2018 ‹ ŠTEVILKA 1 ‹ JAN. FEB. MAR. ‹ LETNIK XXVI ‹ ISSN 1318-1882

01 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 Fundation, v Sloveniji pa je kot član CEPIS (Council of European Professional Informatics) 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. Posebno pomembno je, da velja spričevalo v 148 državah, ki so vključene v program ECDL. Doslej je bilo v svetu izdanih že več kot 11,6 milijona indeksov, v Sloveniji več kot 17.000, in podeljenih več kot 11.000 spričeval. Za izpitne centre v Sloveniji je usposobljenih osem organizacij, katerih logotipe objavljamo.

AGORA

LJUDSKA UNIVERZA MURSKA SOBOTA

ŠOLSKI CENTER Novo mesto

spin

ISER

LJUDSKA UNIVERZA CELJE
Cankarjeva ulica 1, 3000 Celje, Slovenija
Telefon:(03) 428-67-50 Telefax: (03) 428-67-58

ACADEMIA

Micro Team

U P O R A B N A
I N F O R M A T I K A
2018 ŠTEVILKA 1 JAN/FEB/MAR LETNIK XXVI ISSN 1318-1882

Znanstveni prispevki

Strokovni prispevki

Informacije

U P O R A B N A
I N F O R M A T I K A

2018 ŠTEVILKA 1 JAN/FEB/MAR LETNIK XXVI ISSN 1318-1882

Ustanovitelj in izdajatelj
Slovensko društvo INFORMATIKA
Litostrojska cesta 54, 1000 Ljubljana

Predstavnik
Niko Schlamberger

Odgovorni urednik
Saša Divjak

Tehnični urednik
Slavko Žitnik

Lektoriranje
Mira Turk Škraba (slov.)
Marvelingua (angl.)

Oblikovanje
KOFEIN DIZAJN, d. o. o.

Prelom in tisk
Boex DTP, d. o. o., Ljubljana

Naklada
100 izvodov

Naslov uredništva
Slovensko društvo INFORMATIKA
Uredništvo revije Uporabna informatika
Litostrojska cesta 54, 1000 Ljubljana
www.uporabna-informatika.si

Revija izhaja četrtletno. Cena posamezne številke je 20,00 EUR. Letna naročnina za podjetja 85,00 EUR, za vsak nadaljnji izvod 60,00 EUR, za posameznike 35,00 EUR, za študente in seniorje 15,00 EUR. V ceno je vključen DDV.

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 RS.

Revija Uporabna informatika je vključena v Digitalno knjižnico Slovenije (dLib.si).

Vabilo avtorjem

V reviji Uporabna informatika objavljamo kakovostne izvirne članke domačih in tujih avtorjev z najširšega področja informatike v poslovanju podjetij, javni upravi in zasebnem življenju na znanstveni, strokovni in informativni ravni; še posebno spodbujamo objavo interdisciplinarnih člankov. Zato vabimo avtorje, da prispevke, ki ustrezajo omenjenim usmeritvam, pošljejo uredništvu revije po elektronski pošti na naslov ui@drustvo-informatika.si.

Avtorje prosimo, da pri pripravi prispevka upoštevajo navodila, objavljena v nadaljevanju ter na naslovu http://www.uporabna-informatika.si.

Za kakovost prispevkov skrbi mednarodni uredniški odbor. Članki so anonimno recenzirani, o objavi pa na podlagi recenzij samostojno odloča uredniški odbor. Recenzenti lahko zahtevajo, da avtorji besedilo spremenijo v skladu s priporočili in da popravljeni članek ponovno prejmejo v pregled. Uredništvo pa lahko še pred recenzijo zavrne objavo prispevka, če njegova vsebina ne ustreza vsebinski usmeritvi revije ali če članek ne ustreza kriterijem za objavo v reviji.

Pred objavo članka mora avtor podpisati izjavo o avtorstvu, s katero potrjuje originalnost članka in dovoljuje prenos materialnih avtorskih pravic. Nenaročenih prispevkov ne vračamo in ne honoriramo. Avtorji prejmejo enoletno naročnino na revijo Uporabna informatika, ki vključuje avtorski izvod revije in še nadaljnje tri zaporedne številke.

S svojim prispevkom v reviji Uporabna informatika boste prispevali k širjenju znanja na področju informatike. Želimo si čim več prispevkov z raznoliko in zanimivo tematiko in se jih že vnaprej veselimo.

Uredništvo revije

Navodila avtorjem člankov

Članke objavljamo praviloma v slovenščini, članke tujih avtorjev pa v angleščini. Besedilo naj bo jezikovno skrbno pripravljeno. Priporočamo zmernost pri uporabi tujk in – kjer je mogoče – njihovo zamenjavo s slovenskimi izrazi. V pomoč pri iskanju slovenskih ustreznic priporočamo uporabo spletnega terminološkega slovarja Slovenskega društva Informatika Islovar (www.islovar.org).

Znanstveni članek naj obsega največ 40.000 znakov, strokovni članki do 30.000 znakov, obvestila in poročila pa do 8.000 znakov.

Članek naj bo praviloma predložen v urejevalniku besedil Word (*.doc ali *.docx) v enojnem razmaku, brez posebnih znakov ali poudarjenih črk. Za ločilom na koncu stavka napravite samo en prazen prostor, pri odstavkih ne uporabljajte zamika.

Naslovu članka naj sledi za vsakega avtorja polno ime, ustanova, v kateri je zaposlen, naslov in elektronski naslov. Sledi naj povzetek v slovenščini v obsegu 8 do 10 vrstic in seznam od 5 do 8 ključnih besed, ki najbolje opredeljujejo vsebinski okvir članka. Pred povzetkom v angleščini naj bo še angleški prevod naslova, prav tako pa naj bodo dodane ključne besede v angleščini. Obratno velja v primeru predložitve članka v angleščini.

Razdelki naj bodo naslovljeni in oštevilčeni z arabskimi številkami.

Slike in tabele vključite v besedilo. Opremite jih z naslovom in oštevilčite z arabskimi številkami. Vsako sliko in tabelo razložite tudi v besedilu članka. Če v članku uporabljate slike ali tabele drugih avtorjev, navedite vir pod sliko oz. tabelo. Revijo tiskamo v črno-beli tehniki, zato barvne slike ali fotografije kot original niso primerne. Slik zaslonov ne objavljamo, razen če so nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme ipd. naj imajo belo podlago. Enačbe oštevilčite v oklepajih desno od enačbe.

V besedilu se sklicujte na navedeno literaturo skladno s pravili sistema APA navajanja bibliografskih referenc, najpogosteje torej v obliki (Novak & Kovač, 2008, str. 235). Na koncu članka navedite samo v članku uporabljeno literaturo in vire v enotnem seznamu po abecednem redu avtorjev, prav tako v skladu s pravili APA. Več o sistemu APA, katerega uporabo omogoča tudi urejevalnik besedil Word 2007, najdete na strani http://owl.english.purdue.edu/owl/resource/560/01/.

Članku dodajte kratek življenjepis vsakega avtorja v obsegu do 8 vrstic, v katerem poudarite predvsem strokovne dosežke.

Ocena učinkovitosti prenove procesa na podlagi strukture procesa

Benjamin Urh, Eva Krhač, Matjaž Roblek, Tomaž Kern
Univerza v Mariboru, Fakulteta za organizacijske vede, Kidričeva 55a, 4000 Kranj
benjamin.urh@fov.uni-mb.si; eva.krhac1@um.si; matjaz.roblek@um.si; tomaz.kern@um.si

Izvleček

V prispevku predstavljamo ocenjevanje učinkovitosti izvajanja poslovnih procesov s pomočjo kazalnikov strukturne učinkovitosti. To metodo lahko uporabimo kot alternativo ocenjevanju učinkovitosti izvajanja poslovnih procesov s kazalniki operativne učinkovitosti. Z vidika porabe časa in/ali vidika nastalih stroškov lahko učinkovitost procesa ocenimo, ko je proces že vzpostavljen oz. implementiran v podjetje, s predstavljeno metodo pa lahko učinkovitost izvajanja poslovnega procesa preverimo že v fazi oblikovanja modela novega ali prenovljenega procesa. V tem primeru je za oceno učinkovitosti namreč potreben le ustrezen model prenovljenega poslovnega procesa. Uporabnost metode smo prikazali na primeru prenove procesa v enem izmed slovenskih podjetij.
Ključne besede: prenova procesov, kazalniki strukturne učinkovitosti, kazalniki operativne učinkovitosti, učinkovitost prenove procesov.

Abstract

Assessment of business process redesign efficiency based on process structure

In this paper, we discuss business process performance efficiency assessment based on structural efficiency indicators. This method can be used as an alternative to process performance efficiency assessment based on operational efficiency indicators. Business process efficiency can be assessed against time and/or incurred costs only when the process has already been established or implemented in a company. With the presented method, business process efficiency can already be verified during the renewed process design stage. In this case, only an appropriate model of a renewed business process is needed to assess efficiency. The applicability of the method was demonstrated on a process renovation case in a Slovenian company.
Keywords: process re-engineering, structural efficiency indicators, operational efficiency indicators, process re-engineering efficiency.

1 UVOD

Poslovni procesi so povezava aktivnosti posameznika, informacijske tehnologije, poslovnih pravil in organizacijskih aktivnosti (Cheng, 2008). Razvoj in hitra razširitev uporabe informacijske tehnologije, v zadnjem času predvsem internetnih in mobilnih aplikacij, vodita k vse hitrejšemu in pogostejšemu prilagajanju in posodabljanju izvajanja poslovnih procesov. Nove tehnologije lahko znatno izboljšajo učinkovitost in uspešnost izvajanja poslovnega procesa, po drugi strani pa lahko povzročijo povečanje kompleksnosti strukture procesa, zmanjšajo fleksibilnost pri izvajanju procesa (podpora izvajanju samo določene različice procesa) in povzročijo večje težave pri medsebojnem povezovanju procesov. S povečevanjem kompleksnosti procesa se znatno povečuje tudi težavnost odkrivanja in razreševanja morebitnih težav v njegovem izvajanju (Cheng, 2008).

V zadnjih desetletjih se vodilni v podjetjih v želji po znižanju stroškov in prihranku časa pogosto odločajo, da bodo hkrati s prenovo poslovnih procesov opravili tudi posodobitev ali implementacijo in integracijo informacijske podpore poslovnega procesa oziroma podjetja (Scheer in Nuttgens, 2000). Da bi upravičili dodatna vlaganja v informacijsko tehnologijo in integracijo različnih komponent je treba poznati odgovor na pomembno vprašanje: »Kakšno je tveganje v smislu povečanja kompleksnosti strukture procesov v želji po izboljšanju učinkovitosti z implementiranjem novih informacijskih rešitev in drugih sprememb?« V resnici je veliko implementacij informacijskih rešitev neuspešnih, ker sta premalo poudarjena struktura poslovnih procesov in menedžment sprememb (Bose, 2002; Jarrar, Al-Mudimigh in Zairi, 2000). Glede na poročila Gartner Group do 70 odstotkov implementacij programskih rešitev ni v skladu s temeljnimi cilji podjetja (Davis, 2002).

Prenove poslovnih procesov (z implementacijo ustrezne informacijske rešitve ali brez nje) se v podje-

tjih lotevajo z bolj ali manj enakim ciljem doseči učinkovitejše in uspešnejše poslovanje podjetja. Prenovo poslovnih procesov lahko izvedejo različno, v zadnjih desetletjih se je namreč izoblikovalo več kot petdeset različnih pristopov (Vila, 2006). Razlike med posameznimi pristopi prenove so predvsem v predlaganem načinu, kako to doseči v podjetju – od hitrih in korenitih (revolucionarnih) sprememb na eni strani do bolj počasnih in postopnih (evolutivnih) na drugi. Vsi pristopi pa poudarjajo potrebo po obvladovanju procesov kot ključu do uspeha. Učinkovitost izvajanja poslovnih procesov je namreč pomembno povezana z uspešnostjo poslovanja (Vila, 2000).

Po uspešno opravljeni prilagoditvi izvajanja procesov oziroma prenovi poslovanja si vodilni v podjetjih v takem trenutku pogosto postavljajo pomembna vprašanja: »Smo dosegli cilj?« »Je to tisto, kar smo potrebovali?« »Kam in kako naprej?« (Urh, Kern, Roblek, 2008). Ob tem vodilni naletijo na zelo zahtevna in pomembna »podvprašanja« za vsako podjetje, kot so:

- kakšna je stopnja učinkovitosti izvajanja poslovnih procesov;
- ali je izvajanje procesa glede na zahteve še sprejemljivo za podjetje;
- ali je treba prilagoditi oziroma spremeniti proces in ali je to smotrno;
- kakšne spremembe ali prilagoditve je treba opraviti v izvajanju procesa;
- kako bodo predvidene spremembe vplivale na učinkovitost izvajanja procesa.

