev življenjepis (do 8 vrstic), v katerem poudarite predvsem delovne dosežke.

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

Revijo tiskamo v črno-beli tehniki s folije, zato barvne slike ali fotografije kot originali niso primerne. Objavljali tudi ne bomo slik zaslonov, razen če niso nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme ipd. naj imajo belo podlago. Po možnosti jih pošiljajte posebej, ne v datoteki z besedilom članka. Disketi z besedom priložite izpis na papirju.

Prispevke pošiljajte po elektronski ali navadni pošti na naslov uredništva revije: ui@drustvo-informatika.si, Slovensko društvo INFORMATIKA, Vožarski pot 12, 1000 Ljubljana; na teh naslovih dobite tudi vse dodatne informacije.

Po odločitvi uredniškega odbora o objavi članka bo avtor prejel pogodbo, s katero bo prenesel vse materialne avtorske pravice na Slovensko društvo INFORMATIKA. Po izidu revije pa bo prejel nakazilo avtorskega honorarja po veljavnem ceniku ali po predlogu odgovornega urednika.

Spoštovane bralke in spoštovani bralci,

pričujoči uvodnik nima namena povzemati vsebine številke revije, kakor je navada sicer. To je opravil odgovorni urednik že v prejšnji številki, ko je pojasnil namen in vsebino objavljenih prispevkov. Referatov, ki so po oceni uredništva zaslužili širšo predstavitev kot zgolj objavo v zborniku posvetovanja Dnevi slovenske informatike 2006, je bilo več kot le za eno številko in vsebina tokratne je nadaljevanje, ki skupaj s prejšnjo tvori celoto najodmevnejših prispevkov s posvetovanja.

Čast in prijetno dolžnost imam, da vas v uvodniku spomnim na trideseto obletnico ustanovitve Slovenskega društva INFORMATIKA. Zdi se, da je minilo le malo časa od tedaj, ko mi je uredništvo zaupalo podobno zadolžitev, namreč uvodnik ob petindvajseti obletnici ustanovitve društva. Tedaj sem v spominu preletel obdobje od ustanovitve dalje in obnovil pomembne dosežke društva v tistem obdobju. Danes, po petih letih, je moj razmislek podoben. Če se je tedaj zaključevalo obdobje mladostne zagnanosti, prihaja društvo sedaj že v obdobje zrelosti. Pet let je za nove dosežke razmeroma kratko obdobje, vendar se je nekaj takih, ki so vredni omembe in zapisa, le nabralo. Prav vsi mogoče res niso bili taki, da bi se z njimi hvalili, vendar jih zaradi korektnosti ne smemo zamolčati. Ob tem se spomnimo na dve modrosti. Prva je iz pesmi Otona Župančiča, ki pravi, da gre le osel samo enkrat na led, človek pa se iz tega, da mu je spodrsnilo, kaj nauči. Druga je novejša, ameriška, ki uči, da tisti, ki nikoli nič novega ne poskusi, tudi nikoli nič novega ne doseže. Srečna okoliščina, ki je mogoče tudi posledica modrosti in izkušenosti, je, da nam ni prav mnogokrat zdrsnilo, imamo pa zato tem več novih dosežkov. V prvi skupini je pravzaprav le soustanovitev foruma za informacijsko družbo, ki ni zaživel. Sicer še vedno ne mislim, da je bilo to dejanje nepotreben ali celo napačen korak, mogoče smo bili ustanovitelji kljub izkušnjam le preveč optimistični.

Več je dosežkov, ki so nam v čast in ki prispevajo k namenu ustanovitve društva. V Slovenijo smo uvedli evropsko računalniško spričevalo ECDL, kar je pomemben prispevek za večjo računalniško pismenost in prisotni smo v vodstvu ustanove ECDL Foundation. Potem ko smo se leta 1998 včlanili v evropsko združenje CEPIS in svetovno organizacijo IFIP, smo prisotni v izvršnih odborih in tehničnih odborih teh asociacij. Vse to priča o ugledu društva in posameznikov, pomembno pa prispeva tudi k vidnosti Slovenije. Bili smo pobudniki in soustanovitelji regionalne organizacije IT STAR, ki razvija novo storitev za člane svojih društev. Razvili smo internetni slovar informatike, ki je viden svetovni dosežek svoje vrste. Dosegli smo status društva, ki deluje v javnem interesu. Vse to in še več v petih letih niso zanemarljivi dosežki za organizacijo, ki je razpolagala z razmeroma skromnimi viri, in veseli nas, da lahko vse to predstavimo. Še bolj nas veseli, ker s tem dokazujemo, da srčnost štiriindvajsetih mož in žena pred tridesetimi leti ni bila zaman.

Kaj pa naprej? Seveda trdno verjamemo, da bomo praznovali še mnogo okroglih obletnic in da se bomo tedaj lahko pohvalili z novimi dosežki. Pred petimi leti smo si zadali cilj, da postanemo vidni in koristni, in ta cilj smo dosegli. Tudi danes imamo cilje in ti morajo biti višji. To kar bi radi dosegli v prihodnosti, je, da društvo postane ne igralec – to je že –, temveč dejavnik. Naj ilustriram: rad bi doživel, da bi država sprejela kak predpis (ali zavrnila njegov sprejem) z obrazložitvijo, da ne more in ne sme prezreti stališča Slovenskega društva INFORMATIKA. Cilj je visok, ni pa nedosegljiv. To potrjujejo dosežki sorodnih nacionalnih in mednarodnih združenj. Samo od vseh nas je odvisno, ali ga bomo dosegli, saj uspeh ni samo rezultat dela predsednika, vodstva društva ali članov, temveč rezultat dela vseh – predsednika, vodstva društva in članov.

Niko Schlamberger,

predsednik Slovenskega društva INFORMATIKA

Slovensko društvo INFORMATIKA

vabi k udeležbi na posvetovanju

Dnevi slovenske informatike 2007

»Z informatiko do novih poslovnih priložnosti«

Portorož, 11.–13. april 2007

Spoštovani,

pred nami je 14. posvetovanje Dnevi slovenske informatike – DSI 2007. Z zadovoljstvom ugotavljamo, da so bila dosedanja posvetovanja zelo uspešna in da so jih udeleženci dobro ocenili. Tudi na tokratnem srečanju bomo skušali zajeti aktualne vsebine z vseh pomembnih področij informatike ter ponuditi dovolj priložnosti za poslovna srečanja in druženje ob skrbno pripravljenih družabnih dogodkih.

Rdečo nit posvetovanja DSI 2007 označuje naslov »**Z informatiko do novih poslovnih priložnosti**«. Dolgo je veljalo, da je informatika oziroma informacijska tehnologija podporna dejavnost, ki omogoča le avtomatsko obdelavo podatkov oziroma nadomeščanje žive delovne sile. O povečanju učinkovitosti poslovanja, zmanjšanju stroškov ter avtomatizaciji poslovnih procesov se je začelo govoriti precej pozneje. M. Hammer je že leta 1991 dejal, da prenove – »radikalne«, kot jo je predlagal –, ne bo mogoče izpeljati brez informatike. To spoznanje je zahtevalo tudi premike pri obvladovanju in upravljanju procesov informacijske tehnologije.

Povečanje konkurenčnosti z informatiko je stalnica vseh razprav zadnjih let, vendar nam informatika oziroma informacijska tehnologija ponujata veliko več: nove poslovne priložnosti, izdelke in storitve, ki jih prej ni bilo, nastanek novih gospodarskih subjektov, oblikovanje povsem novih potreb potrošnikov na globalni ravni in s številnimi multiplikativnimi učinki. Nekatere tehnologije vplivajo na spremembe življenjskih navad, odpirajo se številna sociološka vprašanja, predvsem glede varovanja zasebnosti, varnosti itd.

Na posvetovanju DSI 2007 bomo skušali odgovoriti na te izzive s kakovostnimi prispevki in razpravami na okroglih mizah. Vljudno vas vabimo, da se nam pridružite.

Pomembni datumi	
Rok za oddajo prispevkov	24. 1. 2007
Obvestilo avtorjem o uvrstitvi v program	14. 2. 2007
Rok za oddajo končnih prispevkov	7. 3. 2007
Posvetovanje	11.–13. 4. 2007

Podrobnejše informacije so vam na voljo na spletnem naslovu www.dsi2007.si

Na svidenje v Portorožu!

Slovensko društvo INFORMATIKA

Primerjava varnostnih mehanizmov brezžičnih tehnologij Bluetooth in Wireless LAN 802.11 WPA

Marko Hölbl, Boštjan Brumen, Tatjana Welzer
Fakulteta za elektrotehniko, računalništvo in informatiko, Univerza v Mariboru, Smetanova 17, 2000 Maribor
{marko.holbl, bostjan.brumen, welzer}@uni-mb.si

Povzetek

Brezžične tehnologije se vedno bolj uveljavljajo in izpodrivajo klasične kabelske povezave. Vedno večji pomen pridobiva področje mobilnih aplikacij v informatiki in s tem tudi brezžične tehnologije. Mednje sodita tudi tehnologiji Bluetooth in Wireless LAN (WLAN) družine standardov IEEE 802.11. Bluetooth je vodilna brezžična tehnologija na področju mobilnih aplikacij, WLAN pa predstavlja alternativno obliko povezovanja računalniških omrežij in informacijskih sistemov. Pomemben vidik brezžičnega povezovanja je zagotavljanje varnosti. Tehnologiji implementirata varnostne mehanizme, tj. overjanje in šifriranje podatkov. V članku analiziramo varnostne mehanizme obeh tehnologij in ju primerjamo s stališča varnostnih mehanizmov. Kriterije smo določili na podlagi varnostnih načel (zaupnost, overjanje in celovitost). Potem smo po zastavljenih kriterijih primerjali obe tehnologiji. Bluetooth ima višjo stopnjo varnosti in bolj izpopolnjen mehanizem varnosti, vendar tudi WLAN WPA ne zaostaja veliko.

Abstract

Comparison of security mechanisms of Bluetooth and Wireless LAN 802.11 WPA

Wireless technologies are establishing their role in the market and are replacing classical cable connections. Mobile application and wireless connection technologies are gaining a significant role in modern IT. The two wireless technologies Bluetooth and Wireless LAN (WLAN) belong to the family of standards IEEE 802.11. Bluetooth is the leading wireless technology from the field of mobile applications, whereas WLAN is an alternative technology for connecting computer networks and information systems. An important aspect of wireless connectivity is security assurance. Both technologies implement security mechanisms, e.g. authentication and encryption. This paper deals with the analysis and comparison of WLAN WPA with Bluetooth (from the security mechanisms perspective). We have defined certain criteria on the basis of the security principles (confidentiality, authentication and integrity). We conducted a comparison of security mechanisms on the basis of the above criteria. Bluetooth offers a higher security level and more improved security mechanisms. Nevertheless, WLAN WPA does not fall behind.

1 Uvod

V sodobnem svetu smo priča razmahu brezžičnega povezovanja različnih naprav – od računalnikov do mobilnih telefonov. Množica tehnologij brezžičnega povezovanja nadomešča žično povezovanje. Mednje sodijo tehnologije kot so Bluetooth, Wireless LAN (angl. Local Area Network) ali tehnologije podatkovnega prenosa prek GSM omrežij (GPRS, EDGE ipd.). Ker je medij, po katerem se prenašajo podatki, prosto dostopen, moramo biti pozorni na varnostne vidike prenosa. Brezžično povezovanje se uveljavlja tudi na področju mobilnih aplikacij in informacijskih sistemov. V članku bomo analizirali varnostne mehanizme tehnologije Bluetooth (Bluetooth specifikacija 1.2) [3] in Wireless LAN z varovalnim mehanizmom WPA (angl. WI-Fi Protected Access) [6]. Pod terminom Wireless LAN (WLAN) razumemo brezžično tehnologijo za povezovanje družine standardov IEEE 802.11. Na podlagi izbranih primerjalnih kriterijev bomo primerjali varnostne mehanizme obeh tehnologij. Pri tem se bomo omejili na varnostne mehanizme specifikacije Bluetooth 1.2 in specifikacije WLAN WPA, ki je namenjen zaščiti povezav WLAN. Pri tehnologiji WLAN je tudi moč zaslediti nove standarde varovanja kot sta WPA2 oz. standard 802.11i, vendar je WPA najbolj razširjen in široko podprt od proizvajalcev brezžične mrežne opreme.

Tehnologija WPA omogoča dva načina delovanja glede na področje uporabe:

- varovanje v srednjih in velikih organizacijah ter
- varovanje v domačih brezžičnih omrežjih in malih podjetjih.

Za vsako področje uporabe so definirani drugi načini oz. mehanizmi varovanja. V prvem primeru uporabljamo standard 802.1X in strežnike RADIUS, ki so namenjeni overjanju in upravljanju s ključi. V drugem primeru pa se uporablja način PSK (angl. Pre-Shared

Key). V okviru slednjega uporabnik ročno vnese vnaprej definiran ključ v vse mrežne naprave. Ker je področje uporabe Bluetootha primerljivo s področjem uporabe WLAN v domačih okoljih in malih podjetjih, bomo izvedli primerjavo varnostnih mehanizmov tehnologije Bluetooth po specifikaciji 1.2 in varovanje WLAN WPA v načinu PSK.

Kljub temu, da je bila pred kratkim sprejeta specifikacija Bluetooth 2.0 [4], le-ta ne bo zajeta v članku, saj definira enake varnostne mehanizme kot specifikacija 1.2.

Članek ne obravnava tehnologij za prenos podatkov po omrežjih GSM oz. UMTS, saj so tehnologije in njihovi varnostni vidiki vezani na infrastrukturo omrežja in dejavnost operaterja. Prav tako nista namenjeni povezovanju naprav v domačih oz. poslovnih okoljih.

Članek je razdeljen v pet delov. Uvodu, v katerem je opisana metodologija, ki jo bomo kasneje uporabili za primerjavo, sledi obravnava tehnologij Bluetooth in WLAN ter primerjava varnostnih mehanizmov.

1.1 Metodologija

Zaradi boljšega pregleda in razumljivosti varnostnih mehanizmov obeh tehnologij bomo naredili kratek splošen pregled tehnologije Bluetooth in WLAN, nato se bomo osredinili na varnostne mehanizme, ki jih posamezna tehnologija vsebuje.

Na področju varnostnih informacijsko-komunikacijskih tehnologij veljajo varnostni principi, ki jih želimo izpolniti [20]:

- overjanje (angl. Authentication),
- zaupnost (angl. Confidentiality),
- celovitost (angl. Integrity) in
- nezanikanje (angl. Non-repudiation).

Pri primerjanju bomo zajeli principe overjanja, celovitosti in zaupnosti. Princip ne-zanikanja bomo izpustili, saj se uporablja na višji komunikacijski ravni.

Primerjava kakovosti varnostne tehnologije je možna prek tehnologij, ki zagotavljajo izpolnjevanje določenega varnostnega principa. Zaupnost zagotavljamo s pomočjo šifriranja in ustreznih algoritmov. Zato bo del primerjave varnostnih mehanizmov primerjava šifrirnega algoritma in njegovih parametrov, ki vplivajo na raven zaščite. Pomemben parameter je dolžina ključa; daljši je ključ, manj verjetno je, da je mogoče izvesti napad z grobo silo (angl. Brute-force Attack) in tako pridobiti podatke. Kot primerjalni kriterij bomo definirali dolžino ključa. Kakovost posameznega algoritma vpliva na odpornost na različne napade. Algoritem ne sme vsebovati varnostnih lukenj, prek katerih je napadalcu omogočen nepooblaščen dostop do podatkov. Zato so drugi primerjalni kriterij morebitni obstoječi napadi ali druge pomanjkljivosti, ki so bile odkrite in objavljene. Tudi zelo kakovosten algoritem ne daje zaščite, če ga naprava ne uporablja. Zato bomo v sklop primerjave vključili kriterij o obveznosti uporabe šifriranja.

Overjanje je zagotavljanje verodostojnosti entitet, udeleženih v komunikaciji. Tudi v primeru overjanja se uporabljajo algoritmi za overjanje in pripadajoči ključi. Kakor pri šifriranju podatkov lahko tudi kakovost overjanja določimo s pomočjo dolžine ključa, karakteristik algoritma (odpornost na napade, varnostne luknje) in obveznosti uporabe overjanja.

Tretji princip, celovitost, zagotavlja, da spreminjanje podatkov ne ostane neopaženo. Če torej napadalec spremeni podatke med prenosom, je to mogoče zaznati. Primerjali bomo algoritme, ki jih oba standarda predvidevata za zagotavljanje celovitosti – ali so znane pomanjkljivost oz. varnostne luknje. Tudi pri tem principu bo kriterij obveznost uporabe tehnologij za zagotavljanje celovitosti.

Za zagotavljanje varnosti je pomembno opredeliti, ali se za overjanje, šifriranje in zagotavljanje celovitosti uporabljajo različni ključi. S tem ko uporabljamo različne ključe pri šifrirnih oz. overitvenih algoritmih, lahko zagotovimo višjo raven varnosti, saj ob pridobitvi enega izmed ključev ne moremo zaobiti vseh mehanizmov varovanja.

Zadnji primerjalni kriterij, ki ga bomo uporabili, so karakteristike gesel/skupnih skrivnosti in postopek generiranja ključev iz gesel. Obravnavali bomo postopke za generiranje ključev na podlagi gesel.

Tabela 1: **Primerjalni kriteriji**

#	Primerjalni kriterij
1.	Razlikovanje med ključi za šifriranje in overjanje
2.	Dolžina ključa
3.	Karakteristike gesel/skupnih skrivnosti
4.	Pomanjkljivost in luknje v uporabljenih algoritmih
5.	Obveznost uporabe overjanja
6.	Obveznost uporabe šifriranja
7.	Obveznost uporabe zagotavljanja celovitosti

Zaradi težavnosti shranjevanja in pomnjenja dolgih ključev tehnologiji nudita mehanizem, ki s pomočjo gesla generira ključ. Ker pomembno vpliva na raven varnosti, ga bomo uporabili za primerjalni kriterij.

V tabeli 1 so strnjeni vsi primerjalni kriteriji, ki jih bomo uporabili.

Za boljšo preglednost bomo strnili ugotovitve v tabelo in na podlagi rezultatov primerjave podali ugotovitve glede ravni varnosti obeh tehnologij.

V nadaljevanju si bomo ogledali tehnologijo Bluetooth in njene varnostne mehanizme.

2 Tehnologija Bluetooth

Bluetooth je tehnologija, ki je bila zasnovana z namenom povezovanja perifernih naprav, mobilnih telefonov, prenosnikov in drugih mobilnih naprav. Za tehnologijo skrbi skupina Bluetooth SIG (Special Interest Group) [1], [14].

Leta 1999 je bila sprejeta prva verzija specifikacije Bluetooth 1.0B. Sledila je vpeljava specifikacije 1.1 [2] in kasneje še 1.2 [3]. Večina današnjih naprav s podporo tehnologiji Bluetooth uporablja specifikacijo 1.2. Nedavno pa je bila sprejeta tudi specifikacija 2.0 [4]. Tehnologija se uporablja za povezovanje različnih brezžičnih naprav. Veliko novejših prenosnih računalnikov je opremljenih s potrebno strojno in programsko opremo za povezovanje s pomočjo Bluetootha.

Bluetooth naprave lahko kategoriziramo na različne načine. Na podlagi porabe električne energije in dosega jih kategoriziramo v tri razrede [5]:

- 3. razred – naprave z močjo signala 1 mW in dosegom od 0.1 do 10 m,
- 2. razred – naprave z močjo signala 1 do 2.5 mW in dosegom 10 m in
- 1. razred – naprave z močjo 100 mW in dosegom do 100 m.

Naprave komunicirajo v frekvenčnem pasu 2.45 GHz in imajo največjo prepustnost 1,4 Mb/s. Zaradi dodatnih storitev, ki so potrebne za vzpostavitev in nadzor povezave in se prenašajo skupaj s podatki prek brezžične povezave, je dejanska prepustnost manjša. Bluetooth naprave se povezujejo v omrežja, ki jih imenujemo piconet. V piconet je lahko povezanih do osem naprav, izmed katerih je ena glavna (angl. Master Device), druge pa so odvisne (angl. Slave Device).

Glede na varnostne mehanizme naprave uvrščamo v tri načine [5]:

- varnostni način 1 (angl. No-security) – naprave se povezujejo in nikoli ne zahtevajo uporabe varnostnih mehanizmov (overjanja in šifriranja);
- varnostni način 2 (angl. Service Level Enforced Security) – naprave, ki se povezujejo v tem načinu vzpostavijo varnostne mehanizme na ravni kanala (naloga je prepuščena višjim ravnem komunikacijskega protokola ali aplikacijam);
- varnostni način 3 (angl. Link Level Enforced Security). Varnostni mehanizmi se vzpostavijo pred vzpostavitvijo povezave. Možni sta dve različni varnostni politiki: vedno zahtevaj overjanje in vedno zahtevaj overjanje in šifriranje.

Razlika med drugim in tretjim načinom je v tem, da pri varnostnem načinu 3 naprave Bluetooth inicializirajo varnostne mehanizme pred vzpostavitvijo povezave. Varnost prenosa je prepuščena Bluetoothu. V varnostnem načinu 2 je varovanje predano višji ravni, ki mora poskrbeti zanj.

Vzpostavitev komunikacijskega kanala med dvema napravama imenujemo vzpostavitev povezave (angl. Pairing). Razlikujemo dva scenarija:

- vzpostavitev povezave med dvema napravama poteka prvič,
- ponovna vzpostavitev povezave dveh naprav (ki sta že vzpostavili povezavo).

Ker je Bluetooth brezžična tehnologija, so pomemben del specifikacije tudi varnostni mehanizmi, ki jih bomo opisali v nadaljevanju. Obravnavali bomo ključe, ki jih definira Bluetooth pri svojih varnostnih mehanizmih in postopke overjanja ter šifriranje.

2.1 Varnostni mehanizmi

2.1.1 Ključi

Varnostni koncept tehnologije Bluetooth vključuje ključe, ki se uporabljajo pri overjanju in šifriranju. Specifikacija definira dve vrsti ključev:

- ključi povezave (angl. Link Key),
- šifrirni ključ (angl. Encryption Key).

Vlogo ključa povezave lahko prevzamejo različni ključi. Ključ povezave se ne uporablja samo pri overjanju, ampak tudi za generiranje šifrirnega ključa. Napravi si izmenjata ključ povezave v procesu vzpostavitve povezave.

Šifrirni ključ, ki je izpeljan iz ključa povezave, uporabljamo za šifriranje podatkov pri prenosu. Po specifikaciji [3] se šifrira samo vsebina paketov (angl. Payload), ne pa tudi režijski podatki (angl. Overhead

data). Pri generiranju ključev se uporablja naslov Bluetooth naprave (angl. Bluetooth Device Address), ki je izviren za vsako napravo.

Ključi povezave

Ključ povezave je rezultat vzpostavitve povezave. Specifikacija predvideva dva tipa ključev glede na trajnost [11]:

- poltrajni ključ (angl. Semi-permanent Key) in
- začasni ključ (angl. Temporary Key).

Med poltrajne ključe povezave prištevamo [3]:

- ključ naprave (angl. Unit Key) in
- kombinacijski ključ (angl. Combination Key).

Prav tako razlikujemo dva tipa začasnih ključev [3]:

- glavni ključ (angl. Master Key) in
- vzpostavitveni ključ (angl. Initialization Key).

Inicializacijski ključ se uporablja za vzpostavitev komunikacije med napravami in obstaja samo za čas vzpostavljanja povezave. Pri vzpostavitvi povezave se v napravi, ki se povezuje, vnese geslo (PIN). Inicializacijski ključ se generira po naslednji enačbi:

$$K_{vzp} = geslo, l_{gesla}, RAND, BD\_ADDR,$$

pri čemer je *PIN* (angl. Personal Identification Number) geslo, l_{gesla} dolžina gesla, *RAND* 128-bitno naključno število in *BD_ADDR* 128-bitni naslov Bluetooth naprave. Parametra geslo in l_{gesla} pridobimo na naslednji način:

$$geslo' = \begin{cases} geslo \cup BD\_ADDR & l_{gesla} \leq 10 \\ geslo \cup BD\_ADDR[0...(15-L)] & 10 < l_{gesla} \leq 15 \\ geslo & l_{gesla} = 16 \end{cases}$$

$$l_{gesla}' = \min(l_{gesla} + 6,16)$$

$\cup$ označuje konkatenacijo dveh nizov. Če je dolžina gesla krajša od 16 zlogov, se izvede bitno zapolnjevanje (angl. Padding) po zgornjem postopku. Inicializacijski ključ se uporablja za izmenjavo drugih ključev povezave.

Ključ naprave nastopa v vlogi ključa povezave in ga kreira naprava samo pri povezovanju z drugimi napravami. Zato je ključ naprave poznan množici naprav. Generira se s pomočjo algoritma E21 ob namestitvi nove naprave:

$K_A = E_{22}$ *(RAND, BD_ADDR)*, pri čemer je *RAND* 128-bitno naključno število in *BD_ADDR* 128-bitni naslov Bluetooth naprave. Med vzpostavljanjem povezave se napravi dogovorita, kateri ključ naprave se bo uporabljal. Ponavadi se uporablja ključ naprave, ki ima manjše pomnilniške kapacitete. Po generiranju se ključ naprave ne prenese neposredno na drugo napravo, marveč se uporabi operacija XOR $K'_A = K_A \oplus K_{vzp}$

Prejemnik lahko pridobi prvotni ključ s pomočjo naslednje enačbe:

$$ključ\_enote'_A \oplus vzpostitve\_ključ =$$
$$= ključ\_enote'_A \oplus vzpostitve\_ključ \oplus vzpostitve\_ključ =$$
$$= ključ\_enote'_A$$

Ključ naprave je varen, če obstaja zaupanje med napravami, ki se povezujejo. Slabost pristopa je možnost, da lahko vsaka naprava, ki ima isti ključ naprave, pooseblja drugo napravo. Specifikacija Bluetooth 1.2 uporabo ključa naprave odsvetuje, vendar zaradi kompatibilnosti za nazaj, ta tip ključev še ni bil odstranjen iz specifikacije.

Kombinacijski ključ se kreira s pomočjo dveh naprav. Za razliko od ključa naprave je ta ključ poznan samo napravama, ki sta ga kreirali. Daje visoko stopnjo varnosti, njegova slabost pa je potreba po pomnilniku, saj mora naprava shraniti kombinacijski ključ za vsako napravo, s katero se povezuje.

Kombinacijski ključ za napravi A in B se generira s pomočjo algoritma E21.

$K_A = E_{21}$ *(*$RAND_A$*,* BD_ADDR_A*)* in
$K_B = E_{21}$ *(*$RAND_B$*,* BD_ADDR_B*)*

Skupni, torej kombinacijski ključ K_{AB}, se izračuna kot $K_{AB} = K_A \oplus K_B$. Seveda je treba pred združevanjem ključev poskrbeti za prenos ključa K_A k napravi B in ključa K_B k napravi A. Ker je postopek prenosa zapleten, lahko bralec podrobnosti prouči v [3], [5].

Prvi začasni ključ povezave je glavni ključ, ki ga kreira glavna naprava pri vzpostavljanju šifrirane povezave z več odvisnimi napravami. Uporablja se za prenos podatkov med odvisno napravo in glavno napravo. Ključ generira glavna naprava s pomočjo algoritma E22:

$K_G = (RAND1, RAND2)$, kjer sta *RAND1* in *RAND2* dve naključi števili. Glavni ključ se na odvisno napravo ne prenese neposredno, ampak odvisni napravi pošlje tretje (javno znano) naključno število RAND3 in $K_{AB} = K_{glavni} \oplus K_{izr}$, pri čemer je K_{AB} kombinacijski ključ, K_{izr} pa izračunamo po naslednjem postopku:

$K_{izr} = E_{22}$ *(K,RAND3,16)*; *K* je trenutni ključ povezave. Odvisna naprava, ki pozna *K* in *RAND3* lahko izračuna glavni ključ kot:

$K_{AB} \oplus E_{22}(K,RAND3,16)$
$= K_{AB} \oplus K_{izr}$
$= K_{glavni} \oplus K_{izr} \oplus K_{izr}$
$= K_{glavni}$

Proceduro je treba opraviti za glavno napravo in vse odvisne naprave, ki se povezujejo z njo.

Šifrirni ključi

Ob ključih povezave predvideva specifikacija Bluetooth tudi tri šifrirne ključe [3]:

- šifrirni ključ K_c (angl. Encrpytion Key),
- omejeni šifrirni ključ (angl. Constrained Encryption Key) in
- ključ vsebine K_p (angl. Payload Key).

Ker je lahko šifrirni ključ daljši od dogovorjene maksimalne dolžine, se ga ne uporablja neposredno. Namesto njega se uporablja omejeni šifrirni ključ, ki je lahko dolg 8 do 128 bitov. Pomembno je omeniti, da ni priporočljivo uporabljati ključev z dolžino manj kot 128 bitov. Krajše dolžine ključev so bile predvidene zaradi omejitev izvoza kriptografije v nekaterih državah. Omejeni šifrirni ključ pridobimo s pomočjo šifrirnega ključa K_c, ključ vsebine K_p pa pridobimo s pomočjo omejenega šifrirnega ključa K_c.

Šifrirni ključ je izpeljan iz ključa povezave in se generira s pomočjo algoritma E_3 na naslednji način:

$K_c = E_3(K_{pov}, COF, RAND)$;

COF (angl. Cipher Offset Number) je nadomestno šifrirno število, E_3 je naključno število in K_{pov} je ključ povezave. *COF* izračunamo kot [3]:

$$COF = \begin{cases} naslov\_naprave \parallel naslov\_naprave \\ \\ ACO \end{cases}$$

Prvi primer velja le, če je ključ povezave enak glavnemu ključu, drugi pa v ostalih primerih. ACO (angl. Authentication Ciphering Offset) je število, ki ga pridobimo v fazi overjanja, ki jo bomo obravnavali v naslednjem razdelku.

Novejše verzije specifikacije ne priporočajo uporabe omejenega šifrirnega ključa oz. priporočajo, da je dolžina omejenega šifrirnega ključa 128 bitov.

Za šifriranje in dešifriranje podatkov se uporablja ključ vsebine K_p, ki ga pridobimo s pomočjo omejenega šifrirnega ključa:

$K_p = E_0(K_c, CLK, RAND, DB\_ADDR)$

K'_c je omejeni šifrirni ključ, *CLK* je 26 bitov trenutne ure naprave, *RAND* je 128-bitno naključno število in *DB_ADDR* je 128-bitni naslov Bluetooth naprave.

V tabeli 2 je pregled vseh ključev, ki jih predvideva specifikacija Bluetooth.

Tabela 2: **Pregled ključev specifikacije Bluetooth**

Namen	Poltrajni	Začasni
Overjanje	▪ Ključ enote ▪ Kombinacijski ključ	▪ Vzpostavitveni ključ ▪ Glavni ključ
Šifriranje		▪ Šifrirni ključ ▪ Omejeni šifrirni ključ ▪ Ključ vsebine

2.2 Overjanje

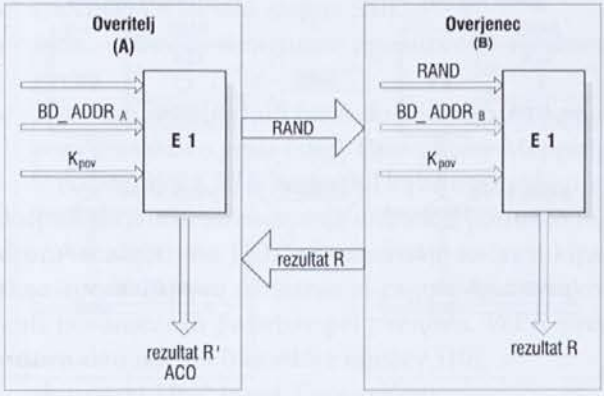
Varnost tehnologije Bluetooth je sestavljena iz dveh delov, ki sta med seboj povezana. Prvi del, ključi, je bil podrobneje obravnavan v prejšnjem razdelku. Drugi del je postopek overjanja in šifriranja. Uspešen zaključek overjanja entitet v komunikaciji je pogoj za uporabo šifriranja.

Overjanje poteka enosmerno, torej ena stran overja drugo ali obratno – ena entiteta v postopku nastopa kot overitelj in druga kot overjenec. Vloge dodeli uporabnik oz. gostitelj pred začetkom postopka overjanja. Slika 1 prikazuje postopke overjanja, kjer je naprava A overitelj in naprava B overjenec.

Najprej stran, ki želi overiti drugo stran, tej pošlje naključno število *RAND*. Algoritem *E1* sprejme naslednje parametre:

- 128-bitno naključno število *RAND*,
- 128-bitna naslova Bluetooth naprav BD_ADDR_A in BD_ADDR_B ter
- ključe povezave K_{pov}.

S pomočjo teh parametrov in algortima *E1* napravi izračunata števili R' (overitelj) in *R* (overjenec). Nato overitelj pošlje število *R* overjencu. Overitelj primerja *R'* z *R*.



Slika 1: **Postopek overjanja pri Bluetoothu**

Če se ujemata ($R = R'$), je postopek overjanja uspel, drugače ne. V primeru, da je postopek overjanja uspel, se izvrši še postopek overjanja v nasprotno smer – vlogi overitelja in overjanca se zamenjata. Naključno število se pri ponovnem overjanju zamenja.

Poleg overitev naprav je rezultat postopka overjanja tudi t. i. *ACO*, ki se uporablja pri generiranju šifrirnega ključa. Vrednost *ACO* se generira sočasno z vrednostjo *R*. Podrobnosti v zvezi z algoritmom *E1* in generiranje *ACO* so v [3], [5].

2.3 Šifriranje podatkov in zagotavljanje celovitosti

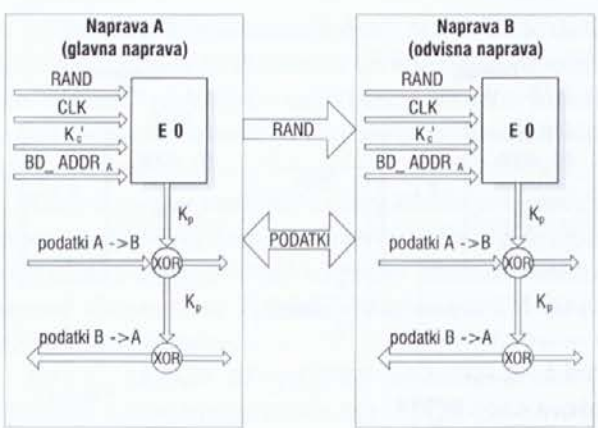
Šifriranje podatkov zagotavlja zaupnost prenesenih podatkov. Ob uporabi šifriranja se ključ samodejno generira. Ob ponovni vzpostavitvi povezave se šifrirni ključ zamenja. Podrobnosti delovanja postopka šifriranja prikazuje slika 2.

Šifriranje poteka s pomočjo algoritma E0 in parametrov [3]:

- 128-bitnega naslova glavne naprave Bluetooth *BD_ADDR*,
- 8–128-bitnega omejenega šifrirnega ključa K_c',
- 128-bitnega naključnega števila *RAND* in
- časovne značke naprave *CLK*.

Algoritem *E0* generira binarni niz ključev (angl. Binary Keystream), ki se po modulu 2 dodajo podatkom (operacija *XOR*). Šifrirani podatki se nato prenesejo k napravi B. Dešifriranje podatkov poteka po enakem postopku [5].

Tehnologija Bluetooth ne vsebuje mehanizma za zagotavljanje celovitosti s stališča varnostnih principov (s pomočjo ključa). Zagotavljanje celovitosti glave poslanega paketa je realizirano s pomočjo kontrolnika napak glave (angl. Header-Error-Check) HEC, ki je velikosti 8 bitov [3]. Vsak paket vsebuje tudi vrednosti CRC (angl. Cyclic Redundancy Check) za zaznavanje napak [3]. Kljub temu pa mehanizma nista namenjena zagotavljanju celovitosti s stališča varnosti, saj samo preverjata, ali je prišlo do napake v paketu, ki je posledica motenj pri prenosu. Prav tako mehanizem zagotavljanja celovitosti ni vezan na ključ. Če pride do napake, je treba paket poslati ponovno.



Slika 2: **Šifriranje pri Bluetoothu**

Bluetooth ni edina tehnologija za brezžično povezovanje. V nadaljevanju bomo obravnavali tehnologijo WLAN, ki je prav tako namenjena brezžičnemu povezovanju.

3 Tehnologija Wireless LAN

Tehnologija Wireless LAN je namenjena povezovanju naprav v omrežja. Nadomešča žična lokalna omrežja (angl. Wired Local Area Network). Kratica WLAN označuje družino standardov IEEE 802.11. Tehnologija je trenutno v velikem razvoju, saj močno olajša vzpostavitev lokalnih omrežij. Uporablja frekvenčni pas 2.4 GHz (IEEE 802.11, IEEE 802.11b, IEEE 802.11g) in 5 Ghz (IEEE 802.11a). Maksimalni prenos variira od 1 Mbit/s (IEEE 802.11) do 54 Mbit/s (IEEE 802.11a in g).

V skupini 802.11 so ključni naslednji standardi [10]:

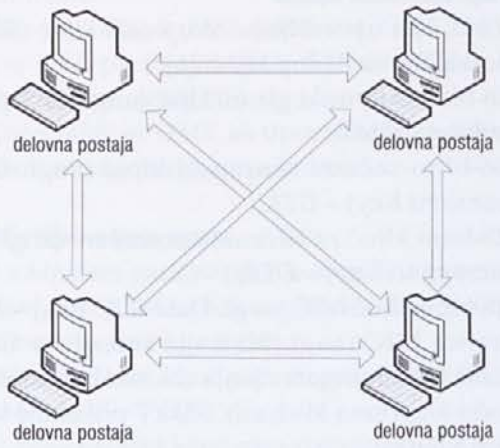
- 802.11 – prvotni standard, ki omogoča prenos podatkov 1 oz. 2 Mbit/s, frekvenčni pas 2.4 GHz, sprejet leta 1999,
- 802.11a – omogoča prenos do 54 Mbit/s, frekvenčni pas 5 Ghz, sprejet leta 1999,
- 802.11b – omogoča prenos do 11 Mbit/s, frekvenčni pas 2.4 Ghz, sprejet leta 1999,
- 802.11d – spremembe, potrebne zaradi omejitev v nekaterih državah,
- 802.11e – nadgraditev ravni *MAC* za zagotovitev storitev kakovosti (angl. Quality of Service),
- 802.11h – spremembe, potrebne zaradi omejitev v Evropi,
- 802.11i – definira dodatne varnostne mehanizme.

Tehnologija WLAN omogoča postavitev dveh tipov omrežij [10]:

- začasna omrežja (angl. Ad-hoc Network),
- infrastrukturna omrežja (angl. Infrastucture Network).