Ob pregledovanju relevantne literature o raziskavah na tem področju najdemo številne predloge za ovrednotenje učinkovitosti izvajanja poslovnih procesov. Večina predlogov se nanaša na ovrednotenje s pomočjo kazalnikov »operativne« učinkovitosti (Dibrell idr., 2008; Frederiksen in Mathiassen, 2008; Sharma, 2009), le malo pa na kazalnike »strukturne« učinkovitosti (Aguilar idr., 2006; Cardoso, 2006; Mendling, 2008). Kazalniki operativne učinkovitosti vključujejo vidik porabe časa in/ali vidik nastalih stroškov (Cardoso, Mendling, Neumann in Reijers, 2006a; Valiris in Glykas, 2004), medtem ko so kazalniki strukturne učinkovitosti povezani z ovrednotenjem strukturne kompleksnosti poslovnih procesov (Cardoso, 2006; Mendling, 2008).

Ocenitev trenutnega stanja učinkovitosti izvajanja poslovnih procesov s kazalniki operativne učinkovitosti se v praksi izvede na podlagi online zbiranja podatkov (ključnih kazalnikov izvajanja[1]) o izvajanju procesa. To pomeni, da se proces v podjetju mora izvajati in da je njegovo izvajanje podprto z ustrezno programsko rešitvijo, ki to omogoča. Oceno učinkovitosti izvajanja procesov s kazalniki strukturne učinkovitosti pa lahko dobimo na podlagi ocene zahtevnosti izvedbe podpore izvajanja procesa z informacijsko tehnologijo ali na podlagi ocene kompleksnosti poteka (modela) procesa (Cardoso, Mendling, Neumann in Reijers, 2006a). Prva možnost od podjetja zahteva, da imajo za predvideno informacijsko podporo procesa dokaj podrobno razdelano oceno zahtevnosti njene implementacije. V drugem primeru pa za oceno strukturne učinkovitosti potrebujemo zgolj ustrezen model poslovnega procesa.

V primerjavi s kazalniki operativne učinkovitosti poslovnih procesov so ocene učinkovitosti izvajanja procesov podane s kazalniki strukturne učinkovitosti sicer bolj grobe, vendar je v tem primeru vložek za pridobitev take ocene bistveno nižji (Cheng, 2008). Po drugi strani pa je strukturna kompleksnost procesov eden glavnih vzrokov za pojavljanje napak in hitro naraščanje stroškov izvajanja procesov (Cardoso, Mendling, Neumann in Reijers, 2006b; Mendling, 2007).

Ker je implementacija prenovljenega poteka procesa oz. procesov povezana z visokimi stroški, si vodilni v podjetjih želijo, da bi oceno predvidenega učinka prenove dobili, še preden se odločijo za investicijo vanjo. V tem primeru torej odpade ocena učinkovitosti izvajanja procesa s kazalniki operativne učinkovitosti, lahko pa uporabimo oceno strukturne učinkovitosti izvajanja poslovnega procesa, saj jo lahko dobimo že na podlagi ustrezno pripravljenega modela prenovljenega stanja poslovnega procesa.

V prispevku bomo v nadaljevanju predstavili uporabo kazalnikov strukturne učinkovitosti pri oceni učinka predloga prenove procesa na izbranem procesu enega izmed slovenskih podjetij. V naslednjem razdelku bomo najprej predstavili metodološka izhodišča za oceno učinka predlaganih sprememb ob prenovi poslovnega procesa. V nadaljevanju bomo na izbranem primeru poslovnega procesa s pomočjo kazalnikov strukturne učinkovitosti in z uporabo predstavljene metodologije prikazali izvedbo ocene učinka predlaganih sprememb na učinkovitost nje-

[1] Ključni kazalniki izvajanja (angl. Key Performance Indicators) so merljive metrike, s katerimi je izražena uspešnost doseganja zastavljenih nalog in ciljev v poslovnem sistemu (Bauer, 2004). Z njimi so lahko izraženi za podjetje strateško pomembni kazalniki ali pa učinkovitost izvajanja nepomembnih procesov ali aktivnosti.

govega izvajanja. Na koncu je podana razprava o primernosti in uporabnosti predstavljene metodologije ter dobljenih rezultatih.

2 METODE, UPORABLJENE V RAZISKOVANJU

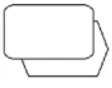
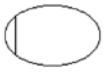
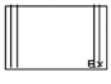
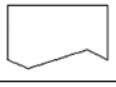
2.1 Modeliranje poslovnih procesov

Ocena strukturne učinkovitosti izvajanja poslovnega procesa je pogojena s predhodno opravljenim posnetkom poslovnega procesa (angl. process mapping) in njegovim zapisom v ustreznem repozitoriju (Aguilar idr., 2006).

Pri izvedbi posnetka obstoječega stanja poslovnega procesa (modeliranje obstoječega stanja in oblikovanje predloga prenovljenega procesa) lahko uporabimo različne metodologije, kot so REAL, BPMN, ARIS, ARMA idr. (po analizah Gartner Group je že vrsto let med najbolj izpopolnjenimi in ustreznimi programsko podprta metodologija ARIS podjetja Software AG). Za naše potrebe smo izbrali metodologijo ARIS in procesno-kontrolni pogled, konkretneje tip modela EPC (angl. Event-driven Process Chain), pri katerem je proces prikazan tako, kot si ga izvajalci najlaže predstavljajo (Pavlović, Kern, Miklavčič, 2009). Model temelji na logiki, da dogodek sproži aktivnost (opravilo) ali več aktivnosti, posledično se aktivnost konča z novim dogodkom ali več dogodki. V nadaljevanju bomo uporabili kratico EPC,[2] kadar bomo želeli poudariti tip modela.

Pri ponazoritvi obstoječega stanja procesa in pripravi predloga prenovljenega stanja smo v modelu uporabili simbole, ki so prikazani v tabeli 1. V njej so prikazana tudi pravila uporabe logičnih operatorjev.

Tabela 1: **Simboli, uporabljeni pri modeliranju modelov procesov EPC**

Naziv	Grafični zapis	Namen uporabe simbola
Dogodek		Določeno stanje ali pojav, ki je vzrok ali posledica nečesa. Vedno obstaja vzrok za izvajanje aktivnosti in aktivnost ima vedno za posledico dogodek ali več dogodkov.
Aktivnost (funkcija)		Naloga, opravilo, procesni korak
Logični operatorji	 - IN - X-ALI - ALI	Razcepijo ali združijo procesno verigo: IN – nadaljujemo obvezno po vseh mogočih poteh, X-ALI – nadaljujemo izključno po eni mogoči poti, ALI – nadaljujemo po kateri koli mogoči poti ali kombinaciji mogočih poti.
Procesni konektor		Uporabljen za prekinitev (prelom) procesa, če je ta preobsežen (presega format A4).
Organizacijska enota		Skupina ljudi, oddelek, služba
Delovno mesto		Delovno mesto izvajalca aktivnosti v organizacijski strukturi (profil zaposlenega, ne konkretna oseba)
Aplikacija		Računalniška aplikacija (naziv aplikacije + ime ali številka ali označba ekranske slike), ki se uporablja pri posamezni aktivnosti
Dokument		Papirnati nosilec sporočil (obrazec, faks), ki je potreben za izvedbo aktivnosti ali se v aktivnosti ustvari

[2] Pri izbiri uporabljenega tipa procesnega modela smo se odločili za model EPC kljub vedno večji priljubljenosti modela BPMN (Johannsen idr., 2014). Če bi nas pri ovrednotenju učinkovitosti izvajanja poslovnih procesov zanimal predvsem vidik poteka procesov – workflow – in podpora procesov z informacijsko tehnologijo, bi bilo smotrno uporabiti obliko modela BPMN. Ker pa so nas pri ovrednotenju učinkovitosti izvajana procesov zanimali tudi drugi vidiki, kot so vpletenost zaposlenih, dokumenti v procesih (v elektronski in tiskani obliki) ter uporaba programskih rešitev pri izvajanju aktivnosti v procesih, smo uporabili obliko zapisa procesnih modelov EPC.

2.2 Ocena strukturne učinkovitosti procesa

Oceno strukturne učinkovitosti procesa lahko izvedemo na podlagi ustreznega modela izvajanja poslovnega procesa (Poniatowski in Wichser, 2006; Bassi in McMurrer, 2007; Fitz-enz, 2009). To je tudi ključna prednost te metode, saj lahko učinkovitost oziroma kompleksnost procesa ocenimo že pred njegovo implementacijo in tako prihranimo pri času in predvsem pri stroških, povezanih z implementacijo.

Analiza procesnega modela

Oceno strukturne učinkovitosti oziroma kompleksnosti modelov izvajanja poslovnih procesov izvedemo v več korakih (Urh, Kokalj in Zajec, 2011). V prvem koraku z analizo modela procesa zberemo osnovne podatke oziroma osnovne kazalce (Aguilar idr., 2006; Cardoso, 2006; Mendling, 2008) za ocenitev učinkovitosti izvajanja procesa po posameznih strukturnih kazalnikih. Pri analiziranju iz modelov procesov zberemo te kazalce:

- število dogodkov v procesu (n_E),
- število začetnih dogodkov procesa (n_{SE}),
- število zaključnih in/ali ponornih dogodkov procesa (n_{FE}),
- število aktivnosti v procesu (funkcije in procesni vmesniki) (n_{PA}),
- število aktivnosti s povezavami na druge procese (procesni vmesniki) (n_{PI}),
- število odločitev med izvajanjem procesa (n_{PD}),
- število mogočih prehodov med aktivnostmi v procesu (n_{AT}),
- število povratnih zank v procesu (n_{LB}),
- število aktivnosti v procesu, v katerih se ustvarja dodana vrednost (n_{VAA}),
- število povezav med delovnimi mesti in aktivnostmi procesa (n_{CPA}),
- število izvajalcev (delovnih mest), ki sodelujejo v procesu (n_{PP}),
- število hierarhičnih ravni izvajalcev, ki sodelujejo v procesu (n_{HLP}),
- število delovnih mest, ki sodelujejo pri izvajanju vseh poslovnih procesov v poslovnem sistemu (n_{PAP}),
- število izvajalcev (delovnih mest) v poslovnem sistemu (n_{PBS}),
- število dokumentov, ki se uporabljajo v procesu (n_{DP}),
- število dokumentov, ki jih je treba ustvariti v procesu (n_{POD}),
- število dokumentov, ki vstopajo v proces (n_{PID}),
- število programskih rešitev, ki se uporabljajo v procesu (n_{SWP}),
- število aktivnosti procesa, katerih izvajanje je podprto s programskimi rešitvami (n_{SWA}).

Izračun kazalnikov strukturne učinkovitosti

V naslednjem koraku na podlagi tako zbranih kazalcev izračunamo kazalnike strukturne učinkovitosti. Nabor kazalnikov za oceno strukturne učinkovitosti izvajanja poslovnih procesov smo glede na objekte oziroma simbole, ki tvorijo modele poslovnih procesov EPC, priredili po Aguilar idr. (2006) in Cardoso (2006). Izbrane kazalnike strukturne učinkovitosti lahko razvrstimo v štiri osnovne skupine (Aguilar idr., 2006), in sicer na kazalnike, ki so izraženi na podlagi:

- ključnih indikatorjev poteka procesa (vitki model EPC)
  - kazalnik začetnih dogodkov procesa
    $$K_{SE} = \frac{n_{SE}}{n_E} \cdot 100 \quad (01)$$
  - kazalnik zaključnih in/ali ponornih dogodkov procesa
    $$K_{FE} = \frac{n_{FE}}{n_E} \cdot 100 \quad (02)$$
  - kazalnik aktivnosti procesa
    $$K_A = \frac{1}{(n_{PA} - n_{PI})} \cdot 100 \quad (03)$$
  - kazalnik odločitev v procesu
    $$K_D = \frac{n_{PD}}{(n_{PA} - n_{PI})} \cdot 100 \quad (04)$$
  - kazalnik dodane vrednosti v procesu
    $$K_{VAP} = \frac{n_{VAA}}{(n_{PA} - n_{PI})} \cdot 100 \quad (05)$$
- ključnih indikatorjev povezav
  - kazalnik povezanosti procesa
    $$K_{PI} = \frac{n_{PI}}{n_{PA}} \cdot 100 \quad (06)$$
  - kazalnik števila prehodov med aktivnostmi
    $$K_{PAT} = \frac{n_{AT}}{(n_{PA} - n_{PI})} \cdot 100 \quad (07)$$
  - kazalnik povratnih zank
    $$K_{LB} = \frac{n_{LB}}{(n_{PA} - n_{PI})} \cdot 100 \quad (08)$$

- ključnih indikatorjev izvajalcev procesa oz. organizacijske strukture
  - kazalnik stopnje vključenosti izvajalcev
    $$K_{CLP} = \frac{n_{CPA}}{(n_{PA} - n_{PI}) \cdot n_{PP}} \cdot 100 \quad (09)$$
  - kazalnik izvajalcev procesa
    $$K_{PP} = \frac{1}{n_{PP}} \cdot 100 \quad (10)$$
  - kazalnik vključenih izvajalcev
    $$K_{PPA} = \frac{n_{PP}}{n_{PAP}} \cdot 100 \quad (11)$$
  - kazalnik hierarhije izvajalcev procesa
    $$K_{HP} = \frac{1}{n_{HLP}} \cdot 100 \quad (12)$$
  - kazalnik obsežnosti izvajanja procesa
    $$K_{EP} = \frac{n_{PP}}{n_{PBS}} \cdot 100 \quad (13)$$
- ključnih indikatorjev izdelkov oz. podpornih objektov (dokumenti, programske rešitve idr.)
  - kazalnik razmerja izhodnih dokumentov
    $$K_{POD} = \frac{n_{POD}}{n_{DP}} \cdot 100 \quad (14)$$
  - kazalnik razmerja vhodnih dokumentov
    $$K_{PID} = \frac{n_{PID}}{n_{DP}} \cdot 100 \quad (15)$$
  - kazalnik razmerja izhodnih dokumentov in aktivnosti procesa
    $$K_{PODA} = \frac{n_{POD}}{(n_{PA} - n_{PI})} \cdot 100 \quad (16)$$
  - kazalnik programskih rešitev procesa
    $$K_{SWP} = \frac{1}{n_{SWP}} \cdot 100 \quad (17)$$
  - kazalnik informacijske podpore aktivnosti procesa
    $$K_{PSWA} = \frac{n_{SWA}}{(n_{PA} - n_{PI})} \cdot 100 \quad (18)$$

Na podlagi naštetih osnovnih kazalcev izvajanja poslovnih procesov tako izračunamo osemnajst kazalnikov (različnih ocen) strukturne učinkovitosti izvajanja poslovnega procesa (Urh, Kokalj in Zajec, 2011).

Končna ocena strukturne učinkovitosti procesa

Pri izračunu končne ocene strukturne učinkovitosti modela izvajanja poslovnih procesov smo morali rešiti problem, kako veliko število izhodiščnih kazalnikov strukturne učinkovitosti združiti v eno enotno oceno. Nekateri kazalniki strukturne učinkovitosti poslovnih procesov so namreč medsebojno povezani (sprememba v izvajanju procesa vpliva na spremembo več kazalnikov strukturne učinkovitosti), nekateri kazalniki strukturne učinkovitosti pa najbolj relevantno izkazujejo stanje oz. imajo največji vpliv na učinkovitost izvajanja posameznega poslovnega procesa.

V raziskavi (Urh, Kokalj in Zajec, 2011) je bilo ugotovljeno, da lahko veliko število izhodiščnih kazalnikov strukturne učinkovitosti izvajanja poslovnih procesov nadomestimo s sedmimi nepovezanimi kazalniki strukturne učinkovitosti in pri tem ohranimo več kot 77 odstotkov variabilnosti osnovnih spremenljivk[3] oz. izhodiščnih kazalnikov strukturne učinkovitosti.

Posamezni nepovezani kazalniki strukturne učinkovitosti poslovnih procesov (faktorji) glede na navedeno raziskavo združujejo (navedeno v nadaljevanju) izhodiščne kazalnike strukturne učinkovitosti izvajanja poslovnih procesov (navedene zgoraj). V navedeni raziskavi so bili z uporabo statistične metode (linearne regresije) ugotovljeni koeficienti, s katerimi so bile oblikovane enačbe za neposredni izračun nepovezanih strukturnih kazalnikov učinkovitosti, ki jih navajamo v nadaljevanju.

- **Organiziranost poslovnega sistema (NSK_01)** združuje kazalnik izvajalcev procesa, kazalnik hierarhije izvajalcev procesa, kazalnik stopnje vključenosti izvajalcev in kazalnik vključenih izvajalcev.
  NSK_01 = –6,947 + 0,016 * SK(10) + 0,013 * SK(12) + 0,005 * SK(09) + 0,060 * SK(11) (19)
- **Kompleksnost poslovnih procesov (NSK_02)** združuje kazalnik odločitev v procesu in kazalnik povratnih zank.
  NSK_02 = –10,602 + 0,048 * SK(04) + 0,064 * SK(08) (20)

[3] Delež pojasnjene variabilnosti osnovnih spremenljivk je skladen s priporočili Fielda (2000) ter Rietvelda in Van Houta (1993), ki predlagajo, da ohranimo faktorje, ki skupno pojasnijo od 70 do 80 odstotkov variabilnosti osnovnih spremenljivk.

- **Dokumentiranost opravljenega dela (NSK_03)** združuje kazalnik razmerja izhodnih dokumentov in aktivnosti procesa ter kazalnik razmerja izhodnih dokumentov.
  NSK_03 = –1,913 + 0,021 * SK(16) + 0,017 * SK(14) (21)

- **Obsežnost poslovnih procesov (NSK_04)** združuje kazalnik aktivnosti procesa in kazalnik števila prehodov med aktivnostmi.
  NSK_04 = –2,222 + 0,071 * SK(03) + 0,022 * SK(07) (22)

- **Medsebojna povezanost procesov (NSK_05)** združuje kazalnik začetnih dogodkov procesa in kazalnik povezanosti procesa.
  NSK_05 = –5,381 + 0,044 * SK(01) + 0,030 * SK(06) (23)

- **Podprtost z informacijsko tehnologijo (NSK_06)** združuje kazalnik programskih rešitev procesa in kazalnik informacijske podpore aktivnosti procesa.
  NSK_06 = –1,545 + 0,018 * SK(17) + 0,021 * SK(18) (24)

- **Ustvarjanje dodane vrednosti (NSK_07)** vključuje kazalnik dodane vrednosti v procesu.
  NSK_07 = –0,335 + 0,095 * SK(05) (25)

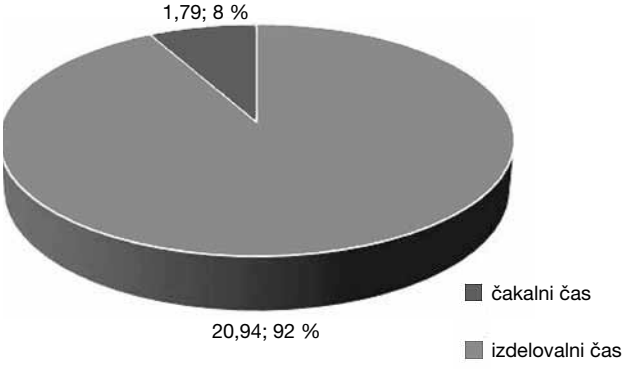
Končno oceno strukturne učinkovitosti izvajanja poslovnih procesov tako lahko izračunamo na podlagi vrednosti posameznega nepovezanega kazalnika strukturne učinkovitosti in njegovega deleža pojasnjene variance.

3 REZULTATI PRIMERA UPORABE PREDLAGANE METODE

V nadaljevanju bomo na primeru izbranega procesa prikazali uporabo predlagane metode ocenjevanja strukturne učinkovitosti in tako pridobljenih rezultatov. Izbrali smo proces izdelave in dodelave zdravstvenih pripomočkov, ki je eden izmed temeljnih (proizvodnih) procesov v enem izmed uspešnejših slovenskih podjetij na področjih izdelave in dodelave zdravstvenih pripomočkov ter ponudbe zdravstvenih storitev. Podjetje je sicer pred leti opravilo prenovo poslovnih procesov z izjemo temeljnih (proizvodnih) procesov.

Z opravljenimi statističnimi analizami in izračuni kazalnikov operativne učinkovitosti so ugotovili, da imajo v procesu izdelave in dodelave zdravstvenih pripomočkov:

- predolge prehodne čase glede na pričakovanja bolnikov,
- prevelik delež čakalnih časov v primerjavi s časi izdelovanja (slika 1),
- velika odstopanja med posameznimi časi izdelovanja,
- velika odstopanja med posameznimi prehodnimi časi,
- veliko administrativnih aktivnosti,
- podvajanje nekaterih administrativnih del,
- pripravo in distribucijo veliko fizičnih dokumentov,
- nizko zasedenost z delom pri zaposlenih,
- neenakomerno porazdelitev zasedenosti z delom med zaposlenimi.



Slika 1: **Distribucija čakalnih in izdelovalnih časov v obstoječem stanju izbranega procesa**

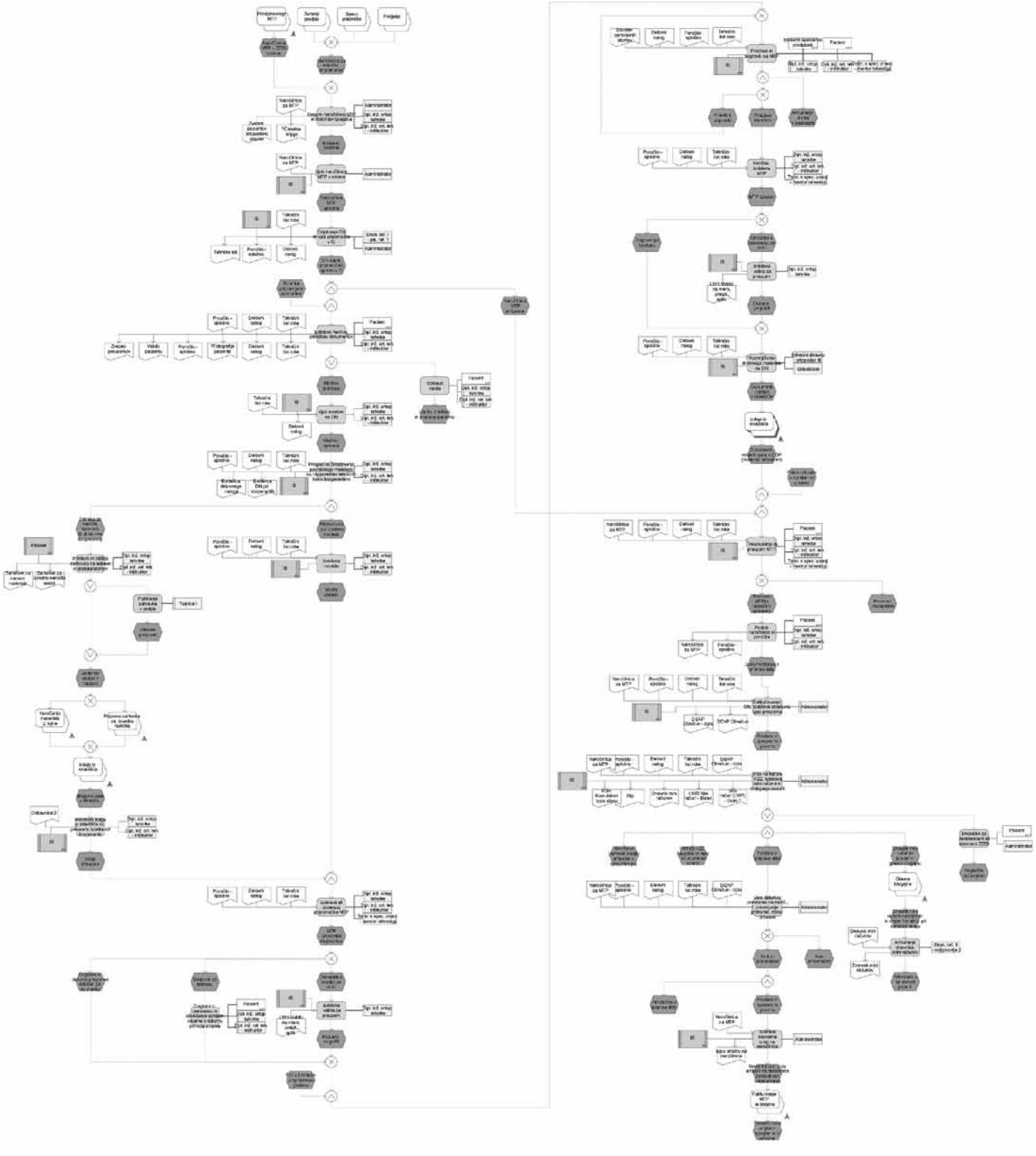
Znižanje deleža časov čakanja so poskusili doseči s povečanjem kapacitet v ozkih grlih, vendar niso dosegli pričakovanih rezultatov, tako da smo se odločili za korenitejšo prenovo procesa.

Model obstoječega stanja

Na sliki 2 je prikazan model obstoječega stanja izbranega temeljnega procesa (As-Is) v podjetju.