Večina omrežij WLAN je infrastrukturnega tipa (angl. Infrastucture Network). Druga vrsta omrežij so začasna omrežja (angl. Ad-hoc Network), pri katerih ne potrebujemo dostopnih točk (angl. Access Point).

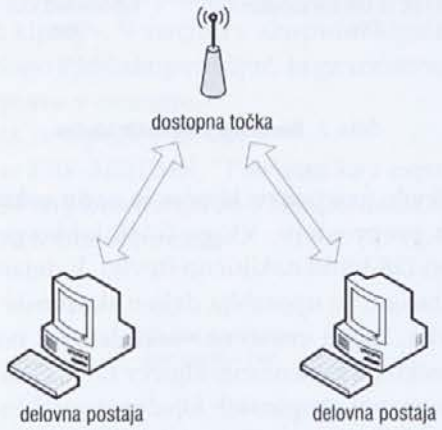
Arhitektura omrežja je bistveno preprostejša, saj ne vsebuje dodatnih omrežnih naprav, ampak samo delovne postaje, ki se povezujejo. Vsaka delovna postaja v omrežju neposredno komunicira z drugimi delovnimi postajami (slika 3).



Slika 3: **Struktura začasnega omrežja**

Varnost v začasnih omrežjih je na nizki ravni; omrežja namreč niso trajna in zato ni potrebe po varnosti.

Drugi tip omrežij so infrastrukturna omrežja, kjer potrebujemo dodatne omrežne naprave, imenovane dostopne točke. Vsaka delovna postaja komunicira z drugo postajo prek dostopne točke (slika 4).



Slika 4: **Shema infrastrukturnega omrežja**

Dostopna točka poskrbi, da se podatkovni paketi ustrezno usmerjajo proti distribucijskemu sistemu (angl. Distribution System), npr. usmerjevalniku.

Vsako omrežje vsebuje identifikacijo množice storitev SSID (angl. Service Set Indentifier), ki ga imenujemo tudi ime omrežja. Namen SSID je identifikacija podatkov glede na omrežje, tj. kateri podatki pripadajo kateremu omrežju.

Ker je medij, po katerem se prenašajo podatki zrak, je treba v omrežjih WLAN poskrbeti tudi za varnost. V nadaljevanju si bomo ogledali vse dejavnike, ki so povezani z varnostjo pri tehnologiji WLAN.

3.1 Varnostni mehanizmi

Analizirali bomo tehnologijo, imenovano WPA (angl. Wi-Fi Protected Access), v načinu PSK (angl. Preshared Key). Standard vsebuje protokol TKIP (angl. Temporal Key Integrity Protocol) za šifriranje podatkov in algoritem Michael za preverjanje celovitosti. WPA je bil vpeljan kot okrnjena različica standarda IEEE 802.11i. Namen WPA je bil povečati raven varnosti in hkrati omogočiti, da se rešitev vpelje samo s programsko nadgraditvijo obstoječih naprav. Zato je WPA samo začasna rešitev, ki jo bo kasneje nadomestil standard IEEE 802.11i, znan pod imenom WPA2 [6].

3.2 Ključi

Varnostni mehanizem WPA v načinu WPA-PSK uporablja t. i. skupni ključ. Skupni ključ se generira na podlagi gesla, saj bi bilo za uporabnika težko, da bi si zapomnil 256 bitov dolgo geslo. V ta namen se uporablja mehanizem, ki uporabnikovo geslo razširi v 256-bitni skupni ključ [9]:

PSK = PBKDF2(geslo, ssid, ssidLength, 4096, 256).

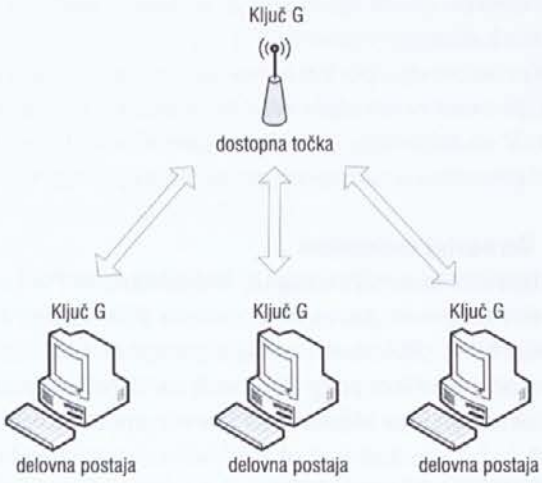
Pri čemer je:

- *geslo* – geslo, ki ga vnese uporabnik, sestavljeno iz ASCI znakov, dolžine 8 do 63 znakov,
- *ssid* – je SSID omrežja, v katerem se nahajajo naprave, zapisan v obliki zlogov,
- *ssidLength* – število zlogov SSID,
- *4096* – število izračunov zgostitvene vrednosti gesla,
- *256* – število izhodnih bitov, ki jih izračuna funkcija za preslikavo gesla (angl. Pass-phrase Mapping).

V načinu WPA PSK je skupni ključ uporabljen kot skupna skrivnost za overjanje entitet. S pomočjo tega ključa in algoritma TKIP se generirajo začasni ključi, ki se uporabljajo za šifriranje in zagotavljanje celovitosti posameznih paketov pri prenosu. WPA predvideva dva načina hierarhije ključev [10]:

- skupinski ključ (angl. Group Key),
- ključ para naprav (angl. Pairwise Key).

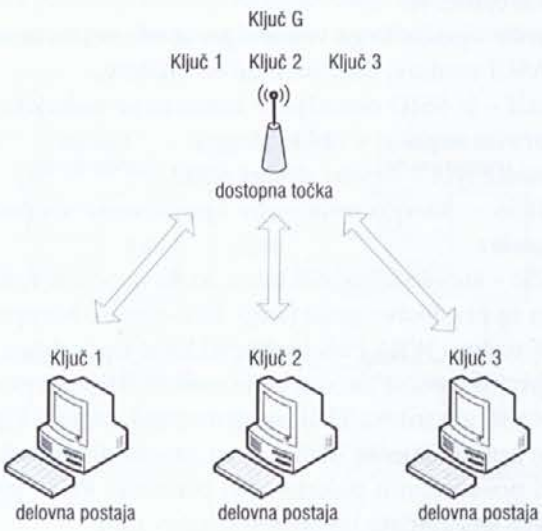
V prvem načinu uporabljajo vse delovne postaje in dostopna točka isto množico ključev (slika 5).



Slika 5: **WPA s skupinskim ključem**

Ta način je primeren za okolja, kjer razpršeno prenašamo podatke (angl. Broadcast). Način je bolj preprost s stališča upravljanja s ključi, a ne omogoča overjanja delovnih postaj, saj je skupni ključ naključno število. Skupinski ključ se v dejanskih implementacijah generira za tem, ko so že generirani posamezni ključi parov naprav.

V drugem načinu uporablja vsak par delovna postaja – dostopna točka različen ključ.



Slika 6: **WPA s ključi parov naprav**

Glede na način delovanja WPA definira več ključev. V nadaljevanju bomo obravnavali vse ključe, ki se uporabljajo v okviru varnostih specifikacij WPA.

Izpeljava ključev oz. vrste le-teh so odvisne od hierarhije ključev, ki jo uporabljamo.

Hierarhija skupinskih ključev

V načinu, kjer uporabljamo skupinski ključ (slika 6), se uporabljajo naslednji ključi [6]:

- 128-bitni skupinski glavni ključ (angl. Group Master Key) – *GMK*,
- 256-bitni začasni skupinski ključ (angl. Group Transient Key) – *GTK*,
- 128-bitni ključ za šifriranje podatkov (angl. Data Encryption Key) – *DEK*,
- 128-bitni ključ MIC (angl. Data *MIC* Key) – *DMK*.

Kratica MIC (angl. Message Intergirty Check) označuje termin zagotavljanja celovitosti podatkov (s pomočjo algoritma Michael). Slika 7 prikazuje hierarhijo teh ključev.

Slika 7: **Hierarhija skupinskih ključev**

Po številu in izpeljavi ključev je način s skupinskim ključem preprostejši. Vlogo *GMK* lahko prevzame poljubno 128-bitno naključno število. V dejanskih implementacijah se uporablja deljen skupinski ključ, ki ga je treba ročno vnesti na vsaki delovni postaji/dostopni točki. Za generiranje ključev *GTK, DEK* in *DMK* se pri hierarhiji skupinskih ključev uporablja *GMK*. S pomočjo *GTK* generiramo ostale tri ključe kot [9]:

GTK = PRF-256(GMK, "Group key expansion" || AA || GNonce),

pri čemer je:

- *PRF-256* generator psevdonaključnih števil, ki generira 256-bitno izhodno vrednost,

- *GMK* 128-bitni skupinski glavni ključ,
- *Group key expansion* niz znakov,
- *AA – MAC* naslov overitelja,
- *GNonce* naključno ali psevdonaključno število in
- || označuje konkatenacijo.

S pomočjo funkcije L lahko nato iz *GTK* pridobimo *DEK* in *DMK*:

DEK = L(GTK, 0, 128), DMK = L(GTK, 128, 256).

Torej je *DEK* prvih 128 bitov *GTK* (0–127) in *DMK* drugih 128 bitov (128–255).

Ključa *DEK* in *DMK* se uporabljata za šifriranje podatkov in zagotavljanje celovitosti.

Hierarhija ključev para naprav

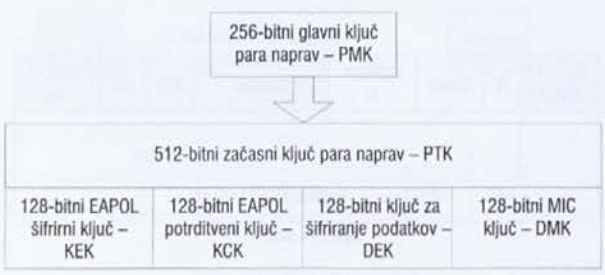
Način s ključem para naprav je s stališča generiranja in upravljanja ključev bolj zapleten (slika 6). Opravka imamo s šestimi ključi [10]:

- 256-bitni glavni ključ para naprav (angl. Pairwise Master Key) – *PMK*,
- 512-bitni začasni ključ para naprav (angl. Pairwise Transient Key) – *PTK*,
- 128-bitni EAPOL šifrirni ključ (angl. EAPOL Key Encryption Key) – *KEK*,
- 128-bitni EAPOL potrditveni ključ (angl. EAPOL Key Confirmation Key) – *KCK*,
- 128-bitni ključ za šifriranje podatkov (angl. Data Encryption Key) – *DEK*,
- 128-bitni *MIC* ključ (angl. Data *MIC* Key) – *DMK*.

Hierarhijo prikazuje slika 8. Zaradi dejstva, da se ključi v parih generirajo za vsaki dve napravi, ki se povezujeta (delovna postaja in dostopna točka), obstaja več ključev. V načinu s skupnim ključem prevzame vlogo *PMK* skupen ključ, ki ga ročno vnesemo v vse naprave v omrežju.

Iz *PMK* se izpelje *PTK* kot:

PTK = PRF-512(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) đđ Max(ANonce,SNonce)),



Slika 8: **Hierarhija ključev para naprav**

pri čemer je:

- *PRF-512* generator psevdonaključnih števil, ki generira 512-bitno izhodno vrednost,
- *PMK* 256-bitni glavni ključ para naprav,
- *Pairwise key expansion* niz znakov,
- *Min in Max* operacija, ki izbere minimalno oz. maksimalno vrednost izmed parametrov, tj. *AA* in *SPA* ter *ANonce* in *SNonce*,
- *AA – MAC* naslov overitelja,
- *SPA – MAC* naslov overjenca,
- ANonce – naključno ali psevdonaključno število overitelja in
- SNonce – naključno ali psevdonaključno število overjenca.

S pomočjo funkcije *L* lahko nato iz *PTK* pridobimo ostale štiri ključe [6], [10]:

KCK = L(PTK, 0, 128),
KEK = L(PTK, 128, 256),
DEK= L(PTK, 256, 384) in
DMK = L(PTK, 384, 512).

KCK je torej 0. do 127. bit, *KEK* 128. do 255. bit, *DEK* 256 do 383 bit in *DMK* 384 do 511 bit.

Ko se postopek izpeljave ključev zaključi, nadaljujemo s postopki overjanja, šifriranja in zagotavljanja celovitosti.

3.3 Overjanje

Overjanje je mehanizem, ki zagotavlja pristnost sistema ali osebe. WPA v načinu PSK predvideva dva načina overjanja [17], [16]:

- odprti sistemi (angl. Open Systems),
- skupni ključ (angl. Pre-shared Key).

Pri odprtih sistemih ni overjanja. Vsakdo lahko dostopa do sistema, saj dostopna točka vsaki omrežni napravi dovoli povezavo v omrežje. Zato tudi ni mogoče uporabljati šifriranja in zagotavljanja celovitosti.

Pri overjanju s skupnim ključem se v vsako delovno postajo in dostopno točko vnese skupni ključ. Overjanje poteka v štirih korakih, v katerih obe napravi druga drugi dokažeta, da poznata skupno skrivnost (skupni ključ). Overjanje poteka v obe smeri (angl. Mutual Authentication). V procesu overjenja se uporabljajo EAPOL sporočila in ključi, ki smo jih omenili v prejšnjem poglavju. Overjanje poteka po štirismernem protokolu. Najprej morata overitelj in overjenec generirati dve naključni števili. Vsaka stran generira svojo naključno vrednost:

- *ANonce* generira overitelj in
- *SNonce* generira overjenec.

Vrednosti *ANonce* in *SNonce* ne smeta biti povezani.

Nato sledi izmenjava štirih sporočil po štirismernem protokolu [10]:

1. Overitelj pošlje sporočilo A, ki vsebuje naključno število ANonce in *AA* (*MAC* naslov overitelja). Sporočilo je poslano nešifrirano in brez mehanizmov za zagotavljanje celovitosti. Po prejetju ima overjenec vse potrebne parametre za izračun *PTK*.
2. Overjenec pošlje sporočilo B, ki vsebuje naključno število SNonce, *SAP* (*MAC* naslov overjenca) in *MIC* za zagotavljanje celovitosti. Izračun *MIC* je mogoč, saj je overjenec v prejšnjem koraku generiral *PTK*. Overitelj uporabi SNonce in *SAP* za generiranje *PTK* in preverjanje vrednosti *MIC*.
3. Overitelj pošlje sporočilo C, ki vsebuje vrednost *MIC*, in začetno zaporedno število, ki označuje, da je overitelj pripravljen začeti s šifriranjem.
4. Overjenec pošlje sporočilo D, ki vsebuje vrednost *MIC* in začetno zaporedno število, ki označuje, da je overjenec pripravljen začeti s šifriranjem.

Celoten postopek je pregledno prikazan na sliki 9.

Po končani izmenjavi in overjanju sta obe strani pripravljeni za pošiljanje in sprejem šifriranih podatkov. Po končani vzpostavitvi hierarhije ključev para naprav je treba izvesti še distribucijo skupinskega ključa. Le-ta se uporablja za t. i. razpršeno pošiljanje podatkov po omrežju. Razpršeno pošiljanje je dovoljeno samo dostopni točki, vendar lahko vsaka delovna postaja »poda zahtevo« dostopni točki za razpršeno pošiljanje. Če želimo uporabljati tudi način skupinskega ključa, je treba še distribuirati skupinski ključ med vsemi delovnimi postajami. Ker je že vzpostavljen varen komunikacijski kanal (varovan s ključi parov naprav), je distribucija skupinskega ključa preprosta:

1. Generiramo *GTK*, s pomočjo katerega bomo generirali vse ostale začasne ključe.
2. Po vzpostavitvi varne povezave s pomočjo ključa para naprav:
   a) pošljemo *GTK* in trenutno zaporedno število vsaki delovni postaji,
   b) počakamo na potrdilo o prejemu.

Podrobnosti v zvezi s hierarhijami ključev, overjanjem in distribucijo ključev dajeta [9] in [10].

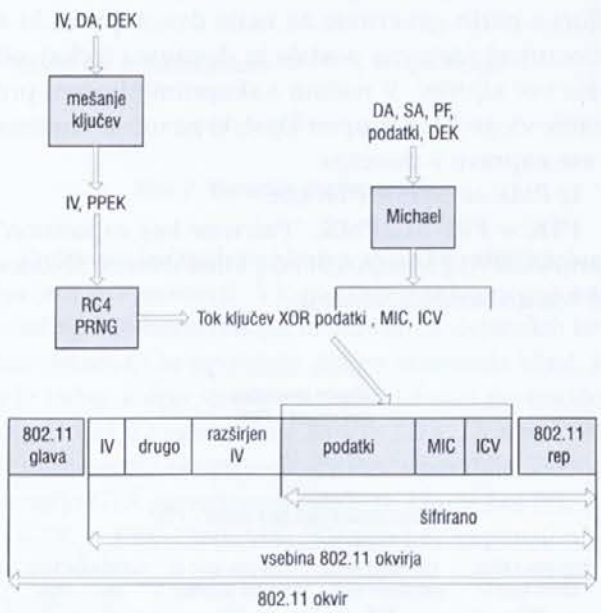
3.4 Šifriranje in zagotavljanje celovitosti

Za zagotavljanje zaupnosti WPA definira šifriranje podatkov. Šifrira se le dejanska vsebina. Potrebni so naslednji parametri za šifriranje:

1. 48-bitni inicializacijski vektor *IV* (angl. Initialization Vector), katerega začetna vrednost je 0 in se povečuje za vsak okvir,
2. *DEK* za šifriranje povezave,
3. naslov pošiljatelja *SA* (angl. Source Address) in naslov prejemnika *DA* (angl. Destination Address),
4. vrednost prednostnega polja *PF* (angl. Priority Field) z začetno vrednostjo 0,
5. *DMK* za zagotavljanje celovitosti.

Postopek šifriranja je prikazan na sliki 10:

Slika 9: **Štirismerni protokol za overjanje in izmenjavo začasnih ključev**

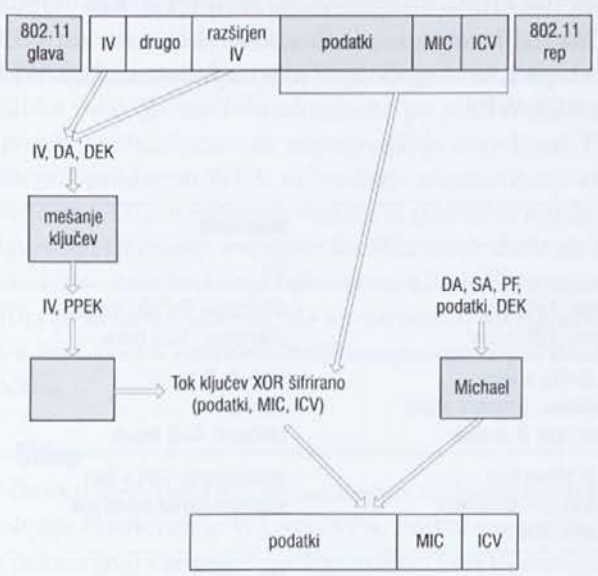


Slika 10: **WPA šifriranje**

1. IV, DA in DEK so vhodni parametri v funkcijo za mešanje ključev KMF (angl. Key Mixing Function), s pomočjo katere izračunamo šifrirne ključe za posamezen paket *PPK* (angl. Per-packet Key).
2. *DA, SA, PF*, podatki in *DMK* so vhodni parametri v algoritem za zagotavljanje celovitosti Michael, s pomočjo katerega izračunamo vrednost *MIC*.
3. Vrednost za preverjanje celovitosti *ICV* (angl. Integrity Check Value) izračunamo s pomočjo *CRC* vrednost (angl. cyclic redundancy check).
4. IV in šifirini ključi za posamezen paket so vhodni parametri za *RC4 PRNG* funkcijo. Ta generira tok ključev, ki je enake dolžine kot podatki, *MIC* in *ICV*.
5. Tok ključev je s pomočjo operacije *XOR* (ekskluzivni-ali) kombiniran s podatki, *MIC* in *ICV*.
6. K šifrirani vsebini paketov dodamo v polji imenovani *IV* polje in razširjeno *IV* polje (angl. IV field), vrednost *IV*. Rezultat nato ovijemo z glavo in repom 802.11.

Dešifriranje poteka podobno in je prikazano na sliki 11.

1. *IV* pridobimo iz *IV* polja in razširjenega *IV* polja. *IV, DA* in *DEK* so vhodni parametri v *KMF*, s pomočjo katere izračunamo *PPK*.
2. *IV* in *PPK* sta vhodna parametra v funkcijo *RC4 PRNG*, ki generira izhodni tok ključev enake dolžine kot šifrirani podatki, *MIC* in *ICV*.
3. Tok ključev je *XOR* kombiniran s podatki, *MIC* in *ICV*. S pomočjo te operacije pridobimo dešifrirane podatke, *MIC* in *ICV*.
4. Za dešifriranje podatke izračunamo *ICV* in ga primerjamo z *ICV*, ki smo ga prejeli in dešifrirali. Če se ne ujemata, zavržemo podatke.
5. *DA, SA*, podatki in *DMK* so vhodni parametri v funkcijo Michael, ki izračuna *MIC*.
6. Izračuna se vrednost *MIC* in se jo primerja z dešifriranim *MIC*. Če se vrednosti ne ujemata, podatke zavržemo. V nasprotnem primeru so podatki predani višji omrežni ravni za nadaljnjo procesiranje.



Slika 11: **WPA dešifriranje**

Mehanizmi za varovanje so pri WLAN enako pomembni kot pri Bluetoothu. Sledi primerjava varnosti obeh tehnologij glede na definirane primerjalne kriterije.

4 Primerjava varnostnih mehanizmov

Primerjali bomo varnosti obeh tehnologij (WLAN in Bluetooth). Pri izvedbi bomo uporabili tabelo kriterijev (tabela 1).

Obe tehnologiji, tako WLAN WPA (na kratko WPA) kot Bluetooth, uporabljata različne ključe za overjanje in šifriranje podatkov. Bluetooth uporablja štiri ključe povezave, WPA pa specificira tri različne ključe glede na hierarhijo ključev:

- DMK, ki je enake bitne dolžine za obe hierarhiji ključev in
- KCK, ki se uporablja v štirismernem protokolu za overjanje in izmenjavo ključev.

Ključe DMK se uporablja pri šifriranju in overjanju. Postopek generiranja DMK je različen glede na to, ali gre za šifriranje ali overjanje.

Bluetooth v fazi vzpostavitve in overjanja uporablja več različnih ključev povezave, ki so namenjeni tako vzpostavitvi povezave (vzpostavitveni ključ) kot kasnejšemu overjanju (ključ enote, glavni ključ in kombinacijski ključ). Pri WPA tehnologiji skupni ključ vnesemo ročno v vse naprave omrežja, zato ne potrebujemo posebnih ključev za fazo vzpostavljanja povezave. Overjanje WPA temelji na skupnem ključu – skupni skrivnosti, postopek overjanja pri Bluetoothu pa temelji na poznavanju gesla naprave (PIN). Pri Bluetoothu je PIN različen za vsako napravo. WPA definira skupni ključ, ki si ga delijo vse naprave. S stališča uporabe različnih ključev za overjanje in šifriranje sta tehnologiji enakovredni.

Pomemben dejavnik pri zagotavljanju varnosti je dolžina uporabljenih ključev. Kratki ključi omogočajo izvedbo napada z grobo silo. Bluetooth definira dolžino ključev med 8 in 128 biti. Ker je priporočena dolžina 128 bitov, sodobne implementacije uporabljajo dolžino 128 bitov. Uporaba variabilne dolžine ključa je pogojena z zgodovino tehnologije (npr. restrikcij nekaterih držav glede uporabe močne kriptografije). WPA specifikacija definira ključe dolžine 128 bitov. Zaradi variabilne dolžine ključa Bluetootha je WPA v prednosti, saj specifikacija definira 128-bitno dolžino ključa. Dolžina ključev pri Bluetoothu pa je odvisna od implementacije.

Tretji primerjalni kriterij so karakteristike gesel oz. skupnih skrivnosti. Tehnologiji predvidevata vnos gesel v naprave, iz katerih se nato generirajo ustrezni ključi. Bluetooth za vsako napravo predvideva svoje geslo oz. PIN. Dolžina PIN je lahko največ 16 števk. V praksi srečamo dolžine od 4 do 8 števk. WPA predvideva dolžino gesla med 8 in 63 znakov. Če uporabljamo kratka in enostavna gesla je WPA dovzeten za t. i. napade s slovarjem (angl. dictionary attack) [7]. Zato je priporočljivo, da so gesla ustrezno dolga in ne vsebujejo znanih besed. Priporočljivo je imeti gesla, ki so sestavljena iz črk, števk in posebnih znakov ali pa čisto naključne nize znakov. PIN, ki ga uporablja Bluetooth, je sestavljen iz števke in ne omogoča kombinacije črk, števk ter posebnih znakov. Priporočljivo je uporabljati vsaj osem števk dolge PIN, ki niso znane številke (npr. rojstni datumi). Glede na tretji kriterij je v prednosti Bluetooth, saj so gesla odvisna od naprave in jih je teže avtomatizirano iskati. To drži ob predpostavki, da uporabljamo PIN, daljši od štirih števk. WPA gesla lahko iščemo s pomočjo ustreznih programov, kar olajša iskanje. Slabost WPA je tudi v skupnem geslu, ki je enako za vse naprave v omrežju.

V kriteriju »pomanjkljivosti in luknje v uporabljenih algoritmih« so zajete znane šibke točke, luknje in druge napake, ki so bile odkrite v posameznih algoritmih ali postopkih določenega varnostnega mehanizma. Za varnostni koncept Bluetootha je bila do zdaj objavljena le ena pomanjkljivost. Napad omogoča pridobitev PIN v postopku vzpostavljanja povezave (angl. Pairing). Podrobnosti so opisane v [18]. Veliko hroščev v programski opremi nekaterih mobilnih telefonov je v praktični uporabi omajalo zaupanje v varnost Bluetootha [19]. Zaradi slabo zasnovanih mobilnikov, ki so podpirali Bluetooth, se je na spletu pojavila kopica programov, ki omogočajo zlorabo Bluetooth [19]. Ker ti napadi niso posledica pomanjkljivosti v specifikaciji Bluetooth, marveč napak in površnosti snovalcev mobilnih telefonov, jih v okviru primerjave ne bomo upoštevali. V zvezi s tehnologijo WPA je znana pomanjkljivost pri izbiri gesla. Možen je napad s slovarjem oz. uganjevanje gesla [11], [8], [7]. Prav tako so se pojavile varnostne pomanjkljivosti v algoritmu RC4, ki ga uporablja WPA [13]. Pomanjkljivosti algoritma RC4 so šibki ključi (angl. weak keys), vendar je mogoče pomanjkljivost izničiti z izločitvijo znanih šibkih ključev. RC4 v kombinaciji z WPA do sedaj še ni bil uspešno kriptoanaliziran in razbit, medtem ko je bila kombinacija WEP in RC4 uspešno kriptoanalizirana in razbita [13]. Ker vsebuje WPA daljši inicializacijski vektor (48 bitov) kot WEP (24 bitov), ni mogoče aplicirati napadov na RC4-WEP na RC4-WPA.

Tabela 3: **Primerjava varnostnih mehanizmov**

Kriterij	**WPA**	**Bluetooth**
Različni ključi za šifriranje in overjanje	Da	Da
Dolžine ključev	šifriranje: 128 bitov overjanje: 128 bitov	šifriranje: 8–128 bitov overjanje: 128 bitov
Karakteristike gesel/skupnih skrivnosti	geslo: 8–63 znakov črke, številke, posebni znaki običajno vsaj 8 znakov	PIN: 4–8 števk številke običajno 4–8 števk
Pomanjkljivost in luknje v uporabljenih algoritmih	napad s slovarjem šibki ključi pri šifrirnem algoritmu RC4	pridobivanje PIN v fazi vzpostavljanja povezave
Obvezna uporaba overjanja	Ne	Ne
Obvezna uporaba šifriranja	Ne	Ne
Obvezna uporaba mehanizmov za zagotavljanjE celovitosti	Ne	Ni na voljo

Glede na peti kriterij (obveznost uporabe overjanja) sta obe tehnologiji glede na specifikacijo, enakovredni. Nobena specifikacija, niti WPA niti Bluetooth, ne predvideva obvezne uporabe overjanja. Kljub temu pa je treba omeniti, da v praksi naprave Bluetooth zahtevajo vnos PIN, vsaj privzetega. Po drugi strani pa lahko uporabnik pri omrežnih napravah, ki podpirajo WPA, le-to izključi. V praktični uporabi ima torej prednost Bluetooth.

Glede na obveznost uporabe šifriranja (šesti kriterij) sta tehnologiji enakovredni s stališča specifikacije. Tehnologiji definirata, da šifriranje vključuje predhodno overjanje. Kljub temu pa je situacija enaka kot pri overjanju. Po specifikaciji sta tehnologiji enakovredni, vendar je v praksi bolj varen Bluetooth.

Zadnji primerjalni kriterij (obveznosti zagotavljanja celovitosti) je odvisen od uporabe šifriranja in overjanja. Bluetooth ne zagotavlja celovitosti s stališča varnosti. Pri tehnologiji WPA to funkcijo opravlja algoritem Michael. Zagotavljanje celovitosti, šifriranje in overjanje so pri tehnologiji WPA med seboj tesno povezani. Ob vnosu skupnega ključa samodejno uporabljamo vse tri. Glede na kriterij je WPA v prednosti pred Bluetoothom, ki nima kriptografskega zagotavljanja celovitosti.

V tabeli 4 je strnjena celotna primerjava. Tehnologiji sta enakovredni glede na dolžino ključa in uporabe različnih ključev za šifriranje in overjanje ter obvezne uporabe šifriranje in overjanja. Razlika je predvsem v karakteristikah gesel/skupnih skrivnosti in v pomanjkljivostih ter luknjah v uporabljenih algoritmih. Glede na te kriterije je boljši Bluetooth. Največja razlika med obema tehnologijama pa je v obveznost uporabe mehanizmov za zagotavljanje celovitosti. Pri tem je v prednosti WPA, saj vsebuje zagotavljanje celovitosti v kriptografskem smislu (s pomočjo ključa – algoritem Michael), medtem ko Bluetooth definira le »klasično« zagotavljanje celovitosti. Glede na izbrane kriterije bi lahko sklenili, da so varnostni mehanizmi in s tem raven varnosti bolj izpopolnjeni pri Bluetoothu.

5 Sklep

V članku smo predstavili varnostne mehanizme tehnologije Bluetooth in WLAN WPA. Podali smo analizo in primerjavo varnostih mehanizmov obeh tehnologij. Določili smo kriterije, ki smo jih izbrali na gesla in mehanizem za zagotavljanje celovitosti. Zato bi morali razvijalci identificirati slabosti v naslednjih revizijah varnostnih mehanizmov Bluetootha in WLAN. Naslednik standarda WPA pri omrežjih WLAN je WPA2 oz. standard IEEE 802.11i. Le-ta vsebuje številne izboljšave na področju varnosti [9], medtem ko Bluetooth verzija 2.0 ne prinaša izboljšav na področju varnosti [4]. Ker je specifikacija že sprejeta in se že implementira v praksi, bi bilo treba morda v naslednji reviziji specifikacije Bluetooth podrobneje analizirati nastale šibke točke in jih izboljšati. Prek obeh vrst brezžičnih tehnologij se namreč prenašajo občutljivi podatki, ki jih je treba dobro zaščititi. Že »narava« prenosnega medija (zrak) zahteva boljše varnostne mehanizme kot prenos prek kabla. Tega se morajo zavedati tudi uporabniki tehnologije.

6 Viri in literatura

[1] Bluetooth Special Interest Group, http://www.bluetooth.com/, nazadnje obiskano 1. 9. 2006.

[2] Bluetooth Specification Version 1.1, Bluetooth SIG, 2001.

[3] Bluetooth Specification Version 1.2, Bluetooth SIG, 2003.

[4] Bluetooth Specification Version 2.0 + EDR, Bluetooth SIG, 2004.

[5] C. Gehrmann, J. Persson, B. Smeets: Bluetooth Security, Artech House, 2004.

[6] D. Halasz: IEEE 802.11i and wireless security, Embedded.com, 2004, http://www.embedded.com/showArticle.jhtml?articleID=34400002, nazadnje obiskano 1. 9. 2006.

[7] G. Fleishman, R. Moskowitz: Weakness in Passphrase Choice in WPA Interface, Wi-Fi Networking News, 2003, http://wifinetnews.com/archives/002452.html, nazadnje obiskano 1. 9. 2006.

[8] G. Fleishman: WPA Cracking Proof of Concept Available, Wi-Fi Networking News, 2004, http://wifinetnews.com/archives/004428.html, nazdanje obiskano 1. 9. 2006.

[9] IEEE Standard 802.11i, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control, (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC), Security Enhancements, IEEE Computer Society, 2004.

[10] J. Edney, W. A. Arbaugh: Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2003.

[11] J. L. MacMichael: Auditing wi-fi protected access (WPA) pre-shared key mode, Linux Journal, Volume 2005 Issue 137, 2005.

[12] J. Walker, Part II: The Temporal Key Integrity Protocol (TKIP), 802.11 Security Series, Platform Networking Group, Intel Corporation, http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf, nazadnje obiskano 1. 9. 2006.

[13] S. Fluhrer, I. Mantin, A. Shamir: Weaknesses in the Key Scheduling Algorithm of RC4, Computer Science Department, The Weizmann Institute, Cisco Systems Inc., August 2001.

[14] The Official Bluetooth Membership Site, https://www.bluetooth.org/, nazadnje obiskano 1. 9. 2006.

[15] WiFi Protected Access (WPA) Overview, Windows Platform Design Notes, Microsoft Corporation, 2003.

[16] Wi-Fi Protected Access (WPA), Version 1.2, Wi-Fi Alliance, 2002.

[17] Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance, 2003, http://main.wi-fi.org/membersonly/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf, nazadnje obiskano 1. 9. 2006.

[18] Y. Shaked, A. Wool: Cracking the Bluetooth PIN, In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MobiSys), pages 39–50, 2005.

[19] Trifinite.stuff, trifinite.org – the home of the trifinite.group, http://trifinite.org/trifinite_stuff.html, nazadnje obiskano 1. 9. 2006.

[20] C. P. Pfleeger, S. L. Pfleeger: Security in Computing, 3rd Ed, Prentice Hall, 2002.

▪

Marko Hölbl je podiplomski študent računalništva in informatike na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Raziskovalno se ukvarja z zaščito in varovanjem podatkov, kriptografijo in zaupnostjo v omrežjih ter inteligentno obdelavo podatkov z metodami strojnega učenja.

▪

Boštjan Brumen je docent na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Na raziskovalnem področju se ukvarja s podatkovnimi bazami, podatkovnim rudarjenjem in varovanjem računalniških sistemov.

▪

Tatjana Welzer je redna profesorica na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, kjer predava na dodiplomski in podiplomski stopnji in vodi laboratorij za podatkovne tehnologije. Na raziskovalnem področju se ukvarja predvsem s podatkovnimi bazami, kakovostjo podatkov, podatkovnim modeliranjem in varovanjem podatkov.

Izbira optimalne odločitve z uporabo večkriterialnega programiranja in mehke logike

Lidija Zadnik Stirn
Univerza v Ljubljani, Biotehniška fakulteta, Večna pot 83, 1000 Ljubljana
lidija.zadnik@bf.uni-lj.si

Povzetek

V podporo za primerjavo in rangiranje večkriterialnih stohastičnih odločitev smo oblikovali matematični model, ki temelji na analitičnem hierarhičnem procesu in teoriji mehke logike. Odločitve so razvrščene na podlagi parnih primerjav in metode mehkih dominantnih povezav. Z modelom lahko izberemo tisto odločitev, ki maksimira hkrati več kriterijev, kot na primer ekonomske, naravovarstvene in socialne, ob upoštevanju številnih omejitev in nejasno definiranih spremenljivk. Model je ilustriran na enostavnem okoljskem problemu.

Ključne besede: večkriterialno odločanje, analitični hierarhični proces, mehke dominantne povezave, optimalno upravljanje okolja

Abstract

SELECTION OF AN OPTIMAL DECISION USING MULTI-CRITERIA PROGRAMMING AND FUZZY LOGIC

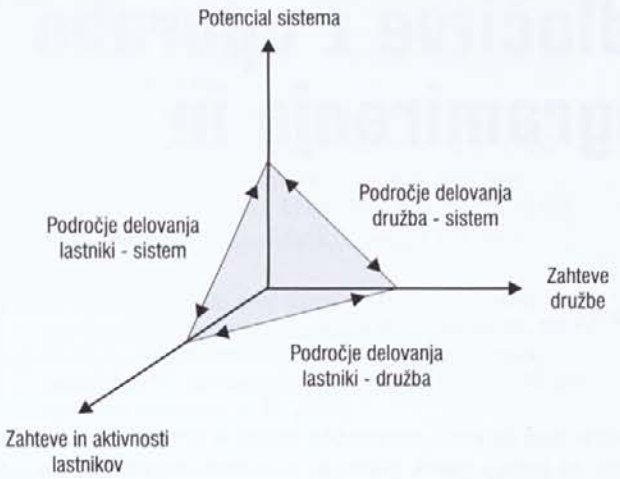
A mathematical decision support model for comparing and ranking multi-criteria stochastic solutions is presented. The model is based on a concept of analytic hierarchy process and fuzzy set theory. The decisions are ranked using pairwise comparisons within fuzzy domination relations. The model enables to determine the decision that jointly maximizes multiple objectives, as for example, economic, ecological and social objectives, subject to prescribed constraints, and respects imprecision. To demonstrate the model, a case study involving management of a simplified environmental system is used.

Keywords: multi-criteria decision-making, analytic hierarchy process, fuzzy domination relations, optimal management of environmental system

1 UVOD

Pri optimalnem upravljanju s kakršnim koli sistemom, bodisi proizvodnim ali okoljskim, stoji odločevalec vedno pred odločitvijo, katero izmed možnih odločitev naj izbere, da bo ravnal najbolj racionalno. V podporo odločevalcem za izbiro optimalne odločitve smo oblikovali matematični model. V modelu smo izhajali iz dejstva, da predstavlja problem izbire optimalne odločitve večkriterialni proces, pri katerem je treba upoštevati ekonomske, socialne in ekološke funkcije oziroma vloge in z njimi povezane konfliktne interese različnih udeležencev v procesu (sistemu) [7]. Upravljanje s sistemom je namreč razpeto med možnosti (potenciale), ki jih daje sistem, zahteve tistih, ki s sistemom gospodarijo (lastniki) in zahtevami, ki jih postavlja družba [1] (slika 1). Nadalje je pomembno pojasniti, da obstoji razlika med funkcijo in vlogo sistema. Funkcije sistema so procesi, ki potekajo v vsakem sistemu neodvisno od človekovih potreb. Gre torej za delovanje sistema, ki se s časom malo spreminja. Glede na to so funkcije stabilne in predvidljive. Kot vlogo sistema pa pojmujemo sposobnost sistema (procesov), da zagotavlja dobrine in storitve, ki posredno ali neposredno zadovoljujejo človekove potrebe. Vloge so izpostavljene spremembam časa, ker se s časom spreminjajo tudi človekove potrebe. Zato so vloge nestabilne in nepredvidljive [3]. Skladno s sliko 1 lahko še poudarimo, da ima sistem, ki ga obravnavamo v tem prispevku, značilnosti javne dobrine. Za javne dobrine pa sta značilni netekmovalnost in neizločljivost [5]. Netekmovalnost pomeni, da se v primeru, če neko dobrino uporablja posameznik, s tem ne onemogoči njene uporabe drugim posameznikom. Neizločljivost pa pomeni, da se porabe neke dobrine ne da prepovedati oz. da koristi od uporabe določene dobrine ni mogoče omejiti le na določeno skupino posameznikov.