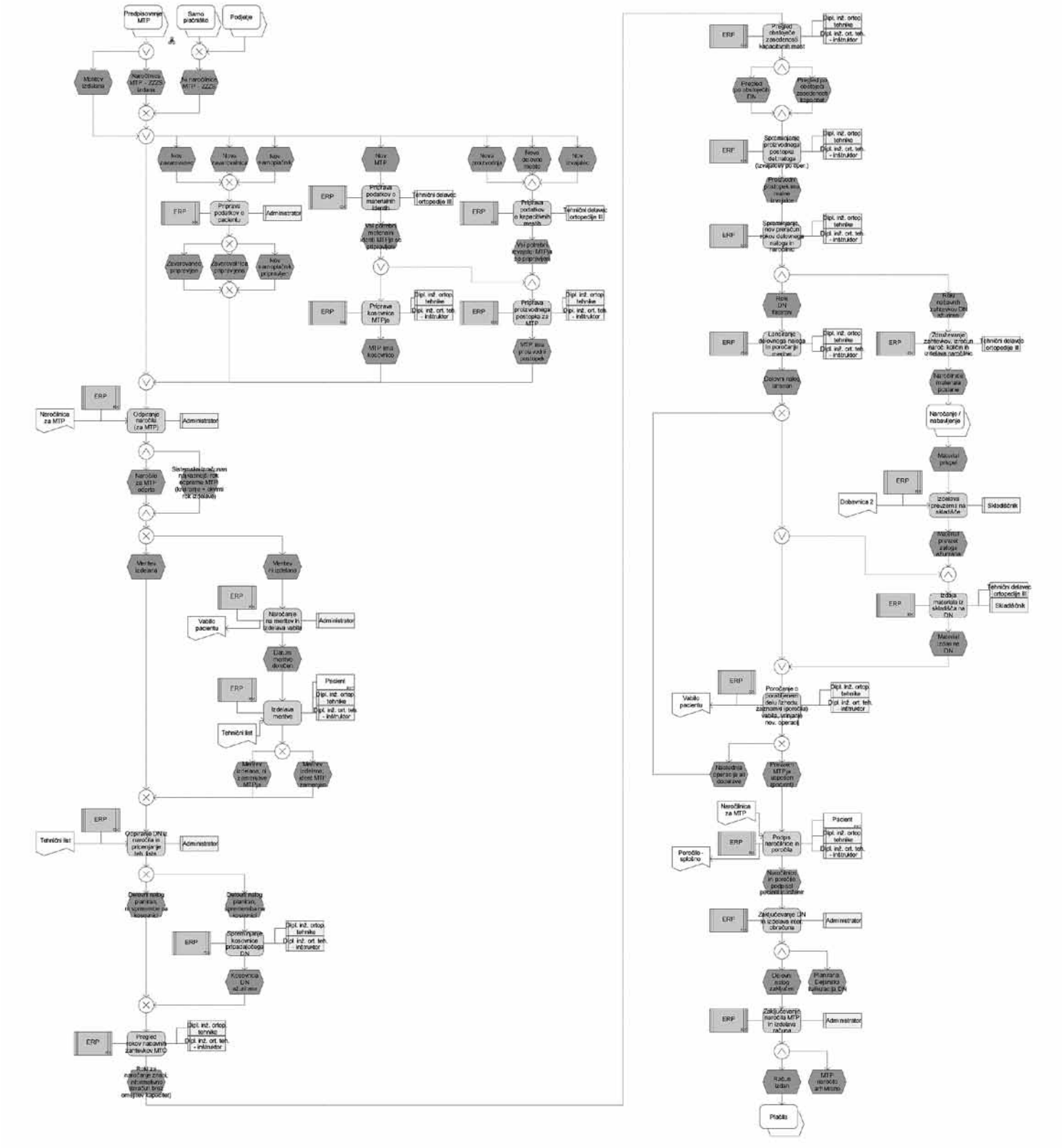
Model predlaganega prenovljenega stanja

Pri oblikovanju modela prenovljenega procesa (To-Be) smo želeli odpraviti čim več pomanjkljivosti, ki so bile ugotovljene pri analiziranju obstoječega stanja procesa (As-Is). V prenovljenem procesu smo tako:



Slika 2: **Model obstoječega stanja izbranega poslovnega procesa**[4]

[4] Kljub obsežnosti modela obstoječega stanja procesa (As-Is) smo se odločili, da na sliki 2 prikažemo proces v celoti, vendar v pomanjšani obliki. S pomanjšanjem modela procesa smo sicer izgubili berljivost vsebine, zapisane v posameznih simbolih, vendar ta ni ključnega pomena pri oceni strukturne učinkovitosti procesa. Strukturno učinkovitost procesa namreč ocenimo na podlagi kompleksnosti strukture oz. sestave modela procesa, ki pa je iz slike razvidna kljub pomanjšanju.



Slika 3: **Model predloga izvajanja izbranega poslovnega procesa po prenovi**

Tabela 2: **Osnovni podatki (kazalci) o izvajanju izbranega procesa**

Osnovni kazalci	Oznaka	Stanje As-Is	Stanje To-Be
Število dogodkov v procesu	n_E	50	45
Število začetnih dogodkov procesa	n_{SE}	8	3
Število zaključnih in/ali ponornih dogodkov procesa	n_{FE}	8	3
Število aktivnosti v procesu (funkcije in procesni vmesniki)	n_{PA}	36	27
Število aktivnosti s povezavami na druge procese (procesni vmesniki)	n_{PI}	10	5
Število odločitev med izvajanjem procesa	n_{PD}	1	0
Število mogočih prehodov med aktivnostmi v procesu	n_{AT}	31	27
Število povratnih zank v procesu	n_{LB}	0	0
Število aktivnosti v procesu, v katerih se ustvarja dodana vrednost	n_{VAA}	6	8
Število povezav med delovnimi mesti in aktivnostmi procesa	n_{CPA}	47	34
Število izvajalcev (delovnih mest), ki sodelujejo v procesu	n_{PP}	11	6
Število hierarhičnih ravni izvajalcev, ki sodelujejo v procesu	n_{HLP}	3	2
Število delovnih mest, ki sodelujejo pri izvajanju vseh poslovnih procesov v poslovnem sistemu	n_{PAP}	88	88
Število izvajalcev (delovnih mest) v poslovnem sistemu	n_{PBS}	141	141
Število dokumentov, ki se uporabljajo v procesu	n_{DP}	25	6
Število dokumentov, ki jih je treba ustvariti v procesu	n_{POD}	23	2
Število dokumentov, ki vstopajo v proces	n_{PID}	8	3
Število programskih rešitev, ki se uporabljajo v procesu	n_{SWP}	2	1
Število aktivnosti procesa, katerih izvajanje je podprto s programskimi rešitvami	n_{SWA}	14	22

- odpravili administrativne aktivnosti, ki ne dodajajo dodane vrednosti,
- zmanjšali število uporabljenih in izmenjanih fizičnih dokumentov,
- odpravili podvajanje dela,
- upoštevali možnosti, ki jih omogoča uporaba informacijske tehnologije in sistema celovite programske rešitve.

Na sliki 3 je prikazan model predlaganega stanja izvajanja izbranega procesa (To-Be) v podjetju po prenovi.

V nadaljevanju prikazujemo izvedbo ocenjevanja učinkovitosti izvajanja procesa po strukturnih kazalnikih za obstoječi način dela (stanje As-Is) in predlagani način dela po prenovi procesa (stanje To-Be).

3.1 Analiza obstoječega in predloga prenovljenega modela procesa

Na podlagi modelov izbranega temeljnega procesa za obstoječi način dela (slika 2) in za predlagani način dela po prenovi procesa (slika 3) smo zbrali podatke za izračun izhodiščnih kazalnikov strukturne učinkovitosti (tabela 2).

3.2 Nepovezani kazalniki strukturne učinkovitosti

Na podlagi zbranih podatkov (kazalcev) o strukturi izbranega temeljnega procesa (tabela 2) in enačb za izračun izhodiščnih kazalnikov strukturne učinkovitosti (enačbe od 01 do 18) smo izračunali ocene nepovezanih kazalnikov strukturne učinkovitosti (enačbe od 19 do 25) za obstoječi način dela in predlagani način dela po prenovi procesa. Zaradi razlik v intervalih vrednosti posameznega nepovezanega kazalnika strukturne učinkovitosti smo dobljene vrednosti pretvorili na enoten ocenjevalni interval. Rezultati, predstavljeni v tabeli 3, so tako preračunani na interval vrednosti od 0 do 5, pri čemer vrednost 0 pomeni slabo strukturno učinkovitost, vrednost 5 pa zelo dobro strukturno učinkovitost izbranega poslovnega procesa glede na posamezni nepovezani kazalnik strukturne učinkovitosti.

Tabela 3: **Ocene strukturne učinkovitosti izvajanj izbranega procesa**

Nepovezani kazalniki strukturne učinkovitosti	Oznaka	Stanje As-Is	Stanje To-Be
Organiziranost poslovnega sistema	NSK_01	3,12	3,53
Kompleksnost poslovnih procesov	NSK_02	2,94	4,51
Dokumentiranost opravljenega dela	NSK_03	0,51	3,86
Obsežnost poslovnih procesov	NSK_04	3,44	3,35
Medsebojna povezanost procesov	NSK_05	3,96	4,41
Podprtost z informacijsko tehnologijo	NSK_06	2,61	5,00
Ustvarjanje dodane vrednosti	NSK_07	1,15	1,80

3.3 Končna ocena strukturne učinkovitosti procesa

Na podlagi ocene strukturne učinkovitosti po posameznem nepovezanem kazalniku strukturne učinkovitosti (tabela 3) in razmerja deleža pojasnjene variance posameznega nepovezanega kazalnika strukturne učinkovitosti, ugotovljene v raziskavi (Urh, Kokalj in Zajec, 2011), smo izračunali končno oceno strukturne učinkovitosti izbranega procesa. V tabeli 4 so podani rezultati tako za model obstoječega izvajanja procesa kakor tudi za predlagani model izvajanja procesa po prenovi.

4 RAZPRAVA O METODI IN REZULTATIH

Razprava o metodi

Temelje za ovrednotenje učinkovitosti izvajanja poslovnih procesov na podlagi strukturne kompleksnosti poslovnih procesov s tako imenovanimi kazalniki strukturne učinkovitosti smo zasledili pri avtorjih Aguilar idr. (2006), Cardoso (2006) in Mendling (2008). Navedeni avtorji ugotavljajo, da izboljšave oz. spremembe v izvajanju (modelu) poslovnega procesa vplivajo na spremembe posameznega ali več kazalnikov strukturne učinkovitosti.

Določena izboljšava oz. sprememba v (modelu) izvajanju procesa se lahko hkrati odrazi v večji ali manjši izboljšavi ali celo poslabšanju posameznega kazalnika strukturne učinkovitosti. Na ta način je zelo težko ugotoviti, kateri kazalnik spremljati in kakšen bo dejanski rezultat predlaganih sprememb. S predstavljeno metodo smo veliko različnih ocen strukturne učinkovitosti, pridobljenih z izhodiščnimi kazalniki strukturne učinkovitosti, združili v eno oceno, ki bolj relevantno oz. celovito podaja oceno strukturne učinkovitosti procesa.

Za večjo verodostojnost predlagane metode je treba v nadaljnjih raziskavah preveriti, kako se glede na posamezno podjetje oziroma panogo spreminjajo enačbe za neposredni izračun nepovezanih strukturnih kazalnikov učinkovitosti in delež pojasnjene variance posameznega nepovezanega strukturnega kazalnika.

Razprava o rezultatih

Na izbranem primeru temeljnega procesa smo pokazali možnost praktične uporabe kazalnikov strukturne učinkovitosti. Rezultati ocenjevanja izbranega procesa (tabeli 3 in 4) kažejo, da bodo predlagane spremembe ob prenovi procesa pozitivno vplivale na učinkovitost njegovega izvajanja. Iz rezultatov ocenjevanja vidimo, da s predlaganimi spremembami ob prenovi procesa (oblikovanje stanja To-Be) dosežemo izboljšanje končne ocene strukturne učinkovitosti z 2,69 na 3,80, kar je posledica:

- nekoliko izboljšane organiziranosti poslovnega sistema (z ocene 3,12 na oceno 3,53), ki je posledica manjšega števila različnih izvajalcev, vključe-

Tabela 4: **Izračun končne ocene strukturne učinkovitosti izbranega procesa**

Nepovezani kazalniki strukturne učinkovitosti	Oznaka	% variance	Stanje As-Is	Stanje To-Be
Organiziranost poslovnega sistema	NSK_01	24,237	3,12	3,53
Kompleksnost poslovnih procesov	NSK_02	12,565	2,94	4,51
Dokumentiranost opravljenega dela	NSK_03	10,328	0,51	3,86
Obsežnost poslovnih procesov	NSK_04	9,303	3,44	3,35
Medsebojna povezanost procesov	NSK_05	8,643	3,96	4,41
Podprtost z informacijsko tehnologijo	NSK_06	6,286	2,61	5,00
Ustvarjanje dodane vrednosti	NSK_07	5,706	1,15	1,80
Končna ocena strukturne učinkovitosti			2,69	3,80

nih v izvajanje procesa, in manjšega števila različnih hierarhičnih ravni, na katerih so ti zaposleni;
- znatno izboljšane kompleksnosti poslovnega procesa (z ocene 2,94 na oceno 4,51), ki je posledica zmanjšanja števila odločitev izvajalcev, vključenih v izvajanje procesa;
- znatno izboljšane dokumentiranosti opravljenega dela (z ocene 0,51 na oceno 3,86), ki je posledica temeljitega zmanjšanja števila »papirnih«, natisnjenih dokumentov, ki jih je treba izdelati med izvajanjem procesa;
- rahlo slabše obsežnosti poslovnega procesa (z ocene 3,44 na oceno 3,35), ki je posledica nekoliko zapletenejših povezav med različnimi možnostmi pri izvajanju procesa;
- nekoliko izboljšane medsebojne povezanosti procesov (z ocene 3,96 na oceno 4,41), ki je posledica jasnejših povezav in prehodov v »povezane« procese (predhodne in posledične), ki jih je treba izvesti v podjetju;
- znatno izboljšane podprtosti z informacijsko tehnologijo (z ocene 2,61 na oceno 5,00), ki je posledica uvedbe podpore izvajanja s celovito programsko rešitvijo (sistem ERP);
- nekoliko izboljšanega ustvarjanja dodane vrednosti (z ocene 1,15 na oceno 1,80), ki je posledica zmanjšanja števila aktivnosti v procesu, v katerih se ne ustvarja dodana vrednost ne za stranko ne za podjetje.

5 SKLEP

V prispevku smo predstavili, kako lahko učinkovitost izvajanja izbranega poslovnega procesa preverimo na podlagi ustrezno pripravljenega modela (model procesa EPC). S pomočjo kazalnikov strukturne učinkovitosti in modela procesa lahko ocenimo učinkovitost izvajanja procesa, ki se v podjetju že izvaja ali pa je model procesa pripravljen bodisi z namenom razvoja in vzpostavitve novega procesa oz. z namenom implementacije prenovljenega stanja procesa.

Na podlagi izračunanih nepovezanih strukturnih kazalnikov smo s preračunom na enotni merilni interval dobili ocene strukturne učinkovitosti izvajanja izbranega temeljnega procesa. Na podlagi izračunanega deleža pojasnjene variance posameznega nepovezanega kazalnika strukturne učinkovitosti smo nato izračunali končno oceno strukturne učinkovitosti izbranega procesa.

Če vodilni v podjetjih želijo oziroma potrebujejo izboljšanje stanja učinkovitosti izvajanja poslovnih procesov, se na podlagi predstavljenega postopka analize strukturne učinkovitosti laže odločijo, kaj bi bilo smiselno storiti (spremeniti organiziranost podjetja, prenesti pooblastila in odgovornosti na nižje ravni, urediti povezanost poslovnih procesov, izpopolniti informacijsko podporo izvajanja procesov, zmanjšati število aktivnosti, ki ne ustvarjajo dodane vrednosti, ali uvesti brezpapirno poslovanje), da bi se učinkovitost izvajanja poslovnega procesa oz. procesov kar najbolj izboljšala.

6 LITERATURA

[1] Aguilar, E. R., Ruiz, F., García, F., Piattini, M. (2006). Applying Software Metrics to evaluate Business Process Models, *CLEI Electronic Journal, Vol. 9, No. 1, Paper 5*.

[2] Bassi, L., McMurrer, D. (2007). Maximizing Your Return on People, *Harvard Business Review, Vol. 85, Iss. 3*, str. 115–123.

[3] Bauer, K. (2004). KPIs: Not All Metrics Are Created Equal, *DM Review, 14(12)*, 42. Retrieved February 19, 2009, from ProQuest Computing database. (Document ID: 750265451).

[4] Bose, R. (2002). Customer relationship management: key components for IT success. *Industrial Management and Data Systems, 102(2)*, str. 89–97.

[5] Cardoso, J. (2006). *Complexity Analysis of BPEL Web Processes*, Accepted for Publication, Software Process: Improvement and Practice Journal, John Wiley & Sons, Ltd.

[6] Cardoso, J., Mendling, J., Neumann, G. in Reijers, H. A. (2006a). A Discourse on Complexity of Process Models. V *Business Process Management Workshops (Vol. 4103)*. Berlin, Heidelberg: Springer.

[7] Cardoso, J., Mendling, J., Neumann, G. in Reijers, H. A. (2006b). A Discourse on Complexity of Process Models. V *Business Process Management Workshops (Vol. 4103,* str. 117–128). Berlin, Heidelberg: Springer.

[8] Cheng, C. (2008). Complexity and usability models for business process analysis. Available from ProQuest Dissertations & Theses Global. Pridobljeno s http://search.proquest.com/docview/ 848640112?accountid=28931.

[9] Davis, R. (2002). *The wizard of oz in CRMLAND: CRM's need for business process management*. Information Systems Management.

[10] Dibrell, C., Davis, P., Craig, J. (2008). Fueling Innovation through Information Technology in SMEs*, *Journal of Small Business Management, Vol. 46, Iss. 2,* str. 203–218.

[11] Field, A. (2000). *Discovering Statistics using SPSS for Windows*. London, Thousand Oaks, New Delhi: Sage publications.

[12] Fitz-enz, J. (2009). Predicting People: From Metrics to Analytics, *Employment Relations Today, Vol. 36, Iss. 3*, str. 1.

[13] Frederiksen, H. in Mathiassen, L. (2008). A Contextual Approach to Improving Software Metrics Practices, *IEEE Transactions on Engineering Management, Vol. 55, Iss. 4*, str. 602–616.

[14] Jarrar, Y. F., Al-Mudimigh, A. in Zairi, M. (2000). *ERP implementation critical success factors-the role and impact of business process management*. Paper presented at the Management of Innovation and Technology, 2000. ICMIT 2000. Proceedings of the 2000 IEEE International Conference on.

[15] Johannsen, F., Leist, S., Braunnagel, D. (2014). Testing the impact of wand and weber's decomposition model on process model understandability. V *International conference on information systems*, Auckland.

[16] Mendling, J. (2008). *Metrics for Process Models: Empirical Foundations of Verification, Error Prediction, and Guidelines for Correctness*. Berlin, Heidelberg: Springer.

[17] Mendling, J. (2007). *Detection and Prediction of Errors in EPC Business Process Models*. Unpublished PhD, Vienna University of Economics and Business Administration (WU Wien).

[18] Pavlović, I., Kern, T., Miklavčič, D. (2009). Comparison of paper-based and electronic data collection process in clinical trials: Costs simulation study, *Contemporary Clinical Trials, Vol. 30, No. 4*, str. 300–316.

[19] Poniatowski, S., Wichser, J. D. (2006). A Better Metric For IT Efficiency, *Optimize, Vol. 5, Iss. 5,* str. 43–46.

[20] Rietveld, T., Van Hout, R. (1993). *Statistical Techniques for the Study of Language and Language Behaviour*. Berlin, New York: Mouton de Gruyter.

[21] Scheer, A.W., Nuttgens, M. (2000). ARIS Arhitecture and Reference Models for Business Process Management. V *Business Process Management: Models, Techniques and Empirical Studies*, str. 376–390; Berlin: Springer.

[22] Sharma, A. (2009). Implementing Balance Scorecard for Performance Measurement, Institute of Chartered Financial Analysts of India (Hyderabad), *The ICFAI Journal of Business Strategy, Vol. 6, Iss. 1*, str. 7–16.

[23] Urh, B., Kern, T., Roblek, M. (2008). Business process modification management, V G. Putnik (ur.), *Encyclopedia of networked and virtual organizations, Hershey, Information Science Reference*, str. 112–120.

[24] Urh, B., Kokalj, Š., Zajec, M. (2011). The importance of structural indicators in assessing the efficiency of business process performance. V Kern, T. (ur.), Rajkovič, V. (ur.), *People and sustainable organization*. Frankfurt am Main [etc.]: Peter Lang, str. 248–270.

[25] Valiris, G., Glykas, M. (2004). Business analysis metrics for business process redesign, *Business Process Management Journal, Vol. 10, Iss. 4*, str. 445–480.

[26] Vila, A. (2000). *Organizacija v postmoderni družbi, Obvladovanje sprememb v organizaciji*, str. 110–210, Kranj: Fakulteta za organizacijske vede.

[27] Vila, A. (2006). Sintetizirana organizacija, Management sprememb. V *Zbornik 25. mednarodne konference o razvoju organizacijskih znanosti, Portorož,* str. 1–12. Kranj: Fakulteta za organizacijske vede.

▪

Benjamin Urh je višji predavatelj, habilitiran za področje Inženiring poslovnih in delovnih sistemov. Na Fakulteti za organizacijske vede Univerze v Mariboru na visokošolskem strokovnem programu predava predmeta Razvoj proizvodov in proizvodnih procesov ter Organizacija proizvodnih procesov. Je avtor ali soavtor več kot sto znanstvenih, strokovnih in drugih publikacij. Raziskovalno delo opravlja na področju prenove poslovnih sistemov in učinkovitosti poslovnih procesov.

▪

Eva Krhač je zaposlena na Fakulteti za organizacijske vede Univerze v Mariboru. Habilitirana je v naziv asistentka za področje inženiringa poslovnih in delovnih sistemov. Trenutno svoje znanje izpopolnjuje na doktorskem študiju s področja inženiringa poslovnih sistemov na Fakulteti za organizacijske vede. Pedagoško delo opravlja pri predmetih na dodiplomski in podiplomski stopnji. Je avtorica ali soavtorica osmih znanstvenih, strokovnih in drugih publikacij.

▪

Matjaž Roblek je zaposlen na Fakulteti za organizacijske vede Univerze v Mariboru kot visokošolski učitelj. Habilitiran je v naziv docent za področje inženiringa poslovnih in delovnih sistemov. Pedagoško delo opravlja pri predmetih Poslovni in proizvodni informacijski sistemi, Menedžment oskrbovalne verige ter Planiranje in vodenje proizvodnje. V sodelovanju z gospodarstvom ima končanih več kot šestdeset raziskovalnih in aplikativnih projektov s področja prenove in informatiziranosti poslovnih procesov. Je avtor ali soavtor več kot sto znanstvenih, strokovnih in drugih publikacij. Trenutno je predsednik akademskega zbora Fakultete za organizacijske vede.

▪

Tomaž Kern je zaposlen na Fakulteti za organizacijske vede Univerze v Mariboru kot visokošolski učitelj. Habilitiran je v naziv redni profesor za področje organizacijskih in informacijskih sistemov. Pedagoško delo opravlja pri predmetih na dodiplomski in podiplomski stopnji. Je avtor ali soavtor več kot štiristo petdeset znanstvenih in strokovnih člankov in drugih publikacij. Je vodja več raziskovalnih projektov in član raziskovalnih skupin v raziskovalnih projektih. Aktivno sodeluje pri prenosu raziskovalnega znanja v prakso. Med drugim je bil prodekan za raziskovalne zadeve, predstojnik inštituta, član upravnega odbora univerze, prorektor za informatiko. Trenutno je član senata univerze.

Prizadevanja Slovenije za obvladovanje groženj v kibernetskem prostoru

[1]Samo Maček, [2]Franci Mulec, [2]Franc Močilar
[1]Generalni sekretariat Vlade RS, Gregorčičeva ulica 20, 1000 Ljubljana
[2]Ministrstvo za zunanje zadeve, Prešernova ulica 25, 1000 Ljubljana
samo.macek@gov.si; franci.mulec@gov.si; franc.mocilar@gov.si

Izvleček

V prispevku so predstavljena prizadevanja Evropske unije in Republike Slovenije za obvladovanje izzivov na področju kibernetske varnosti. Terorizem ter organizirani in kibernetski kriminal čedalje bolj ogrožajo demokratično družbo in njene vrednote. EU je v zvezi s tem sprejela številne ukrepe. Z Evropsko agendo za varnost [3] je vzpostavila smernice za odzivanje EU na varnostne grožnje za obdobje 2015–2020. Kibernetska varnost je postala integralni del nacionalne varnosti držav in mednarodne skupnosti.