Ob upoštevanju opisanih dimenzij večkriterialnega procesa so osnovni elementi modela za izbiro optimalne odločitve pri upravljanju s sistemom stanje (konfiguracija) sistema, možne odločitve in kriterialne funkcije. Ker pa imamo pri določanju stanj in kriterijev opravka z nejasno definiranimi spremenljivkami, smo v modelu uporabili mehko logiko. V modelu odločitve razvrstimo po pomembnosti in določimo optimalno z metodo parnih primerjav in



Slika 1: **Upravljanje s sistemom je razpeto med družbo, lastnike in sistem**

metodo mehkih dominantnih povezav. Pri tem obstojita dve možnosti: ali da so vsi kriteriji enako pomembni ali pa da so nekateri pomembnejši od drugih. V primeru, da so nekateri kriteriji pomembnejši, določimo kriterijem tako imenovane uteži. Pri tem uporabimo metodo analitičnega hierarhičnega procesa. Vse metode so na kratko predstavljene v naslednjem poglavju, kateremu sledi aplikacija modela in metod.

2 METODE, KI SESTAVLJAJO MODEL

2.1 Analitični hierarhični proces in mehka logika za identifikacijo kriterijev

Izhajamo iz dejstva, da odločevalec pozna vse možne odločitve pri upravljanju s sistemom. Metodologija za določitev odločitev je opisana v [6]. Za vrednotenje odločitev in izbiro optimalne uporabimo kriterije. Določitev in vrednotenje kriterijev je kompleksna naloga. V predloženem modelu opišemo kriterije z atributi in nato uporabimo metodo analitičnega hierarhičnega procesa (AHP, [4]) v kombinaciji z mehko logiko [8]. Metoda AHP lahko upošteva mnenje številnih ekspertov in uporabi kvantitativne kot tudi kvalitativne podatke. Temelji na parnih primerjavah, ki izražajo pomen posameznega atributa z (0, 9) naraščajočo lestvico. Hierarhija kriterijev in atributov je predstavljena v obliki dveh nivojev. Na prvem nivoju se nahajajo kriteriji, na drugem pa atributi, ki določajo težo vpliva posameznega kriterija. V modelu izračunamo težo vpliva posameznega kriterija poenostavljeno, in sicer kot linearno kombinacijo vplivov posameznih atributov, pri čemer upoštevamo tudi dejstvo, da imajo nekateri atributi večji vpliv (težo) na kriterij kot drugi. Skupen vpliv vseh atributov z vrednostmi x na kriterij k (k=1,2,...,n, če imamo n kriterijev) označimo kot c_k (na sliki 2 zapisan v kvadratku kriterija k) in ga izračunamo kot vsoto produktov med funkcijo pripadnosti u_x in utežjo w_x posameznih atributov:

$$c_k = \sum_x w_x u_x \qquad (1)$$

Uteži atributov w_x izračunamo z metodo AHP na podlagi parnih primerjav med atributi. Uteži normaliziramo, tako da zavzamejo vrednosti med 0 in 1 in da velja $\sum w_x = 1$. Vrednosti u_x izražajo pripadnost atributa z vrednostjo x določenemu kriteriju. V modelu zaradi enostavnosti uporabljamo linearno funkcijo pripadnosti:

$$u_x = u(x) = \begin{Bmatrix} 0 & \text{če } x < \alpha \\ 1 - \dfrac{\beta - x}{\beta - \alpha} & \text{če } \alpha \le x \le \beta \\ 0 & \text{če } x > \beta \end{Bmatrix} \qquad (2)$$

kjer je x vrednost atributa, ki jo v konkretnem sistemu dobimo z anketami, á in â pa sta mejni vrednosti posameznega atributa (tabela 1). Tudi vrednosti c_k so med 0 in 1 (slika 2). Vrednost c_k blizu 1 pomeni, da kriterij k veliko prispeva k celotni koristi posamezne odločitve, medtem ko pa vrednosti c_k blizu 0 povedo, da kriterij k malo pripeva k celotni koristi odločitve.

2.2 Metoda parnih primerjav za razvrščanje odločitev

Odločitve $d_1,...,d_i,.....,d_m$ in njim pripadajoče vrednosti kriterijev (odločitveni faktorji) $c_1,....,c_k,....,c_n$ določajo vrstice oziroma stolpce matrike $X=(x_{ik})$. Elementi x_{ik} matrike X povedo, kako pomemben je posamezni kriterij oziroma odločitveni faktor c_k za posamezno odločitev d_i (slika 2). Ker x_{ik} izvirajo iz anket (kvalitativnih podatkov), jih v modelu najprej normaliziramo, to pomeni, da pretvorimo njihove vrednosti v vrednosti med 0 in 1. To naredimo tako, da vsak element matrike X delimo z največjim elementom v vrstici, v kateri se ustrezni element nahaja, kot kaže enačba (3). Tako dobimo matriko $Y=(y_{ik})$.

X:		c_1	....	c_k	.....	c_n
	d_1			..		
	...			..		
	d_i	..	..	x_{ik}		
	...					
	d_m					

$$y_{ik} = \frac{x_{ik}}{\max_i x_{ik}}, k = 1,...,n \quad (3)$$

Primerjave med odločitvami izvedemo s pomočjo mehkih podobnostnih primerjav kot je opisano v [2]. Z elementi matrike Y izračunamo elemente matrike $R=(r_{ij})$ kot je definirano z enačbo (4), kjer je d ustrezna funkcija, ki meri razliko med y_{ik} in y_{jk} in c konstanta, ki mora biti izbrana tako, da velja $0 \le r_{ij} d \le 1$. Za vrednost konstante c je to edini pogoj, sicer pa izbira vrednosti konstante c nima vpliva na določitev podobnosti med odločitvami. Za funkcijo $d(y_{ik},y_{jk})$ navadno izberemo kar direktno razliko $y_{ik}-y_{jk}$ ali pa absolutno vrednost razlike $y_{ik} - y_{jk}$. Če je vrednost r_{ij} blizu vrednosti 1, pomeni, da sta odločitvi d_i in d_j primerljivi (podobni), če pa je vrednost r_{ij} blizu 0, odločitvi d_i in d_j nista primerljivi.

$$r_{ij} = 1 - c \left| \sum_{k=1}^{n} d(y_{ik}, y_{jk}) \right| \quad (4)$$

2.3 Metoda mehkih dominantnih povezav za identifikacijo optimalne odločitve

Določanje dominantnih odločitev temelji na mehkih dominantnih povezavah, kot je definirano v [2]. Dominantne odločitve iščemo prek parov odločitev d_i in d_j, ki nastopajo v matriki Y. Za vsak par odločitev d_i in d_j definiramo matriko $D_k(i,j)$, kjer je k=1,2,..., n in pomeni indeks kriterija:

$$D_k(i,j) = \begin{cases} 1, če\ y_{ik} - y_{jk} > 0 \\ 0, če\ y_{ik} - y_{jk} < 0 \\ 0.5, če\ y_{ik} - y_{jk} = 0 \end{cases} \quad \text{za k=1,2,...,n} \quad (5)$$

Na podlagi matrik $D_k(i,j)$ izračunamo matriko $R'=(r_{ij}')$:

$$r_{ij}' = \begin{cases} \sum_{k=1}^{n} D_k(i,j), če\ i \neq j \\ 0, če\ i = j \end{cases} \quad \text{za i,j=1,2,...,m} \quad (6)$$

Nato v matriko R' dodamo še stolpec s_i in vrstico b_j, kjer sta s_i in b_j določena kot vsota i-te vrstice oziroma j-tega stolpca matrike R'. Vsota vrstice, s_i, pove stopnjo, glede na katero odločitev d_i dominira nad drugimi odločitvami, medtem ko b_j meri dominiranost drugih odločitev nad odločitvijo d_j.

3 OKOLJSKI PROBLEM ZA ILUSTRACIJO MODELA IN METOD

Izberimo okoljski sistem, na primer gozd, ki predstavlja proizvodni sistem in ima hkrati vlogo javne dobrine. Interdisciplinarna skupina ekspertov je z namenom, da se določi optimalna strategija upravljanja s tem sistemom, raziskala procese v sistemu, in sicer z ekonomskega, okoljskega, socialnega, tehnološkega in družbenega vidika (na sliki 2 imamo tako na nivoju 1 podanih pet kriterijev; k=1 za ekonomski kriterij, ..., k=5 za družbeni kriterij) ter določila vse možne odločitve [6]. V našem primeru obravnavamo štiri odločitve d_1, d_2, d_3 in d_4 (na sliki 2 imamo prikazano le odločitev d_1; za vse druge odločitve bi bila slika podobna). Tu bomo natančno prikazali le potek računanja vrednosti, ki nastopajo v matriki X, za odločitev d_1, saj je postopek računanja za druge odločitve podoben.

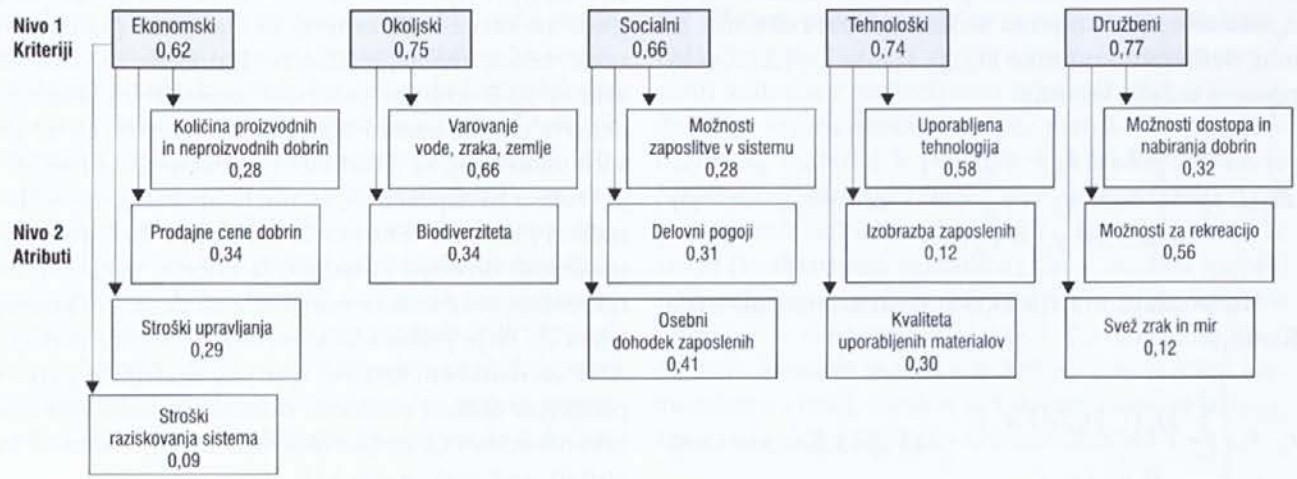
Tako imamo v tabeli 1 za odločitev d_1 dane povprečne vrednosti (vrednosti iz anket, opisanih v [6]) za vrednosti atributov x, limitne vrednosti á in â, u(x) za d_1, izračunan po (2), in uteži w_x. Uteži so bile dobljene s pomočjo ekspertnih mnenj. Eksperti so namreč naredili parno primerjavo za 4 atribute (količina proizvodnih in neproizvodnih dobrin, prodajne cene dobrin, stroški upravljanja in stroški raziskovanja sistema) glede na ekonomski kriterij, za 2 atributa (varovanje vode, zraka, zemlje, biodiverziteta) glede na okoljski kriterij, za 3 atribute (možnosti zaposlitve v sistemu, delovni pogoji, osebni dohodek zaposlenih) glede na socialni kriterij, za 3 atribute (uporabljena tehnologija, izobrazba zaposlenih, kvaliteta uporabljenih materialov) glede na tehnološki kriterij in za 3 atribute (možnosti dostopa in nabiranja dobrin, možnosti za rekreacijo, svež zrak in mir) glede na družbeni kriterij (slika 2). Tu je prikazano le računanje uteži z metodo AHP za družbeni kriterij, kjer je v matriki A parnih primerjav atribut možnosti dostopa in nabiranja dobrin označen s Q, atribut možnosti za rekreacijo s P in atribut svež zrak in mir s H:

$$A = \begin{matrix} Q \\ P \\ H \end{matrix} \begin{bmatrix} Q & P & H \\ 1 & 1/2 & 3 \\ 2 & 1 & 4 \\ 1/3 & 1/4 & 1 \end{bmatrix} \rightarrow A^2, \quad (A^2)^2, \quad \ldots\ldots \rightarrow \begin{bmatrix} w_1 = 0.32 \\ w_2 = 0.56 \\ w_3 = 0.12 \end{bmatrix}$$

Tabela 1: **Podatki o atributih za odločitev d_1 glede na ankete iz [6], enačbo (2) in metodo AHP**

Atribut	Odločitev d_1 x vrednost	α	β	$u(x)/d_1$	w_x
Količina proizvodnih in neproizvodnih dobrin	2.67	1.82	4.50	0.32	0.28
Prodajne cene dobrin	3.69	1.60	4.30	0.77	0.34
Stroški upravljanja	3.54	1.22	4.20	0.78	0.29
Stroški raziskovanja sistema	2.42	1.08	3.80	0.49	0.09
Varovanje vode, zraka, zemlje	4.50	2.30	4.60	0.96	0.66
Biodiverziteta	3.27	2.45	4.80	0.35	0.34
Možnosti zaposlitve v sistemu	2.77	1.82	3.95	0.45	0.28
Delovni pogoji	3.13	1.90	4.05	0.57	0.31
Osebni dohodek zaposlenih	4.50	2.10	4.90	0.88	0.41
Uporabljena tehnologija	3.69	2.10	4.65	0.62	0.58
Izobrazba zaposlenih	3.40	1.80	4.10	0.82	0.12
Kvaliteta uporabljenih materialov	4.15	2.15	4.25	0.95	0.30
Možnosti dostopa in nabiranja dobrin	3.83	2.10	4.15	0.84	0.32
Možnosti za rekreacijo	4.62	3.12	4.98	0.81	0.56
Svež zrak in mir	2.82	1.84	4.12	0.43	0.12

Z uporabo podatkov za $u(x)/d_1$ in w_x v formuli (1) izračunamo vpliv posameznih kriterijev na odločitev d_1: c_1=0.62, c_2=0.75, c_3=0.66, c_4 = 0.74, in c_5=0.77 (zapisani so na nivoju 1 na sliki 2). Podobno izračunamo vrednosti c_k za druge tri odločitve. Rezultate zberemo v matriki X. Po (3) izračunamo matriko Y.



Slika 2: **Kriteriji in atributi za ocenjevanje odločitve d_1**

X:

	c_1	c_2	c_3	c_4	c_5
d_1	0.62	0.75	0.66	0.74	0.77
d_2	0.73	0.62	0.56..	0.72	0.92
d_3	0.60	0.72	0.68	0.69	0.79
d_4	0.74	0.67	0.66	0.71	0.85

Y:

	c_1	c_2	c_3	c_4	c_5
d_1	0.84	1	0.97	1	0.84
d_2	0.99	0.83	0.82..	0.97	1
d_3	0.81	0.96	1	0.93	0.86
d_4	1	0.89	0.97	0.96	0.92

Uporabimo (4) in izračunamo matriko R, kjer smo vzeli za $d(y_{ik},y_{jk}) = y_{ik} - y_{jk}$ in $c=0.6$:

R:

	d_1	d_2	d_3	d_4
d_1	1	0.98	0.95	0.96
d_2	0.98	1	0.86	0.92
d_3	0.95	0.86	1	0.89
d_4	0.96	0.92	0.89	1

Iz matrike R lahko povzamemo, da sta najbolj primerljivi odločitvi d_1 in d_2, ki bi lahko tvorili eno skupino odločitev, če bi odločitve razvrščali v skupine.

Z namenom, da bi odločitve razvrstili po pomembnosti in določili glede na izbrane kriterije optimalno, izračunamo po (6) matriko R', ki sledi iz matrik $D_k(i,j)$, $k=1,2,3,4,5$, ki so izračunane po (5).

$D_1(i,j)$:

	d_1	d_2	d_3	d_4
d_1	0.5	0	1	0
d_2	1	0.5	1	0
d_3	0	0	0.5	0
d_4	1	1	1	0.5

$D_2(i,j)$:

	d_1	d_2	d_3	d_4
d_1	0.5	1	1	1
d_2	0	0.5	0	0
d_3	0	1	0.5	1
d_4	0	1	0	0.5

$D_3(i,j)$:

	d_1	d_2	d_3	d_4
d_1	0.5	0	1	0.5
d_2	0	0.5	0	0
d_3	1	1	0.5	1
d_4	0.5	1	0	0.5

$D_4(i,j)$:

	d_1	d_2	d_3	d_4
d_1	0.5	1	1	1
d_2	0	0.5	1	1
d_3	0	0	0.5	0
d_4	0	0	1	0.5

$D_5(i,j)$:

	d_1	d_2	d_3	d_4
d_1	0.5	0	0	0
d_2	1	0.5	1	1
d_3	01	0	0.5	0
d_4	1	0	1	0.5

R':

	d_1	d_2	d_3	d_4	s_i
d_1	0	2	4	2.5	8.5
d_2	2	0	3	2	7
d_3	2	2	0	2	6
d_4	2.5	3	3	0	8.5
b_i	6.5	7	10	6.5	

Iz vrednosti stolpcev s_i v matriki R' sklepamo, da imata odločitvi d_1 in d_4 isti rang in sta bolj pomembni kot odločitvi d_2 in d_3. Velja torej: $d_1 = d_4 > d_2 > d_3$. Katero odločitev naj bi sprejeli, d_1 ali d_4, pa bi se lahko odločili šele na podlagi nadaljnjih raziskav (posteriorna analiza). Na podlagi vrednosti v matriki R namreč sklepamo, da ti dve odločitvi nista enakovredni, pač pa konkurenčni.

4 SKLEP

Predstavili smo model, ki ga je mogoče uporabiti za iskanje optimalnih odločitev v različnih sistemih, tako proizvodnih kot okoljskih in socialnih, ob upoštevanju številnih kriterijev, ki so merjeni s kvantitativnimi kot tudi kvalitativnimi kriteriji. Vrednosti posameznih kriterijev, ki so opisani z atributi, so dobljene z anketami (v anketiranje je pogosto vključena tudi širša javnost) ali pa so zbrane kot tehnični podatki. Testiranja modela so pokazala, da je uporabnost modela predvsem v tem, da odločevalcu ne sugerira optimalne odločitve na osnovi vhodnih podatkov, temveč mu omogoča preverjanje variant in usklajevanje možnih rešitev z različnimi eksperti in uporabniki sistema.

5 VIRI IN LITERATURA

[1] BACHMANN, P., BERNASCONI, A.: Neue Wege der forstlichen Plannung. Bundesamt fuer Umwelt, Bern, 1996.

[2] KAUFMANN, A. Introduction to the theory of the fuzzy subsets. Academic Press, New York, 1975.

[3] MAVSAR, R.: Socio-ekonomski pomen gozdov v Alpskem prostoru. Zbornik gozdarstva in lesarstva 77, 2005, str. 143–158.

[4] SAATY, T. L. Fundamentals of Decision Making and Priority Theory. RWS Publications, Pittsburgh, 1994.

[5] TAJNIKAR, M.: Mikroekonomija s poglavji iz teorije cen. Ekonomska fakulteta, Ljubljana, 2003.

[6] ZADNIK STIRN, L.: A framework for generating development project alternatives. University of Ljubljana, Biotechnical Faculty, Ljubljana, 2003, 147 str.

[7] ZADNIK STIRN, L.: Decision making in natural resources and the environment regarding the interactions between experts and society. V: *Quantitative modeling of human market interactions*, The International Institute for Advanced Studies in Systems Research and Cybernetics, Windsor (Ont., Can.), 2004, str. 36–40.

[8] ZIMMERMANN, H. J. Fuzzy Sets: Decision Making and Expert Systems. Kluwer, Boston, 1987, 335 str.

▪

Lidija Zadnik Stirn je doktorica informacijsko-upravljavskih znanosti in profesorica za področje operacijskih raziskav na Univerzi v Ljubljani. Na Biotehniški fakulteti poučuje kvantitativne metode, matematične metode in metode operacijskih raziskovanj. Bila je gostujoči učitelj na univerzah v Trierju, ZRN in Washington v Seattlu, ZDA. Njeno raziskovalno delo je usmerjeno predvsem na področje metod optimiranja in v oblikovanje matematičnih modelov, ki služijo kot podpora pri sprejemanju optimalnih odločitev pri upravljanju z različnimi sistemi ob upoštevanju ekonomskih, okoljevarstvenih in socialnih ciljev. Je predsednica sekcije za operacijske raziskave in podpredsednica SDI.

▪

KOLEDAR PRIREDITEV

ICCD 2006 – International Conference on Computer Design	1.–4. okt. 2006	San Jose, ZDA	http://www.iccd-conference.org
ASPLOS XII – 12th International Conference on Architetural Support for Programming Languages and Operating Systems	21.–25. okt. 2006	San Jose, ZDA	http://www.princeton.edu/asplos06
Poslovna konferenca Menedžment poslovnih procesov – MPP 2006 Kako do konkurenčnega gospodarstva in uprave	30. nov.–1. dec. 2006	Ljubljana, Slovenija	
HiPEAC 2007 – International Conference on High Performance Embedded Architectures & Compilers	29.–30. jan. 2007	Ghent, Belgija	http://www.hipeac.net/conference
Dnevi slovenske informatike 2007 – DSI 2007 Z informatiko do novih poslovnih priložnosti	11–13. apr. 2007	Portorož, Slovenija	http://www.dsi2007.si

Vpliv razmerij v projektni skupini na kakovost uporabniške rešitve

Alenka Kolar
Elektro-Slovenija, d. o. o., Hajdrihova 2, Ljubljana
alenka.kolar@eles.si

Povzetek

V slovenskih podjetjih, ki imajo oddelek za informatiko, izdelamo veliko uporabniških rešitev, potrebnih za podporo poslovnih procesov, znotraj projektnih skupin, sestavljenih iz »hišnih« programerjev in analitikov ter izvajalcev nalog na projektu iz zunanjih podjetij. Razmerja med člani projektne skupine, ki jih sodelujoči vzpostavimo med delom ali zunaj njega, pomembno vplivajo na kakovost izdelka – uporabniške rešitve.

Ključne besede: razmerja, uporabniška rešitev, projektno delo, kakovost, javna naročila

Abstract

INFLUENCE OF REALTIONSHIPS IN PROJECT TEAM ON THE QUALITY OF SOFTWARE APPLICATION

In Slovenian enterprises that have an informatics department a number of software applications necessary to support business processes in combined project teams is being developed. The teams are composed of domestic programmers and analysts and of outsourced personnel. It is evident that the relationships that have formed among project team members during the time of the project have an important influence on the quality of developed application.

Keywords: relationships, software application, project work, quality, public procurement

1 POLOŽAJ RAZVOJA UPORABNIŠKIH REŠITEV

1.1 Splošno

V slovenskih podjetjih naletimo na več načinov obvladovanja in razvoja uporabniških rešitev, namenjenih podpori poslovnim procesom. Velikost oddelka za informatiko je navadno odvisna od tega, ali podjetje kupi rešitev, kot npr. Oracle e-Business Suit, SAP ali Navision, ali pa v celoti ali delno programira rešitve z različnimi orodji in na različnih bazah podatkov. V obeh primerih se pojavlja oddajanje določenih nalog zunanjim izvajalcem (angl. outsourcing), saj podjetja, ki jim programiranje ne predstavlja temeljne dejavnosti, ne razpolagajo z vsemi znanji in dovolj velikim številom ljudi, potrebnih za izvedbo večjih razvojnih projektov.

Obvladovanje projektov (*project management*) je oblika poslovnih procesov, ki je predvsem poznana v gradbeništvu in povezanih dejavnostih, ko govorimo o gradnji cest, zgradb, izdelavi turbin za elektrarne ipd. Na področju informatike je obvladovanje projekta razvoja uporabniške rešitve precej abstrakten pojem. Dejstvo je, da pri inženirskem projektu priprava projekta stane mnogo manj in traja krajši čas kot izvedba samega projekta. V informacijskih projektih pa je zato pripravljalni čas neredko daljši in zahteva vključitev visokoizobraženih zaposlencev kot prvin poslovnega procesa. Izdelek – uporabniška rešitev – je za večino nekaj neoprijemljivega, kakovost tega izdelka pa teže določljiva. Uporabniška rešitev namreč ima nekaj določil storitve, kot so zanesljivost, varnost, dostopnost in razumevanje strank, kar niso pogoste lastnosti izdelka. Če se na inženirskih projektih pogovarjajo gradbeniki in nosilci sorodnih poklicev med seboj, se morajo na projektih informacijske tehnologije pogovarjati ljudje različnih strok z različnimi specialnimi znanji. Pogosto to predstavlja večji problem v sporazumevanju kot pogovor dveh ljudi z različnim maternim jezikom.

1.2 Javna podjetja in javno naročilo

Podjetja v javni lasti pri naročanju zunanjih storitev omejuje Zakon o javnih naročilih [ZJN], ki predvidi pogoje, ki jih predpiše naročnik in jih morajo izpolniti dobavitelji. Najpogostejši pogoj je cena. Avtorji zakona so se pri zahtevah nedvomno posvetili »običajnim projektom«, povezanim predvsem z naročanjem opreme, manj pa so imeli v mislih projekte razvoja uporabniških rešitev.

Opredeliti zahteve uporabnikov v jeziku razvijalcev je v okvirih, ki jih postavlja zakon, dokaj težko. Vsi, ki so kdaj pisali take zahteve, vedo, kako zelo se

med potekom projekta spreminjajo zahteve in kako težko je naknadno prilagajati programe novim pobudam uporabnikov. V prispevku prikazujem drugačen pogled na javne razpise. Zakonsko namreč ni dopustno, da diskriminatorno predpišemo, s kakšnimi ljudmi želimo delati. Ob tem ko predpišemo zahteve glede strokovnih znanj zunanjih izvajalcev, ni v navadi zahtevati od njih določenih značajskih lastnosti, ki pripomorejo k uspešnosti projektne skupine. Zavedati se moramo, da zgolj predpisati, katere standarde naj pri delu zunanji sodelavci uporabljajo, nikakor ne zadošča. Tako je navadno cena tista, ki odločno vpliva na določitev zunanjega dobavitelja, v našem primeru izvajalca storitve razvoja (analize in programiranja) uporabniške rešitve.

2 STANDARDI IN METODE DELA

Informatiki skušamo s sodobnimi orodji podpreti poslovne funkcije in procese. Ti so običajno popisani v priročniku kakovosti, izdelanem po standardu ISO 9000/2000 [ISO9000/2000]. Vendar pa njihova opredeljenost znotraj standarda ni dovolj podrobna, niso popisane razne izjeme in učinki posameznega procesa, naj si gre za poročila o davku na dodano vrednost, ki jih oddajamo davčni upravi, ali plačilni list zaposlenega. ISO standard torej razvijalcem uporabniške rešitve ne zadošča, poda jim le temeljno usmeritev procesa.

Razvoja uporabniških rešitev se tako ali drugače dotika še precej mednarodnih standardov, ki pa v okoljih razvoja uporabniških rešitev v slovenskih podjetjih niti ne predstavljajo temelja ali opore pri razvoju niti ne dajejo smernic za razvoj.

V slovenskem okolju postajajo priljubljene smernice ITIL (Information Technology Infrastructure Library) [ITIL]. Ta pa se ne ukvarja toliko s procesi, ki jih informacijska tehnologija podpira, pač pa z organiziranjem same dejavnosti – temeljnih procesov v oddelku informatike. ITIL se opira na besedo »sledljivost«. Gre za sledljivost sprememb v informacijski infrastrukturi in uporabniških rešitvah. ITIL se ne ukvarja s sestavo projektnih skupin, primernih razvoju, niti ne podaja kakršnihkoli smernic v ta namen. Za premostitev problema pomanjkanja ustreznega standarda je novembra 2005 izšla serija standardov ISO/IEC 20000 *Service Management Standards*.

Jezik, ki ga teorija pogosto predvidi in naj bi olajšal sporazumevanje med uporabniki in razvijalci uporabniških rešitev je UML (Unified Modelling Language). Uporablja se v objektnem programiranju, saj naj bi zagotavljal uporabo najboljše prakse iz svetovnih razvojnih hiš. Vsakdanjost je nekoliko drugačna. Slovenska podjetja namreč uporabljajo relacijske baze podatkov in pogosto nimajo strokovnjakov, ki bi se znali sporazumevati v UML. Ko poteka razvoj nenadzorovano ali ad hoc, se nihče ne ukvarja z risanjem diagramov UML. Kadar je zakon sprejet tako rekoč za nazaj, ga je treba informacijsko nemudoma podpreti in vsak se znajde po svoje.

EMRIS (Enotna metodologija razvoja informacijskih sistemov) [EMRIS] je v slovenski državni upravi poznana, vendar jo v prakso podjetja, razen teorije same, niso prenesla v večjem obsegu. Informatiki jo ocenjujejo za nekoliko »postopkarsko« in zamudno v primerih popravkov ter potrebe po razvoju, kadar je treba tega zaradi zunanjih dejavnikov udejanjiti dobesedno čez noč.

3 AGILNA METODOLOGIJA RAZVOJA

Leta 2000 je James A. Highsmith razvil in objavil metodo Adaptive Software Development (prilagodljivi razvoj programske opreme), ki je ena izmed možnosti agilne metodologije razvoja programske opreme. Ustrezala naj bi sodobnim zahtevam poslovanja v nenehno spreminjajočem se, negotovem in nepredvidljivem okolju. Sporočilo metodologije avtorji pogojujejo s štirimi predpostavkami:

- **Posamezniki in sodelovanje** imajo prednost pred procesi in orodji.
- **Delujoči programi** imajo prednost pred izčrpno dokumentacijo.
- **Sodelovanje z uporabnikom** ima prednost pred pogajanji o pogodbi.
- **Hiter odziv na spremembe** ima prednost pred sledenjem načrtom.

Ljudje postanejo pomembnejši od predpisov, spodbujeno je sodelovanje med ljudmi, ki sodelujejo pri razvoju nove programske opreme. Motivacijo posameznika in skupine je treba spodbujati, ne pa omejevati s tehničnimi podrobnostmi. Metoda gotovo moti vse, ki želijo postopke predvsem dokumentirati in prisegajo na neprekinjeno sledljivost. Ti bi se morali zavedati, da v tem primeru govorimo o programiranju in ne o rezultatih nekih meritev.

Pogled razvojnika je usmerjen h kupcu. Manj pa je pogled kupca uporabnika usmerjen k dobavitelju. V mešanih razvojnih skupinah se morajo vsi počutiti dobro in težiti k skupnemu cilju. Uporabnik ni samo

nekdo, ki plača račun za opravljeni razvoj. V primeru razvoja s pomočjo zunanjega izvajanja dejavnosti namreč nastopata dve vrsti »kupcev«: programer in končni uporabnik iz podjetja naročnika.

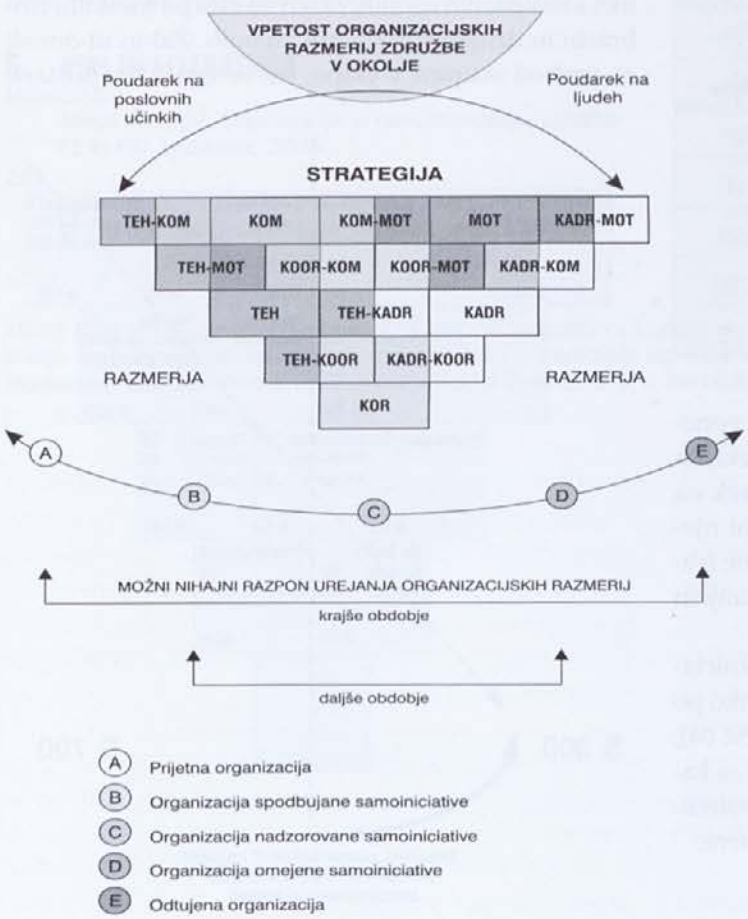
Vsaka formalna metoda razvoja naj bi v podjetju prispevala k večji učinkovitosti razvoja uporabniške rešitve in njeni kakovosti [Vavpotič 05]. Večina podjetij pa metode ne formalizira in deluje v skladu s svojo dobro prakso, ki se seveda razlikuje od podjetja do podjetja, tako kot se razlikujejo ljudje v skupinah in njihova zgodovina sodelovanja pri razvijanju uporabniških rešitev.

4 RAZMERJA

4.1 Teorija organizacije

Po Lipovcu [Lipovec 74] predstavlja organizacija sestavo razmerij. Mihelčič [Mihelčič 03] predvidi, da vsako podjetje nastane zaradi razmerij tehnične narave, saj ni drugega pomembnejšega razloga za ustanovitev podjetja, kot je možnost ustvarjanja in prodaje proizvodov ter storitev. Rosabeth Moss Kanter [Kanter 94] pravi, da so podobno kot razmerja med ljudmi tudi poslovna družabništva živi sistemi, ki imajo nešteto možnosti. Združbe, ki bodo znale izrabiti te možnosti ter učinkovito obvladovati svoje povezave, bodo okrepile svojo vrednost v sredstvih/naložbah.

Na sliki 1 je prikazan grozd organizacijskih razmerij. Grozd je rezultat študije, izdelane na Gospodarski zbornici Slovenije leta 1988 [Mihelčič 88]. Prikazan je preplet petih vrst razmerij (tehnične, kadrovske, koordinacijske, komunikacijske in motivacijske narave) ter združitev po dveh izmed njih, ki jih zasledimo v vsaki združbi in tudi v projektni skupini. Glede na zaznane poudarke na posameznih razmerjih ali kombinaciji razmerij vemo, da se združba ali skupina nagibata ali k poslovnim učinkom (proizvodom oziroma storitvam) ali k ljudem in delu z njimi.



Slika 1: **Grozd organizacijskih razmerij**

4.2 Vplivni dejavniki

Leta 2003 smo anketirali dobavitelje izdelave (programiranja) uporabniških rešitev za podjetje v javni lasti. Prosili smo jih, naj primerjajo podjetje z najboljšim podjetjem, ki mu dobavljajo enako storitev. Ugotovitve so pokazale, da je dobaviteljem, ki pogosto opravljajo svoje delo v prostorih naročnika in se srečujejo s programerji v podjetju ter uporabniki razvitih uporabniških rešitev, najbolj pomembno:

- sodelovanje s »hišnimi« programerji in skrbniki uporabniških rešitev;
- da ob razvoju hišni programerji aktivno sodelujejo in sproti prevzemajo (dele) rešitev;
- predpisana oblika predane dokumentacije ob koncu projekta;
- ugodni delovni pogoji (prostor, svetloba, delovni pripomočki ipd.);
- zapisane zahteve.

Ko potrebe zunanjih dobaviteljev uvrstimo v prikazani organizacijski grozd razmerij, ugotovimo, da je poudarek na dobrem počutju in s tem na občutku smiselnosti v delo vložene večje energije, v razmerjih komunikacijske in motivacijske narave.

Kljub pomanjkljivostim v omenjenih razmerjih pa podjetje dosega pri projektih

razvoja programske opreme dobre rezultate. Kateri so torej dejavniki, ki povečujejo ali pa zmanjšujejo možnost uspeha projekta? Iz teorije, odgovorov ankete in izkušenj izvedem štiri vrste dejavnikov, ki vplivajo na kakovost razmerij v projektni skupine (preglednica 1). Številke v stolpcih pomenijo težo posameznega dejavnika in so določene na podlagi pomena posameznega dejavnika na kakovost razmerij v projektni skupini.

Preglednica 1: **Vplivi in njihova teža na kakovost razmerij v projektnem timu**

Biološko opredeljivo	**Vpliv**	**Sposobnosti**	**Vpliv**
Starost	25	Komuniciranje	100
Spol	50	Širok pogled	100
Prilagodljivost	75	Spoštovanje	75
Kemija	75	Skromnost	50
"Tisto nekaj"	50	Vodja	75
		Hobiji	25
Pridobljeno	**Vpliv**	**Zunanji vpliv**	**Vpliv**
Izobrazba	25	Standardi	25
Strokovno znanje	25	Pogoji dela	50
Skupna stvarnost	50	Število ljudi v skupini	50
Skupni cilj	50	Uporabniki	100
		Obvestila	75

Ko razmerja in dejavnike, ki vplivajo nanje, vpnemo v grozd (slika 1), ugotovimo, da je v projektnih skupinah razvoja uporabniških rešitev poudarek na ljudeh, na vsakem posamezniku in ustvarjanju njegovih povezav z drugimi člani projektne skupine (slika 2). Povezave pa ustvarjamo tako s komuniciranjem kot tudi s standardi ter predpisi.