Ukrepom na ravni EU se prilagaja in jim sledi tudi Slovenija. V začetku leta 2016 je vlada sprejela strategijo kibernetske varnosti, aprila 2017 pa Uradu Vlade Republike Slovenije za varovanje tajnih podatkov razširila delovno področje in ga določila za nacionalni organ za kibernetsko varnost. S tem je bila določena podlaga za učinkovito in celovito zagotavljanje kibernetske varnosti v državi. S širšega vidika je pomembna krepitev zaupanja na državni ravni, strokovna usposobljenost zaposlenih in prenos znanja na področju kibernetske varnosti. Prav zadnje še posebej, saj se znova in znova izkazuje, da je najšibkejši člen še vedno človek. Tehnologija ne more zagotavljati varnosti, če uporabniki niso ustrezno usposobljeni, se ne zavedajo groženj ali ne upoštevajo ukrepov, s katerimi jih je mogoče obvladovati. V članku je opisano, kako se na spremenjeno strukturo groženj v kibernetskem prostoru odzivajo državni organi, ki zagotavljajo delovanje sistemov, ključnih za nemoteno izvajanje funkcij države. Dejavnosti na operativni ravni sledijo evropskim in nacionalnim usmeritvam. Predstavljeni so tudi operativni ukrepi, s katerimi obvladujemo naraščajoče grožnje in so vključeni v vladni informacijski sistem ter sisteme na področju zunanjih zadev.

Ključne besede: kibernetska varnost države, informacijski sistemi, grožnje, strategija, varnostni ukrepi.

Abstract

Efforts of the Republic of Slovenia in the management of cyberspace threats

The paper presents the current efforts of the EU and the Republic of Slovenia (RS) aimed at managing the challenges faced in the field of cyber security. Terrorism and organized cybercrime are becoming major threats to the democratic society and its values. The European Union (EU) has adopted a number of measures in this respect. The European Agenda on Security has established guidelines for the response of the EU to security threats for the period between 2015 and 2020. Cyber security has become an integral part of every country's national security as well as of the security of the international community.

Slovenia has been adapting to and following the measures undertaken at the EU level. At the beginning of 2016, the Government of the RS has adopted a strategy on cyber security and in April 2017 established a national body in charge of cyber security. From the broader perspective, it is important to boost confidence at the state level, professional competence of employees and knowledge transfer in the field of cyber security. These tasks and documents will set up the basis for the effective and comprehensive provisioning of cyber security in the country. This is particularly important since the human factor always turns out to be the weakest link. Technology cannot guarantee security if users are not properly trained, are not aware of the threats or do not apply the measures aimed at managing these threats.

We will demonstrate how government bodies respond to the modified structure of risks in cyberspace where the seamless implementation of the functions of the state is ensured through the functioning of systems that are vital for attaining this objective. Activities carried out at the operational level follow European and national policies and guidelines. In this context, we also provide examples of operational measures aimed at coping with the growing risks that are implemented in the government information system and the systems in the field of foreign affairs.

Keywords: cyber security, information systems, threats, strategy, precautions.

1 UVOD

Evropska unija (EU) in njene države članice se spoprijemajo z velikimi izzivi na področju varnosti. Terorizem ter organizirani kriminal in kibernetska kriminaliteta čedalje bolj ogrožajo družbo v vsej Evropi. K temu prispevajo tudi kriza, spori in politična nestabilnost v neposredni soseščini. V zadnjem času se je struktura groženj zelo spremenila. Poglavitni viri groženj so hacktivizem, interesi nacionalnih držav in organizirana kriminaliteta. [2, 4]

Sistemi, ki so ključni za varnost in delovanje države, so med možnimi tarčami organiziranega kriminala ali kibernetskega terorizma. Motivacija za napade se v primerjavi z običajnim spletnim kriminalom lahko izraža tudi v želji po doseganju družbenih ali političnih sprememb.

Da prihodnost bojevanja pripada kibernetskemu prostoru, je že leta 1984 v futurističnem romanu Nevromant predvidel pisatelj William Gibson. [6] Številni napadi na kritično infrastrukturo (npr. električna omrežja), državne in politične subjekte ter druge sisteme, pomembne za delovanje družbe, dokazujejo, da se je vizija romana že uresničila, napadi v kibernetskem prostoru pa imajo lahko uničujoče posledice v realnem svetu.

Kibernetska varnost pomeni sposobnost zaščititi, varovati ali braniti kibernetski prostor pred kibernetskimi napadi. Kibernetska grožnja pomeni možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja ali sistema. [9]

EU in Slovenija sta dejavno začeli krepiti kibernetsko varnost in zaščito ključnih informacijsko-komunikacijskih sistemov z obvladovanjem groženj v kibernetskem prostoru.

2 UREJANJE KIBERNETSKE VARNOSTI NA RAVNI EU – IZBRANI MEJNIKI

Pregled dejavnosti na področju urejanja kibernetske varnosti EU smo omejili zgolj na tiste z najpomembnejšim vplivom na zdajšnja prizadevanja v Sloveniji.

Podlaga za sodelovanje med državami in zasebnimi podjetji v boju proti kaznivim dejanjem v kibernetskem prostoru je Konvencija Sveta Evrope o kibernetski kriminaliteti, podpisana novembra 2001 v Budimpešti. Slovenija jo je ratificirala leta 2004. [14]

Evropska komisija je leta 2013 objavila strategijo kibernetske varnosti EU z naslovom Odprt, varen in zavarovan kibernetski prostor ter predlog direktive o varnosti omrežij in informacij. Strategija je celostna vizija EU, kako najučinkoviteje preprečiti kibernetske motnje in napade. Direktiva je ključni del splošne strategije za zagotovitev varnega in zaupanja vrednega digitalnega okolja v EU. [2, 5]

Aprila 2015 je Evropska komisija predstavila Evropsko agendo za varnost, s katero je vzpostavila smernice za odzivanje EU na varnostne grožnje v obdobju od leta 2015 do 2020. Z njo je nadomestila predhodno strategijo notranje varnosti za obdobje od leta 2010 do 2014. Glavno odgovornost za varnost imajo še vedno države članice. Pri spopadanju s čezmejnimi grožnjami (terorizem, organizirani kriminal in kibernetska kriminaliteta) pa morajo države sodelovati tako med seboj kot z ustanovami EU. Potreben je učinkovit in usklajen odziv na ravni celotne EU. Evropska agenda za varnost je torej skupna agenda Unije in držav članic ter zagotavlja podlago za sodelovanje in skupno ukrepanje Unije. [3, 4]

Julija 2016 je Evropski parlament sprejel tako imenovano Direktivo NIS (Network and Information Security) – uredbo o varnosti omrežij in informacij, ki bo poenotila nekatere ukrepe držav članic za zaščito informacijskega oziroma kibernetskega okolja. [13]

Namen direktive je zagotoviti:

- ustrezno pripravljenost držav članic na dejanske grožnje v kibernetskem prostoru z zagotavljanjem zadostnih odzivnih zmogljivosti,
- vzpostavljanje mreže sodelovanja med članicami na operativni in strateški ravni,
- dvig kulture informacijske varnosti v različnih sektorjih, ki so ključni za družbo in gospodarstvo ter čedalje bolj odvisni od informacijskih tehnologij. [11]

Na ravni EU imajo še posebno pomembno vlogo na področju boja proti kibernetski kriminaliteti Evropol (Evropski policijski urad) center za boj proti kibernetski kriminaliteti, Urad za evropsko pravosodno sodelovanje (Eurojust) ter Agencija EU za varnost omrežij in informacij (ENISA).

Najvišji predstavniki EU in zveze NATO so 9. julija 2016 v Varšavi podpisali skupno izjavo, v kateri so poudarili pomen nadaljnje krepitve medsebojnega sodelovanja. Izpostavljene so zlasti hibridne grožnje in kibernetska varnost, poudarek pa je tudi na izgradnji obrambnih sposobnosti tako v Evropi kot s partnerskimi državami. [17]

3 UREJANJE PODROČJA KIBERNETSKE VARNOSTI V SLOVENIJI

Usmeritvam EU na področju zagotavljanja kibernetske varnosti sledi tudi Slovenija. Februarja lani je

vlada sprejela nacionalno strategijo kibernetske varnosti, ki opredeljuje grožnje kibernetskega prostora, deležnike, področja udejanjanj, cilje in ukrepe za njihovo izvedbo. Cilj strategije je vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti (do leta 2020), ki bo preprečeval varnostne incidente in tudi odpravljal njihove posledice. To bo podlaga za varnejše delovanje infrastrukture, pomembne za delovanje državnih organov in gospodarstva, pa tudi za življenje vsakega posameznika. [12]

Eden izmed temeljev zagotavljanja kibernetske varnosti je kriptografska zaščita. Jeseni 2016 je vlada sprejela Strategijo kriptografske zaščite podatkov v RS. V njej so opredeljeni cilji, za dosego katerih so oblikovani okvirni načrti in ukrepi za vrednotenje kriptografskih rešitev, spodbujanje razvoja in uporabe kriptografskih rešitev, zagotavljanje kriptografskih rešitev, raziskovanje na področju kriptologije, usposabljanje uporabnikov kriptografskih rešitev in zagotavljanje kadrovskih virov.

Obvladovanje kriptografske zaščite komunikacij je pomemben del vsake samostojne države. Še posebej je pomembno, da imamo usposobljene posameznike iz gospodarstva in državne uprave ter z akademskega področja, ki sodelujejo in so sposobni pripraviti ter izdelati strokovne in sodobne kriptografske rešitve. Veseli smo, da ima tudi Slovenija razvijalce kakovostnih kriptografskih rešitev tako za nižje kot tudi za višje stopnje zaupnosti. Javna razkritja o namernih zlorabah nekaterih tujih kriptografskih rešitev z dejavnim sodelovanjem proizvajalcev zaradi nacionalnih interesov so povečala zaupanje v rešitve, razvite v državah EU, posledično pa tudi rast njihovih cen. Tako je zavzemanje države za razvoj slovenskih kriptografskih rešitev še bolj utemeljeno.

Vlada je v začetku aprila 2017 določila, da Urad Vlade Republike Slovenije za varovanje tajnih podatkov (UVTP) prevzame naloge nacionalnega organa za kibernetsko varnost oz. osrednje koordinacije nacionalnega sistema kibernetske varnosti. [18]

Vzpostavitev navedenega organa ni zgolj zahteva strategije, ampak tudi Direktive NIS, pomeni pa tudi izpolnitev zaveze, dane zvezi NATO. Ne nazadnje pa to kot eno od prednostnih nalog predvideva tudi Resolucija o strategiji nacionalne varnosti RS in je prva v nizu nujnih nalog za učinkovito in celovito ureditev področja v Sloveniji. [1]

Urad za varovanje tajnih podatkov bo na strateški ravni koordiniral zmogljivosti za zagotavljanje varnosti omrežij in informacijskih sistemov ter obvladovanja incidentov na vseh ravneh v državi, predstavljal enotno kontaktno točko v okviru mednarodnega sodelovanja, zagotavljal usklajeno delovanje in partnerstvo vseh pristojnih deležnikov v javni upravi, spodbujal in podpiral sodelovanje z znanstvenoraziskovalnimi institucijami, spodbujal sodelovanje z gospodarskimi družbami in zagotavljal povezovanje in sodelovanje z ustreznimi partnerji na mednarodni ravni.

Urad za varovanje tajnih podatkov je ključni in povezovalni element državnih zmogljivosti na področju kibernetske varnosti in je odločilnega pomena za pripravljenost, ukrepanje, koordinacijo, izmenjavo informacij, usklajevanje ter odzivanje na kibernetske grožnje oziroma incidente. Pri spremljanju stanja na področju kibernetske varnosti bo sodeloval z drugimi državnimi organi in koordiniral njihovo delo na tem področju. Organom bo predlagal ukrepe za izboljšanje kibernetske varnosti, jim svetoval, organiziral usposabljanja, odgovarjal na strokovna vprašanja ipd.

Pri tem bodo imeli posebno vlogo Slovenski center za posredovanje pri omrežnih incidentih SI-CERT na ARNES-u, Agencija za komunikacijska omrežja in storitve RS (AKOS), Institut Jožef Stefan in druge znanstvenoraziskovalne ter izobraževalne institucije ter subjekti kritične infrastrukture, ki se po potrebi vključujejo v načrtovanje in izvajanje dejavnosti kibernetske varnosti.