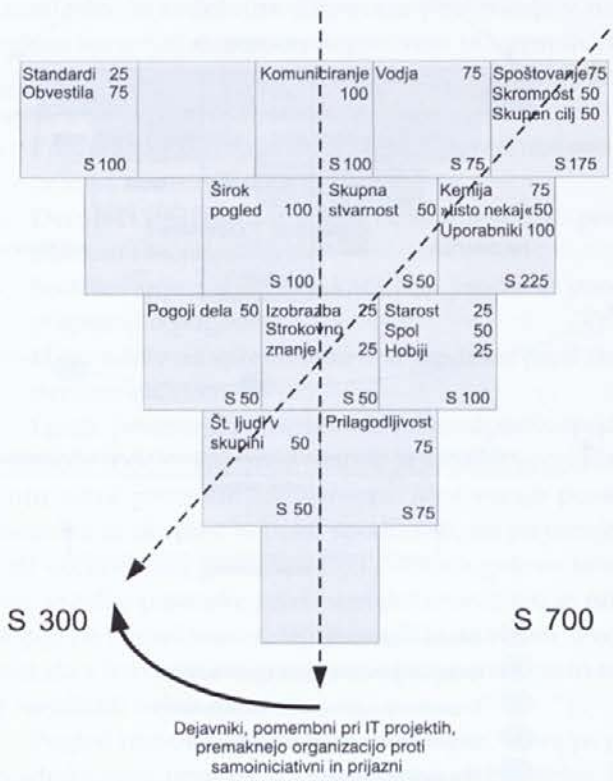
Premik od organizacije nadzorovane samoiniciative k organizaciji spodbujene samoiniciative lahko po metodi predstavljeni v [Mihelčič 88] in [Mihelčič 04], ocenjujemo z izidom 60. Ta izid pomeni, da je za kakovostno ekipo za izdelavo uporabniške rešitve potrebna prijazna organizacija spodbujene samoiniciative.

4.3 Predvideti uspeh

V podjetjih, ki se jih posredno dotikamo s člankom, programiranje uporabniških rešitev za podporo poslovanju ni temeljna dejavnost podjetja. Oddelki informatike predstavljajo manjši del zaposlenih v podjetju (povprečno okrog 5 %).

Projektno skupino za razvoj nove uporabniške rešitve sestavljajo zaposleni v informatiki, njihovi zunanji dobavitelji (največkrat programerji in ne tako pogosto analitiki procesov, saj je za uspeh projekta pomembno, da vsaj nekaj analitikov prihaja iz podjetja in ne od zunaj) ter uporabniki rešitve, ki izvajajo neko drugo funkcijo v podjetju oz. so nosilci dela poslovnega procesa, ki ga bo podprla rešitev.

Projektno skupino sestavi vodja projekta, tega pa določi lastnik projekta – notranji kupec. Pri dopolnjevanju skupine z zaposlenimi iz podjetja naletimo na ovire, ki jih navadno postavljajo funkcijski vodje – nihče ne želi izgubiti najboljših ljudi. Zunanje sodelavce moramo največkrat pridobiti z javnimi razpisi. V splošno prakso pa žal ne sodi, da bi ene ali druge sodelavce izbirali na podlagi osebnosti, njihovega načina dela s sodelavci ali po katerem koli v preglednici 1 navedenih sodilih, razen morda po formalni izobrazbi in drugih strokovnih znanjih. Žal to ni dovolj za prehod skupine v ekipo, kar se zgodi, ko postane



Slika 2: **Uteženost grozda razmerij z vplivnimi dejavniki in zasuk proti prijazni organizaciji**

namen skupine razumljiv vsem članom in vsak odigra predpisano vlogo tako, da v največji meri uveljavi svojo nadarjenost in usposobljenost.

Projektni vodja je tako pred zahtevno nalogo z razpoložljivimi kadri doseči največ. Kateri dejavniki so najbolj in kateri manj pomembni? Pri iskanju odgovora si lahko pomaga s preglednico 1. Projektna skupina, v kateri ni dovolj pomembnih dejavnikov, je vnaprej obsojena na neuspešno delo, družba pa na nekakovosten izdelek.

5 SKLEP

Pravila, standardi in dokumentacija omejujejo in hkrati pomagajo projektnim skupinam pri razvoju uporabniških rešitev. Ker gre pri razvoju uporabniških rešitev za podporo poslovanja za multidisciplinarne skupine iz različnih okolij, so lastnosti posameznika v skupini, ki šteje do deset članov, izredno pomembne. Žal jih iz različnih vzrokov ne moremo vedno izbirati, če pa jih poznamo, utegnemo iz ugodnih součinkovanj teh lastnosti potegniti najboljše učinke.

6 VIRI IN LITERATURA

Mihelčič 03
Miran Mihelčič: Organizacija in ravnateljevanje, Založba FE in FRI, Ljubljana, 2003.

ZJN
Zakon o javnih naročilih, Uradni list Republike Slovenije št. 39/00, 12. 5. 2000.

ISO9000/2000
PSIST ISO/DIS 9000:2000; Sistem vodenja kakovosti – Zahteve, 3. izdaja; maj 2000.

ITIL
ITIL; The Key to Managing IT Service; Best practice for Service Delivery, Office of Goverment Commerce, London, 2001.

EMRIS
Krisper, Marjan; Rupnik, Rok; Bajec, Marko; Rožanec, Alenka; Zrnec, Aljaž; Vavpotič, Damjan; Osojnik, Rok; Tomažič, Roman: Enotna metodologija razvoja informacijskih sistemov (EMRIS); Vlada Republike Slovenije; Center vlade za informatiko, 2003.

Vavpotič 05
Vavpotič, Damjan; Bajec, Marko; Krisper, Marjan: Meauring and improving software development methodology value by considering tehnical and social suitability of its constituent elements, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, 2005.

Lipovec 74
Filip Lipovec, Teorija organizacije, Univerza v Ljubljani – Ekonomska fakulteta, Ljubljana, 1974.

Mihelčič 04
Miran Mihelčič, Principles of Organization Analysis: Sugestion of Method and Application in Practice, EGOS Library, 2004.

Kanter 94
Rosabeth Moss Kanter; Collaborative Advantege: The Arto f Alliances, Harvard Business Review, julij–avgust 1994, 96–108.

Mihelčič 88
Miran Mihelčič, Cita Bračko, Janez Gabrijelčič, Miro Kline, Janez Šček, Ivan Štucin: Metodologija ugotavljanja kakovosti ali popolnosti organizacije (gospodarskih) združb; raziskovalno delo. Gospodarska zbornica Slovenije, 1988.

Alenka Kolar je leta 1972 diplomirala na Fakulteti za strojništvo v Ljubljani in leta 1998 magistrirala na Fakulteti za organizacijske vede v Kranju. Zaposlena je bila na Uradu za standardizacijo in meroslovje kot vodja laboratorija za maso, nato v avtomobilski industriji kot vodja zagotavljanja kakovosti, od leta 1999 pa dela v Elektro-Slovenija, d. o. o, kjer od leta 2001 vodi službo v sektorju za poslovno informatiko.

Pomen odločitvenih modelov za pogajanja v e-poslovanju

Andrej Bregar, Matjaž B. Jurič
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova ulica 17, Maribor
andrej.bregar@uni-mb.si, matjaz.juric@uni-mb.si

Povzetek

Z informacijskimi tehnologijami podprta nerutinska poslovna opravila, kakršna so povpraševanja po naročnikovim potrebam karseda prilagojenih storitvah na elektronskem trgu, zahtevajo avtomatizirana pogajanja, ki verodostojno ujamejo večkriterijske preferenčne strukture vseh potencialnih partnerjev. Zato so v prispevku predstavljene temeljne pogajalske strategije in metode večkriterijske odločitvene analize, po katerih posegajo agenti ponudnikov in odjemalcev storitev, da bi dosegli soglasje glede transakcij, ki maksimizirajo korist vseh udeleženih strani.

Ključne besede: poslovanje B2B in B2C, avtomatizacija pogajanj, pogajalske strategije, večkriterijska odločitvena analiza, podpora odločanju, agenti

Abstract

THE ROLE OF DECISION MODELS IN AUTOMATED NEGOTIATIONS FOR E-BUSINESS

Information technology supported non-routine business tasks, such as provision of services/products which are available on the electronic market in the form highly customized to the needs of clients, require automated negotiations that credibly capture preference structures of all potential partners. Thus, fundamental negotiation strategies and multiple criteria decision-making methods are presented. They can be applied by agents of service providers and customers in order to reach the agreement on transactions that maximize the utility of all involved parties.

Keywords: B2B and B2C e-commerce, negotiation automation, negotiation strategies, multi-criteria decision analysis, decision support, agents

1 UVOD

Zadnja leta smo priča valu poslovanja B2B in B2C prek spleta [8]. Večina trenutnih sistemov za e-poslovanje predstavlja zgolj pasivne kataloge, ki omogočajo nakupovanje proizvodov in koriščenje storitev pod vnaprej določenimi neprilagodljivimi pogoji [11]. Opazno manjši je delež aktivnih aplikacij e-poslovanja, ki so zmožne posredovati pri sklepanju pogodb ali pomagati pri odločanju o tem, kakšne proizvode/storitve potrebuje kupec. Toda bistvena pomanjkljivost tovrstnih sistemov je, da se osredotočajo predvsem na zagotavljanje čimbolj ugodne cene. Četudi je le-ta pomemben vidik transakcij, je treba v praksi upoštevati še številne druge dejavnike. Podjetja želijo pridobiti in ohranjati stalne stranke, ki jih zanimajo poleg cene tudi garancijski pogoji, rok dobave, renome in zgodovina poslovanja ponudnika ipd. Zato je potrebna programska oprema, ki upošteva različne kriterije, relevantne za uporabnike na obeh straneh, in za katero je neizogibno zagotoviti maksimizacijo koristi, omogočiti kompenzacijo kriterijev ter dopustiti, da cena ne bo najbolj pomembna.

Tem zahtevam je mogoče zadostiti z aplikacijo metod večkriterijske odločitvene analize, ki so že vrsto let eden od temeljev sistemov za podporo odločanju [12, 14]. Bistveno je, da te metode niso statične. Na podlagi opazovanja preferenc in obnašanja kupcev lahko namreč z namenom povečanja njihovega zadovoljstva sistemi e-poslovanja v realnem času spreminjajo pogoje prodaje proizvodov oziroma storitev [10]. Ker pa so prisiljeni gledati tudi na svojo korist, morajo vplivati na odločitve kupcev, še preden ti zaključijo s transakcijami. To daje motivacijo za razvoj inteligentnih agentnih sistemov; če so agenti avtonomni, se lahko pogajajo v imenu svojih lastnikov – ponudnikov in odjemalcev storitev. Podlaga za formalno pogajalsko analizo so prav metode večkriterijskega odločanja [13].

2 AVTOMATIZIRANA POGAJANJA

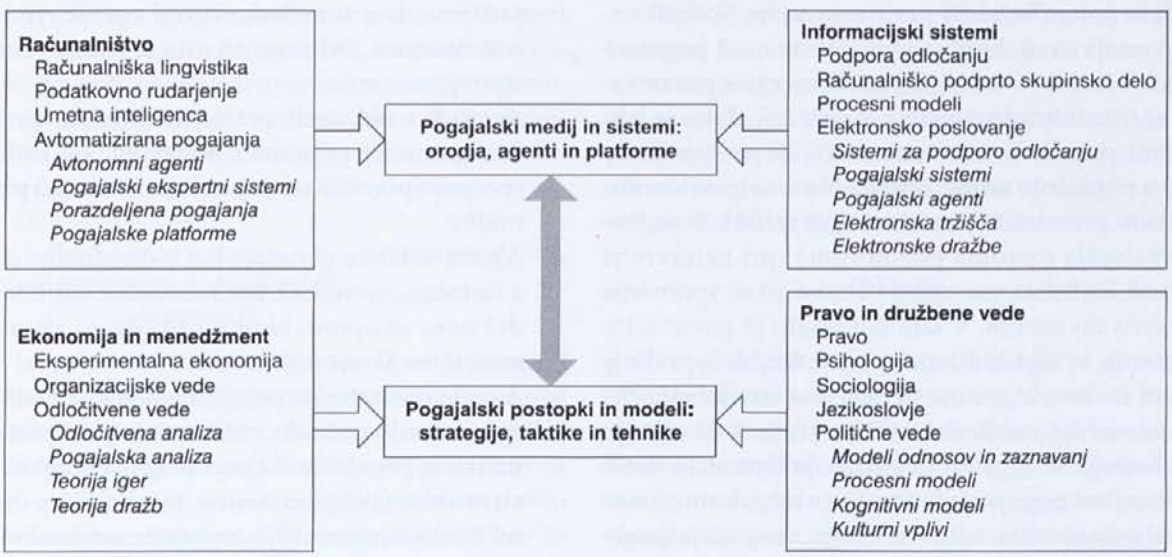
Pogajanje je proces, v katerem skupina ljudi/agentov medsebojno komunicira z namenom, da bi zadostili skupnim ciljem, ki premoščajo potencialno delno nezdružljive individualne cilje [11, 13, 17]. Ker avtomatizacija pogajanj občutno skrajša čas, ki je zanje potreben, in ker hkrati učinkovito odpravlja nezainte-

resiranost ljudi, postajajo pogajanja koordinacijski mehanizem za interakcijo med prodajalci in kupci na elektronskih tržiščih. Formalizacija pogajanj je tako kritični dejavnik uspeha elektronskih tržišč in je deležna precejšnje pozornosti znotraj domene agentnih sistemov e-poslovanja. Vendar kljub občutnemu napredku v zadnjih letih podpora pogajanjem v neki meri še vedno ostaja pomemben izziv e-poslovanja B2B in B2C [20]. To je predvsem posledica dejstva, da je mnogokrat pogajalske procese teže formalizirati kakor klasične poslovne procese. Kompleksnost domene pojasnjuje slika 1 [2], ki prikazuje njeno interdisciplinarnost in medsebojne vplive različnih področij znanosti.

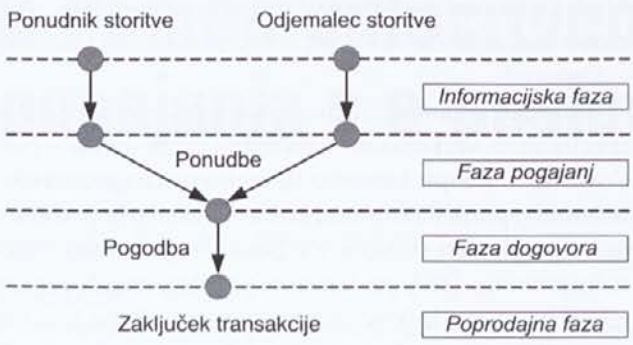
Posledica interdisciplinarnosti je obstoj množice raznolikih elektronskih sistemov pogajanja, ki jih formalno kategorizira montrealska taksonomija [17]. V praksi prihaja najpogosteje do zamenjav med elektronskimi pogajanji in avkcijami (dražbami), kajti besedišče velikokrat iz propagandnih razlogov tvorijo marketinški oddelki razvijalcev programske opreme. Avkcije so ozko usmerjene in upoštevajo ceno kot edini kriterij. Po drugi strani vpeljujejo pogajanja različne mehanizme, kot so večkriterijsko izražanje preferenc, kompenzacija med kriteriji, simultano izboljševanje zaželenosti, ki vodi v situacije, v katerih pridobijo vse udeležene strani (»*win-win*«) itd. Za pogajanja prav tako velja, da kot podlaga za izmenjavo storitev in dobrin niso relevantna zgolj za poslovni svet, temveč predstavljajo primerno obliko skupinskega odločanja tudi v nekomercialnih – recimo političnih in pravnih – domenah.

Poleg avkcij, katerih popularnost je rezultirala v specifičnem »avkcijskocentričnem« pogledu na e-poslovanje, v sklopu katerega je vsaka izmenjava strukturiranih sporočil obravnavana kot avkcija, je pomemben tip spletnih storitev v e-poslovanju primerjalno nakupovanje [10], pri katerem je integriranih več trgovin oz. ponudnikov storitev, uporabnik pa ima en vmesnik za povpraševanja, posredovana vsakemu od njih. Najboljša ponudba je izbrana s pogajanji.

Proces pogajanja je v poslovnih aplikacijah sestavni del procesa dogovarjanja dveh ali več agentov glede koriščenja storitev oziroma nakupa proizvodov in ga je mogoče umestiti v širši kontekst tržnih transakcij, kot je razvidno iz slike 2 [8]. Proces poteka v več korakih. V posameznem koraku je dogovor lahko sprejet ali ne. Če ni, pride do podajanja protiponudb. Princip pogajanja tako temelji na spremembi ponudbe agenta (kar je zanj manj ugodno), da bi bila dosežena sprememba ponudb drugih agentov. Iz tega razloga morajo agenti ocenjevati protiponudbe in se odločati glede na lastno pogajalsko strategijo o izvedbi nadaljnjih akcij. Formalno je ponudba n-terica elementov, ki predstavljajo kriterije, kot so cena, garancija ali čas dobave, in so korelirani z določeno mero ustreznosti, najpogosteje s funkcijo koristnosti ali mehkim prednostnim indeksom.



Slika 1: **Shematska ponazoritev področij pogajanj**



Slika 2: **Faze tržnih transakcij**

Mehanizem pogajanja združuje pogajalski protokol in pogajalsko strategijo agentov [2]. Imeti mora nekaj značilnosti, med katerimi sta iz vidika teorije odločanja najpomembnejši:

- *individualna racionalnost*, ki pomeni, da agent sodeluje v pogajanjih samo, če je to v njegovem lastnem interesu, in
- *Pareto učinkovitost*, ki pravi, da je rezultat učinkovit, če ne obstaja neki drugi rezultat, ki je bolj ugoden za enega agenta in hkrati ni manj ugoden za drugega agenta.

Agenti se morajo najprej v sklopu t. i. metapogajanja zediniti glede protokola, ki strukturira proces, vpeljuje pravila dopustnega obnašanja udeležencev in določa pogoje, pod katerimi nastopi interakcija med njimi. Tako je opredeljeno, kakšne pogodbe smejo biti sprejete in kakšne sekvence ponudb so dovoljene. Šele potem se lahko pogajanje začne. Specifikacija zaporedja akcij, ki jih agent izvede med pogajanjem, je določena s strategijo, pri čemer je s posameznim protokolom združljivih več strategij. Tako se lahko agent pogodi že v prvem krogu ali pa vztraja do preteka pogajanju namenjenega časovnega intervala. V vsakem primeru morajo strategije težiti k doseganju ravnovesja oziroma ekvilibruma, pri katerem je vrednost bodisi za vse agente enaka ali se spreminja od agenta do agenta. V tem kontekstu je govor o integrativnih in distributivnih pogajanjih. Cilj prvih je poiskati rešitev, ki zadovolji prav vse strani (situacija tipa »*win-win*«), medtem ko težijo druga k doseganju učinkovitega kompromisa (situacija tipa »*win-lose*«) [20]. Rezultat pogajanja je torej konsenz, kompromis ali nestrinjanje. Formalno podlago zanje daje pogajalska analiza [13], ki integrira odločitveno analizo in teorijo iger ter tako premosti neskladje med kvantitativnimi/kvalitativnimi deskriptivnimi in normativnimi modeli. Sloni na progresivnem procesu, ki se začne z neučinkovito ponudbo in vodi do Pareto optimalnih rezultatov. Poudarja praktične vidike, kot so nepopolne informacije, ne povsem racionalno obnašanje in nezavezanost.

3 POGAJALSKI AGENTI

Protokol uvaja v proces pogajanj strukturo, ki je pogoj za delovanje avtonomnih agentov. Le-ti nadomestijo človeške pogajalce v vseh odločevalskih, komunikacijskih in pogajalskih aktivnostih. Lahko so predstavniki drugih entitet ali delujejo iz svojih lastnih interesov. Ker nadzirajo celoten proces vključno s specifikacijo ponudb in sprejemanjem končnih odločitev o sklenitvi ali zavrnitvi sporazuma, morajo poleg splošnih lastnosti agentov – avtomatizacije dela, zavedanja, zmožnosti učenja in sodelovanja, avtonomnosti, prilagodljivosti, mobilnosti ter inteligence – imeti tudi sposobnost ocenitve lastnih preferenc, tako da zmorejo vrednotiti različne dogovore in izbirati med njimi. To pa kliče po implementaciji ustreznih odločitvenih metod. Značilnosti agentov, ki realizirajo avtomatizirana pogajanja, so [11]:

- Agent ima lahko vlogo kupca, prodajalca ali posrednika.
- Racionalnost agenta je lahko popolna ali omejena. Če je popolna, je zmožen opraviti poljubno število kompleksnih izračunov v končnem časovnem intervalu.
- Agent poseduje znanje o dobrinah in potencialno tudi znanje o tem, kako drugi agenti vrednotijo iste dobrine. Od tega znanja je močno odvisna strategija agenta.
- Agent je v nekaterih primerih zavezan, da po podani ponudbi preneha s pogajanji, vse dokler ne sprejme sporočila o odobritvi ponudbe ali protiponudbe.
- Agenti se lahko obnašajo kot individualne entitete z lastnimi interesi ali kot nesebične entitete, ki so del neke skupine. Lahko tudi iščejo ravnovesje med tema skrajnostima.
- Agentova strategija pogajanja odloča o dajanju in sprejemanju ponudb, oblikovanju protiponudb in umiku iz pogajanja. Čeprav je konceptualno neodvisna od ostalih parametrov, je v določeni meri korelirana z zavezanostjo, znanjem, racionalnostjo in socialnim obnašanjem. Bistvena predpostavka je, da so agenti individualno racionalni, zaradi česar

ne sprejemajo dogovorov, na podlagi katerih bodo na slabšem, kot so sicer.

4 ODLOČITVENI MODELI ZA AVTOMATIZIRANA POGAJANJA

Elektronska pogajanja zahtevajo od avtonomnih agentov sprejemanje odločitev [9]. Pri tem so aplicirane metode iz domene odločitvene analize, posebej večatributne teorije koristnosti [12].

4.1 Temeljne odločitvene metode

Kot temeljna preskriptivna teorija, ki določa, na kakšen način naj bi bile odločitve sprejete, da bi maksimizirale korist, je bila večatributna teorija koristnosti aplicirana v različnih tipih pogajanj. Kot primerna se je izkazala tako za kooperativne kot nekooperativne domene in za različne možne kardinalnosti interakcij – »ena proti ena«, »več proti ena« in »več proti več« [11]. Četudi so v praksi najpogostejša pogajanja tipa »več proti ena«, ki so značilna za dražbe, v sklopu katerih en agent prodaja, drugi pa kupujejo, ali primerjava proizvodov/storitev, kjer en agent kupuje, medtem ko jih več prodaja, je že najpreprostejši scenarij pogajanj tipa »ena proti ena« v kooperativnih domenah tako zapleten, da zaradi specifičnih težav, kakršna je možnost več ravnovesij, zahteva upoštevanje konceptov kompleksnejših scenarijev. K temu scenariju pristopa protokol monotonega popuščanja (*monotonic concession protocol*), ki operira na prostoru pogodb, ki so hkrati individualno racionalne in Pareto optimalne. Agenta skušata maksimizirati svoje koristi in se pogajata v krogih, pri čemer posamezni agent v vsakem krogu izgubi, kar pomeni, da ponudi možnost, ki da večjo korist drugemu in manjšo njemu. Pogajanje se konča, ko sta agenta zadovoljna z dogovorom ali ko ta spodleti. Strategija sloni na izračunu stopnje izgube ob nedoseganju kompromisa:

$$tveganje_i = \begin{cases} 1 & , koristnost_i(\delta_i) = 0, \\ \dfrac{koristnost_i(\delta_i) - koristnost_i(\delta_j)}{koristnost_i(\delta_i)} & , \text{sicer}. \end{cases}$$

Pri tem sta i in j indeksa agentov, δ_i in δ_j pa njuni ponudbi. Če je $tveganje_i \leq tveganje_j$, agent i poda novo zanj slabšo ponudbo, ki ravno še spremeni ravnovesje. V splošnem je ne glede na scenarij pogajanja za agenta zaradi pridobivanja strateške prednosti dobro oceniti koristnosti nasprotnih pogajalcev. To je še posebno dragoceno pri kompleksnih, dolgoročnih pogajanjih.

Pri pogajanjih, kjer je na eni strani več agentov, je najbolj običajna rešitev prav tako izračun agregiranih vrednosti z uporabo funkcije koristnosti. Protokol monotonega popuščanja je bil zato razširjen tudi na pogajanja tipa »ena proti mnogo«. Izračun stopnje tveganja upošteva v tem primeru zgolj agenta, katerega ponudba je ocenjena z najnižjo stopnjo koristnosti, kajti ta ponudba utegne pri iskanju kompromisa voditi do potencialno najizrazitejše popustitve:

$$tveganje_i = \begin{cases} 1 & , koristnost_i(\delta_i) = 0, \\ \dfrac{koristnost_i(\delta_i) - \min\{koristnost_i(\delta_j) \mid j \in A\}}{koristnost_i(\delta_i)} & , \text{sicer}. \end{cases}$$

Koncept Pareto učinkovitosti zagotovi blagostanje celotne skupine pogajalskih agentov le pod pogojem, da vsak agent po pravici razkrije svoje preference glede omejenih virov. Takrat je lahko vsak vir alociran natanko tistemu agentu, ki ga najbolj ceni. Vendar pa se v stvarnih pogajalskih situacijah pogosto zgodi, da popolne preferenčne informacije bodisi niso na voljo bodisi jih agenti iz strateških razlogov skrijejo oziroma poneverijo z namenom, da bi pridobili čim večji delež vira. To dejstvo upošteva Brams-Taylorjev mehanizem zmagovalca (*winner mechanism*), ki razdeli množico omejenih virov med dva ali več pogajalcev [7]. Eksperimenti so pokazali, da konvergirajo v primeru tekmovalnih preferenc in neomejenega skupnega znanja bilateralno oziroma multilateralno sprejete odločitve proti rezultatom, ki so le redko pravični. Če se veča stopnja negotovosti glede preferenc, pa se izboljšata tako pravičnost kot učinkovitost.

Najbolj preprost primer Brams-Taylorjevega mehanizma je vezan na dva pogajalca in dva vira. Naj bo u_i koristnost pogajalca A, da pridobi celoten vir i. Če mu je dodeljen delež a_1 vira 1 in delež a_2 vira 2, je potemtakem njegovo zadovoljstvo s sprejetim dogovorom izraženo s funkcijo koristnosti $u_A(a_1, a_2) = a_1u_1 + a_2u_2$. Ta funkcija je lahko normalizirana:

$$U_A(a_1, a_2) = \frac{u_A(a_1, a_2)}{u_1 + u_2} = a_1\rho_A + a_2(1 - \rho_A)$$

pri čemer velja $0 \leq U_A(a_1, a_2) \leq 1$ in kjer je $\rho_A = u_1 / (u_1 + u_2)$ relativna zaželenost vira 1 glede na vir 2. Agent A iz lastne koristi praviloma ne oznani dejanske vrednosti ρ_A, temveč vrednost $r_A = T(\rho_A)$. Funkcija T predstavlja strategijo agenta in določa njegovo ponudbo. Upoštevaje ponudbi r_A in r_B, ki odražata deklarirane navidezne preference nasprotujočih si agentov A in B, razdeli Brams-Taylorjev mehanizem vire tako, da sta

navidezni koristnosti obeh pogajalcev enaki in da je alokacija virov Pareto učinkovita. Rezultat je dobljen kot rešitev problema linearnega programiranja:

$$\max_{a_1,a_2} U_A^*(a_1,a_2)$$
$$\text{glede na } U_A^*(a_1,a_2) = U_B^*(1-a_1,1-a_2), \text{ kjer je } U_A^*(a_1,a_2) = a_1 r_A + a_2(1-r_A)$$

Pomanjkljivost pristopov na temelju funkcije koristnosti je, da se poznavanje agentovih preferenc reducira na eno samo vrednost. Posledično je razumevanje preferenc omejeno. Ta problem rešuje metoda pogajanja med enim ponudnikom storitev in več odjemalci, ki temelji tako na konceptih preferenčnega modeliranja kot tudi matematične relacijske analize [18]. V tem kvantitativnem odločitvenem modelu multilateralnega pogajanja ponudnik registrira določeno storitev na elektronskem trgu in priskrbi njen opis z ozirom na več karakterističnih kriterijev. Prodajni agent nato prejme različne ponudbe zainteresiranih potencialnih kupcev, pri čemer sestoji vsaka takšna ponudba iz vrednosti po posameznih kriterijih. Zato je prodajalec soočen s problemom izbire tistega kupca, s katerim se bo nadalje pogajal, da bi tržil storitev oziroma proizvod. Formalna analiza na osnovi parnih primerjav prodajalčevih preferenc in kupnih ponudb razkrije odvisnosti med ponudbami in hkrati izpostavi tudi odvisnosti med kriteriji. Ker je izpeljana delna razvrstitev kupcev, ki v primeru konfliktnih preferenc upošteva relacijo neprimerljivosti, so zajete vse relevantne informacije, katerih bogatost se ohranja skozi proces analize. Na njihovi osnovi lahko pogajalec identificira kupca, na katerega se mu splača fokusirati pogajanja.

Matematični postopek metode sestoji iz nekaj razmeroma preprostih operacij. Prodajni agent preslika prejete ponudbe potencialnih kupcev, ki so podane z vektorji kriterijskih vrednosti, v mehke prednosti, katere izrazi z matriko P. Primerjave vrstic matrike P izpostavijo odvisnosti med večkriterijskimi ponudbami:

$$d(P_i,P_j) = \frac{1}{n}\sum_{k=1..n} \min\left(1, 1 - P_{ik} + P_{jk}\right)$$

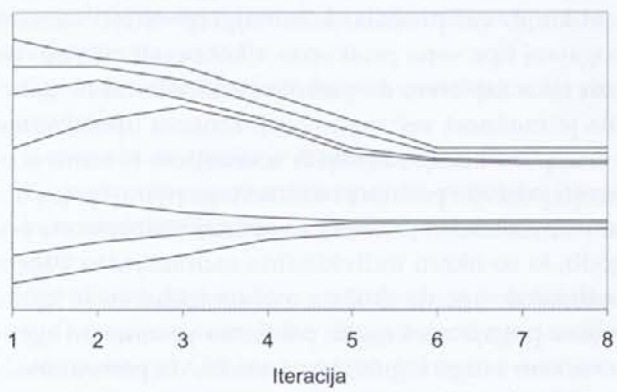
Na podlagi vrednosti $d(P_i, P_j)$ je dobljena mehka binarna relacija, katere tranzitivno zaprtje je relacija kvazireda Q na množici kupcev B. Relacija Q je izostrena z α-rezi, tako da za stopnjo zaupanja α velja $(b_i, b_j) \in Q_\alpha$, če je ponudba kupca b_i največ tako dobra kot ponudba kupca b_j. Na osnovi relacije kvazireda je definirana ekvivalenčna relacija, ki razdeli množico B v več ekvivalenčnih razredov:

$$(b_i,b_j) \in E_\alpha \Leftrightarrow (b_i,b_j) \in Q_\alpha \wedge (b_j,b_i) \in Q_\alpha$$
$$[b_i]_\alpha = \{b_j \mid (b_i,b_j) \in E_\alpha\}$$

Končno inducira relacija kvazireda med ekvivalenčnimi razredi prednostno relacijo $\leq_\alpha$ ki razvrsti ponudbe kupcev po zaželenosti:

$$[b_i]_\alpha \leq_\alpha [b_j]_\alpha \Leftrightarrow (b_i,b_j) \in Q_\alpha$$

Za avtomatizirana pogajanja v e-poslovanju sta zelo pomembna še dva koncepta – doseganje konsenza in formiranje koalicije agentov. Pristopi iskanja konsenza najpogosteje temeljijo na modeliranju »mehkih« mnenj [3]. V nekaterih primerih vključujejo še druge tehnike, kot na primer gručenje [15]. Aplikacija slednjega utegne rezultirati v delnem konsenzu, ki ne pomeni poenotenega mnenja vseh pogajalskih entitet, ampak izloči dve ali več skupin agentov, katerih preference se ujemajo. Slika 3 prikazuje primer razvoja delnega konsenza skozi osem iteracij.



Slika 3: **Razvoj delnega konsenza**

Ker nekaterih nalog ne more samostojno opraviti en sam agent, se lahko zgodi, da je potrebno dinamično formiranje koalicije več agentov. Delna rešitev problema je alokacija opravil, ki pa je možna le, če so opravila elementarna, to pomeni, da posamezen agent v celoti opravi njemu dodeljena opravila. Boljša sta pristopa na podlagi teorije iger in agregacije preferenc s Choquetovim integralom, ki upošteva interakcije med kriteriji in odvisnosti med agenti [1]. Oba pristopa sta takšna, da je doseganje koalicije zagotovljeno v vseh modelih koordinacije, vključno s kooperativnimi večagentnimi sistemi, tekmovalnimi sistemi in nehierar-

hičnimi sistemi brez osrednjega koordinatorja agentne združbe. Za kooperativne agente velja, da brez zadržkov izmenjujejo informacije ter lahko celo opravijo naloge v imenu drugih agentov brez zahteve po vračilu uslug. Po drugi strani je v tekmovalnem večagentnem sistemu izmenjava informacij med agenti omejena. Le-ti maksimizirajo zgolj svoje lastne preferenčne funkcije.

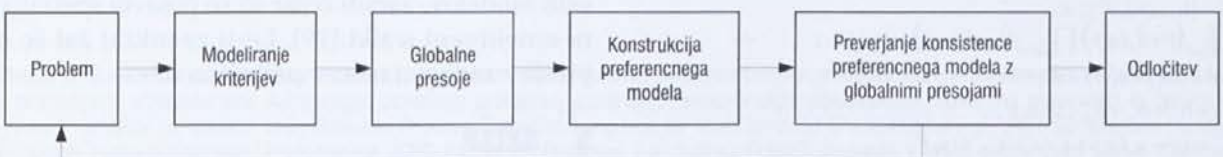
4.1 Reševanje problema izvabljanja preferenčnih informacij

Eden temeljev odločitvene teorije je racionalnost. Čeprav principi racionalnosti in aksiomi teorije koristnosti pri ocenitvi alternativ velikokrat niso upoštevani, je omejeno racionalnost v praksi še vedno mogoče doseči, kar pa zahteva rigorozen način zbiranja informacij, na osnovi katerega je vzpostavljena verodostojna preferenčna struktura v obliki funkcije koristnosti ali prednostnih relacij. Ta naloga je še posebej težavna zaradi množice več pogosto konfliktnih kriterijev in ciljev odločanja. V večagentnih sistemih pa se problem še poglobi. Da bi lahko pogajalski proces delegirali agentu, mora namreč le-ta biti parametriziran z odločevalčevimi preferencami. Elicitacija teh preferenc z obstoječimi metodami ni zadostno avtomatizirana, zato predstavlja ozko grlo. Poleg tega delujejo sistemi e-poslovanja v dinamičnem, hitro se spreminjajočem okolju. Posledično preference tekom pogajanja ne smejo ostajati konstantne, ampak se morajo prilagajati, kajti v dinamičnem okolju so lahko samo na ta način dobljeni pozitivni rezultati, ki se odražajo v dobičku. To pa pomeni naslednje:

- izvabljanje preferenc mora biti inkrementalno;
- na začetku procesa avtomatiziranega e-poslovanja morajo biti upoštevane zgolj delne informacije, medtem ko naj bodo holistične informacije pridobljene med pogajanjem na podlagi že ovrednotenih alternativ in uspešnosti izvršenih transakcij;
- agenti se morajo skozi proces pogajanja učiti in prilagajati svoje preferenčne strukture;
- vnaprej je zelo težko pravilno matematično specificirati preference.

Zgornjim zahtevam lahko delno zadostijo metode umetne inteligence. Eden od pristopov, ki je preizkušen v praksi, je sklepanje na podlagi primerov [10]. Pogajalski informacijski sistem indeksira pretekle primere, jih izbira in prilagaja novim situacijam ter se na podlagi uspešnosti rešitev uči. Vendar pa sta bistveni pomanjkljivosti metod umetne inteligence, da ne dopuščajo konstruktivnega učenja in da ne formalizirajo večkriterijskih preferenc na analitično ustrezen način, ampak jih najpogosteje predstavijo kot črne škatle. Zato je boljša rešitev združitveno-razdružitveni pristop, ki izpelje točne numerične vrednosti parametrov odločitvenega modela na podlagi globalne presojevalne hevristike [4]. Filozofija razdruževanja je zgraditi model iz preferenčnih struktur, ki se nanašajo na omejeno množico ocenjenih alternativ – referenčnih primerkov stvarnih odločitev. Postopek razdruževanja zgolj inducira preferenčne informacije ter jih formalizira v obliki parametrov modela, zato je kombiniran s klasičnimi metodami agregacije. Iterativno-interaktivno prepletanje združitvenih in razdružitvenih faz, prikazano na sliki 4, pomaga poglobiti znanje o problemski domeni in izboljšati dojemanje preferenc [16].

Na podlagi navedenih ugotovitev je bila v sklopu lastnih raziskav definirana metoda iskanja skupinskega konsenza, ki je primerna za implementacijo v okviru večagentnega pogajalskega sistema [3, 6]. Metoda skozi več iteracij prilagaja preferenčne parametre najbolj nesoglasnih agentov, tako da se njihove odločitve karseda poenotijo z mnenjem skupine, to pa posledično zagotovi konvergenco ponudb. Soočena je s problematiko dihotomijskega sortiranja ter ujame preferenčne informacije z upoštevanjem konceptov



Slika 4: **Shematski prikaz združitveno-razdružitvene analize**

Slika 5: **Združitveno-razdružitveni postopek iskanja skupinskega konsenza**

psevdokriterija in prednostne relacije. Njen združitveno-razdružitveni postopek prikazuje slika 5.

Na podlagi globalnih preferenc kot tudi uporabniško specificiranih omejitev izpelje parametre modela optimizacijski matematični program:

maksimiziraj τ
glede na
$\tau \le \sigma(a_i) - \lambda, \forall a_i \in \widetilde{C}_k^+,$
$\tau \le \lambda - \sigma(a_i) + \varepsilon, \forall a_i \in \widetilde{C}_k^-,$
$0 \le q_j \le p_j \le u_j \le v_j \le b_j - D_j^-, \forall j = 1,\ldots,n,$
$lw_j \le w_j \le uw_j, \forall j = 1,\ldots,n,$
$\lambda \in [0.5, 1].$

Matematični program maksimizira robustnost odločitvenih parametrov posameznega agenta. Pokazano je bilo, da metrike korelacije med kategorijami, v katere uvrstijo alternative različni odločevalci, in metrike robustnosti specificiranih in/ali samodejno izpeljanih parametrov poskrbijo za učinkovito izmenjavo mnenj agentov in uspešno usmerjajo postopek k doseganju konsenza [5]. Težava programa je, da se sooča z odsekoma linearnimi funkcijami z neznanimi segmenti. Analogno velja tudi za metrike robustnosti, ki minimizirajo normirane razdalje med izvornimi in na novo izpeljanimi parametri. Zato je problem razbit na več podproblemov, ki se nanašajo na pod-

$$\Delta_v(a_i) = \min\left[\sum_{j\in F}(\delta_j)^r \Big/ \sum_{j\in E}\left(2\cdot(b_j - p_j - D_j^-)\right)^r\right]^{1/r}$$

z izpeljavo
$\widetilde{d}_j(a_i)$ in $k_j, \forall j \in F$
glede na
$E = \{1,\ldots,n\}, F \subseteq E,$
$\prod_{j\in F}\left(1-\widetilde{d}_j(a_i)\right)\prod_{j\in E\setminus F}\left(1-d_j(a_i)\right) = \widetilde{d}(a_i),$
$0 \le \widetilde{d}_j(a_i) \le 1, \forall j \in F,$
$\delta_j = \delta_j^u + \delta_j^v + \delta_j^{uv}, \forall j \in F,$
$\delta_j^u = u_j - g_j(a_i) + \widetilde{d}_j(a_i)/k_j, \forall j \in F,$
$\delta_j^v = v_j - g_j(a_i) - \left(1-\widetilde{d}_j(a_i)\right)/k_j, \forall j \in F,$
$\delta_j^{uv} = v_j - u_j - 1/k_j, \forall j \in F,$
$\left(1-\widetilde{d}_j(a_i)\right)/\left(D_j^+ - D_j^- - g_j(a_i)\right) \le k_j \le \widetilde{d}_j(a_i)/\left(g_j(a_i) - p_j\right), \forall j \in F.$

množice parametrov in so rešeni z implementacijo specifičnih nelinearnih optimizacijskih programov, podprtih z ustreznimi algoritmi. Za informacije, vezane na princip veta, je definiran naslednji program, katerega obrazložitev je dosegljiva v literaturi [5]:

Bistvenega pomena za pogajalske sisteme je torej inteligentna interakcija med uporabnikom in pogajalskim agentom. Pri tem uporabnik nalaga agentu zahteve in omejitve, ki so bodisi simbolične bodisi kvantitativne, izražene v obliki matematičnih enačb. Slednje so še posebej relevantne za modele iz domene operacijskih raziskav in odločitvene analize, v katero spada tudi omenjena združitveno-razdružitvena metoda.

Postopek interakcije med uporabnikom in agentom se začne z uporabnikovo specifikacijo preferenc, zahtev in omejitev. Glede na njih skuša agent poiskati eno ali več rešitev. Zaradi nedostopnosti informacij in virov se lahko zgodi, da podane zahteve niso v celoti izpolnjene. Tedaj uporabnik pogosto zavrne rešitev. Posledično je nujno dinamično prilagajanje preferenc in izvajanje dodatnih pogajanj. Interakcija se konča, ko je med pogajalci dosežen dogovor, ki je sprejemljiv tako za uporabnika kot za njegovega agenta.

Učinkovit pogajalski sistem mora omogočiti dodeljevanje prioritet zahtevam in omejitvam, s čimer zagotovi fleksibilnost. V primeru nižjih prioritet je namreč dovoljeno popuščanje, ki pa rezultira v manjši verodostojnosti in zaželenosti s pogajanjem sklenjene pogodbe. Vendar možnosti, kakršna je specifikacija prioritet, znatno doprinesejo h kompleksnosti pogajalskih modelov, zaradi česar so se pojavili specializirani omejitveni jeziki [19]. Le-ti zaenkrat žal še niso prešli v zadostni meri v praktično rabo.

5 SKLEP

Računalniška podpora pogajalskim procesom vedno bolj vpliva na način sodelovanja podjetij s kupci, dobavitelji in drugimi poslovnimi partnerji. Podjetja so se

tradicionalno pogajala bilateralno – z osebnim stikom, s pismi, po telefonu itd. Toda takšna pogajanja je težko upravljati, so časovno potratna, zahtevajo velik miselni napor, so podvržena nesporazumom ter trpijo za omejeno transparentnostjo, omejenim številom udeleženih strani in visokimi transakcijskimi stroški. Ker vodijo zato k neučinkovitim kompromisom, ima nova generacija sistemov za e-poslovanje, ki temeljijo na avtomatiziranih pogajanjih, neizpodbiten potencial in bržkone daje novo dimenzijo koordinaciji poslovnih opravil. Okrepila je pomen virtualnih organizacij, zabrisala mejo med proizvodi in storitvami, podjetjem zmanjšala stroške in dala kupcem možnost aktivnega sodelovanja, saj omogoča ne glede na morebitno kombinatorično kompleksnost primerjavo med storitvami ter popolno prilagoditev potrebam kupcev v realnem času na način, ki je personaliziran, občutljiv na lokacijo, skladen z visokimi kakovostnimi standardi in cenovno ugoden. Pri tem ima bistven pomen tehnologija agentov, ki prevzemajo vloge prodajalca, kupca, posrednika, svetovalca ali ponudnika informacij. Tako smemo brez zadržkov predpostaviti, da bo avtomatizirano pogajanje postalo dominanten način delovanja agentov v e-poslovanju. In v veliki meri ga bodo omogočile prav metode odločitvene analize.

6 VIRI IN LITERATURA

[1] AKNINE, S. idr.: A multi-agent coalition formation method based on preference models, Group Decision and Negotiation, 2004, 13 (6), str. 513–538.

[2] BICHLER, M. idr.: Towards a structured design of e-negotiations, Group Decision and Negotiation, 2003, 12 (4), str. 311–335.

[3] BREGAR, A.: Iskanje skupinskega konsenza s sortiranjem alternativ na osnovi koncepta psevdokriterija, Zbornik posvetovanja DSI, 2003, str. 395–401.

[4] BREGAR, A.: Združitveno-razdružitveni pristop: nadgradnja strojnega učenja kot osnova konstruktivni specifikaciji kvantitativnih odločitvenih modelov, Zbornik posvetovanja DSI, 2005, str. 151–157.

[5] BREGAR, A.: Extension of the aggregation/disaggregation principle to computer-guided convergent group decision making processes, Zbornik konference EWG DSS, 2005, str. 95–107.

[6] BREGAR, A. idr.: An alternative sorting procedure for interactive group decision support based on the pseudo-criterion concept, Journal of Systemics, Cybernetics and Informatics, 2003, 1 (4), str. 66–71.

[7] DANIEL, T. E., PARCO, J. E.: Fair, efficient and envy-free bargaining: An experimental test of the Brams-Taylor Adjusted Winner mechanism, Group Decision and Negotiation, 2005, 14 (3), str. 241–264.

[8] GRIEGER, M.: Electronic marketplaces: A literature review and a call for supply chain management research, European Journal of Operational Research, 2003, 144 (2), str. 280–294.

[9] KOEHNE, F. idr.: Decision support in electronic negotiation systems, Zbornik konference IFIP TC8 DSS, 2004, str. 421–429.

[10] KWON, O. B., SADEH, N.: Applying case-based reasoning and multi-agent intelligent system to context-aware comparative shopping, Decision Support Systems, 2004, 37 (2), str. 199–213.

[11] LOMUSCIO, A. idr.: Classification scheme for negotiation in e-commerce, Group Decision and Negotiation, 2003, 12 (1), str. 31–56.

[12] POWER, D. J., SHARDA, R.: Model-driven decision support systems, Decision Support Systems, 2006.

[13] RAIFFA, H., RICHARDSON, J.: Negotiation analysis, Belknap Harvard University Press, 2002.

[14] SHIM, J. P. idr.: Past, present and future of decision support technology, Decision Support Systems, 2002, 33 (2), str. 111–126.

[15] SIMAS, T. idr.: Fuzzy consensus for inter-agents negotiation, Poročilo projekta EEII, IST-1999-10304.

[16] SISKOS, Y., SPYRIDAKOS, A.: Intelligent multicriteria decision support: Overview and perspectives, European Journal of Operational Research, 1999, 113 (2), str. 236–246.

[17] STROEBEL, M.: The Montreal taxonomy for electronic negotiations, Group Decision and Negotiation, 2003, 12 (2), str. 143–164.

[18] VAN DE WALLE, B.: Coping with one-to-many multi-criteria negotiations in e-markets, Zbornik konference DEXA, 2001, str. 747–751.

[19] WANG, H. idr.: Modeling constraint-based negotiating agents, Decision Support Systems, 2002, 33 (2), str. 201–217.

[20] WEIGAND, H. idr.: B2B negotiation support, Group Decision and Negotiation, 2003, 12 (1), str. 3–29.

Andrej Bregar je diplomiral in magistriral na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer je zaposlen kot asistent. Področja njegovega znanstveno-raziskovalnega dela so odločitveni in inteligentni sistemi, večkriterijska odločitvena analiza, pogajalska analiza, operacijske raziskave, računalniška podpora skupinskemu delu, razvoj informacijskih sistemov ter tehnologije XML. Objavil je več člankov na konferencah in v revijah doma in v tujini. Leta 2003 je prejel nagradi za najboljša prispevka na mednarodnih znanstvenih konferencah AMCIS in WMSCI.

Dr. Matjaž B. Jurič je izredni profesor na Inštitutu za informatiko Fakultete za elektrotehniko, računalništvo in informatiko v Mariboru. Ukvarja se s storitvenimi arhitekturami, kompozicijo poslovnih procesov, integracijo, elektronskim poslovanjem, spletnimi storitvami in optimizacijo zmogljivosti. Je avtor oz. soavtor knjig Business Process Execution Language for Web Services (Packt Publishing), .NET Serialization Handbook, J2EE Design Patterns Applied, Professional J2EE EAI in Professional EJB (Wrox Press), poglavja v knjigi More Java Gems (Cambridge University Press) in Technology Supporting Business Solutions (Nova Science Publishers), objavljal je v revijah SOA-Web Services Journal, eAI Journal, Java Report, Java Developers Journal in na konferencah kot so OOPSLA, Oracle Open World, Java Development, BEA Forum, Wrox Conferences itd. Sodeloval je pri številnih projektih doma in v tujini, med drugim tudi pri razvoju RMI-IIOP, sestavnega dela platforme Java 2 in je član BPEL Advisory Boarda.

Podporni informacijski sistem za simulacijo kinematike lokomotornih sistemov

Dušan Heric, Božidar Potočnik
Fakulteta za elektrotehniko, računalništvo in informatiko
Univerza v Mariboru, Smetanova ulica 17, 2000 Maribor, Slovenija
dusan.heric@uni-mb.si

Povzetek

V članku je predstavljen podporni informacijski sistem za simulacijo kinematike lokomotornih sistemov. Namenjen je za analizo, načrtovanje in tudi za izvajanje virtualnih operativnih posegov na sklepih. Kirurgu lahko predstavlja veliko pomoč, saj mu pomaga pri sprejemanju odločitev o izvedbi operativnega posega. Predstavljeni podporni informacijski sistem je bil apliciran na kolenskem sklepu, kjer smo ocenili natančnost razpoznanih struktur. Ocenitev je bila izvedena na osnovi primerjave računalniških odčitkov z ročnimi odčitki eksperta.

Sistem sestoji iz petih programskih komponent, in sicer: a) kreatorja 3D mreže, b) skrbnika materialov, c) sistema za reševanje numeričnih enačb, č) komponente za modeliranje in d) komponente za prikazovanje rezultatov simulacije. Vhod v sistem je MR-slika, izhod pa simulacija giba sklepa. Predstavljeni sistem dovoljuje tudi ročno modeliranje, ki vključuje spremembo veličine sil, materialov in kontakte kit na objektih. S tovrstnimi spremembami neposredno vplivamo na rezultat simulacije.

Ključne besede: obdelava slik, obdelava medicinskih podatkov, vizualizacija medicinskih podatkov

Abstract

Support Information System for Locomotor Systems Kinematics Simulation

This paper presents an information system for locomotor systems kinematics simulation. It is specifically designed for analysis, planning and for virtual surgery operative interventions on joints. The proposed information system helps the surgeon decide upon surgical operation realization. It has been applied to the knee joint, where the accuracy of detected structures has been assessed. The assessment has been performed by comparing computer detected objects with experts' manual annotations.

The proposed system is made up from five components: a) 3D mesh creator, b) material manager, c) numerical solution system, d) modeller, and e) presenter of simulation result. The input into this system is MR-image, while the output is the simulation of joint motion. The proposed system supports manual modelling, including changing of force values, materials and tendon/hamstring contact points on objects. Those modifications have a direct influence to the simulation result.

Keywords: picture processing, medical data processing, visualisation of medical data

1 Uvod

Pomanjkanje časa je danes glavni krivec za prekoračitev zastavljenih rokov, za površno opravljeno delo ali storitev. Vendar pa se minimalni tolerančni prag pri oceni kakovosti opravljenih storitev med področji razlikuje. Tako je recimo v oglaševalni industriji več prostora za napake, kakor pa v medicini. Napake v medicini lahko namreč dolgoročno obremenjujejo tako posameznika kakor družbo.

Znano je, da so v medicini pereč problem čakalne vrste. Te so posledica pomanjkanja kadra, zastarelih postopkov analize in obdelave medicinskih podatkov. Bolnišnice so danes že dokaj dobro opremljene z napravami za zajemanje medicinskih slik (npr. računalniška tomografija (CT), X-žarki, magnetnoresonančne naprave (MR), ultrazvočne naprave itd.), ki olajšajo zdravniku analizo, planiranje in zdravljenje pacientov. S tem napravami se skrajša tudi čas diagnosticiranja [11, 12]. Dopolnilo tem napravam so sistemi, ki omogočajo navigacijo, manipulacijo podatkov, izračun raznih metrik nad mrežo objektov in navsezadnje tudi simulacijo [12]. Vendar je tovrstnih sistemov malo. Tako se zdravniki soočajo z novim problemom, da morajo ob poplavi medicinskih slik hitro, kakovostno in natančno diagnosticirati poškodbe in bolezni pri pacientih.

Sodobno medicinsko diagnosticiranje vključuje zajemanje, analizo in obdelavo velike količine podatkov

pacienta [12]. Večino slikovnih podatkov dobimo z neinvazivnimi postopki, kot so npr. ultrazvočna, magnetnoresonančna preiskava in računalniška tomografija. Nad dobljenimi slikovnimi podatki je mogoče zgraditi modele posameznih organov in nad njimi izvajati simulacije ter preučevati različne scenarije. Omogočeno je tudi kronološko spremljanje sprememb pacienta. Takšen pristop prinaša dodatno težo pri planiranju operativnih posegov, ker simulacija informira kirurga z dodatnimi informacijami, pomembnimi za potek operativnega posega. Najbolj izpopolnjeni postopki pa omogočajo tudi testiranje specifičnih detajlov operativnega posega (npr. operativni poseg v navideznem prostoru).

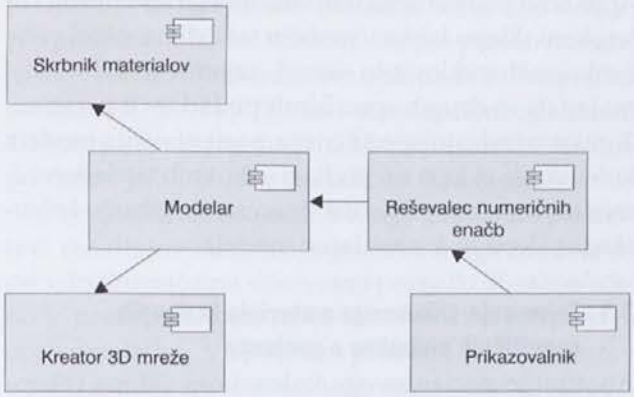
V tem prispevku bomo predstavili podporni informacijski sistem za simulacijo kinematike lokomotornih sistemov. Osnovni cilj sistema je predvsem izboljšanje klinične prakse s pomočjo rezultatov simulacije sklepa. Opisani podporni sistem prinaša naslednje klinične izboljšave: a) neinvazivno napovedovanje in diagnosticiranje, b) planiranje ter c) pooperativna verifikacija in evalvacija uspešnosti zdravljenja. Sistem se lahko uporablja za statično (npr. zlomi in zvini) in dinamično analizo lokomotornih sistemov (npr. hoja).

V okviru našega dela smo sistem aplicirali na kolenski sklep, saj je ta največji in najbolj obremenjen v človeškem telesu. Obremenitve v kolenu so pri vsakdanji hoji na stiku stegnenice in golenice 4–7-krat, pri skokih pa celo več kot 24-krat večje od teže telesa [1]. Tudi zdravljenje sklepa traja več let, zato je pomembno, da zdravnik dobi kakovostne, natančne in nazorne informacije o kinematiki pacientovega kolena po možnosti še pred izvedbo posega.

2 Zgradba podpornega informacijskega sistema

Podporni informacijski sistem je modularni in generično zgrajen. Sestavljen je iz petih glavnih komponent (slika 1), ki so povezane s porazdeljenim sistemom CORBA [2].

Vhod v naš sistem je MR-slika, posneta v načinu T2 [9]. V prvem koraku se iz nje rekonstruira geometrijsko telo, ki je opisano s končnimi elementi [3]. Postopek rekonstrukcije je popolnoma samodejen in temelji na poravnavi referenčne slike s ciljno sliko. Referenčno sliko izberemo med zdravimi predstavniki ciljnega lokomotornega sistema. Slabost uporabljenega postopka je ročna tvorba 3D mreže lokomotornega sistema za referenčno sliko. Temu opravilu se lahko izognemo tako, da sliko segmentiramo po rezinah. Z izpopolnjenimi postopki za razpoznavo robov [10] izračunamo sliko robov na vsaki rezini. Nato te slike robov povežemo v 3D mrežo in dobimo površine objektov. Tovrstni pristop je časovno hitrejši, ne zahteva referenčne slike in je domensko naravnan. Zahteva pa, da mu dodamo enoličen opis objektov, ki jih želimo razpoznavati na sliki. Osnoven namen kreatorja 3D mreže je segmentacija kosti, hrustanca ter ostalih objektov, ki so vključeni v opazovani lokomotorni sistem.



Slika 1: **Komponentni diagram podpornega informacijskega sistema za simulacijo kinematike lokomotornega sistema. Komunikacija med komponentami poteka prek porazdeljenega sistema CORBA.**

Po prvem koraku imamo le prostorske in površinske informacije o opazovanih objektih na MR-sliki. To omogoča ocenitev razsežnosti objektov in površinske deformacije. Neznane pa ostajajo materialne lastnosti. Zato sistem vključuje dve komponenti, in sicer skrbnika materialov in komponento za modeliranje lokomotornega sistema. Skrbnik materialov je namenjen za spreminjanje parametrov lastnosti materialov in vključuje tudi bazo materialov. Na drugi strani pa komponenta za modeliranje omogoča povezovanje objektov lokomotornega sistema z materiali, spreminjanje veličine sil, dodajanje, odstranjevanje in prestavljanje prilepkov kit na kosti. Tovrstne spremembe neposredno vplivajo na potek simulacije in omogočajo simuliranje kirurškega posega. Korak modeliranja je lahko samodejen, če obstaja model referenčne 3D mreže.

Kvaliteta simulacije giba je odvisna od uspešnosti in natančnosti modeliranja. Simulacijo izvaja sistem za reševanje numeričnih enačb. Tovrstna simulacija je

priporočljiva v okoliščinah, ko želimo simulirati kirurški poseg. V takšnem primeru nimamo na razpolago psevdodinamičnih MR posnetkov [8] in rezultat simulacije je edina vizualna informacija, na podlagi katere lahko sprejme odločitve o poteku kirurškega posega. Tako lahko kirurg zagotovi optimalno kinematiko lokomotornega sistema v danih okoliščinah. Rezultat simulacije prikažemo s komponento za vizualizacijo podatkov, ki podpira navigacijo in manipulacijo objektov.

3 Podporni informacijski sistem in kolenski sklep

Aplikacijo podpornega informacijskega sistema na kolenskem sklepu lahko v grobem razdelimo v štiri večje funkcionalne sklope, in sicer: 1. zajemanje slikovnega materiala in drugih specifičnih podatkov o pacientu, 2. rekonstrukcijo specifičnega pacientovega modela kolenskega sklepa na podlagi slikovnih podatkov, 3. modeliranje in predpisovanje scenarija gibanja kolenskega sklepa in 4. simulacijo modela.

3.1 Zajemanje slikovnega materiala in drugih specifičnih podatkov o pacientu

Anatomijo pacientovega kolenskega sklepa rekonstruiramo iz MR posnetkov. Slikovne posnetke zajemamo dvakrat, in sicer s statičnim in psevdodinamičnim MR protokolom. V prvem primeru dobimo visokokakovostne posnetke dimenzije 512 x 512 točk (sagitalni prerezi kolenskega sklepa), na podlagi katerih rekonstruiramo anatomijo pacientovega kolena.

S psevdodinamičnim zajemanjem slik pa posnamemo rahlo obremenjeno in hkrati skrčeno koleno. S tem merjenjem dejansko zbiramo informacije o obnašanju kolena pri različnih aktivnostih pacienta (npr. hoja). Te slike zajemamo v nižji ločljivosti 256 x 256 točk in v šestih različnih položajih, od 0 do 40 stopinj. Med psevdodinamičnim snemanjem pacient rahlo pritiska (sila do 300 N) na pedal posebej izdelane naprave za merjenje sile v magnetnoresonančnem polju. Izmerjene podatke o sili uporabimo v koraku modeliranja.

3.2 Rekonstrukcija specifičnega pacientovega modela kolenskega sklepa

V nadaljevanju rekonstruiramo 3D model pacientovega kolenskega sklepa iz slikovnih podatkov. V trenutni izvedbi opazujemo le tri glavne kolenske kosti, in sicer stegnenico, golenico in pogačico ter njihove pripadajoče hrustance. Za boljšo stabilnost sistema pa smo v model dodali še lateralni in medialni meniskus.

Kolenski sklep lahko rekonstruiramo a) klasično, kjer segmentacijske rezultate na posameznih rezinah povežemo v 3D mrežo [7] ali pa b) s postopkom registracije [6]. Pri slednjem postopku konstruiramo 3D šablono (mrežo) kolenskega sklepa iz slikovnih podatkov referenčnega in tipičnega kolena. Referenčne podatke in podatke pacienta nato poravnamo. Ta poravnava vrne preslikavo, s katero zatem preslikamo šablono kolena v specifično 3D mrežo pacientovega kolena. Slika 2 prikazuje opisani postopek rekonstrukcije kolenskega sklepa.

Slika 2: **Shematski diagram konstrukcije specifične pacientove 3D mreže kolenskega sklepa iz MR slikovnih podatkov**

3.3 Modeliranje in predpisovanje scenarija gibanja kolenskega sklepa

Z naslednjim funkcionalnim sklopom nato izdelano 3D mrežo pacientovega kolena avtomatsko preoblikujemo v 3D model kolena. Dejansko gre za model, sestavljen iz končnih elementov, in sicer iz 3464 heksaedernih elementov z osmimi vozlišči. Modeliranje izvajamo v komercialnem programskem okolju PAM [5]. Okolje PAM sestoji iz treh modulov, in sicer a) modula Generis, ki je namenjen modeliranju, b) modula Safe, s katerim simuliramo modele, ter c) modula View, ki ga uporabljamo za vizualizacijo in analiziranje simulacijskih rezultatov.

V okolju Generis nato dodamo k osnovni, rekonstruirani anatomiji pacientovega kolenskega sklepa še

dodatne kolenske strukture, kot so sprednje in zadnje križne vezi, mišična vlakna ter kite.

Na koncu tem gradnikom priredimo le še ustrezne materiale in strukturne lastnosti. Čeprav se te lastnosti spreminjajo v odvisnosti od temperature in starosti posameznega pacienta, smo modeliranje poenostavili do te mere, da smo vsakemu pacientu priredili iste lastnosti materialov.

3.4 Simuliranje modela

V zadnjem koraku pa vzpostavljeni model, sestavljen iz končnih elementov, simuliramo s programskim orodjem PAM Safe. V splošnem lahko simuliramo poljubno mnogo različnih scenarijev, tj. funkcionalnih aktivnosti pacienta (npr. hoja, skakanje po eni nogi). V našem delu smo s postavljenim modelom modelirali in simulirali zgolj krčenje kolena. Postavljeni scenarij je predvideval, da koleno iz popolnoma stegnjenega položaja skrčimo do približno 60 stopinj.

Zakaj je simuliranje in modeliranje kolenskega sklepa sploh potrebno, če pa lahko te informacije izluščimo že iz psevdodinamičnih slik? Odgovor je na dlani. Komponentna zasnova nam namreč ob osnovnem modelu gibanja omogoča še preizkušanje in analiziranje kinematike kolena tudi glede na druge scenarije. Tako lahko na primer opazujemo kinematiko kolenskega sklepa v primeru poškodb križnih vezi ali celo meniskusa (v fazi modeliranja ju preprosto odstranimo iz modela). Vsekakor največja prednost pa je, da lahko opravimo virtualno analizo kolenskega sklepa v primeru vsaditve implantanta meniskusa različnih velikosti (meniskus v modelu zamenjamo z ustreznim modelom implantanta). S takšnimi simulacijami ima zdravnik še pred kirurškim posegom na voljo informacije za detajlno planiranje operativnega posega ter izbiro ustreznega implantanta meniskusa. Pri mnogih kirurških posegih se morebitne komplikacije pokažejo šele čez leto ali več. S predlaganim modeliranjem in podpornim sistemom pa lahko deloma že vnaprej predvidimo morebitne zaplete ter ustrezno korigiramo operativni poseg.

4 EVALVIRANJE PODPORNEGA SISTEMA

Predstavljeni podporni sistem, apliciran na kolenskem sklepu, smo vizualno evalvirali na dveh pacientih. Oba pacienta sta imela pretrgane sprednje kolenske križne vezi. Ocenjevanje smo izvedli z dvema ločenima pristopoma. V prvem pristopu smo kvantitativno izmerili in kvalitativno ocenili natančnost razpoznanih kolenskih struktur. Poseben poudarek smo dali kirurško najbolj zanimivim območjem v kolenu. Z drugim pristopom pa smo ocenjevali pravilnost simulacije oz. predikcijo kolenske kinematike.

Pri kvantitativnem ocenjevanju anatomskih struktur kolena smo primerjali kolenske strukture v vsaki slikovni rezini. Dejansko smo primerjali rezultate našega sistema z označbami eksperta, ki smo jih obravnavali kot zlato pravilo. Ocenjevali smo tri glavne kolenske kosti ter njihove pripadajoče hrustance. Natančnost razpoznanih struktur smo ovrednotili z naslednjimi merami, in sicer razmerji R1 in R2 [4], Hausdorffovo razdaljo [4] in povprečno absolutno razdaljo (MAD) [4]. Povprečno razmerje R1 je bilo 0.92 in povprečni standardni odklon 0.06; povprečno razmerje R2 je bilo 0.91 in standardni odklon 0.05. Povprečna razdalja HD je bila 2.78 mm s standardnim odklonom 1.89 mm. Povprečna razdalja MAD pa je bila 0.52 mm, pri čemer je bil standardni odklon 0.12 mm.

Psevdodinamično ocenjevanje temelji na primerjavi rezultatov simulacije postavljenega modela in psevdodinamičnimi slikovnimi posnetki. Končno oceno je postavil ekspert na osnovi vizualne primerjave obeh rezultatov. V opisanem primeru dveh pacientov s pretrganimi sprednjimi križnimi vezmi je ekspert podal končno oceno, da je pri obeh pacientih v simulaciji vidna prevelika in nenaravna translacija stegnenice napram golenici, vzrok pa je lahko pretrgana ali oslabljena sprednja križna vez. Takšno mnenje potrjuje primernost in uporabnost podpornega sistema za simulacijo lokomotornih sistemov.

5 SKLEP

Preliminarni simulacijski rezultati so obetavni. Poglejmo najprej pacientove 3D mreže kolenskega sklepa rekonstruirane iz visokokvalitetnih statičnih MR slik. Te mreže so začetni položaj kolena v simulaciji. Rezultati so pokazali, da opisano generično okolje uspešno in s primerno natančnostjo rekonstruira anatomske strukture v kolenu. To še posebej velja v klinično pomembnih delih kolenskega sklepa. Rahla nedoslednost se pokaže pri rekonstrukciji hrustanca. Ta problem se pojavi zato, ker je ta kolenska struktura izredno tanka. Študirajmo še simulirane kinematike kolenskega sklepa. Vizualni pregled rezultatov je pokazal fiziološko pravilnost kinematike kolenskega sklepa. To je potrdila tudi primerjava z rezultati iz literature. Razmerja med kolenskimi sklepnimi strukturami so očitna in brez večjih anatomskih deformacij. Še posebej nas je zanimal meniskus, katerega položaj in oblika sta bila prav tako brez

očitnih fizioloških površinskih deformacij. Majhno nenatančnost smo zasledili le pri pogačici, kjer smo opazili rahlo polzenje pogačice v ekstremnem položaju pokrčenja kolena (fleksija kolena okrog 90 stopinj).

Predstavljeno generično okolje omogoča individualno modeliranje specifične pacientove anatomije kolenskega sklepa iz MR slik. Modele razrešujemo z numeričnim simuliranjem na podlagi metode končnih elementov. Rezultat je simulirana kinematika kolenskega sklepa na podlagi izbranega scenarija. Bistvene izboljšave so vsekakor boljša vizualizacija kinematike kolena v klinično nejasnih primerih, s tem pa je povezano tudi boljše preoperativno planiranje in odločanje.

VIRI IN LITERATURA

[1] Beillas, P., Papaioannou, G., Tashman, S., Yang, K. H.: A new method to investigate in vivo knee behavior using a finite element model of the lower limb, Journal of Biomechanics, 2004, št. 37 str. 1019–1030.

[2] Ahmed, M. S.: Corba programming unleashed, SAMS, corp., Indianapolis, 1999.

[3] Machnel, R.: Finite elements: their design and performance, MARCEL DEKKER, INC., New York, 1994.

[4] Heric, D., Potočnik, B.: Image Processing Verification Tool-IPVT, Zbornik referatov NORSIG 2004, 2004, str. 13–16.

[5] ESI Group: PAM-SAFE FEATURES & SPECIFICATIONS, http://www.esi-group.com/Products/Safety/features_html, 2006.

[6] Brown, L. G.: A survey of image registration techniques, ACM Computing Surveys, 1992, str. 325–376.

[7] Heric, D., Zazula, D., Scale Adaptive Edge Detection using Maximum Entropy, Zbornik referetov IWSSIP05, 2005, str. 463–466.

[8] Potočnik, B., Zazula, D., Cigale, B., Heric, D., Đonlagiæ, D., Cibula, E., Tomažič, T.: A patient-specific knee joint computer model using "in vivo" compressive load data from the optical force measuring system, 2006, poslano v recenzijo Medical Engineering and Physics.

[9] Yan, H.: Signal Processing for Magnetic Resonance Imaging and Spectroscopy, Marcel Dekker, Inc. New York, 2002.

[10] Russ, J. C.: The Image Processing Handbook, 2nd ed. CRC Press, Boca Raton, 2000.

[11] Bankman, I. N.: Handbook of Medical Imaging: Processing and Analysis, Academic Press, 2000.

[12] Yoo, T. S: Insight into Images, A K Peters, Ltd. Massachusetts, 2004.

Dušan Heric je leta 2002 diplomiral na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru in se zaposlil na evropskem projektu SimBio. Po končanem projektu se je zaposlil v laboratoriju za sistemsko programsko opremo kot mladi raziskovalec. Njegovo raziskovalno področje vključuje računalniško obdelavo slik in signalov. Svoje raziskovalne dosežke objavlja v strokovnih in znanstvenih publikacijah.

Božidar Potočnik je v letih 1995 in 1998 diplomiral ter magistriral na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, kjer je leta 2000 uspešno obranil doktorsko disertacijo z naslovom Razpoznavanje objektov iz zaporedja slik s postopki predikcije. Za svoje raziskovalne dosežke je prejel več priznanj. Leta 2002 je bil tudi lokalni koordinator evropskega projekta SimBio. Od leta 2002 je docent na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, kjer predava šest predmetov. Njegovo raziskovalno področje vključuje segmentacijske postopke pri napredni računalniški obdelavi slik, razpoznavanje vzorcev in biomedicino. Je član združenja IEEE in Slovenskega združenja za razpoznavanje vzorcev.

Dinamični prikaz časovnih omrežij

Darko Brvar[1], Andrej Mrvar[2] in Vladimir Batagelj[3]
Univerza v Ljubljani
Univerzitetni podiplomski študijski program statistika[1]
Fakulteta za družbene vede[2], Fakulteta za matematiko in fiziko[3]
darko.brvar@siol.net, andrej.mrvar@fdv.uni-lj.si, vladimir.batagelj@fmf.uni-lj.si

Povzetek

Časovna omrežja lahko prikažemo statično ali dinamično. Pri statičnem prikazu omrežje prikažemo s sliko ali zaporedjem slik, pri dinamičnem pa gre za zvezno prehajanje med časovnimi rezinami omrežja, kjer sledi prejšnjih slik omrežja postopno izginjajo. Statične prikaze časovnih omrežij lahko izdelamo s programskim paketom Pajek. V članku bomo predstavili program PajekToSvgAnim, ki temelji na slikovnem jeziku SVG in programskem jeziku Python in ki je programski dodatek programskemu paketu Pajek za dinamični prikaz časovnih omrežij. Prikazali bomo delovanje programa PajekToSvgAnim na nekaterih znanih primerih časovnih omrežij.

Abstract

DYNAMIC VISUALIZATION OF TEMPORAL NETWORKS

Temporal networks can be visualized statically or dynamically. While static visualization presents networks with pictures, dynamic visualization shows continuous passes of networks between time points with traces of previous network pictures. Static visualization can be produced using program package Pajek. We will present program PajekToSvgAnim, based on graphical language SVG and programming language Python, as addition to program package Pajek for dynamic visualization of temporal networks. Program PajekToSvgAnim will be demonstrated on some well-known examples of temporal networks.

1 Časovna omrežja

1.1 Definicija grafa in omrežja

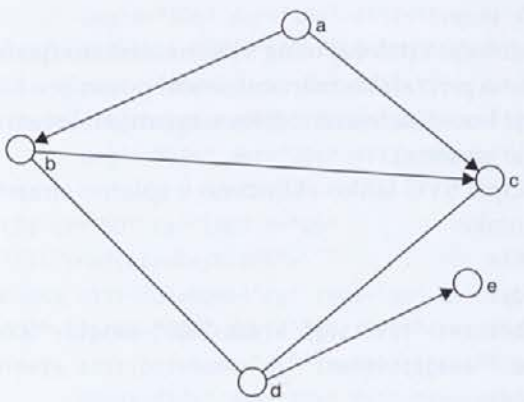
Graf G je definiran kot par $G = (V, L)$, kjer je V množica točk in L množica povezav. Povezave so lahko usmerjene ali neusmerjene. Predpostavljamo, da je bralec seznanjen z osnovami teorije grafov (na primer [12]).

Graf postane omrežje, če vsebuje dodatne podatke o točkah in/ali povezavah. Omrežje N lahko torej definiramo kot četverico množic $N=(V, L, F_V, F_L)$, kjer je V množica točk, L množica povezav, F_V množica lastnosti točk in F_L množica lastnosti povezav.

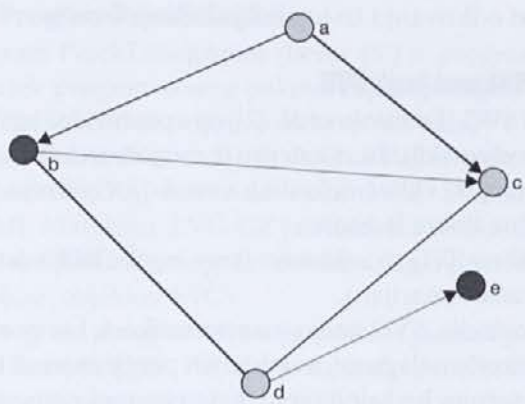
Množica lastnosti točk F_V je množica funkcij $f: V \rightarrow X$, kjer množica X lahko predstavlja množico oznak točk, razbitje točk ali množico številskih lastnosti točk. Na sliki lahko številsko lastnost prikažemo kot velikost točke ali njeno koordinato, imensko lastnost pa kot barvo, obliko lika ali kot oznako točke.

Množica lastnosti točk F_L pa je množica funkcij $g: L \rightarrow Y$, kjer je Y množica številskih lastnosti povezav. Na sliki jih prikažemo z izpisom vrednosti, debelino črte ali sivino.

Primer: Na sliki 1.1a je prikazan graf z množico točk {a, b, c, d, e}, množico usmerjenih povezav {(a, b), (a, c), (b, c), (d, e)} in množico neusmerjenih povezav {(b: d),(c: d)}. Na sliki 1.1b pa je prikazan isti graf z imensko lastnostjo točk (razbitjem), predstavljeno z dvema barvama ter s številsko lastnostjo povezav,



Slika 1.1a: **Primer grafa**



Slika 1.1b: **Graf z dodatnimi lastnostmi**

predstavljeno z različnimi debelinami (barve niso razvidne zaradi črnobelega tiska, zato se članek nahaja tudi na spletni strani [2]).

1.2 Definicija časovnega omrežja

Časovno omrežje je omrežje, v katerem se prisotnost posameznih točk in povezav pa tudi njihove lastnosti spreminjajo skozi čas. Zato ga lahko definiramo na naslednji način:

Časovno omrežje N_T definiramo kot peterico množic $N_T=(V, L, F_V, F_L, T)$, kjer je V množica točk, L množica povezav, F_V množica lastnosti točk, F_L množica lastnosti povezav in T množica linearno urejenih časovnih trenutkov.

Točke in povezave, ki pripadajo časovnemu omrežju, niso nujno prisotne v vseh časovnih trenutkih. Pri tem velja logična omejitev, da je povezava prisotna v določenem časovnem trenutku, če sta v tem trenutku prisotni tudi obe njeni krajišči.

1.3 Časovna socialna omrežja

Pri analizi časovnih socialnih omrežij se zanimanje vrti okrog razumevanja, kako se omrežje razvija in spreminja skozi čas, in okrog iskanja načinov za razvoj modelov socialnih procesov, ki bi pomagali pojasniti opažene strukture (Doreian et al. [6]). Jedro zanimanja je torej dinamika medosebnih odnosov, ki je pomembna za razumevanje socialnega omrežja. Pri tem se pojavi problem, da se te dinamike ne da na zadovoljiv način prikazati s statičnim prikazom (Bearman, Everett [4]). Rešitev je dinamični prikaz časovnih omrežij, ki raziskovalcem odpira vrata na naslednjih področjih:

- pri odkrivanju značilnosti razvoja omrežja,
- pri spremljanju razvoja izbranih delov omrežja (tirov),
- pri odkrivanju izstopajočih delov omrežja.