Urad za varovanje tajnih podatkov bo na strateški ravni izvajal in koordiniral zmogljivosti za zagotavljanje kibernetske varnosti na nižjih ravneh v državi, obenem pa bo enotna kontaktna točka pri mednarodnem sodelovanju. Sodeloval bo z ustreznimi organi EU, zveze NATO in organi drugih mednarodnih organizacij in držav ter skrbel za izvrševanje sprejetih mednarodnih obveznosti in pogodb na področju kibernetske varnosti. [18]

Kibernetski napadi so pogosto usmerjeni na sisteme kritične infrastrukture, saj imajo težave v njihovem delovanju lahko uničujoče posledice za delovanje širše družbe. Pri opredeljevanju meril za določitev kritične infrastrukture zato izhajamo iz posledic, ki bi jih imelo nedelovanje za državo, gospodarstvo in nekatere druge dejavnosti. [10] Prav zdaj se ureja tudi to področje. Ministrstvo za obrambo je pripravilo predlog Zakona o kritični infrastrukturi in ga poslalo v medresorsko obravnavo. Temeljni namen

predloga je sistemska ureditev zagotavljanja neprekinjenega delovanja in celovitosti kritične infrastrukture.

Ministrstvo za javno upravo je dne 7. septembra 2017 v javno obravnavo poslalo osnutek Zakona o informacijski varnosti, ki bo na obravnavano področje predvidoma z letom 2019 prinesel večje spremembe. Med drugim predvideva ustanovitev novega nacionalnega organa za kibernetsko varnost, ki bo te naloge prevzel od UVTP, in ureditev pristojnosti, nalog, organizacije in delovanja enotne kontaktne točke ter posameznih skupin za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (CSIRT) na področju zagotavljanja informacijske varnosti in kibernetske obrambe. [9]

Navedene aktivnosti pomenijo začetek obvladovanja izzivov na področju kibernetske varnosti in bodo zahtevale sodelovanje gospodarstva, akademske sfere ter pristojnih organov javne uprave.

4 UKREPI VAROVANJA

Aktivnosti in usmeritve EU in posameznih držav na področju kibernetske obrambe se preko akcijskih načrtov in različnih izvedbenih aktov odražajo tudi na operativni ravni. Informacijski sistemi, ki so ključni za varnost in delovanje države, so lahko tarča organiziranega kriminala, kibernetskega terorizma ipd. Zato pri njihovem upravljanju med drugim izvajamo tudi nekatere v nadaljevanju predstavljene varnostne ukrepe, ki jim pri običajni osebni in poslovni uporabi informacijske tehnologije (pogosto) ne namenjamo posebne pozornosti. Pri njihovi implementaciji sta zelo pomembna tudi sodelovanje z upravljavci podobnih sistemov ter medsebojna izmenjava izkušenj preko primerov dobrih praks.

Izbor in usposobljenost kadrov

Za obvladovanje groženj v kibernetskem prostoru sta najpomembnejša strokovna usposobljenost zaposlenih in prenos znanja. Vedno znova se izkaže, da je najšibkejši člen človek. Tehnologija ne more zagotavljati varnosti, če uporabniki niso ustrezno usposobljeni, se ne zavedajo tveganj ali ne upoštevajo ukrepov, s katerimi jih je mogoče obvladovati. Na Ministrstvu za zunanje zadeve izobražujemo vse zaposlene o grožnjah in ravnanjih v kibernetskem prostoru, tako diplomate, informatike, druge zaposlene kot študente na praksi. Pri tem uporabljamo tudi e-učilnico Ministrstva za obrambo. Seveda se zavedamo, da je nekajurno izobraževanje premalo (v naši nekdanji skupni državi so podobna izobraževanja potekala tudi po več tednov).

Za dejanji, ki so v nasprotju z interesi države ali delodajalca, pogosto stojijo nezadovoljni posamezniki, zamere iz preteklosti ali nasprotni politični interesi. S tajnimi vsebinami zato lahko delajo samo preverjene osebe, za katere lahko zagotovimo, da so vredne zaupanja. Zato pred izdajo dovoljenja za dostop izvedemo postopek varnostnega preverjanja – opravi ga pristojni državni organ (MNZ, MORS ali SOVA). V postopku zberejo podatke o morebitnih varnostnih zadržkih. Nekatera možna tveganja, ki jih preverjajo, so:

- zasvojenost z alkoholom, drogami ali druge oblike zasvojenosti,
- bolezen ali duševne motnje,
- stiki s tujimi varnostnimi in obveščevalnimi službami,
- članstvo ali sodelovanje v organizacijah ali skupinah, ki ogrožajo vitalne interese države ali političnih, obrambnih in varnostnih zvez, katerih del je Slovenija,
- neizbrisani disciplinski ukrepi,
- tekoči kazenski postopki,
- sodelovanje v tujih oboroženih silah ali drugih oboroženih formacijah,
- finančne obveznosti in prevzeta jamstva ter lastništvo nepremičnin,
- lastnosti in druge okoliščine, zaradi katerih bi bili lahko izpostavljeni izsiljevanju ali drugim oblikam pritiska (povzeto po Zakonu o tajnih podatkih).

Izolacija sistemov

Podatki, ki so zelo pomembni za varnost oziroma interese države, se obravnavajo samo v posebnih sistemih, ki so fizično popolnoma ločeni od druge informacijsko-komunikacijske infrastrukture in niso povezani z internetom.

Namenske šifrirne rešitve

Zaščita prenosa podatkov je med ključnimi vidiki kibernetske varnosti. To se je dodatno potrdilo z razkritjem zlorab nekaterih splošno uveljavljenih (priznanih) produktov. Uporabljajo se lahko samo rešitve, ki so ustrezno preverjene in imajo izdano potrdilo o varnostni ustreznosti.

Zaščita pred neželenimi elektromagnetnimi emisijami – TEMPEST

Gre za posebno namensko opremo, ki je zaščitena pred odtekanjem podatkov prek elektromagnetnega sevanja in prevodne (podatkovne, napajalne) infrastrukture. Obravnavane vsebine namreč tako lahko nenadzorovano odtekajo iz sistemov. Zahteve določa Natov standard SDIP-27, ki ima določeno stopnjo tajnosti in ni javno objavljen.

Fizični ukrepi varovanja

Ključne sestavine sistema se namestijo v varnostnih območjih. Gre za poseben stalno varovan prostor iz betona in jekla s protivlomno zaščito in tehničnimi ukrepi varovanja, v katerem je samo nujno pohištvo ter čim manj opreme in napeljav. Osnovni pogoji, ki jim mora ustrezati varnostnotehnična oprema, so določeni s sklepom vlade. [16]

Preprečevanje optičnih napadov

Oprema je postavljena tako, da je preprečeno prestrezanje zaslonske slike, neposredno ali prek odboja.

Preprečevanje akustičnih napadov

Redno izvajanje protiprisluškovalnih pregledov in preprečevanje napadov prek vibracij okenskih stekel (z laserskim mikrofonom) in predmetov v prostoru. Med te ukrepe je mogoče uvrstiti tudi prepoved vnosa naprav, ki omogočajo snemanje zvoka ali slike.

Uporaba neinformacijske opreme

V nekaterih posebnih primerih je tveganje uporabe informacijske tehnologije ne glede na posebne varnostne ukrepe še vedno lahko previsoko. Vsebine se obravnavajo v tako imenovanih gluhih sobah brez elektronske opreme. Morebitni dokumenti se izdelajo na papirju, med lokacijami pa jih prenašajo le pooblaščeni in posebej usposobljeni kurirji.

5 SKLEP

Kibernetska varnost je postala integralni del varnosti držav in mednarodne skupnosti. Grožnje presegajo meje virtualne sfere in lahko povzročijo uničujoče posledice v resničnem svetu. Obravnavati jih moramo na različnih ravneh, od kritične infrastrukture držav, sistemov, ki so pomembni za delovanje družbe, do posameznikov. Slovenija je dejavno pristopila k obvladovanju izzivov na tem področju. Z ustanovitvijo nacionalnega organa za kibernetsko varnost se postavljajo temelji za celovito obravnavo problematike in usklajevanje dejavnosti na strateški ravni. Motivi kibernetske kriminalitete se izražajo predvsem v želji po vplivu na družbene in politične spremembe. Tarča takih napadov so zato sistemi kritične infrastrukture oziroma informacijsko-komunikacijski sistemi, ki so ključni za delovanje države. Ker so teroristične in kriminalne združbe pri napadih tehnično usposobljene in inovativne, je treba temu prilagoditi tudi varovanje, ki se mora izvajati na različnih ravneh. Sem spadajo ukrepi, na katere pri običajni poslovni ali osebni uporabi računalniške opreme niti ne pomislimo. Predvsem pa so pomembni krepitev zaupanja na državni ravni, strokovna usposobljenost kadra in prenos znanja na področju kibernetske varnosti. Kljub tehniki se namreč pogosto izkaže, da je najšibkejši člen še vedno človek.

6 LITERATURA IN VIRI

[1] Državni zbor RS, Resolucija o strategiji nacionalne varnosti RS. (2010). Uradni list RS, št. 27/2010.

[2] Evropska komisija, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013). http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (obiskano 10. 9. 2017).

[3] Evropska komisija, Evropska agenda za varnost. (2015). europa.eu/rapid/press-release_IP-16-1445_sl.pdf (obiskano 16. 9. 2017).

[4] Evropska komisija, Evropska agenda za varnost: Vprašanja in odgovori. (2015). europa.eu/rapid/press-release_MEMO-15-4867_sl.pdf (obiskano 16. 9. 2017).

[5] Evropska komisija, Načrt kibernetske varnosti EU za zaščito odprtega interneta ter svobode in priložnosti na spletu – sporočilo za medije. (2013). http://europa.eu/rapid/press-release_IP-13-94_sl.htm (obiskano 16. 9. 2017).

[6] Gibson, W. (1984). *Neuromancer*. New York: Ace Science Fiction Books.

[7] Government Business Council, Achieving Holistic Cybersecurity: 2016 Progress Report. (2016). http://www.govexec.com/insights/reports/achieving-holistic-cybersecurity-2016-progress-report/127435/ (obiskano 16. 9. 2017).

[8] Maček, S., Močilar, F., Mulec, F. (2016). Osnovni koncepti zagotavljanja kibernetske varnosti. *Sodobne tehnologije in storitve OTS 2016: zbornik enaindvajsete konference, Maribor, 14. in 15. junij 2016*.

[9] Ministrstvo za javno upravo, Javna obravnava osnutka predloga Zakona o informacijski varnosti – redni postopek, številka: 007-644/2017-1. (2017).

[10] Ministrstvo za obrambo, Veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v RS. (2014). http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture (obiskano 16. 9. 2017).

[11] SI-CERT, EU enotno k zaščiti interneta, https://www.cert.si/eu-enotno-k-zasciti-interneta/ (obiskano 16. 9. 2017).

[12] Strategija kibernetske varnosti. (2016). http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Startegija_KV.pdf (obiskano 16. 9. 2017).

[13] Svet EU, Direktiva 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji – Direktiva NIS. (2016). *Uradni list EU, 194*, 1–30.
[14] Svet Evrope, Konvencija Sveta Evrope o kibernetski kriminaliteti. (2001). http://www.svetevrope.si/sl/dokumenti_in_publikacije/konvencije/185/ (obiskano 16. 9. 2017).
[15] Urad za varovanje tajnih podatkov, Nacionalni organ za kibernetsko varnost. (2017). http://www.uvtp.gov.si/si/medijsko_sredisce/novica/article/335/1360 (obiskano 16. 9. 2017).
[16] Vlada RS, Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja. (1994). *Uradni list RS,* št. *94/06.*
[17] Vlada RS, Sporočila za javnost. (2016). http://www.vlada.si/predsednik_vlade/ sporocila_za_javnost/a/premier_dr_cerar_varsavski_vrh_prelomen_za_ustreznejse_odzive_zaveznistva_na_sodobno_varnostno_okolje_63 (obiskano 16. 9. 2017).
[18] Vlada RS, Vladno gradivo, številka 007-8/2017/11. (2017). http://vrs-3.vlada.si/MANDAT14/VLADNAGRADIVA.NSF/ 18a6b9887c33a0bdc12570e50034eb54%2F3c2877f0c0cfeb87c12580f3002993fa%2F%24FILE%2FVG_sklep.doc (obiskano 16. 9. 2017).

▪

Samo Maček je po izobrazbi magister znanosti s področja računalništva in informatike. Zaposlen je kot vodja Sektorja za informatiko v Generalnem sekretariatu Vlade RS, kjer med drugim opravlja naloge na področju informacijske varnosti, informacijskih sistemov za obravnavanje tajnih podatkov, razvoja spletnih aplikativnih rešitev ter upravljanja dokumentnih in relacijskih baz podatkov. Pred tem je vodil Oddelek za organizacijo in kadrovsko informatiko na Ministrstvu za notranje zadeve. Razvil je številne informacijske rešitve, ki so v uporabi v vladnem informacijskem sistemu, organih državne uprave in gospodarskih družbah.