2 Slikovni jezik SVG

Jezik SVG (Ferraiolo et al. [7]) je označevalni jezik za opis vektorskih slik, s katerim je mogoče izdelati spletne strani, ki vključujejo slike z visoko ločljivostjo. Ima številne dobre lastnosti:

- slike v SVG so vektorske (brez izgube ločljivosti pri transformacijah),
- datoteke .SVG imajo manjšo velikost, kar pomeni hitrejše nalaganje, in lahko jih pregledujemo kar s spletnim brskalnikom, v katerega prej namestimo prosto dostopen dodatek za pregledovanje,
- v spletnem brskalniku deluje tudi iskanje nizov/besedil v sliki SVG,
- osnova jezika SVG je označevalni sestav XML, ki ima danes že vodilno vlogo pri izmenjavi najrazličnejših podatkov na spletu in tudi drugje.

2.1 Zgradba opisa SVG

Opis SVG lahko definiramo kot samostojno datoteko ali kot vgrajeno datoteko v spletni strani. Spodnji primer predstavlja samostojno datoteko .SVG:

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.0//EN"
          "http://www.w3.org/Graphics/SVG/1.1/DTD/
svg11.dtd">
<svg xmlns="http://www.w3.org/2000/svg"
     width="300" height="300" x="0" y="0">
  ....
  ....
  ....
</svg>.
```

Prva vrstica vsebuje najavo XML glede na to, da je jezik XML osnova jezika SVG. Druga in tretja vrstica vsebujeta povezavo z opisom 'slovnice' jezika SVG (angl. Document Type Definition ali krajše DTD), ki mora biti tako kot najava XML sestavni del vsake datoteke .SVG.

Četrta in peta vrstica vsebujeta značko SVG, ki označuje, da gre za opis SVG. Značka SVG ima naslednje lastnosti:

- `xlmns`:
  obvezna lastnost, ki določa imenski prostor jezika SVG,
- `height` in `width`:
  določata velikost okna SVG na zaslonu,
- `x` in `y`:
  določata položaj okna SVG na zaslonu (jezik SVG ima privzeti koordinatni sistem postavljen tako, da je koordinatno izhodišče v zgornjem levem vogalu zaslona).

Opis SVG lahko vključimo v spletno stran tudi z datoteke:

```
<html>
<body>
<embed src="test.svg" width="500" height="500"
type ="image/svg+xml" />
</body>
</html>.
```

To naredimo z uporabo značke EMBED, ki ji določimo naslednje lastnosti:

- `src:`
  spletni naslov datoteke .SVG (če se nahaja v drugi mapi kot datoteka .HTML, je potrebno navesti celotno pot),
- `height in width:`
  velikost vgrajenega okna SVG na spletni strani,
- `type:`
  zvrst datoteke oblike MIME (programski standard, ki definira enostaven mehanizem za opisovanje vsebinskih tipov datotek, ki se pošiljajo prek spleta) – za datoteke SVG so predvidene vrednosti image/svg, image/svg-xml in image/svg+xml.

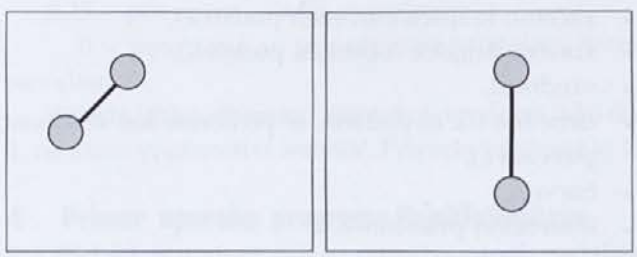
2.2 Dinamični prikaz objektov v jeziku SVG

Jezik SVG ima za dinamični prikaz objektov na voljo več značk. Spoznali bomo osnovno značko animate, ki se uporablja za dinamični prikaz sprememb vrednosti lastnosti objektov SVG skozi čas. Oglejmo si primer grafa na dveh točkah, povezanih z neusmerjeno povezavo, ki se po določenem času počasi premakne na drug položaj (slika 2.1):

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.0//EN"
       "http://www.w3.org/TR/2001/PR-SVG-20010719/
DTD/svg10.dtd">
<svg width="250" height="200"
   xmlns="http://www.w3.org/2000/svg" ver-
sion="1.1">
   <rect x="2" y="2" width="246" height="196"
     fill="none" stroke="blue" stroke-width="2" />
   <line x1="50" y1="100" x2="100" y2="50"
        stroke-width="7" stroke="black">
   <animate attributeName="x1" from="50" to="150"
            begin="10s" dur="10s" fill="freeze"/>
   <animate attributeName="y1" from="100" to="150"
            begin="10s" dur="10s" fill="freeze"/>
   <animate attributeName="x2" from="100" to="150"
            begin="10s" dur="10s" fill="freeze"/>
  </line>
  <circle cx="50" cy="100" r="15"
style="fill:red;stroke:black">
   <animate attributeName="cx" from="50" to="150"
            begin="10s" dur="10s" fill="freeze"/>
   <animate attributeName="cy" from="100" to="150"
            begin="10s" dur="10s" fill="freeze"/>
  </circle>
  <circle cx="100" cy="50" r="15"
style="fill:red;stroke:black">
   <animate attributeName="cx" from="100" to="150"
            begin="10s" dur="10s" fill="freeze"/>
  </circle>
</svg>.
```

Iz primera lahko vidimo, da ima značka animate naslednje lastnosti:

- `attributeName:`
  ime lastnosti nadrejenega objekta, ki se ji spremeni vrednost;
- `from in to:`
  stara in nova vrednost te lastnosti;
- `begin:`
  začetek dinamičnega prikaza spremembe vrednosti lastnosti;
- `dur:`
  trajanje animacije;
- `fill:`
  izbira, ki vpliva na to, ali nadrejeni objekt po koncu dinamičnega prikaza ohrani novo vrednost lastnosti (freeze) ali jo zamenja s staro vrednostjo (remove).



Slika 2.1: **Dve točki in povezava med njima na začetku in na koncu dinamičnega prikaza**

3 Program PajekToSvgAnim

Program PajekToSvgAnim (Brvar [5]) je programski dodatek programskemu paketu Pajek (Batagelj, Mrvar [3], [8], [10]) za pripravo dinamičnih opisov v SVG razvoja časovnih omrežij. Iz vhodne Pajkove projektne datoteke .PAJ izdela datoteke .SVG, .SVG.GZ in .HTML (datoteka .SVG.GZ je stisnjena oblika GZIP datoteke .SVG, ki omogoča hitrejše nalaganje in hitrejši prikaz objektov SVG).

Program je napisan v programskem jeziku Python (Van Rossum [11]). Python je tolmačeni interaktivni objektni programski jezik in tako kot programski jezik Java omogoča izdelavo modulov, razredov, izjem

in dinamičnih podatkovnih tipov. Omogoča tudi izdelavo samostojno izvedljivih prevedenih programov.

Na začetku vhodne Pajkove datoteke se nahajajo podatki o celotnem omrežju, torej o vseh točkah in povezavah skupaj z njihovimi lastnostmi. Sledijo podatki o omrežjih v posameznih časovnih rezinah. Za ta omrežja so podani samo podatki o tistih točkah in povezavah, ki so v rezini dejansko prisotne.

Na koncu vhodne datoteke se nahaja še točkovno razbitje, pri katerem za vsako točko navedemo, ali je v prikazu njena oznaka vidna ali ne (vrednost 1: oznaka je vidna, vrednost 0: oznaka ni vidna).

Lastnosti točk in povezav v posameznih omrežjih so standardne lastnosti, ki so določene že v programskem orodju Pajek. Tako lahko točki določimo naslednje lastnosti:

- oznako,
- kooordinati x in y (in z),
- vrednost,
- obliko,
- razteg v smeri x,
- razteg v smeri y,
- barvo,
- interval(e) prisotnosti (npr. [1-3, 7, 12-15]).

Povezavi pa lahko določimo naslednje lastnosti:

- začetno krajišče (obvezen podatek),
- končno krajišče (obvezen podatek),
- vrednost,
- debelino (če ni podana, se privzame kar vrednost povezave),
- barvo,
- interval(e) prisotnosti.

Program PajekToSvgAnim upošteva naslednje posebnosti časovnih omrežij:

- zvezno spreminjanje koordinat točk,
- izginjanje točk in povezav in pojavljanje novih točk in povezav glede na to, ali je določena točka oziroma povezava prisotna v določenem časovnem trenutku,
- spreminjanje velikosti točk in debelin povezav brez izgube ločljivosti,
- prikaz večkratnih omrežij na istih točkah.

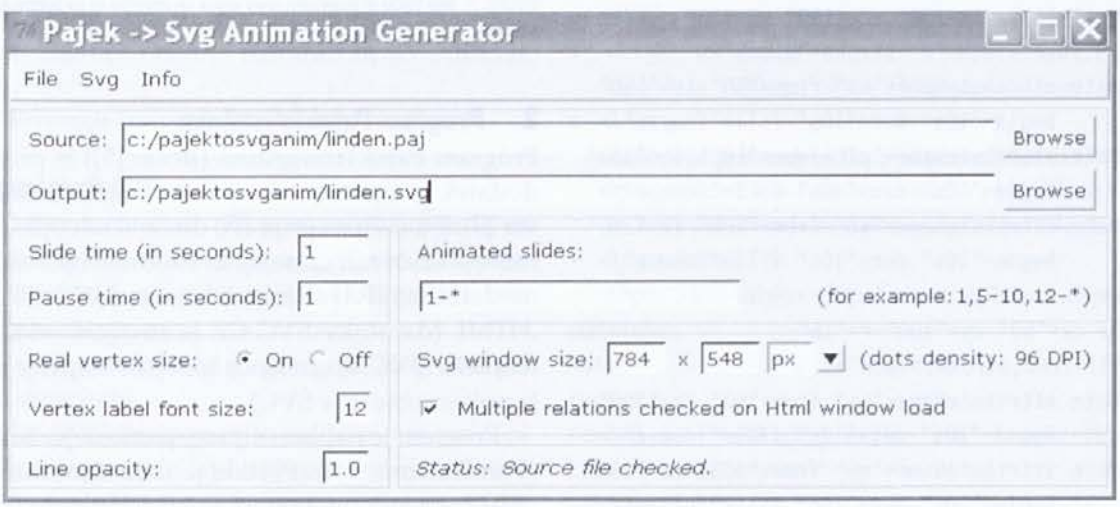
V program je vgrajenih več izbir, ki se lahko določajo v slikovnem uporabniškem vmesniku (slika 3.1). Poleg osnovnih izbir vhodne Pajkove datoteke in imena ter poti izhodne datoteke .SVG omogoča še naslednje izbire:

- dolžino trajanja dinamičnega prikaza prehoda omrežja iz ene rezine v drugo (Slide time),
- dolžino trajanja statičnega prikaza rezine pred dinamičnim prikazom prehoda v naslednjo rezino (Pause time),
- številski seznam dinamičnih prehodov med rezinami, ki naj se prikažejo (Animated slides).

Primer: Animated slides: 1, 5-10, 12-*.

V tem primeru si prikazi omrežja sledijo v naslednjem vrstnem redu:

- dinamični prikaz prehoda od prve do druge rezine,
- statični prikazi od druge do pete rezine,
- dinamični prikazi prehodov med peto do enajsto rezino (poleg vmesnih statičnih prikazov),
- statična prikaza enajste in dvanajste rezine,
- dinamični prikazi prehodov med dvanajsto in zadnjo rezino (poleg vmesnih statičnih prikazov);



Slika 3.1: **Izbira vhodne Pajkove datoteke v programu PajekToSvgAnim**

- možnost izbire med dvema velikostima oblik točk: dejansko velikostjo, ki je podana v vhodni datoteki, in enotno velikostjo (Real Vertex Size On/Off),
- velikost pisave oznak točk (Vertex label font size),
- velikost okna SVG (Svg window size),
- možnost izbire označitve relacij v spletnem sestavku z vgrajeno sliko SVG (ob vsaki naložitvi sestavka) v primeru večkratnega omrežja (Multiple relations checked on Html window load),
- neprosojnost povezav (Line opacity).

Program najbolj preprosto uporabimo tako, da kar poženemo izdelavo datotek .SVG, .SVG.GZ in .HTML z ukazom Svg → Generate. Če je izdelava datotek uspešna, se prikaže ustrezno sporočilo. Dinamični prikaz si ogledamo tako, da odpremo izdelano datoteko .HTML, ki poleg okna SVG vsebuje še izbiro prikaza oznak točk in izbiro prikaza relacij v primeru večkratnega omrežja. Datoteka .HTML je povezana s stisnjeno datoteko .SVG.GZ zaradi hitrejšega prenosa izdelanih objektov v oknu SVG.

V nadaljevanju si oglejmo nekaj primerov, v katerih lahko uporabimo eno ali več od zgoraj naštetih izbir.

1. Če si želimo bolj podrobno ogledati dinamične prikaze prehodov med rezinami, potem povečamo dolžino trajanja dinamičnega prikaza prehoda omrežja iz ene rezine v drugo. Privzeta dolžina trajanja je 1 sekunda.
2. Če nas zanimajo statični prikazi posameznih rezin, potem povečamo dolžino trajanja statičnega prikaza rezin. Privzeta dolžina trajanja je 1 sekunda.
3. Če ima omrežje veliko rezin, se večkrat osredotočimo le na nekaj dinamičnih prikazov prehodov med izbranimi rezinami in ne na vse prehode. V tem primeru si lahko pomagamo z možnostjo določitve številskega seznama dinamičnih prikazov prehodov, ki naj se prikažejo. Privzeti seznam je 1-*, kar pomeni dinamični prikaz vseh prehodov.
4. Možnost izbire med dejansko velikostjo točk, ki je podana v vhodni datoteki, in enotno velikostjo za vse točke je možnost, ki jo poznamo iz programskega paketa Pajek. Uporabimo jo, ko nas dejanske velikosti točk ne zanimajo ali pa ko so točke prevelike za prikaz.
5. Možnost izbire velikosti pisave oznak točk je klasična možnost, ki jo tudi poznamo iz programskega paketa Pajek. Privzeta velikost pisave je 12.
6. Če želimo dinamični prikaz vključiti v svojo spletno stran, si lahko pomagamo z možnostjo določitve velikosti okna SVG. Pri tem lahko izbiramo med enotami cm, inch, px. Privzeta velikost okna je velikost celotnega zaslona.
7. Če imamo opravka z večkratnim omrežjem z velikim številom relacij, se lahko zgodi, da bo dinamični prikaz nepregleden. V tem primeru si pomagamo z možnostjo izbire označitve relacij v spletnem sestavku z vgrajeno sliko SVG, s katero lahko sami določimo, katero relacijo želimo prikazati. Po privzetem se prikažejo vse relacije.
8. Če omrežje vsebuje večkratne povezave, se lahko zgodi, da določene povezave na prikazu ne bodo vidne, ker bodo prekrite z drugo povezavo, ki povezuje isti točki. V programskem paketu Pajek je to rešeno z uporabo ukaza Net → Transform → SortLines → LineValues → Descending, ki uredi povezave po vrednosti padajoče, v programu PajekToSvgAnim pa lahko določimo stopnjo neprosojnosti povezav. Pri tem si lahko pomagamo z naslednjo lestvico:

   1 – povezave so popolnoma neprosojne,
   0.75 – povezave so delno prosojne,
   0.5 – povezave so srednje prosojne,
   0.25 – povezave so zelo prosojne,
   0 – povezave so popolnoma prosojne, torej nevidne.

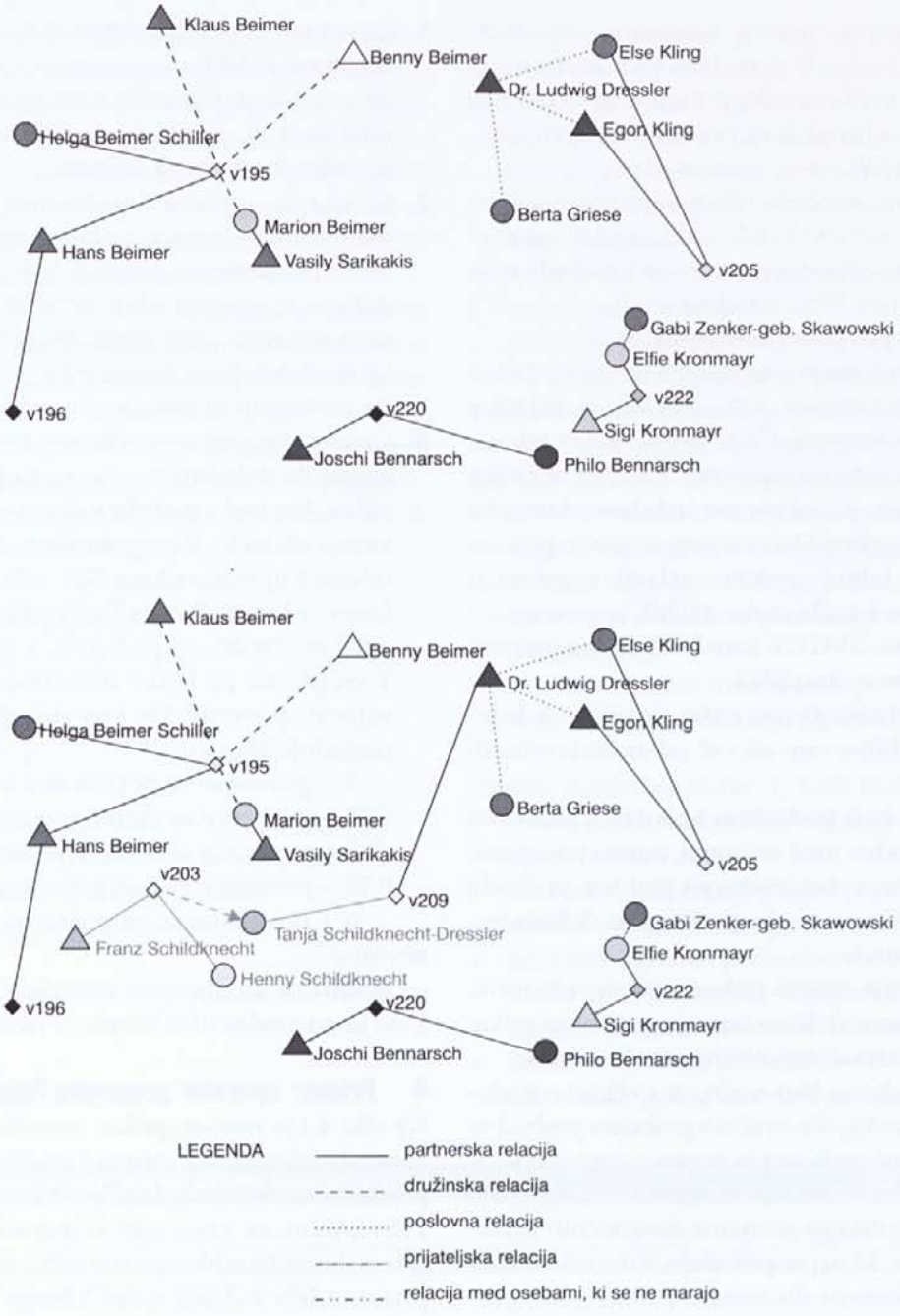
Seveda lahko izberemo katerokoli vrednost od 0 do 1, ne samo vrednosti iz lestvice. Privzeta vrednost je 1.

4 Primer uporabe programa PajekToSvgAnim

Na sliki 4.1 je narisan prikaz omrežja zgodb nadaljevanke Lindenstrasse (Mutzel [9], Batagelj [1]) z nepremičnimi točkami, izdelan s programom PajekToSvgAnim, za prvo rezino (prva zgodba) in malo zatem, ko se že rahlo opazijo točke in povezave, ki so prisotne šele v drugi rezini (druga zgodba). Delno prosojne na novo prihajajoče točke in povezave (npr. točka z oznako v209 in povezava od te točke do točke z oznako Dr. Ludwig Dressler) postajajo tem bolj vidne, čim bolj se bliža druga rezina. Več takih spletnih prikazov (v barvah) je dosegljivih na spletni strani (Batagelj [2]).

5 Sklep

Zaradi povečanega zanimanja za raziskovanje časovnih omrežij in zaradi dejstva, da prikaz omogoča boljši



Slika 4.1: **Prikaz prve rezine omrežja Lindenstrasse z nepremičnimi točkami, izdelan s programom PajekToSvgAnim, in med prehodom**

vpogled v značilnosti omrežij tako pri začetnem raziskovanju omrežij kot tudi pri predstavitvi rezultatov raziskav, se je v zadnjem času pojavila potreba po dinamičnem prikazu omrežij.

V ta namen je bil izdelan PajekToSvgAnim kot programski dodatek programskemu paketu Pajek za dinamični prikaz časovnih omrežij.

S pomočjo programa PajekToSvgAnim lahko izdelamo zvezne prehode časovnih omrežij med časovnimi rezinami. Pri posameznem prehodu omrežja iz ene rezine v drugo se vidijo sledi prejšnjih slik omrežja, torej sledi tistih točk in povezav omrežja, ki v naslednji rezini niso več prisotne. To nam omogoča, da lahko bolj natančno sledimo spremembam omrežja skozi

čas kot doslej, ko smo imeli na voljo le statične slike omrežja.

Program PajekToSvgAnim ima za različne potrebe uporabnikov vgrajenih kar nekaj izbir, ki se lahko določajo v slikovnem uporabniškem vmesniku. Če si želimo npr. bolj podrobno ogledati dinamične prikaze prehodov med rezinami, povečamo dolžino trajanja dinamičnega prikaza prehoda omrežja iz enega rezine v drugo. Če želimo dinamični prikaz vključiti v svojo spletno stran, si lahko pomagamo z možnostjo določitve velikosti okna SVG. Če pa imamo opravka z večkratnim omrežjem z velikim številom relacij, uporabimo možnost izbire označitve relacij v spletnem sestavku z vgrajeno sliko SVG, s katero lahko sami določimo, katere relacije želimo prikazati.

6 Viri in literatura

[1] BATAGELJ, Vladimir: *Pajek Datasets*. [URL: http://vlado.fmf.uni-lj.si/pub/networks/data/].

[2] BATAGELJ, Vladimir: *Pajek to SVG Anim*. [URL: http://vlado.fmf.uni-lj.si/pub/networks/pajek/svgAnim/].

[3] BATAGELJ, Vladimir, MRVAR, Andrej: *PAJEK 1.02, Program for Large Network Analysis*. [URL: http://vlado.fmf.uni-lj.si/pub/networks/pajek/].

[4] BEARMAN, P., EVERETT, K.: *The Structure of Social Protest. Social Networks 15*, 1993, str. 171.

[5] BRVAR, Darko: *Dinamični prikaz časovnih omrežij*. Magistrsko delo. Ljubljana, 2005.

[6] DOREIAN, P., KAPUSCINSKI, R., KRACKHARDT, D., SZCZYPULA, J.: *A Brief History of Balance Through Time*. Journal of Mathematical Sociology 21(1-2), 1996, str. 113.

[7] FERRAIOLO, J., JUN, F., JACKSON, D.: *Scalable Vector Graphics (SVG) 1.1 Specification*. W3C Recommendation. [URL: http://www.w3.org/TR/2003/REC-SVG11-20030114/]

[8] MRVAR, Andrej: *Analiza in prikaz velikih omrežij*. Doktorska disertacija. Ljubljana, 1999.

[9] MUTZEL, P.: *GD99 contest: Lindenstrasse network*, 1999. [URL: http://kam.mff.cuni.cz/conferences/GD99/contest/graphs/A.html]

[10] de NOOY, Wouter, MRVAR, Andrej, BATAGELJ, Vladimir: *Exploratory Social Network Analysis with Pajek*. New York: Cambridge University Press, 2005

[11] VAN ROSSUM, G.: *Python*. [URL: http://www.python.org/2.4/].

[12] WILSON, Robin. J., WATKINS, John J.: *Uvod v teorijo grafov*. Sigma, št. 63, DMFA Slovenije, Ljubljana, 1997.

Mag. Darko Brvar je univerzitetni diplomirani inženir matematike. Konec leta 2005 je zaključil podiplomski študij statistike, smer družboslovna statistika. Ukvarja se z dinamičnim prikazom časovnih omrežij. Temo magistrskega dela je predstavil širši strokovni javnosti na Dnevih slovenske informatike aprila 2006.

Doc. dr. Andrej Mrvar je zaposlen na Fakulteti za družbene vede, kjer predava predmete s področja informatike in analize podatkov. Ukvarja se predvsem s teorijo grafov, algoritmi na grafih in omrežjih in analizo podatkov. Je soavtor programa za analizo in prikaz velikih omrežij Pajek. Letos je pri založbi Cambridge University Press izšla monografija W. de Nooy, A. Mrvar, V. Batagelj: Exploratory Social Network Analysis with Pajek.

Dr. Vladimir Batagelj je zaposlen kot redni profesor na Fakulteti za matematiko in fiziko, kjer predava predmete s področja diskretne in računalniške matematike. Ukvarja se predvsem s teorijo grafov, algoritmi na grafih in omrežjih, kombinatorično optimizacijo, analizo podatkov in uporabo informacijske tehnologije v izobraževanju. Je član več domačih in mednarodnih strokovnih združenj. Sam ali kot soavtor je napisal več visokošolskih in srednješolskih učbenikov, priročnikov in poljudnih del, številne znanstvene, strokovne in poljudne članke. Je soavtor programa za analizo in prikaz velikih omrežij Pajek.

Videonadzor in varnost v mestnih prostorih: kritična ocena dosedanjih izkušenj

Zdravko Mlinar, akademik
Slovenska akademija znanosti in umetnosti, Novi trg 3, Ljubljana
zdravko.mlinar@fdv.uni-lj.si

Povzetek

Problemi varnosti in razvoj informacijske tehnologije so privedli do eksplozivnega širjenja videonadzora v mestih. Ob sicer močni opori v stališčih prebivalcev in vidnih neposrednih učinkih postaja vse bolj sporna težnja k njegovi vsebinski, prostorski in časovni totalizaciji. Videonadzorne tehnologije večinoma ne nadomeščajo dosedanjih oblik fizičnega varovanja s pomočjo grajenega okolja in nadzornega osebja, še zlasti če gre za nasilje (nad ženskami). Videonadzor po eni strani krepi težnje k normalnemu, običajnemu in konformnemu življenju v mestu ter s tem slabi osnovo za inovativnost, z zagotavljanjem večje varnosti pa lahko skupno in javno življenje v mestu tudi bogati in razgiba.

Ključne besede: videonadzor, IKT, učinki, kritika, družbenoprostorske spremembe, varnost, mesto, zasebnost, javni prostori, homogenizacija, konformizem, inovativnost, ženske, prostorska sociologija

Abstract

VIDEO SURVEILLANCE IN URBAN AREAS: A CRITICAL ASSESSMENT OF PAST EXPERIENCE

Security concerns and the development of information technology have led to explosive expansion of urban video surveillance. Apart from its strong support amongst the public and tangible direct effects the trend towards its substantive, spatial and temporal totalization is increasingly questionable. In the main video surveillance technology does not replace earlier forms of physical security using structures of the built environment and security personnel, particularly with regard to violence (to women). On the one hand video surveillance reinforces the bent towards the normal, usual, the conformable and thereby undermines innovativeness but at the same time it can enrich and dynamize common and public urban life by ensuring greater security.

Keywords: video surveillance, ICT, effects, criticism, sociospatial changes, security, town, privacy, public places, homogeneity, conformity, innovativeness, women, spacial sociology

1 UVOD[1]

V preteklosti so prebivalci (po)skrbeli za varnost kot posamezniki in kot skupnost predvsem s svojim grajenim okoljem. Hiša je bila fizični okvir varnega doma, podobno kot je mestno obzidje – vzemimo Kopra, Izole in Pirana – simboliziralo zaščito meščanov pred tujo nevarnostjo. Kako pa (naj) se odzivamo na probleme varnosti ljudi in prostorskega (ne)reda naših mest v informacijski dobi? Ali grajeno okolje izgublja ali le spreminja svojo dosedanjo vlogo? Koliko in kako njegovo dosedanjo vlogo prevzema informacijsko-komunikacijska tehnologija (IKT)? In še zlasti, kaj nam kažejo izkušnje o želenih in neželenih učinkih videonadzora s kamerami?

Nenehne inovacije na IKT in razširjanje njihove rabe nakazujejo vse več možnosti za nadzor in obvladovanje dogajanja v vsakdanjem življenjskem okolju. Kot take naj bi dopolnjevale ali pa celo nadomeščale dosedanja prizadevanja načrtovalcev, da bi s prostorsko organizacijo grajenega okolja zagotovili varnost in kakovost življenja v mestnih naseljih. Toda nastopanje v imenu varnosti lahko prihaja tudi v nasprotje z nekaterimi temeljnimi pridobitvami mestne civilizacije, med katere sodijo večja individualnost ter osebna in družinska zasebnost, kot tudi bogastvo raznovrstnosti v javni sferi mesta. Pri tem se pojavlja več nejasnosti v zvezi z vprašanjem, kako na te pridobitve vplivajo nove nadzorne in še zlasti videonadzorne tehnologije. Njihov vpliv ni le enosmeren, temveč je

[1] *Pri zbiranju obsežnega gradiva o tej temi, ki bo predmet še nadaljnjih konkretnejših obdelav, so sodelovali tudi mag. Dušan Koman, bibliotekar (SAZU), ter podiplomska študenta FDV Aljoša Silič, univ. dipl. soc., in Matic Kavčič, univ. dipl. soc., za kar se jim zahvaljujem. Hvaležen sem tudi komandirjem policijskih postaj v Kopru, Izoli in Piranu, predstavnikom podjetij G7, Sintal in Janez, Davorju Kravanji, upravniku študentskega doma Korotan v Portorožu, Branku Mlinarju za informacije o videonadzoru v stanovanjskih stavbah in še mnogim drugim, ki so mi posredovali svoje izkušnje, ki jih bom vključeval še v prihodnje objave.*

odvisen od vrste okoliščin, ki jih želim osvetlili v tem besedilu.

Glede na to, da se videonadzor prav v zadnjem desetletju eksplozivno in – kot je videti – nezadržno širi, se bom namerno bolj posvetil predvsem kritičnemu razkrivanju njegovih posledic v družbeno-prostorskem in fizičnem kontekstu mesta. Pri tem bom upošteval protislovne težnje, ko vsakdo poskuša uveljavljati prost dostop do (informacij o) drugih in hkrati povsem obvladovati dostop drugih do sebe bodisi na individualni bodisi na kolektivni ravni (dva zakona dostopnosti).

S krepitvijo svobode in moči posameznika (tehnološko, finančno, informacijsko) pa se (avtomatično) ne povečuje posameznikov občutek odgovornosti do ožjega in širšega okolja. Ne gre torej preprosto za nekakšen linearni trend napredovanja k vse bolj odgovornemu in discipliniranemu vedenju. Tako se odpirajo vprašanja, kako omejevati destruktivno delovanje, npr. vandalizem, kriminal, nasilje, da pri tem ne bi zmanjševali, marveč bi povečevali možnosti za ustvarjalnost in inovativnost.

V svoji obravnavi se bom opiral tako na bogatejše mednarodne izkušnje, kot tudi na izkušnje iz Slovenije in še zlasti iz Slovenske Istre oziroma z obalnega območja, ki je tudi sicer predmet mojega obsežnejšega prostorskosocioloških raziskovanja. To raziskovanje zadeva spremembe v vsakdanjem življenjskem okolju z vidika informatizacije ter dolgoročnih procesov individualizacije in globalizacije. Pri tem me zanimajo spremembe, ki jih nova IKT prinaša v kontekstu bivalnega in delovnega okolja ter javne mestne sfere. Videonadzor je dejansko najmanj razširjen in preučen v stanovanjskih območjih in to bo seveda vplivalo tudi na vsebino moje obravnave.

S tem besedilom poizkušam prispevati: 1. k preseganju nejasnosti in dilem v usmerjanju nadaljnjega širjenja (omejevanja) videonadzora, 2. k ozaveščanju o njegovi potencialni vlogi v urbanističnem planiranju in arhitekturnem oblikovanju v mestnih prostorih in 3. k pojasnjevanju razmerij med fizičnim (grajenim) in virtualnim prostorom nasploh. Ob tem ko se pretežno omejujem na lokalni kontekst, pa se že nakazuje tudi potreba po vključevanju videonadzora na daljavo npr. z digitalnimi spletnimi kamerami, vključenimi v svetovna omrežja, z upoštevanjem satelitskih komunikacij ipd., kar že močno prestopa okvire današnjih razprav o televiziji zaprtega kroga (CC-TV).

2 NEKATERE DOSEDANJE OBRAVNAVE

Več avtorjev je že prikazalo, kako je prišlo do širjenja videonadzora v mestih (nekaterih) evropskih držav in preučevalo njegove posledice. Najcelovitejši pregled so pripravili v okviru evropskega raziskovalnega projekta *Urban Eye* (Hempel, Töpfer, 2002). S širšega sociološkega vidika in v kontekstu postmoderne, globalne informacijske družbe so najbolj znana dela kanadskega sociologa Davida Lyona (2004), najbolj bogate izkušnje pa so si pridobili v Veliki Britaniji in jih tudi objavili v številnih delih (npr. Graham, Brooks in Heery, 1995, Norris in Armstrong, 1999, Haggerty in Ericson, 2000, Honess in Charman, 1992). S prostorskosociološkega vidika in še zlasti glede na varnost žensk v protorsko-časovnih okvirih vsakdanjega mestnega življenja izstopajo analize finske avtorice Hille Koskela (Koskela, 2000, 2004), ki so bile – podobno kot prispevki še več drugih avtorjev – objavljene v reviji *Surveillance & Society*. Pri nas je videonadzor obravnaval Štefan Gostič z Ministrstva za notranje zadeve RS, s pravnega vidika (varstvo osebnih podatkov) pa je videonadzor raziskovala Jana Savkovič (Savkovič, 2004). Tehnično gledano in glede na različne oblike zagotavljanja varnosti v delovni, bivalni in javni mestni sferi so si bogate izkušnje pri nas pridobili v podjetjih, ki se posvečajo varovanju oseb in premoženja (Sintal, G7, Janez idr.) in v zvezi s tem je pisal npr. Igor Rot (Rot, 2005). V tej obravnavi se opiram še na gradivo Inšpektorata za varovanje osebnih podatkov (Jože Bogataj). Za razliko od številnih avtorjev, ki se ukvarjajo s tehnologijo, je moje zanimanje zlasti usmerjeno na posledice njene uporabe; te pa so še zelo malo preučene.

3 KAKO IN ZAKAJ SE ŠIRI VIDEONADZOR

V devetdesetih letih se je število videonadzornih kamer nameščenih v javnih in drugih mestnih prostorih – kot so ugotovili v okviru evropskega raziskovalnega projekta Mestno oko (Urban Eye) – v svetovnem merilu zelo hitro povečalo; od Londona do Teherana, Berlina do Pekinga so začeli videoopremo uporabljati v spopadanju s kriminalom in vandalizmom. Vseskozi pa gre za razhajanja med zagovorniki, ki jim nadzor predstavlja nujno in učinkovito ukrepanje za večjo varnost, ter nasprotniki, oponenti, ki v tem vidijo poseganje v zasebnost.

V ospredju tega dogajanja je Velika Britanija z vrsto znanih primerov učinkovite uporabe videonadzo-

ra po posameznih mestih. V mestu King's Lynn so namestili šestdeset na daljavo usmerjenih videokamer, da bi snemale dogajanje na znanih 'problemskih točkah' v neposredni povezavi s sedeži policije. Zmanjšanje pouličnega kriminala, ki je sledilo, je preseglo vsa pričakovanja; na nadzorovanih in bližnjih območjih je upadel na eno sedemdesetino prejšnjega. Prihranki v stroških policijskega patruliranja, kot o tem piše David Brin, so poplačali izdatke za opremo v nekaj mesecih. V škotskem mestu Airdrie so ugotovili, da se je zaradi videonadzora zmanjšal kriminal za 75 %. Toda izkušnje iz Glasgowa so drugačne: kamere v središču mesta niso imele vidnejšega učinka; v celoti gledano je bilo nekaj pozitivnih nekaj negativnih in dosti 'mešanih' posledic.

Največjo odmevnost in vpliv na ozaveščanje javnosti o pomenu videonadzora (tudi v evropskem merilu) pa je imel primer, ko sta leta 1993 dva enajstletna fanta v nakupovalnem središču Liverpoola ugrabila dveletnega otroka Jamieja Bulgerja, ki se je nekoliko oddaljil od svoje matere, in ga kasneje na grozovit način umorila. Ugrabitev so posnele videokamere in posnetki na trakovih so omogočili, da so oba storilca prijeli in obsodili. Izzvano javno mnenje (za podoben primer je šlo pred kratkim v Italiji) pa je vplivalo na vlado, da je video nadzor posvojila kot sredstvo svoje politike reda in varnosti in ponudila veliko finančno pomoč lokalnim oblastem, šolam, bolnišnicam in drugim za uvajanje videonadzora. Pri tem pa poudarek prehaja od nadzorovanja kriminala k vzdrževanju javnega reda. Danes navajajo, da v Veliki Britaniji deluje že štiri milijone videokamer. Londončan mora računati s tem, da ga bodo v enem živahnem dnevu kar tristokrat ujele oziroma 'posnele' različne videokamere.

Na Koprskem in na celotnem obalnem območju se nakazujejo številni izzivi, ki povečujejo pozornost in ozaveščenost o potrebi in o možnostih uvajanja (video)nadzora. Npr. starši dostikrat ne upajo pustiti otroka samega iz stanovanja; zaradi varnosti otrok je koprska občina postavila visoko ograjo okrog otroškega igrišča, na več mestih so šolarji naleteli na igle narkomanov, na Verdijevi in Cankarjevi ulici v Kopru je nasilnež napadel dve dekleti ter eno posilil; grafiti so se pojavili na stolnici in drugod, na številnih mestih se je pojavljal vandalizem (na trgih, v Badaševici, na pokopališču, v Žusterni, na parkirišči, na cestah – uničevali 'potopne valje'); nadalje v Piranu, kjer so poškodovali spomenik Tartiniju, v Portorožu pred starim hotelom Palace idr.[2] Navedli bi lahko še veliko različnih primerov kriminala in asocialnega vedenja v delovnih, bivalnih in javnih prostorih. V širšem kontekstu pa tudi primere, ki zadevajo urbanizem in arhitekturo ter grajeno okolje, npr. nedovoljene gradnje in druge posege v prostor.

Večje zanimanje ta tehnične oblike reševanja problemov varnosti izraža tudi spremembe v odnosih med ljudmi v (mestnih) naseljih. Po izkušnjah predstavnika podjetja za zasebno varovanje G7 upada pripravljenost ljudi iz bližnje okolice, da bi pomagali prizadetim v kritičnih situacijah. To nakazujejo tudi nekateri komentarji v zvezi z lanskoletnim posilstvom v Kopru. Po drugi strani pa usmeritev k novim tehnološkim rešitvam – kot je videonadzor – lahko še oslabi njihov občutek odgovornosti do dogajanja v okolici. Vodstva policije v primorskih mestih in drugod pa se ravno zavzemajo za tesnejšo povezanost policistov in občanov v »boju proti kriminalu« (Primorske novice, 6. 4. 2006).

Odzivnost podjetij za zasebno varovanje temelji na trženju in se torej prvenstveno usmerja tja, kjer so naročniki z denarjem. Bogomir Šuštar, Sintal Istra, ugotavlja, da naročil za namestitev videonadzora v javnih prostorih doslej niso dobili. Po nekaterih ocenah se okrog 90 % dejavnosti zasebnega varovanja v Sloveniji nanaša na podjetja in ustanove in le preostanek predtavlja (video)nadzor na stanovanjskih območjih in v javnih mestnih prostorih. Pri tem v podjetjih dostikrat ne gre več toliko za vprašanja varnosti, temveč prevladuje interes lastnika oziroma menedžmenta, da nadzoruje vedenje zaposlenih na delovnem mestu, čeprav to ni več povsem v skladu z zakonom o varstvu osebnih podatkov, ki teži k omejevanju rabe videonadzora. Koprska občina se ni – kot ugotavlja Ivan Lozej – bolj zaradi finančnih omejitev kot zaradi kakšnih načelnih pomislekov odločila za

[2] *Gre za zelo pestre pojavne oblike vandalizma tako pri nas kot drugod po svetu. V spletnem pozivu slovenske policije, da bi zaustavili vandalizem in skrbeli za 'javni red in mir' ga predstavljajo takole: »Uničevanje spomenikov, klopi, igral na otroških igriščih, dreves in parkov, telefonskih govorilnic, skrunitev grobov, razbijanje veliko okrasnih plošč na zidovih, šip in uličnih svetilk, pisanje po zidovih, prevračanje smetnjakov, uničevanje prometnih in drugih znakov, parkiranih avtomobilov, nogometni huliganizem, metanje kamnov na mimovozeča vozila, v okna vlakov, nastavljanje skal na železniške proge ipd. so postali nekako del našega vsakdana, vendar nikakor ne del, s katerim bi se lahko kar tako sprijaznili, saj vandalizem poleg neposrednih posledic v okolju zapušča tudi motnje v družbenih odnosih ter lahko vodi v brezbrižnost, strah in razkroj. Vandalizem sam po sebi kliče vandalizem. V mnogih deželah je postal veliko zlo mestnega pa tudi vaškega življenja.« (http: //www.policija.si/si/preventiva/jrm/vandalizem.html)*

videonadzor. Prav hitro zniževanje stroškov za uvedbo in delovanje videonadzornih sistemov je odločilno pripomoglo k njegovemu širjenju po svetu in pri nas. Drugi dejavnik pa je razvoj tehnologije.

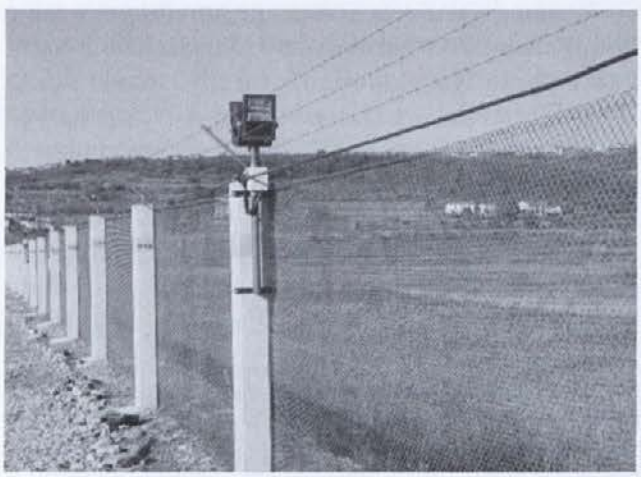
4 IZPOPOLNJEVANJE (VIDEO)NADZORNIH TEHNOLOGIJ IN POSLEDICE

Čeprav se v tem besedilu osredotočam na družbenoprostorske posledice uporabe (video)nadzornih tehnologij, moram na kratko prikazati tudi nekatere najbolj značilne izpopolnitve tehnologije. Splošna ocena, ki jo najpogosteje zasledimo v literaturi, je: videokamere postajajo manjše, hitrejše in cenejše ter nudijo bolj kakovostno sliko. Že iz tega sledijo posledice, ki se kažejo v dramatičnem širjenju videonadzora v zadnjih desetih in še zlasti zadnjih petih letih. Bistvenega pomena je prehod od analognega snemanja na trak k digitalizaciji, kar hkrati omogoča avtomatizacijo in povečuje zmožnosti shranjevanja in hitrega iskanja posnetkov. Velike količine digitalnih informacij se hrani na trdih diskih ali na optičnih shranjevalnih sistemih. Vse večja je tudi ločljivost posnetkov in s tem večja možnost prepoznavanja oseb in predmetov (npr. s starimi kamerami dostikrat ni bilo mogoče prepoznati registrskih tablic na avtomobilih, zato je bilo dosti pobegov na bencinskih črpalkah). Zumiranje (zoom) omogoča veliko približanje opazovanega z večje oddaljenosti; uporabljajo pa tudi vrtljive kamere, ki jih lahko usmerjajo na daljavo. Širokopasovna dostopnost npr. prek omrežja optičnih kablov, kakršno ravno sedaj v Kopru vzpostavlja podjetje Gratel, omogoča hiter pretok velike količine informacij, tako da v prihodnje videonadzor ne bo več toliko omejen le na posamezne točke (kamere), kar so označevali kot »televizijo zaprtega kroga« (CC-TV). Zlasti v mestih se vse bolj uporablja brezžični prenos slike, čeprav za sedaj še z manjšo zanesljivostjo. S 'spletnimi kamerami' (IP), prek računalnika in interneta je mogoče nadzorovati dogajanje na izbranih lokacijah po vsem svetu.[3] Sicer pa danes v razširjenih videonadzornih omrežjih lahko poiščejo in sledijo posamezniku podnevi in ponoči v množici ali avtomobilu, ki vozi po mestu. Ob meji v dolini Dragonje policisti uporabljajo tudi že termovizijo, ko ponoči ob meji odkrivajo prebežnike.

V stanovanjskih stavbah dosedanje audiodomofone vse bolj nadomeščajo videodomofoni. S tem ko obiskovalec lahko ob vhodu npr. v študentski dom neposredno vzpostavi stik s stanovalcem, ki ga želi obiskati, se nadzor individualizira in niso več potrebni dežurni vratarji oziroma receptorji in poseben prostor zanje.

Številne novosti prinaša t. i. biometrika, ki vsaj deloma vključuje tudi videonadzor, kot je npr. prepoznavanje obrazov (sicer pa vključuje tudi prepoznavanje prstnih odtisov, vzorce roženice idr.). Nasploh pa je treba upoštevati, da gre za zelo veliko razliko med (video)nadzorno tehnologijo, ki je dostopna širšemu krogu ljudi, in visoko profesionalno, vrhunsko tehnologijo, ki si jo lahko privoščijo le banke, državne organizacije ipd.

[3] *Istrski pesnik Bert Pribac je npr. po vrnitvi iz Avstralije lahko še naprej spremljal, kako je z njegovo hišo v Canberri.*



Slika 1: **Fizično zagotavljanje varnosti – ograja in reflektorji**

Slika 2: **Videonadzorni pregled na območju Luke Koper**

Tako tehnično kot sociološko gre za pomembno – lahko bi rekli paradigmatsko – spremembo s tem, ko se povečuje pretočnost vse večjih količin informacij prek optičnih omrežij in brezžičnih povezav. Omrežna organizacija omogoča spremljanje (mobilnosti) oseb in predmetov v lokalnem in globalnem merilu. Spreminja pa se tudi vzorec prostorske organizacije samih varnostno-nadzornih služb. Doslej je bilo značilno, da je bil videonadzor zamejen na določeno lokacijo v televiziji zaprtega kroga in so le avdio zasnovani alarmni (npr. protipožarni ali protivlomni) sistemi vključevali navezavo na varnostnonadzorne centre ter intervencijsko službo. Tehnične in stroškovne omejitve so večinoma zamejevale videonadzor – prostorsko – na lokacijo uporabnika in – časovno – na naknadno ugotavljanje dogodkov in prepoznavanje subjektov za nazaj.

5 OD GRAJENEGA OKOLJA K IKT IN NAZAJ

Nove IKT, kot je npr. televizija zaprtega kroga, ne bi smeli obravnavati same zase, temveč skupaj oz. v razmerju do že do sedaj znanih možnosti zagotavljanja reda in varnosti v mestnih naseljih. Že klasična spoznanja npr. o »ubranljivem prostoru« (*defensible space*), ki jih je predstavil Oskar Newman (1972) in so bila z veliko pozornostjo sprejeta v urbanističnem načrtovanju (gl. tudi Coleman, 1990), so vsaj v posamičnih primerih vplivala na izboljšanje razmer v javnih in zasebnih območjih mest. Videonadzorne tehnologije večinoma ne razveljavljajo dosedanje prakse, temveč jo nadgrajujejo in dodajajo še nove možnosti. Ob tem se pojavljajo celo pozivi, da bi oživili »naravni« nadzor prebivalcev drug nad drugim (Oc, 1991). Gre za prizadevanja, da bi poleg IKT upoštevali tudi metode nadzora brez tehnologije, npr. neposredno opazovanje, ali s preprostejšo tehnologijo.[4]

V stanovanjskem načrtovanju so si prizadevali, da bi – po sicer nekoliko tradicionalni predstavi – mati iz kuhinje lahko skozi okno opazovala otroka pri igri na prostem. Podobno bi lahko imeli stanovalci iz svojih stanovanj pregled nad okolico in dostopi do stanovanjske stavbe. Newman (1972) je dokazal, da je preglednost bistvena sestavina bivalnega okolja. Hudodelci radi delujejo neopazovani v prikritih in odmaknjenih prostorih, stanovalci pa se počutijo varnejši in imajo občutek, da bolj obvladujejo svoje domače okolje, če imajo zagotovljen nemoten vizualni nadzor nad dogajanjem v okolici svojega bivališča. Nasploh je bilo ugotovljeno, da se kriminal pojavlja največkrat v stanovanjskih blokih, kjer 1.) so možnosti »naravnega« nadzora omejene, 2.) je velika anonimnost, npr. veliko stanovanj na en vhod v stavbo, in 3.) je več možnih poti za pobeg. Tako je bila vzpostavljena jasna povezava med načrtovanjem prostorske organizacije grajenega okolja in kriminalom oz. vandalizmom. Različne urbanistične rešitve so imele za posledico tudi različne stroške za policijo, sodišča, zapore, različne zavarovalnine, kot tudi socialne posledice zaradi žrtev kriminala.

Tudi novejše obravnave videonadzornih tehnologij opozarjajo na nekatere prednosti nekdanjih načinov zagotavljanja varnosti prebivalcev ali pa vsaj terjajo hkratno upoštevanje enih in drugih. Kot bomo še videli, videokamere (televizija zaprtega kroga) ne morejo povsem nadomestiti neposredne fizične navzočnosti in pomoči drugih,[5] še zlasti ko gre za ženske, ki se čutijo ogrožene, ko se v nočnem času gibljejo v javnih mestnih prostorih (gl. tudi Trench et al., 1992). Izkušnje pri nas, npr. v Kopru, ko je šlo za garaže v Prisojah (z dolgoletno problematiko nereda in različnih prestopnikov, ki so ogrožali javno varnost), in po svetu nesporno kažejo, da izboljšana razsvetljava skupnih površin povečuje varnost in namembno rabo prostorov. To je torej že klasični »protistrup« proti neredu in koncentraciji prestopnikov v neosvetljenih (pol)javnih prostorih.

V usmeritvah Sveta Evrope (gl. npr. Preprečevanje kriminalitete, 2003) je nakazano, da tehnično zavarovanje območij z videonadzornimi sistemi vzbuja številne pomisleke, hkrati pa te usmeritve opozarjajo na neizkoriščene možnosti, da se z načrtovanjem in oblikovanjem okolja ustvarja »branjene prostore« in bolj varna bivalna okolja: spodbujali naj bi občutek odgovornosti in pripadnosti okolju, vračanje ljudi v

[4] *Iz lastnih opažanj lahko opozorim na zelo preprosto rešitev vprašanja, kako številni potniki po končanem letu na letališču prevzemajo prtljago v prostoru, kjer je videti, da bi lahko kdorkoli vzel karkoli. Ker ni znano, ali je med čakajočimi na dostavo prisoten tudi lastnik, čakajoči nadzorujejo drug drugega oz. vsi nadzorujejo vse. Četudi gre za množico potnikov v letalskem prometu – še posebej v visoki turistični sezoni – se praviloma vse odvija gladko, brez posebnih intervencij. Seveda pa to ne izključuje dodatnih načinov nadzora.*

[5] *Že Jane Jacobs (1961) je ugotovila, da prisotnost drugih ljudi pogosto odvrača od kriminala, in nakazala, da več srečevanja pomeni manjšo verjetnost kriminala na ulicah. Sicer pa je ilustrativna tudi ugotovitev, »če si pijan ponoči, ne misliš na kamere na ulici« (Honess, Charman, 1992, 20). Videokamere torej ne bodo zmanjšale nereda in nasilja zaradi pijančevanja.*

središča mest,[6] oživljanje dejavnosti v sicer zapuščenih ulicah; prizadevali naj bi si za to, da ne bi prihajalo do koncentracije socialno izključenih ljudi in prestopnikov na enem mestu, hkrati pa naj bi omogočali vključevanje vseh skupin v dinamiko mestnega življenja. Glede mladoletniškega prestopništva pa opozarjajo, da »nasilje na televiziji zmanjšuje meje med dovoljenim in nedovoljenim«.[7]

Prav zadnja ugotovitev zadeva tudi splošno temo o razmerju med informacijsko sfero (virtualnim prostorom) in fizičnim okoljem, kar obravnavam na drugem mestu.[8] Ostaja še veliko odprtih vprašanj o tem, kdaj uvajanje novih možnosti za nadzor in obvladovanje dogajanja v prostoru na podlagi inovacij v IKT pomeni odpravljanje, kdaj pa dopolnjevanje in nadgrajevanje prejšnjih načinov takšnega prizadevanja.

»Hiše sramote«. Ilustrativni primer izkušnje o tem, kako lahko elektronski (sicer ne nujno ravno video) nadzor povezujemo z urejanjem prostora oziroma urbanizmom, do česar pri nas še nismo prišli, predstavlja spletna stran z imenom »Hiše sramote«, ki jo je vzpostavilo mesto Toledo v ZDA. V tem mestu so spretno izkoristili novo tehnologijo v prizadevanjih, da bi odločno ukrepali proti lastnikom zapuščenih in zanemarjenih nepremičnin. Računali so na to, da bodo z dozo starega, znanega zdravila, tj. s spodbujenim javnim prezirom vplivali na najbolj razvpite in uporne lastnike, da bodo upoštevali pravila javnega in stanovanjskega reda. Na spletni strani so objavili imena in naslove lastnikov v okviru širšega programa za revitalizacijo mestnih sosesk. V osmih od dvanajstih primerov so dosegli zastavljeni cilj.

Medtem ko je praviloma v ospredju vprašanje, kako z vidika varstva zasebnosti (osebnih podatkov) čim bolj omejiti javni nadzor in izpostavljanje pridobljenih informacij širšemu krogu ljudi, je šlo v tem primeru prav za nasprotno. Izpostavili so jih sicer le besedno, lahko pa bi jih tudi slikovno; upravičeno pa toliko, kolikor so te nepremičnine posegale tudi v javno sfero življenja v mestu. Glede morebitne uporabnosti teh izkušenj pri nas in konkretno na območju Slovenske Istre pa bi jih kazalo še bolj temeljito preučiti. Veliko zapuščenih in razpadajočih hiš na istrskem podeželju, ki imajo svoje solastnike raztresene po vsem svetu, predstavlja velik izziv za to, da bi se oprli tudi na internet. Vprašljivo pa je, kakšen pa bi bil odziv v smislu sramote in preziranja oziroma moralnega pritiska na njih.

Če bi zanemarjene oziroma zapuščene hiše ali druge objekte predstavili na spletu tudi vizualno, bi (verjetno) dosegli še večji učinek. Razmišljanja o prostorskem (ne)redu pri nas še ne sežejo tako daleč. V praksi pa je že prišlo do tega, da so ravno z iskanjem prek interneta našli enega od solastnikov prazne hiše v koprskem zaledju; to je bil izseljenec v Avstraliji. S tem je bilo omogočeno, da je kupec lahko pridobil lastnino in oživil to nepremičnino sredi naselja. Veliko število nerešenih problemov zapuščenih nepremičnin na podeželju Slovenske Istre na vsakem koraku blokira razvojna prizadevanja in terja iskanja novih rešitev tudi v nakazani smeri.

6 KRITIČNE UGOTOVITVE O (NE)NAMERAVANIH IN (NE)ŽELENIH UČINKIH

Ob dinamičnem širjenju videonadzora so v ospredju predvsem pričakovanja o neposrednih učinkih v delovni, bivalni in javni mestni sferi, bolj ob strani pa ostajajo posredni in še zlasti nenameravani in neželeni oz. stranski učinki glede na osnovno (dostikrat predvsem z dobičkom motivirano) izhodišče. Ti postajajo v polni meri prepoznavni šele v širšem vsebinskem ter prostorskem in časovnem kontekstu. Zato – kot sem že nakazal – bom na tem mestu večjo pozornost posvetil prav tem zapostavljenim in kritičnim obravnavam širjenja videonadzora na podlagi IKT.

Današnja tehnologija videonadzora daje določeno oporo poenostavljenemu razumevanju celotne problematike, kot da gre za nekakšno elektronsko panacejo (zdravilo za vse bolezni) za kriminal in druge oblike ogrožanja varnosti in reda v mestih nasploh. Toda raziskovalci so opozorili, da vpleteni akterji pri promociji videonadzornih sistemov (varnostna podjetja, svetovalci, politiki, akterji za oživljanje mestnih območij) vplivajo na pretirano pripisovanje uspeha le tehnološkim rešitvam. Splošna usmeritev se bolj nagiba k olepševanju kot k skrbi in pozitivni preobrazbi v zvezi z mestnim kriminalom (Graham et al., 1995, 22).

[6] *Če se v urbanističnem načrtovanju predvidi stanovanjska območja v mestnih jedrih, se s tem ustvari bolj žive ulice in »naravni nadzor«. V novejšem času se nasploh uveljavlja ideja, da je mogoče okrepiti nadzor in varnost z »mešano strukturo« prebivalstva in »mešano rabo« prostora (Trench et al., 1992, 287, 292).*

[7] *Ostaja pa še vrsta drugih vplivov (vzgoja, družina, šola), ki prestopajo okvire te obravnave.*

[8] *Že dalj časa potekajo razprave in raziskave npr. o tem, ali širjenje komunikacij nadomešča fizično mobilnost ljudi in stvari. Vse bolj postaja jasno, da ne gre preprosto za alternativo, ampak za bolj zapleteno razmerje (več o tem v Mlinar, 2004).*

Takšna zožena usmeritev hkrati pomeni nekakšno razdolžitev lastnega angažiranja ljudi. Pretirano zaupanje v tehnologijo dostikrat spremlja tudi podcenjevanje pomena medčloveških odnosov in vodi k zanemarjanju globljih vzrokov, zaradi katerih prihaja do neželenih pojavov v današnjih mestnih naseljih. Nadzorne in še zlasti videotehnologije ne odpravljajo vzrokov, temveč nas usmerjajo bolj na simptome, na zunanje znake družbenih problemov.

Gre za paradoks: tako kot po eni strani različna poročila in raziskave kažejo, da visok delež ljudi odobrava nadaljnje širjenje videonadzora, pa po drugi strani preseneča bogata vsebina kritičnih odzivov na dosedanje izkušnje, kot sledi:

1. Pridobitve in izgube. Z uvedbo ali razširjanjem videonadzora je sicer mogoče – bolj ali manj uspešno – doseči zastavljeni cilj, npr. večjo varnost ljudi in premoženja na nekem območju mesta, toda pri tem se zanemarja dejstvo, da to dostikrat pomeni tudi določeno izgubo z vidika neke druge vrednote, npr. individualne ali družinske zasebnosti. Izbrana nadzorna tehnologija je lahko sredstvo za uveljavljanje in za izničenje iste vrednote glede na to, kdo in kako jo uporablja. Videokamera, s katero vodstvo podjetja spremlja delo na daljavo na domu, lahko posega v zasebnost družine; videokamera lahko nadzira dostopnost do družinske hiše ali pa stanovalcu (podjetniku) omogoča spremljanje dogajanja v domači hiši na daljavo itd.[9] Ista nadzorna tehnologija torej lahko dobiva povsem različne in nasprotne vloge.

2. Težnje k totalizaciji. Številne kritike dosedanje prakse videonadzora opozarjajo na nesprejemljivo težnjo k njegovemu vsebinskemu oz. predmetnemu razširjanju in torej k vse večji inkluzivnosti/totalizaciji. Glede na to se civilno družbena skupina *US Privacy International Group* (Marc Rotenberg) zavzema za upor politiki nadzora kriminala, ki prehaja v družbeno nadzorstvo (nasploh). Z razširjanjem nadzora lahko pride do sprevrženih učinkov: namesto da bi se ljudje počutili bolj varne, se lahko strah in nezaupanje med njimi še povečata; v mestu z vse bolj razširjenim videonadzorom konec koncev ne bi bilo prijetno živeti (Koskela, 2000, 247).

3. Prostorski vidiki. Najpogostejša kritična ocena prikazov o dosežkih videonadzora opozarja na to, da sicer z uvedbo takega nadzora na določenem območju zares upade kriminaliteta (vandalizem, tatvine, grafiti, nasilje itd.), vendar pa pri tem ne preverjajo, če se ta ni »preselila« na druga območja. Z videonadzorom se praviloma najprej zaščitijo bogatejša območja z višjimi sloji prebivalstva, kar potem vpliva na poslabšanje razmer v bližnjih, revnejših predelih; včasih pa gre za prehod iz javnih mestnih prostorov oz. območij na stanovanjska območja.

Kot so pokazale policijske izkušnje v Kaliforniji, se pojavljajo omejitve zmogljivosti videonadzora (v smislu televizije zaprtega kroga), kadar naj bi spremljali določeno dogajanje na širšem območju, npr. razpršene trgovske in zabaviščne aktivnosti. V takih primerih, še zlasti če gre za veliko mobilnost ljudi, se je težko opirati na fiksne videonadzorne sisteme. Policisti se s težavo pravočasno odzovejo na kriminalna dejanja, ki jih vidijo na zaslonu (Nieto, 1997).

Pogosto se pojavljajo tudi problemi nekako v nasprotnem smislu, ko videokamere, nameščene v javnem prostoru mestnega naselja, zajemajo vidno polje, ki (po)sega v zasebne prostore, kar sproža negativne odzive prizadetih.

Poseben primer te problematike predstavljajo zaprta, ograjena, elitna naselja oz. soseske, t. i. *gated communities*, ki se prav sedaj začenjajo pojavljati tudi v Sloveniji. V svetu imajo s tem že veliko izkušenj, s katerimi bi se morali bolj seznaniti organi državne in lokalnih oblasti, projektanti, nepremičninske agencije in seveda podjetja, ki se ukvarjajo z varovanjem ljudi in premoženja. Nekateri tudi te primere označujejo kot »varovana« naselja/soseske. Ob vse večji odprtosti Slovenije v Evropo in v svet se povečuje mobilnost ljudi in stvari, tudi nevarnih, kot so teroristi, orožje in droge, ter premoženjska neenakost, kot tudi razlike in nasprotja med etničnimi in verskimi skupinami. S tem pa se spreminja tudi prostorska organizacija mestnih naselij, kar predstavlja izhodišče tudi za načrtovanje varnosti ljudi v tako spremenjenih okoljih.[10]

S podjetniškega vidika se prav v nakazanih razmerah nakazujejo velike možnosti za širšo rabo najnovejših varnostnih oz. nadzornih tehnologij. Poleg doslej znanih in prevladujočih oblik varovanja posameznih objektov je – po mednarodnih izkušnjah sodeč – pred nami težnja k privatizaciji in varovanju

[9] *Primer iz prakse Sintala, ko to želi podjetnik s pomočjo dlančnika, medtem ko je na morju na jadranju. Sicer pa mi je znan primer, ko je posameznik v svojem stanovanju prikrito namestil spletno kamero, da je lahko spremljal ravnanje čistilke v času, ko je bil zdoma.*

[10] *Še vedno ostaja odprta tema o deteritorializaciji in glokalizaciji (ne)varnosti v času, ko prehajamo od »prostora krajev« k »prostoru tokov«. To so zadevale tudi nekatere obravnave na letnem srečanju Slovenskega sociološkega društva (Izola, 2005) z naslovom* Varnost in tveganja v sodobni slovenski družbi.

kar celih predelov mest, pa čeprav v Sloveniji le v manjšem merilu. Videonadzor se tako pojavlja skupaj s fizičnimi preprekami kot sredstvo za obvladovanje selektivne dostopnosti v določen predel mesta. Primer za to je Rezidenca park Lucija v Luciji pri Portorožu.[11]

Pojavljajo pa se tudi manjši stanovanjski kompleksi (bloki), ki so zgrajeni in jih upravljajo po ameriških zgledih kot osamosvojene enote in jih označujejo kot kondominije.

Seveda pa lahko takšna privatizacija urbaniziranega in širšega prostora ter segmentalno reševanje problemov varnosti še poveča neenakost in zaostri oz. poslabša razmere v preostalih območjih, ki si ne morejo privoščiti takšnega ekskluzivizma niti glede fizične strukture niti glede videonadzorne tehnologije. To pa se bo ali pa se ne bo reševalo glede na razmerja politične moči na lokalni in državni ravni.

4. Časovna razsežnost delovanja in učinkovanja videonadzora. Podobno kot z vsebinskega (predmetnega) in prostorskega se tudi s časovnega vidika pojavlja zahteva, da je treba čim bolj omejiti in skrčiti opazovanje, da ne bi (prekomerno) posegali v zasebnost in osebne pravice opazovanih. To velja tako za čas snemanja kot za čas hranjenja podatkov bodisi v analogni ali digitalni obliki. Še posebej sporno pa je časovno razširjanje nadzora na podlagi vnaprejšnjega sumničenja, da bi kdo lahko storil kaj neprimernega oz. kaznivo dejanje. Kritiki na to opozarjajo zlasti takrat, kadar gre za predsodke o tem, da se prav določene kategorije ali skupine ljudi, npr. glede na poreklo, nagibajo h kriminalu.

Pri ocenjevanju učinkov in uspešnosti uvajanja in delovanja videonadzornih sistemov je treba pri časovnem vidiku upoštevati naslednjo pomanjkljivost: večinoma je videonadzor bolj učinkovit le krajši čas, ko gre še za novost in presenečenje, kot pa kasneje, ko pride že do določene navajenosti in se zmanjša pozornost do te novosti.

Slika 3: **Rezidenca Park Lucija (ograjeno in videonadzorovano naselje)**

Županja in varnostni sosvet v občini Izola v praksi uveljavljajo sicer znano »teorijo razbitih oken«, po kateri se je treba takoj odzvati na vsak vandalizem in takoj vzpostaviti prejšnje stanje. V nasprotnem primeru povzročeni nered postane izziv in gojišče za še nadaljnje nerede.[12]

V zvezi s tem nam IKT prinaša velike možnosti, s popolnejšimi in hitreje posredovanimi informacijami o povzročenem neredu lahko npr. skrajšamo čas odziva nanj in tako »v kali« preprečimo morebitno nadaljnje ponavljanje in kopičenje takšnih dejanj.

5. Težnja k »sterilizaciji« in konformnosti. Nadzorni sistemi so praviloma usmerjeni na razkrivanje vsega odstopajočega, odklonskega, neobičajnega, nenormalnega. Pri tem elektronski nadzor igra podobno vlogo, kot jo je nekdanji neformalni nadzor v manjših krajih na osnovi tesne medsebojne povezanosti in medsebojnega poznavanja ljudi. Čeprav se neformalni nadzor danes dostikrat jemlje za zgled, je vendarle treba upoštevati, da se s tem hkrati oži osnova za inovativnost. Prav spodbujanje inovativnosti pa je temeljna zahteva v okviru slovenskih in evropskih prizadevanj za pospešeno vstopanje v družbo znanja.

Nadzor, ki po eni strani via facti deluje izključevalno do odklonskosti in teži k »ohranjanju normalnega med tistimi, ki že so normalni«, tako »normalizira mestni prostor« (Koskela, 2000, 253). To hkrati pomeni, da siromaši značilno bogastvo raznovrstnosti v mestu. Prečiščeno okolje pa teži tudi k duhovni sterilnosti.

Med najpogostejše kritike in prikaze negativnih posledic videonadzora sodijo tiste, ki opozarjajo, da postajajo javni mestni prostori vse bolj podobni komercialno obvladovanemu režimu in vzdušju v nakupovalnih središčih. Gre le še za nekakšno navidezno in popačeno javnost, v kateri so dobrodošli le ljudje kot potrošniki, ne pa tudi drugi, ki bi sicer prispevali k bogastvu raznovrstnosti kot tipični značilnosti mestnega

---

[11] *Tudi na drugi strani Piranskega zaliva, v naselju Alberi, je bilo zgrajeno podobno zaprto in varovano naselje* Residencije Skiper Savudrija *(zaradi prvotnih motivov italijanskih investitorjev so ga* Primorske novice *najprej predstavile kot »kolonijo Padanije«), ki pa je pretežno turističnega značaja.*

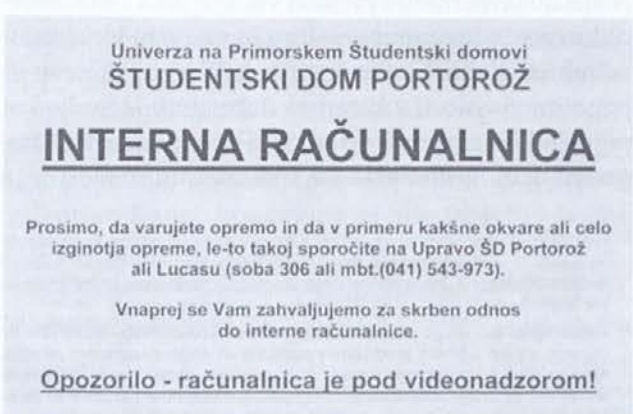
[12] *To potrjujejo tudi druge izkušnje iz moje raziskave na območju Slovenske Istre, npr. v zvezi s črnimi gradnjami v podeželskih krajih v koprskem zaledju. Kjer na prvo črno gradnjo v kraju ni bilo odziva oblasti, je to pomenilo ohrabritev za druge potencialne črnograditelje. Vsaj do neke mere to potrjujejo tudi opažanja Ivana Lozeja, da so bili potencialni vandali v koprski občini bolj zadržani in so imeli bolj spoštljiv odnos do sedežev v novih avtobusih kot pa v drugih, ki so bili že »načeti«.*

življenja. Neposredno ali posredno gre torej za izključevanje vseh, ki ne prispevajo h komercialni uspešnosti določenih mestnih območij.

Ne nazadnje pa ima prav videonadzor nespodbuden vpliv na tiste, ki bi želeli javno in legalno izraziti svoj protest; na udeležence povsem legalnih sindikalnih demonstracij se npr. z videonadzorom ustvarja pritisk, kar jim povzroča ali poveča zaskrbljenost zaradi morebitnih slabih posledic zanje. V tem smislu torej videonadzor jemlje pogum legalnemu in legitimnemu javnemu kritičnemu nastopanju in krepi konformizem.

Glede na navedeno je spornost videonadzora, ko gre za javne prostore, predvsem spornost njegove »očiščevalne«, filtrirne vloge, torej to, kar je sicer njegova temeljna funkcija, ko gre za varovanje individualne in družinske zasebnosti. Vendar pa tako v literaturi v svetu kot v praksi pri nas ostaja sporno to, kako in koliko naj se upošteva zasebnost tudi v javnih prostorih. Zelo preprosto utemeljevanje v smislu »kdor ima poštene namene, nima kaj skrivati v javnosti« očitno še ne razrešuje vseh vprašanj.

6. Obogatitev skupnih prostorov. Navzlic navedenemu pa razkrivamo tudi bolj pozitivne izkušnje. Vzemimo primer videonadzora v računalniški učilnici študentskega doma *Korotan* v Portorožu. Brez takšnega nadzora marsikje nočejo namestiti računalnikov v skupne prostore, kar ima za posledico, da je kolektivna sfera v njih osiromašena, saj se morajo stanovalci omejevati le na tisto, s čimer razpolaga vsak sam zase, npr. študent v svoji sobi. Nova oblika nadzora v smislu televizije zaprtega kroga pa je omogočila obogatitev na kolektivni ravni zaradi zmanjšanega tveganja, da bi kdo odtujil opremo, ki je v skupnem prostoru na voljo vsem.



Slika 4: **Univerza na Primorskem, Študentski domovi (interna računalnica)**

Uvedba videonadzora torej vendarle ne pomeni že kar nasploh osiromašenja skupnega življenja. Navedeni primer nam kaže, da je mogoče tudi nasprotno. Toda kdaj in pod kakšnimi pogoji je tako, bi morali še bolj raziskati. Kdaj je videonadzor (predvsem) pogoj za bogatejše javno mestno življenje, kdaj pa vodi do nasprotnih učinkov? Njegova vloga se lahko izraža bolj v omejevanju in preprečevanju ali pa predstavlja obliko sodelovanja (skrbi in pomoči).

7. Opazovalci in opazovani: ženske kot objekt opazovanja. Neenaka porazdelitev vlog opazovalcev/nadzornikov in opazovanih/nadzorovanih po posameznih kategorijah prebivalcev je že nasploh problematična. Za tistega, ki opazuje, je značilna moč, tako kot je za tistega, ki je opazovan, značilna nemoč. Še prav posebej se zaostrujejo razlike po spolu, saj se ženske iz več razlogov in na več načinov pojavljajo v vlogi objekta opazovanja in nadzora ali pa so sicer zaradi fizične premoči moških bolj ogrožene. Večina tistih »za kamerami«, ki opravljajo videonadzor, je moških, večina tistih pod nadzorom pa žensk. S tem je povezana tudi ugotovitev, da je videonadzor manj uspešen tedaj, ko gre za nasilni kriminal, tako kot npr. pri spolnem nasilju, bolj uspešen pa tedaj, ko gre za kriminal v zvezi s premoženjem (različne poškodbe, vozila, tatvine, vlomi). Spolno nadlegovanje je teže odkrivati in prekiniti z nadzornimi kamerami, laže ga odkrivajo policisti ter njihove patrulje in varnostniki.[13]

Med slabimi izkušnjami iz različnih držav dostikrat navajajo primere, da so varnostniki operaterji snemali ženske v sanitarijah ali v prostorih za preoblačenje, delali bližnje posnetke izpostavljenih delov telesa in pripravljali videosekvence na trakovih, ki so jih kazali na hišnih zabavah; ali ko so vojaki snemali ženske brez zgornjega dela kopalk na bližnjih plažah in kasneje natisnili slike ter jih obešali na stene.

S prikazanim smo se približali značilni podtemi, ki se kot problem pojavlja v zvezi z videonadzorom, tj. voajerizmu. Pri voajerizmu gre za pretirano zanimanje za zasebnost drugih, še zlasti za doživljanje spolnega zadovoljstva ob gledanju (na prikrit način) spolnega občevanja ali žensk kot predmeta poželenja. Nova IKT nudi vse več možnosti za širjenje voajerizma kot ene od privlačnih oblik zabave. »Kultura voajerizma« dobiva svojo podlago v množični rabi mobilnih tele-

[13] *Ta vprašanja so se v javnosti zelo zaostrila, ko je v Kopru prišlo do posilstva v javnem prostoru skoraj v središču mesta, blizu sedeža občine.*

fonov s kamerami (Wood, 2005, Koskela, 2004). To izstopa zlasti na Japonskem, kjer moški zasledujejo ženske (s kratkimi krili) na ulicah, med ženskami pa se širi strah pred takšnim prikritim snemanjem.

7 SKLEPNA MISEL

Opravljeni pregled izkušenj z uvajanjem, delovanjem in učinki videonadzora v mestnih naseljih na podlagi nove IKT v Evropi in v ZDA, še zlasti pa v Veliki Britaniji in tudi že pri nas nam je pokazal tako njegovo nezadržno in dinamično širjenje kot tudi številne nenameravane in neželene posledice. Prikazana spoznanja nadgrajujejo dosedanjo prakso prostorskega in urbanističnega uveljavljanja reda in kakovosti življenja v delovni, bivalni in javni mestni sferi, hkrati pa opozarjajo na nevarnost, da popoln nadzor lahko vodi v izničenje temeljnih vrednot mestne civilizacije. Kljub povedanemu ugotavljam, da je treba in da je mogoče ob upoštevanju doseženih spoznanj z videonadzorom krepiti medsebojno dopolnjevanje in presegati izključevanje med varnostjo in svobodo ter zasebno in kolektivno sfero mestnega življenja. V tem smislu naj bi kritično ocenjene izkušnje prispevale k preseganju neenotnosti oz. nesoglasij in negotovosti ob uvajanju (video)nadzornih tehnologij, še zlasti v javni sferi naših mest.

8 VIRI IN LITERATURA

[1] Anti – CCTV, http://www.spy.org.uk/wtwu.htm, 2. februar 2006 (marec 2006).

[2] ARTICLE 29 Data Protection working party: Opinion 4/2004 on the processing of personal data by video surveillance, 11750/02/EN, WP 89, Brussels, 2004.

[3] BANISAR, David et al.: Privacy & Human Rights, 1999, http://www.privacyinternational.org/survey/index99.html (marec 2006).

[4] BRIN, David: The transparent society: Will technology force us to choose between privacy and freedom?, 1998.

[5] BERIT, LANG, Silke: The impact of video systems on architecture, Swiss Federal Institute of Technology, Zurich, (2004).

[6] COLEMAN, Alice: Utopia on trial: Vision and reality in planned housing, London, Hilary Shipman, 1990.

[7] FLORIDA, Richard: The rise of the creative class: and how it is transforming work, leisure, community and everyday life, New York, Basic Books, 2002.

[8] GOLDSMITH, Stephen: The coming digital polis, City Summer, 2000, 10 (3).

[9] GOSTIČ, Štefan: Video nadzor v dejavnosti zasebnega varovanja, referat (tipkopis), Ljubljana, MNZ.

[10] GRAHAM, Stephen, BROOKS, John, HERRY Dan: Towns on the television: CCTC Surveillance in british towns and cities, Newcastle, University of Newcastle, GURU, 1995.

[11] HAGGERTY, K. D., ERICSON, R.: The surveillant assemblage, The British Journal of Sociology, 2000, 51 (4): 605–22.

[12] HEMPEL, Leon, TÖPFER, Eric: Urban eye: Inception report, WP 1, Berlin, Technical University Berlin, 2002.

[13] HONESS, Terry, CHARMAN, Elizabeth: Closed circuit television in public places: its acceptability and perceived effectiveness, London, Home Office Police Department, 1992.

[14] JACOBS, Jane: The death and life of great american cities, Harmondsworth, Penguin, 1961.

[15] JAVNI RED IN MIR, http: //www.policija.si/si/preventiva/jrm/vandalizem.html).

[16] KOSKELA, Hille: Webcams, tv shows and mobile phones: empowering exhibitionism, Surveillance & Society, 2004, 2 (2/3): 199–215.

[17] KOSKELA, Hille: žThe gaze without eyes': video-surveillance and the changing nature of urban space, Progress in Human Geography, 2000, 24 (2): 243–265.

[18] KOVAČIĆ, Matej: Zasebnost na internetu, Ljubljana, Mirovni inštitut, 2003.

[19] LYON, David: Globalizing surveillance: Comparative and sociological perspectives, International Sociology, junij 2004, 19 (2): 135–149.

[20] Mc GRAIL, Brian A.: Confronting electronic surveillance: Desiring and resisting new technologies. V: Steve Woolgar (ur.) Virtual society, Oxford University Press, (2002, 115-136).

[21] MLINAR, Zdravko: Prostorska sociologija in planiranje ob vstopanju v informacijsko družbo. V Anton Prosen et al. (ur.), Prostorske znanosti za 21. stoletje: 63–79, Ljubljana, Fakulteta za gradbeništvo in geodezijo, 2004.

[22] MLINAR, Zdravko: Teledelo in prostorsko-časovna organizacija bivalnega okolja, Teorija in praksa, 2003, 40 (6,): 1012–1039.

[23] NEWMAN, Oscar: Defensible space, New York, Macmillan, 1972.

[24] NIETO, Marcus: Public video surveillance: Is it an effective crime prevention tool?, Sacramento, Cal., California Research Bureau, 1997.

[25] NORRIS, Clive, ARMSTRONG, Gary: The maximum surveillance society: The rise of CCTV, 1999.

[26] OC T.: Planning natural surveillance back into city centres, Town and Country Planning, september 1991: 237–239.

[27] Preprečevanje kriminalitete v urbanih okoljih: Priročnik za lokalno samoupravo, Ministrstvo za notranje zadeve RS, Ljubljana, 2003.

[28] ROT, Igor: Video nadzorni sistemi, Sintalček – časopis koncerna Sintal, 2005 (28): 16–17.

[29] SAVKOVIČ, Jana:Video nadzor z vidika varstva osebnih podatkov, Pravna praksa, 2004 (14): X–XVI.

[30] Slovensko sociološko društvo: Varnost in tveganja v sodobni slovenski družbi, Letno srečanje, 2005, Izola.

[31] STANLEY, Jay, STAINHARDT, Barry: Bigger monster, weaker chains: the growth of an American Surveillance Society, (2003), http://www.aclu.org/Files/OpenFile.cfm?id=11572.

[32] TERRASERVER, http: //.terraserver.microsoft.com/ (marec 2006).

[33] TRENCH, Sylvia, OC, Taner, TIESDELL, Steven: Safer cities for women: Perceived risks and plannng measures, TPR, 1992, 63 (3): 279–296.

[34] WOOD, David: People watching people, Surveillance & Society, 2005, 2 (4): 474–478.

[35] WRIGHT, David : The dark side of ambient intelligence, Info, 2005, 7 (6): 33–51.

[36] Zakon o varstvu osebnih podatkov, Uradni list RS, št. 86/04.

Zdravko Mlinar je upokojeni zaslužni profesor sociologije Univerze v Ljubljani in redni član Slovenske akademije znanosti in umetnosti. S svojim delom se je uveljavil kot utemeljitelj prostorske sociologije na raziskovalnem in pedagoškem področju kot tudi v profesionalno-društvenih aktivnostih v slovenskem in mednarodnem merilu. Raziskoval je družbenoprostorske spremembe v mestih in na podeželju in pojasnjeval dolgoročne zakonitosti družbenega razvoja, še zlasti z vidika osamosvajanja (individualizacije) in povezovanja (globalizacije) in glede na vpliv informacijsko-komunikacijske tehnologije. Med njegovimi deli so npr. Developmental Logic of Social Systems (s H. Teunejem) 1978; Humanizacija mesta, 1983; Protislovja družbenega razvoja, 1986; Individualizacija in globalizacija v prostoru, 1994; Globalization and Territorial Identities (ur.), 1992.

PRVA KONFERENCA TEHNOLOŠKE PLATFORME ZA PROGRAMSKO OPREMO IN STORITVE – POMEN PROGRAMSKE OPREME IN STORITEV

Uresničujejo se ambiciozne vizije o povezovanju, delovanju in poslovanju v svetu brez meja, svetu virtualnih organizacij in skupnosti, kjer je znanje glavna dobrina in kjer informacije potujejo s hitrostjo misli, storitve pa so dostopne vsakomur in povsod. V ta namen se v EU vzpostavljajo in delujejo tehnološke platforme, ki so namenjene združevanju in usmerjanju finančnih ter raziskovalno-razvojnih potencialov podjetij ter organizacij z namenom razviti tehnologije in rešitve, potrebne za popolno in dokončno uresničitev omenjene vizije.

Evropska tehnološka platforma, imenovana NESSI (Nessi European Software & Services Initiative), naslavlja področje programske opreme in storitev tako z vidika razvoja infrastrukturnega ogrodja kot z vidika organizacijskih, pravnih in metodoloških osnov, potrebnih za uveljavitev storitveno naravnanega, na znanju temelječega gospodarstva, ki naj bi prispevalo k večji blaginji in kakovosti življenja v informacijski družbi. NESSI (http://www.nessi-europe.com/) v svojem strateškem programu opredeljuje cilje, ki naj bi jih Evropa dosegla na obravnavanem področju do leta 2010 oz. 2020, hkrati pa izvaja aktivnosti, usmerjene k uresničitvi zastavljenega programa tudi v povezavi z drugimi tehnološkimi platformami.

NESSI postavlja svoje raziskovalno-razvojne aktivnosti v evropske dimenzije in odraža celotno vrednostno verigo nove ekonomije znanja, ki jo želimo doseči. Glavna evropska politika razvoja zagovarja izboljšave na področju kakovosti življenja ter povezovanja državljanov s pomočjo informacijsko-komunikacijskih tehnologij. V svojem razvoju želi upoštevati perspektive vseh članov EU, saj mora imeti evropski prebivalec neposredno korist od rasti »ekonomije znanja«, pa naj si bo v vlogi zaposlenega, delodajalca ali zgolj potrošnika vladnih, komercialnih in drugih storitev.

Skladno z evropsko vizijo se je vzpostavila tudi slovenska tehnološka platforma za programsko opremo in storitve, ki želi kot odprt mrežni sistem pospešiti ustvarjanje in širjenje znanja, vpeljavo novih tehnologij v poslovno in osebno življenje ter večanje konkurenčnosti celotnega gospodarstva z lastnostmi, kot so globalizacija in tehnološke inovacije, odprtokodni standardi, povezovanje, uporabniška naravnanost, kontekstno odvisno obnašanje, zasebnost, prilagodljiva tehnologija (prehod iz programiranja v sestavljanje), k uporabniku usmerjeno inženirstvo, multidisciplinarnost ter lažje vključevanje malih podjetij v posamezne segmente razvoja.

Kot eden ključnih principov napredka so opredeljeni odprti standardi in modeli, ki so se uveljavili kot verodostojna pot do kakovostnih programskih komponent, storitev in rešitev. Prilagodljivost in odzivnost poslovnih procesov bo podprta skozi razvoj in uporabo interoperabilnih in odprtih standardov, ki bodo omogočili oblikovanje novega »odprto-storitvenega« tržišča in poenostavitev mednarodnega poslovanja. V prihodnosti bo celoten sistem naklonjen dinamičnemu oblikovanju novih »ekosistemov«, ki bodo ugodni tudi za specializirana mala in srednje velika podjetja (SME), hkrati pa bodo upoštevali in ohranjali značilnosti lokalnih okolij (jezik, kultura, lokalni tržni pogoji).

Skladno s celovito vizijo delovanja platforme NESSI bo v sklopu konkretnih projektov (skupin) članov nacionalne platforme naslovljenih sedem raziskovalnih področij in sicer v povezavi s šestimi principi (slika). Pri tem bo pozornost namenjena infrastrukturni ravni, integraciji storitev in ravni semantike, pa tudi vidikom kot so npr. zaupanje in varnost, kakovost in zanesljivost ter upravljavske storitve. K podpori uresničevanja zastavljenih ciljev bodo oz. so že usmerjeni tudi mehanizmi za spodbujanje raziskav in razvoja, ki jih zagotavljata tako slovenska država kot EU. Ministrstvo za visoko šolstvo, znanost in tehnologijo je letos že objavilo razpis za razvojno-raziskovalne projekte, za katere je zahtevalo njihovo skladnost s strateškimi raziskovalnimi programi, ki so nastali v okviru obstoječih tehnoloških platform. Ministrstvo za visoko šolstvo, znanost in tehnologijo je že lansko leto prek javnega razpisa podprlo vzpostavitev tehnoloških platform, kar bo nadaljevalo tudi letos – tako za obstoječe kot tudi za nove platforme s področja informacijsko-komunikacijske tehnologije, kot je NESSI. Prav tako so bile tehnološke platforme tako ali drugače že vključene tudi v letošnje javne razpise Ministrstva za gospodarstvo.

Na prvi konferenci nacionalne tehnološke platforme za programsko opremo in storitve, ki je v organizaciji Inštituta za informatiko potekala v prostorih Fakultete za elektrotehniko, računalništvo in informatiko v Mariboru 12. junija 2006, so sodelovali tudi pomembni predstavniki evropske komisije in evropske platforme NESSI, kar dokazuje in zagotavlja, da bo Slovenija s svojim znanjem in dosežki tudi tokrat aktivna udeleženka v procesu uresničitve skupnih, ne le evropskih, temveč tudi globalnih vizij in ciljev, povezanih z informacijsko družbo – družbo znanja.

V svojem uvodnem nagovoru je predstavnik Ministrstva za visoko šolstvo, znanost in tehnologijo, podsekretar mag. Samo Zorc, poudaril pomen področja razvoja tehnologij, produktov in storitev s področja informacijsko-komunikacijske tehnologije, ki predstavlja bistveni element za nadaljnji uspešen razvoj informacijske družbe. Le združevanje razvojnih potencialov, v katera so lahko vključena tudi mala inventivna podjetja, bo omogočalo razvoj novih e-storitev, aplikacij in izdelkov, ki bodo tako lahko konkurenčna na globalnem trgu. Slovenija se lahko v tovrstna svetovna gibanja vključi le z učinkovitim izkoriščanjem svojega znanja, izkušenj in raziskovalno-razvojnih potencialov, predvsem z agilnostjo in inovativnostjo.

Na konferenci je sodeloval tudi predstavnik EU, vodja enote »Software technologies« na direktoratu za informacijsko družbo in medije, g. Villasante. V svoji predstavitvi »The Software and Services Challenge« je zmožnost razvoja programske opreme in storitev opredelil kot ključno dobrino informacijske družbe. Tudi zato bo v evropskih programskih dokumentih za naslednje obdobje raziskavam in razvoju na področjih, ki jih naslavlja NESSI, dodeljena še večja pozornost in pomen. Programska oprema in storitve namreč predstavljajo enega ključnih faktorjev za vsa tri prioritetna področja EU – enotni evropski informacijskih prostor, inovacije in investicije v raziskave ter e-vključenost.

Predsednik slovenske platforme, dr. Domajnko, je predstavil pomen programske opreme in storitev v luči lizbonske strategije in strategije i2010 v luči transformacije slovenskega (in evropskega) gospodarstva v smeri dinamične, konkurenčne in na znanju temelječe ekonomije. Pomen in prispevek tehnološke platforme se bo odražal predvsem v oblikovanju novih delovnih mest za visoko izobraženo delovno silo, dolgoročnem načrtovanju nadaljnjega razvoja panoge v smislu sodelovanja med gospodarstvom in univerzami, oblikovanju prioritet in doseganju potrebnega konsenza zanje, vzpostavitvi ustrezne razvojno-raziskovalne infrastrukture ter v vključevanju in soustvarjanju skupne razvojne strategije EU za področje programske opreme in storitev.

Predstavnik evropske platforme NESSI, Jose M. Cavanillas, podpredsednik izvršilnega odbora evropske platforme NESSI, je opredelil vlogo nacionalnih tehnoloških platform in izrazil zadovoljstvo z intenzivnostjo aktivnosti in rezultati dela slovenske tehnološke platforme. Udeležencem in slovenskim podjetjem je namenil poziv in spodbudo v svoji sklepni ugotovitvi, da ni ovir, da ne bi tudi na področju programske opreme in storitev postali eni izmed ključni akterjev tudi v svetovnem merilu. Ne nazadnje je g. Cavanillas že na generalni skupščini NESSI v Bruslju 8. junija 2006 ob španski nacionalni platformi izpostavil slovensko tehnološko platformo za programsko opremo in storitev kot primer izjemno aktivne in agilne nacionalne platforme.

Strokovni koordinator tehnološke platforme za programsko opremo in storitve dr. Marjan Heričko je podrobneje predstavil strateški razvojni program nacionalne platforme, dosedanje aktivnosti, načela organiziranosti in plan dela za prihodnje obdobje. Sledile so predstavitve predstavnikov podjetij; g. Smekar iz družbe Hermes Softlab, d. d., je predstavil izkušnje pri izvozu znanja ter priložnosti in pasti pri delovanju na globalnem trgu, g. Dolenc iz podjetja IskraTel je opisal vizijo in prednosti oblikovanja ekosistema razvojnih potencialov in podjetij, ki lahko tako s skupnimi močmi dosežejo preboj na globalnem trgu. Pozitivne izkušnje malih podjetij pri sodelovanju v evropskih raziskovalnih projektih je predstavil mag. Gregor Pipan iz podjetja XLAB, d. o. o., ki je vključeno v štiri projekte šestega okvirnega programa. Predvsem je poudaril pomen naložb v nova znanja in razvoj inovativnih programskih rešitev ter izpostavil dejstvo, da so nepovratna sredstva cenejša od kredita. Dr. Korošec iz Nove KBM je predstavil odličen primer inovativnega medpanožnega povezovanja storitev na primeru integracije storitev mobilnega operaterja ter bančnega sektorja.

Na podlagi storitvenih platform, ogrodij, tehnologij in metodoloških pristopov, ki bodo rezultat razvojno-raziskovalnih aktivnosti članov NESSI, bodo te lahko v prihodnje razširjene in dopolnjene še s storitvami drugih področij, kot so npr. storitve elektronskega sklepanja in overjanja pogodb, zavarovalniške storitve ter storitve e-uprave.

Prva konferenca tehnološke platforme za programsko opremo in storitve se je zaključila z okroglo mizo, na kateri so predstavniki nacionalne platforme skupaj z uglednimi gosti iz tujine skušali identificirati priložnosti in izzive, povezane s sodelovanjem slovenskih akterjev v evropski platformi NESSI ter transformacijo evropskega gospodarstva v storitveno, na znanju temelječo družbo. Več informacij o prvi konferenci, na kateri je sodelovalo skoraj sto udeležencev, je na voljo na *http://nessi-slovenia.com*.

Katera so strateška področja?

Februarja in marca 2006 so na Gospodarski zbornici Slovenije potekale delavnice, na katerih so sodelovali posamezniki, ki v slovenskih podjetjih in organizacijah skrbijo za raziskovalno-razvojne usmeritve. V razpravi in kritični presoji strategij in usmeritev razvoja posameznih akterjev na področju programske opreme in storitev v Sloveniji smo identificirali sedem strateških področij raziskav, ki so predstavljena v stolpiču na sliki. Njihov podrobni opis je objavljen v strateškem razvojnem programu *(http://nessi-slovenia.com)*. Svoj interes za aktivno vključenost v delovanje slovenske tehnološke platforme za programsko opremo in storitve je doslej izrazilo že več kot štirideset slovenskih podjetij, organizacij in institucij, ki aktivno sodelujejo pri raziskavah in razvoju na predstavljenih strateških področjih oz. se še nameravajo pridružiti tem aktivnostim.

Strateška področja raziskav slovenske TP za programsko opremo in storitve ter principi, na katerih temeljijo

Poslanstvo

Slovenska tehnološka platforma za programsko opremo in storitve, povezana z evropsko platformo NESSI, predstavlja odprto mesto združevanja znanj, strategij in potencialov za hitrejši razvoj mednarodno konkurenčne in prodorne panoge. Vplivali bomo na večjo povezljivost in globalno dostopnost e-storitev ter na hitrejše vpeljevanje raziskovalnih spoznanj in novih tehnologij v poslovno in zasebno življenje.

Marjan Heričko,
strokovni koordinator tehnološke
platforme za programsko opremo in storitve

POSLOVNA KONFERENCA
MENEDŽMENT POSLOVNIH PROCESOV – MPP 2006

Kako do konkurenčnega gospodarstva in uprave

Informacija in vabilo avtorjem prispevkov

Konferenca Kako do konkurenčnega gospodarstva in uprave bo potekala v organizaciji Inštituta za poslovno informatiko pri Ekonomski fakulteti v Ljubljani in soorganizatorjev ter pod pokroviteljstvom Ministrstva RS za gospodarstvo in Ministrstva RS za javno upravo 30. novembra in 1. decembra 2006 v hotelu Mons v Ljubljani. Tema konference je usmerjena v vprašanja upravljanja sprememb in prenovo poslovanja ter zagotavljanja uspešnosti in konkurečnosti gospodarstva in uprave. Namen konference je obravnava ključnih dejavnikov sprememb poslovanja v slovenskih podjetjih in upravi ter možnosti in priložnosti, ki jih v praksi na tem področju nudijo sodobni metodološki pristopi in orodja.

Cilj konference in ciljna tematska področja

Cilj poslovne konference je izmenjava izkušenj o upravljanju sprememb oz. razvoju poslovnih strategij in novih poslovnih modelov ter uvajanju poslovnih procesov in njihovi informatizaciji. Na konferenci bodo obravnavani primeri projektov ki so se dokazali v praksi in neposredno vplivajo na povečanje konkurenčnosti in uspešnosti slovenskega gospodarstva in uprave.

Ciljna tematska področja konference so:

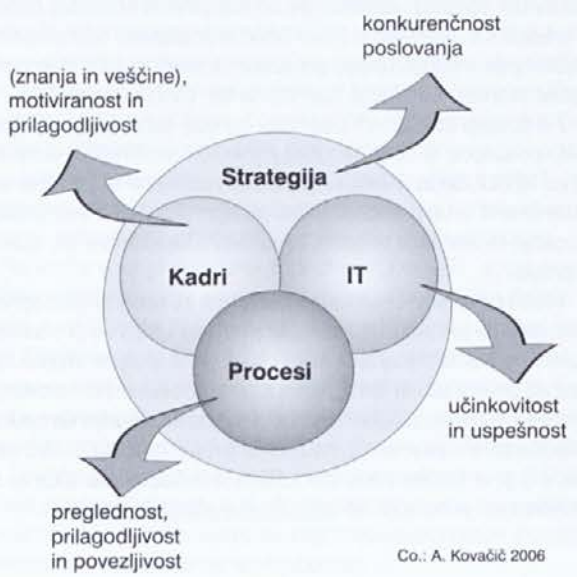
- Poslovna strategija in poslovni modeli, konkurenčnost poslovanja
- Upravljanje sprememb
- Menedžment poslovnih procesov (celovita prenova poslovanja, modeliranje in prenova poslovnih procesov idr.)
- Upravljanje kakovosti
- Primerjanje značilnosti (Benchmarking)
- Menedžment kadrov
- Menedžment znanja
- Organizacija poslovanja in poslovnih procesov
- Informatizacija poslovanja, celovite programske rešitve (ERP), krmiljenje procesov (WF)
- Elektronsko poslovanje in medorganizacijsko povezovanje
- Metode in orodja strateškega načrtovanja, analiziranja in spremljanja poslovanja ter izvajanja sprememb

Upravljanje sprememb in prenova poslovanja

Zahteva po uspešnosti poslovanja in zagotavljanju konkurenčnosti v vse bolj dinamičnem poslovnem okolju je povezana s prilagajanjem, ponekod tudi s korenito spremembo poslovne strategije, poslovnega modela in poslovnih procesov. Projekti upravljanja sprememb oz. zastavljenih strateških ciljev zahtevajo temeljito in sprotno koordinirano delovanje in spreminjanje ključnih dejavnikov sprememb poslovanja: ljudi (kadrov), poslovnih procesov in informacijske tehnologije (IT).

Poslovni procesi so pogojeni in skladni z dejavnostjo poslovanja podjetja, vendar so pogosto razdrobljeni in skriti za organizacijskimi strukturami zaradi obremenjenosti podjetij s funkcijsko/oddelčno naravnanim načinom poslovanja. Zaradi tega prihaja do tako imenovanih funkcijskih silosov, ki zavirajo ali omejujejo neoviran potek poslovnih procesov. Vodje posameznih organizacijskih enot zasledujejo svoj lokalni optimum izvajanja poslovnega procesa, kar pa največkrat ni optimum poslovanja celotnega podjetja. Prenova poslovnih procesov zahteva temeljit vnovični premislek o poslovnih procesih in njihovo korenito preoblikovanje, da bi dosegli njihovo preglednost, prilagodljivost in povezljivost ter izboljšali ključne kazalnike učinkovitosti, kot so stroški, kakovost storitev in hitrost izvajanja. Naloga prenove poslovnih procesov je izbrati, usposobiti ali izumiti poslovni proces, da bi z njim zadovoljili potrebe zaposlenih v podjetju in zunanje partnerje.

Informacijska tehnologija (IT, informatika) pomeni ključno tehnologijo in ima najpomembnejšo vlogo pri prenovi poslovnih procesov, vendar zgolj z njenim vključevanjem v avtomatizacijo posameznih postopkov največkrat dosežemo, globalno gledano, slabe, če ne celo negativne rezultate. Od informatike oziroma uporabe sodobne informacijske tehnologije pričakujemo dvig kakovosti, znižanje stroškov in skrajševanje časa izvajanja tako ugotovljenih poslovnih postopkov oziroma posameznih aktivnosti v njih. Razprave o tem, kakšna je dejanska vrednost in pomen informatike v podjetju, so vse pogostejše tako v akademskih kot v poslovnih krogih. Po eni strani smo bili vse do leta 2002 priča neprestani rasti naložb v informatiko, ki so v razvitih zahodnih državah dosegle 5–7 odstotkov vrednosti prihodkov, z namenom povečevanja poslovne uspešnosti in konkurenčne prednosti. Po drugi strani pa so se vzporedno pojavljale razne raziskave, na podlagi katerih je moč sklepati, da naložbe v informatiko vplivajo zgolj na učinkovitost, nimajo pa želenega vpliva na uspešnost poslovanja. Ne glede na različne poglede ugotavljamo, da naložbe v informatiko v naših srednjih in večjih podjetjih v povprečju še vedno ne presegajo dveh odstotkov (raziskava EF IPI, 2005).



Kljub novemu, drugačnemu pogledu na poslovne procese in možnosti, ki jih daje sodobna informacijska tehnologija pa prenova poslovanja sloni in je odvisna tudi od načina organiziranja človeških virov. V boju za konkurenčnost poslovanja so edino trajno konkurenčno orožje podjetja njegovi zaposleni. **Človeške vire/kadre** kot dejavnik prenove obravnavamo predvsem s stališča možnosti povečanja razpoložljivosti (motiviranosti), prilagodljivosti in produktivnosti obstoječih kadrovskih potencialov. Prednost pri prenovi poslovanja in izvajanju sprememb imajo kadri, ki so širše izobraženi, imajo poslovna znanja in razumejo vlogo poslovnih procesov ter znajo neposredno uporabljati sodobno informacijsko tehnologijo.

Ko se podjetje loti prenove poslovanja, mora razen o racionalizaciji, standardizaciji, poenostavitvi in informatizaciji poslovnih procesov najprej razmišljati o strateških vidikih, ki omogočajo uspešno in učinkovito izvajanje prenovljenih procesov. Gre predvsem za pripravljenost podjetja in zaposlenih na spremembe, menedžment in uvajanje teh sprememb ter zagotavljanje znanj, veščin, pogojev, orodij in tehnologije, potrebnih za udejanjanje sprememb oz. prenove poslovanja. Prenove poslovanja torej ne gre obravnavati le s stališča kadrovskih in organizacijskih sprememb ali samo uvedbe sodobne informacijske tehnologije. Oboje je zlasti pri nas kar pogosta praksa.

Projekti prenove poslovanja se v podjetjih začnejo najpogosteje kot odgovor menedžmenta na ključna vprašanja poslovne uspešnosti oziroma vprašanja o načinu in predmetu poslovanja (ali proizvajamo prave izdelke in/ali nudimo prave storitve). Cilj projektov je doseči konkurenčno enakost ali prednost pred tistimi, ki so doslej postavljali pravila in standarde (best in class), ali pa spremeniti poslovna pravila in ustvariti novo opredelitev najboljšega v panogi (breakpoints). V obeh primerih potekajo takšni projekti ob uporabi in uvajanju informacijske tehnologije v poslovni proces s ciljem zagotavljanja konkurenčne prednosti. Ker prenova poslovanja zahteva korenite spremembe v poslovanju organizacij, morajo biti pred njenim začetkom izpolnjeni nekateri pogoji. Menedžment mora najprej zavreči neuporabna (uveljavljena) poslovna pravila in postopke, ki jih je upoštevalo pri poslovanju. Po drugi strani je treba opustiti tudi neprimerna organizacijska in izvedbena načela in modele. Šele tedaj je mogoče začeti vnovično načrtovanje organizacije. Menedžment mora upoštevati spremenjeno poslovno vlogo in strateške cilje, ko opredeljuje in oblikuje strategijo organizacije in si prizadeva tudi praktično izpeljati prenovo postopkov. Gre za projekt, ki je usmerjen v korenite spremembe poslovanja organizacije. Poteka ne glede na obstoječe organizacijske pregrade med funkcionalnimi celotami in sodi med projekte z visoko stopnjo tveganja.

Podobno je tudi prenova poslovanja uprave usmerjena v radikalno spremembo načina in mehanizmov funkcioniranja države, zmanjšanje obsega in pomembnosti birokracije ter opuščanje starega načine razmišljanja in ravnanja. E-uprava zahteva spremembo obstoječih organizacijskih in poslovnih modelov, poslovnih procesov in postopkov ter poslovnih pravil. Nova doktrina e-uprave predpostavlja in pogojuje uporabo informacijske tehnologije in telekomunikacijske infrastrukture, ki omogočata upravi na strateški ravni razvijanje njene vizije in poslanstva, na taktični oziroma izvedbeni ravni pa udejanjanje te vizije z izvajanjem poslovnih procesov oziroma ponujanjem storitev svojim uporabnikom (organizacijam, občanom). Uspešne dežele bodo zato, da bi dosegle večjo poslovno učinkovitost in uspešnost, v prihodnjih nekaj letih korenito preuredile in prenovile poslovne procese ter tehnološko infrastrukturo javnega sektorja.

Zakaj torej takšna konferenca pri nas?

Prenova poslovanja zahteva temeljit vnovični premislek o poslovnih procesih in njihovo korenito preoblikovanje, da bi dosegli velike izboljšave ključnih poslovnih kazalnikov, kot so stroški, kakovost izdelkov ali storitev in hitrost. Naloga prenove poslovanja je izbrati, usposobiti ali izumiti poslovni proces, da bi z njim zadovoljili potrebe zaposlenih v podjetju in zunanje partnerje.

Tudi v naši vsakdanji praksi pogosto naletimo na ugotovitev, da postajajo spremembe edina stalnica v poslovanju organizacije. Večina organizacij jemlje to resnico preveč z lahkoto ali kot nujno zlo, temu primerne so tudi težave pri vpeljevanju sprememb. Glavna problema v tem procesu sta pomanjkanje aktivnega sodelovanja in pomoči nadrejenih v organizaciji ter odsotnost močnega vodstva in lastnikov. V organizaciji obstajajo skupine, ki različno gledajo na spremembe. Pobudniki sprememb največkrat dosežejo začetno podporo le ožje skupine. Od tega, kako predstavijo pomen sprememb za organizacijo večini, je odvisna mobilizacija teh ljudi. Najtrši nasprotniki se največkrat sploh ne pustijo prepričati, zato je toliko bolj pomembna podpora kritične mase zaposlenih.

Tudi percepcija in ravnanje menedžerjev na področju informatike sta navadno stroškovno naravnana. Od informatike v večini primerov pričakujejo večjo učinkovitosti in preglednosti izvajanja poslovnih procesov, poslovna uspešnost pa je drugotnega pomena ali pa po njihovem mnenju težko dosegljiva ali celo nedosegljiva. Odgovor na vprašanje o poslovni vrednosti informacijske tehnologije ni zgolj v informatizaciji, temveč predvsem v njeni vključitvi v proces prenove poslovanja (kadri in znanja, poslovna pravila, informacije in informacijska tehnologija ter organiziranost in poslovna kultura) in prenove poslovnih procesov podjetja.

Michael Hammer, »oče« prenove (reinženiringa) poslovanja pravi, da sta dve tretjini poskusov prenove poslovanja, s katerimi se je srečal, izpuhteli v plamenih, zatrti zaradi odpora ljudi, da bi sledili, in zaradi nesposobnosti višjega menedžmenta ter strahu srednjega menedžmenta, da bi do spremembe dejansko prišlo. Ocenjujemo, da je pri nas več kot polovica projektov prenove poslovanja neuspešnih. To so primeri, ko je projekt zaradi nedoseganja ciljev predhodno prekinjen, ko zastavljenih ciljev nikoli ne doseže, tudi ko nekajkrat prekorači načrtovane časovne in stroškovne parametre. Kje so vzroki?

Tveganje za uspešno izvedbo projekta prenove poslovanja organizacije je visoko, veliko je odprtih vprašanj in dilem, pa tudi praktičnih izkušenj. Več kot utemeljen razlog za konferenco, ki bo obravnavala probleme in rešitve:

- upravljanja sprememb in prenova poslovanja v podjetjih,
- upravljanja sprememb in prenova poslovanja v upravi ter
- metode in orodja za upravljanje sprememb in prenovo poslovanja.

Vabimo vas, da se udeležite konference. Avtorje, ki bi želeli predstaviti na konferenci svoje ugotovitve, predvsem pa praktične izkušnje, vabimo, da svojo prijavo, povzetek prispevka na eni strani formata A4 in življenjepis pošljete po elektronski pošti na naslov *mpp@ef.uni-lj.si*.

Dr. Andrej Kovačič,
predsednik programskega odbora konference

Pristopna izjava

Želim postati član Slovenskega društva INFORMATIKA

Prosim, da mi pošljete položnico za plačilo članarine 8.040 SIT (33,55 €) (kot študentu 3.480 SIT) (14,52 €)) in me sproti obveščate o aktivnostih v društvu. V članarini je upoštevan DDV v višini 20 %.

(ime in priimek, s tiskanimi črkami)

(poklic)

(domači naslov in telefon)

(službeni naslov in telefon)

(elektronska pošta)

Datum: Podpis:

Članarina 8.040 SIT vključuje revijo Uporabna informatika. Študenti imajo posebno ugodnost: plačujejo članarino 3.480 SIT (3.480 €) in za to prejemajo tudi revijo.
Cene v evrih so informativne; izračunane so po centralnem paritetnem tečaju 1 € = 239,640 SIT.
Izpolnjeno naročilnico ali pristopno izjavo pošljite na naslov:
Slovensko društvo INFORMATIKA, Vožarski pot 12, 1000 Ljubljana

Lahko pa izpolnite obrazec na domači strani društva: **http://www.drustvo-informatika.si**

Naročilnica na revijo UPORABNA INFORMATIKA

Revijo naročam(o)
- ☐ s plačilom letne naročnine 8.000 SIT (33,81 €)
- ☐ izvodov po pogojih za podjetja 20.000 SIT (83,46 €) za eno letno naročnino in 14.000 SIT (58,48 €) za vsako nadaljnjo naročnino
- ☐ po pogojih za študente letno 3.500 SIT (14,61 €)

V cenah je upoštevan DDV v višini 8,5 %.

(ime in priimek, s tiskanimi črkami)

(podjetje) (davčna številka)

(ulica, hišna številka)

(pošta)

Datum: Podpis:

Naročnino bomo poravnali najkasneje v roku 8 dni po prejemu računa.
Cene v evrih so informativne; izračunane so po centralnem paritetnem tečaju 1 € = 239,640 SIT. Izpolnjeno naročilnico ali pristopno izjavo pošljite na naslov:

INTERNET

Vse bralce revije obveščamo, da lahko najdete domačo stran društva na naslovu: **http://www.drustvo-informatika.si**
Obiščite tudi spletne strani mednarodnih organizacij, v katere je včlanjeno naše društvo: IFIP: **www.ifip.or.at** ECDL: **www.ecdl.com** CEPIS: **www.cepis.com**

SLOVENSKO DRUŠTVO INFORMATIKA

PREGLED PODELJENIH PRIZNANJ SDI

	Leto	Ime in priimek	Obrazložitev
1.	1994	Tomaž Banovec	Za organizacijski prispevek k razvoju slovenske informatike in oživitvi delovanja Slovenskega društva INFORMATIKA
2.	1994	dr. Ferdinand Mam	Kot starosti slovenskih informatikov za življenjsko delo in prispevek k razvoju slovenske informatike
3.	1994	mag. Katarina Puc	Za strokovni prispevek k tehničnemu urejanju revije Uporabna informatika in organizacijski prispevek k pripravi posvetovanja Dnevi slovenske informatike '94
4.	1995	dr. Janez Grad	Za življenjsko delo na področju razvoja in uveljavitve informatike v Sloveniji
5.	1995	dr. Andrej Kovačič	Za uspehe pri prenašanju teoretičnih spoznanj v izobraževanje in podjetništvo
6.	1995	dr. Mirko Vintar	Za popularizacijo informatike in posebej za ustanovitev revija Uporabna informatika
7.	1996	Franc Košir	Za dosežke na področju informatizacije storitev zdravstvenega zavarovanja
8.	1996	Niko Schlamberger	Za prispevek k delovanju društva in za dosežke pri uveljavljanju teoretičnih spoznanj v praksi
9.	1996	dr. Ivan Rozman	Za trajno uspešno in vidno znanstveno delo na področju informatike
10.	1997	dr. Vladislav Rajkovič	Za dolgoletno uspešno delo na področju informatike v izobraževanju
11.	1997	Marin Silič	Za dosežke pri informatizaciji državnih organov
12.	1997	Stane Štefančič	Za uspešno uvajanje novih metod pri prenovi informacijskih sistemov
13.	1998	Ljubica Djordjević	Za trajni prispevek k delovanju SDI
14.	1998	dr. Ivan Vezočnik	Za uspehe pri uveljavljanju metodologij informatike v praksi in za prispevek k vidnosti in delovanju SDI
15.	1999	dr. Matjaž Gams	Za razvoj slovenskega izrazoslovja na področju informatike
16.	1999	dr. Marjan Krisper	Za dosežke v prenosu teoretičnih spoznanj v poslovna okolja
17.	1999	dr. Anton Železnikar	Za mednarodno uveljavitev slovenskih dosežkov v informatiki
18.	2000	dddr. Viljem Rupnik	Za prispevek k mednarodni uveljavitvi slovenskih dosežkov na področju operacijskih raziskovanj in teoretične prispevke
19.	2001	mag. Peter Jermol	Za dosežke pri informatizaciji delovanja in zakonodajnega postopka Državnega zbora
20.	2001	Oracle Software	Za trajno sodelovanje s Slovenskim društvom INFORMATIKA
21.	2001	Telekom Slovenije	Za prispevek k vidnosti Slovenskega društva INFORMATIKA
22.	2002	dr. Jože Gričar	Za prispevek k teoriji in praksi elektronskega poslovanja
23.	2002	Mobitel, d. d.	Za trajno sodelovanje in prispevek k vidnosti SDI
24.	2002	Genis, d. o. o.	Za dosežke pri prenosu teoretičnih spoznanj v prakso
25.	2003	dr. Lidija Zadnik Stirn	Za uspešno vodenje sekcije za operacijske raziskave, organiziranje mednarodnih posvetovanje SOR in vključevanje v dejavnosti društva
26.	2003	Marand, d. o. o.	Za trajno pokroviteljstvo dejavnosti društva: finančno in organizacijsko podporo posvetovanja DSI, revije Uporabna informatika in domačih strani društva
27.	2004	prof. dr. Ivan Meško	Za dosežke pri razvoju metod s področja operacijskih raziskav in za delovanje v Sekciji za operacijske raziskave od začetka delovanja te sekcije
28.	2004	dr. Mojca Indihar Štemberger	Za uspešno delo v društvu, posebej za njen prispevek h kakovosti organizacije in izvedbe posvetovanj Dnevi slovenske informatike v letih 2002 - 2004
29.	2004	Infos, d. o. o.	Za uspešno sodelovanje z društvom pri organizaciji posvetovanja Dnevi slovenske informatike, s čimer se je povečala vidnost posvetovanja v zadnjih 3 letih, in za prireditev INFOS kot prispevek k vidnosti informatike nasploh
30.	2005	Franc Žerdin	Za uspešno uvedbo evropskega računalniškega spričevala ECDL v Slovenijo
31.	2005	dr. Jurij Jaklič	Za razvoj in uvedbo informacijskih rešitev v prakso in posebej za dosežek pri omrežni izvedbi terminološkega slovarja Islovar
32.	2005	dr. Vladimir Batagelj	Za znanstvenoraziskovalno delo na področju informatike in posebej za uvajanje informatike v izobraževanje
33.	2005	Statistični urad Republike Slovenije	Za trajno in uspešno sodelovanje z društvom
34.	2006	dr. Tatjana Welzer Družovec	Za dosežke v pedagoško-znanstvenem delu in uporabni informatiki
35.	2006	Marjana Kajzer Nagode	Za uspehe pri uvajanju ECDL v Sloveniji
36.	2006	Ixtlan Team, d. o. o.	Za razvoj informacijskih sistemov v javni upravi
37.	2006	prof. dr. Klaus Brunnstein	Za dolgoletno naklonjenost in sodelovanje pri razvoju informatike v Sloveniji.
38.	2006	IFIP TC9 "Relationship between Computers and Society"	Ob 30-letnici ustanovitve in za trajno sodelovanje s SDI, še posebej ob izvedbi konference HCC7 v Mariboru

ISSN 1318-1882

9 771318 188001