▪

Franci Mulec je magistriral na Fakulteti za organizacijske vede Univerze v Mariboru. Zadnjih 15 let se ukvarja z razvojem in zagotavljanjem informacijske varnosti visoko varnih sistemov. Je arhitekt več sistemov Republike Slovenije, član ISACA (Information Systems Audit and Control Association) in nosilec CISA (Certified Information Systems Auditor).

▪

Franc Močilar je diplomiral in magistriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zadnjih 15 let se ukvarja z zagotavljanjem informacijske varnosti. Leta 2005 je opravil izpit in pridobil potrdilo CISSP (Certified Information Systems Security Professional) mednarodne neprofitne organizacije ISC2 (http://www.isc2.org) za preverjanje znanj in podeljevanje ter vzdrževanje potrdil s področja varovanja informacij. Zaposlen je na Ministrstvu za zunanje zadeve RS.

Zakonodajni in tehnični vidik varovanja osebnih podatkov v slovenskih zdravstveno-informacijskih sistemih

Luka Hrgarek, Leon Bošnjak, Tatjana Welzer Družovec, Aida Kamišalić
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Koroška cesta 46, 2000 Maribor
{luka.hrgarek leon.bosnjak tatjana.welzer aida.kamisalic}@um.si

Izvleček

Varovanje osebnih podatkov je problematika, ki je vsak dan bolj aktualna. Različne novodobne kršitve zasebnosti nastajajo tudi zaradi hitrega tehnološkega razvoja, ki mu zavedanje o potrebah po varovanju podatkov kljub naporom stroke ne sledi dovolj hitro. Omenjena problematika je v zdravstvu še posebno prisotna in pomembna. Velika večina zdravstvenih podatkov je digitaliziranih. Dostopnost in varnost teh podatkov lahko zato hitro postane vprašljiva. Vsi, ki so vključeni v zdravstvene procese, se morajo zavedati, da je varno in pravilno ravnanje s temi podatki ključnega pomena.

Direktiva Evropskega parlamenta o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takšnih podatkov določa smernice za vse države članice Evropske unije. Ta priporočila morajo države članice upoštevati in spoštovati v svojih zakonodajah, povezanih z varstvom osebnih podatkov. V Sloveniji varstvo osebnih podatkov v zdravstvu obravnavajo Ustava Republike Slovenije, Zakon o varstvu osebnih podatkov in Zakon o pacientovih pravicah.

V članku se bomo osredinili na pregled direktiv Evropske unije, slovenske zakonodaje in dokumentacije s področja varovanja osebnih podatkov v zdravstvu. Pregledali bomo dostopno dokumentacijo o bolnišničnih informacijskih sistemih po Sloveniji. Z analizo de facto stanja v slovenskem zdravstvu želimo ugotoviti, kako dobro se slovensko zdravstvo prilega zakonodaji: na kakšen način so implementirani zakonsko zagotovljeni varnostni mehanizmi, kako so podatki zaščiteni pri prenosu in kako sistemi in osebje varujejo osebne podatke bolnikov.

Ključne besede: zdravstveno-informacijski sistemi, zasebnost podatkov, zaupnost podatkov, zakonodaja.

Abstract

Legislative and technical aspects of protection of personal data in Slovenian healthcare information systems

Privacy is an issue that is becoming increasingly more relevant. Various contemporary privacy violations are also linked to rapid technological development. Despite efforts in healthcare to increase the awareness of the necessity of data protection, users remain slow to adapt these changes. The aforementioned issues are particularly pressing and important in healthcare. The vast majority of healthcare data is digitized. Availability and security of such data can quickly become questionable. Those involved in healthcare processes should be aware that safe and proper handling of such data is crucial.

The Directive of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data provides guidelines for all Member States of the European Union. Member States must take into account and comply with these recommendations within their laws related to personal data protection. In Slovenia, the protection of personal data in healthcare is addressed by the Constitution, the Personal Data Protection Act and the Patient Rights Act.

In this article, we focus on the review of the directives of the European Union, the Slovenian legislation and technical documentation from the field of personal data protection in healthcare. We review the available documentation on hospital information systems in Slovenia. By analyzing the de facto situation in Slovenian healthcare, we determine how well it adheres to the legislation: how security mechanisms provided by law are implemented, how data is protected and how the systems and personnel protect the personal data of patients.

Keywords: healthcare information systems, data privacy, data confidentiality, legislation

1 UVOD

Povprečna starost prebivalstva v Sloveniji se veča, prav tako se podaljšuje življenjska doba. S tem se povečuje tudi potreba po storitvah v zdravstvu. Z napredkom, ki smo mu priča v sedanjem času, prihajajo nove tehnologije, katerih uporaba prinaša veliko izzivov. Vsaka nova vpeljava tehnologij odpira različna etična in varnostna vprašanja. Pred obdobjem naprednega računalništva in komunikacijskih tehnologij je bilo združevanje informacij tudi o eni sami osebi naporno, časovno potratno in močno odvisno od muhavosti človeških čuvajev teh podatkov (Hough, 2009). Varovanje zasebnosti lahko bolnišnicam z elektronsko izmenjavo podatkov koristi, vendar samo v primeru, če se bolniki zavedajo, da bodo njihove zdravstvene informacije obravnavane zaupno. Le na podlagi tega bodo namreč pripravljeni posredovati natančne podatke. Po drugi strani pa zaščita zasebnosti za elektronsko izmenjavo informacij pomeni višji strošek, kar zmanjša korist (Miller in Tucker, 2009).

Na področju zdravstva srečujemo pojme, kot so elektronska zdravstvena kartoteka, storitve eNaročanja in eRecepti, ki se arhitekturno izvajajo v različici modela odjemalec – strežnik, v katerem vsa vmesna komunikacija poteka prek interneta. To komunikacijo je treba zavarovati, sicer so podatki izpostavljeni napadom: kraji, nepooblaščenem spreminjanju in ponarejanju. V postopku razvoja programske opreme razvijalci pogosto izberejo linijo najmanjšega odpora in rešitev razvijajo z vidika funkcionalnosti, medtem ko je varnost stranskega pomena. Takšen površen pristop se »obrestuje« v vseh razvijalskih domenah, še posebno pa v zdravstvu.

Zdravstveni podatki so občutljivi osebni podatki (Zakon o varstvu osebnih podatkov RS, 2004), katerih razkritje pomeni invaziven vdor v posameznikovo zasebnost. Westin definira zasebnost kot »trditev posameznikov, skupin ali institucij, da lahko sami zase odločajo, kdaj, kako in v kakšnem obsegu bodo drugim razkrili informacije o sebi«. Poleg občutljivih osebnih podatkov morajo zdravstvene institucije varovati tudi druge občutljive podatke, ki niso nujno osebni podatki (slika 1). Danes se v svojem digitalnem življenju prostovoljno odpovedujemo različnim vidikom zasebnosti in razkrivamo več informacij, kot se sami zavedamo. Čeprav takšno početje za namene izkoriščanja ugodnosti, ki nam jih ponujajo socialna omrežja, morda ni varnostno kritično, pogosto pozabljamo, da je področje zdravstvenih podatkov veliko bolj občutljivo.

Slika 1: **Odnos med osebnimi in občutljivimi podatki**

Zdravstveni podatki so kot posebna kategorija domensko specifičnih podatkov izpostavljeni različnemu osebju, ki dostopa do njih in jih uporablja. Prav tako marsikje s temi podatki upravljajo z zastarelo programsko opremo, ki še vedno deluje, vendar ne zagotavlja vseh potrebnih konceptov varnosti in zasebnosti. Pri upravljanju in varovanju podatkov je treba zagotoviti tudi njihovo sledljivost, saj s tem omogočamo možnost kasnejšega ugotavljanja zlorab. Sledljivost je prav tako preventivni mehanizem, saj lahko v nekaterih primerih že zavedanje o tem odvrne posameznika, da bi neupravičeno dostopal do osebnih podatkov (Informacijski pooblaščenec RS, 2008). Kljub visokim moralnim standardom, ki jih vsi bolniki pričakujemo od zdravstvenih delavcev, je izjemno pomembna zakonodaja, ki predpisuje, »kdaj, kako in v kakšen obsegu« je treba podatke varovati.

V članku bomo povzeli evropsko in slovensko zakonodajo s področja varnosti zdravstvenih podatkov, pregledali javno dostopno dokumentacijo o zdravstveno-informacijskih sistemih v Republiki Sloveniji ter njihovo prileganje obstoječi zakonodaji. Konkretno smo se osredinili na varovanje komunikacijskih poti, saj so te najbolj izpostavljene napadalcem. Po drugi strani gre pri varovanju prostorov, sistemske programske opreme ter uporabi in obdelavi podatkov, ki jih ZVOP in prilegajoča zakonodaja prav tako naslavljata, za občutljive informacije, do katerih nezdravstveno osebje nima dostopa.

2 ZAKONODAJA

2.1 Evropska zakonodaja

Krovni dokument evropske zakonodaje, ki omenja varstvo osebnih podatkov, je Listina Evropske unije o temeljnih pravicah. Ta v svojem 8. členu pravi, da »ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj«.

Direktiva Evropskega parlamenta in Sveta o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu v svojem 25. členu govori o zagotavljanju pretoka osebnih podatkov med državami članicami, hkrati pa tudi o potrebi po varstvu temeljnih pravic posameznikov – v tem primeru varstvu osebnih podatkov. V nadaljevanju se sklicuje na Direktivo 95/46/ES Evropskega parlamenta in Sveta iz leta 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takih podatkov, pri čemer je posameznikom zagotovljena pravica dostopa do lastnih osebnih podatkov o zdravju.

Ena ključnih komponent digitalnega zdravstva je elektronska zdravstvena kartoteka (angl. Electronic health record, EHR), ki je sistematična zbirka elektronsko hranjenih zdravstvenih informacij o pacientu in populaciji v digitalni obliki (Gunter in Terry, 2005). Ti zapisi so na voljo različnim vejam zdravstvene dejavnosti, saj lahko v eni elektronski zdravstveni kartoteki hranimo demografske podatke, zgodovino bolezni, seznam alergij, imunizacijski status, radiološke zapise in podobno. Celovita in obširna elektronska zdravstvena kartoteka lahko zdravniku zagotovi boljši pregled nad bolnikovim zdravstvenim stanjem, kar omogoča sprejetje celovitejših diagnoz in posledično ustreznejših ukrepov. Prav tako pa lahko množica medicinskih informacij, ki so vsebovane v elektronski zdravstveni kartoteki, pomeni grožnjo posameznikovi zasebnosti, saj so na enem mestu shranjeni vsi podatki o bolniku (npr. podatki o spolno prenosljivih boleznih, duševnih motnjah, odvisnostih od drog ali alkohola) in je do njih laže dostopati in jih replicirati kot podatke na papirnatih zapisih (Adamski, 2014).

Zaradi stopnje občutljivosti podatkov, ki so hranjeni v elektronski zdravstveni kartoteki, ravnanje z njo pogosto obravnava zakonodaja. V tabeli 1 vidimo, katere države članice EU imajo urejeno zakonodajo glede elektronskih zdravstvenih kartotek. Čeprav področje zdravstvenih podatkov ureja v različnih zakonih, slovenska zakonodaja ne obravnava pojma elektronska zdravstvena kartoteka. Obstoječi nacionalni sistem eZdravje podpira storitvi eRecept in eNaročanje, hkrati pa spletni portal Zavoda za zdravstveno zavarovanje Slovenije omogoča dostop do osebnih podatkov zavarovanca, izbranega zdravnika in zobozdravnika. Prav tako portal ZZZS omogoča prikaz seznama obiskov zdravnika in podatke o stroških zavarovanja za posamezni obisk, ne vključuje pa nobenih medicinskih podrobnosti obiska.

Tabela 1: **Določitev posebnih pravil o vsebini elektronskih zdravstvenih kartotek po državah članicah EU (Adamski, 2014)**

Avstrija	✓	Latvija	✓
Belgija		Litva	✓
Bolgarija		Luksemburg	✓
Ciper		Madžarska	
Češka		Malta	
Danska	✓	Nizozemska	
Estonija	✓	Poljska	
Finska	✓	Portugalska	✓
Francija	✓	Romunija	✓
Nemčija	✓	Slovaška	✓
Grčija		Slovenija	
Hrvaška	✓	Španija	✓
Irska		Švedska	✓
Italija	✓	Združeno kraljestvo	

2.2 Slovenska zakonodaja

Ustava Republike Slovenije v svojem 38. **členu (Varstvo osebnih podatkov) zagotavlja varstvo osebnih podatkov in prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja. Podrobnosti glede zbiranja, obdelovanja, namena uporabe, nadzora in varstva tajnosti osebnih podatkov določa Zako**n o varstvu osebnih podatkov. (Ustava Republike Slovenije, 2006)

Zakon o varstvu osebnih podatkov (ZVOP) definira osebni podatek kot »kateri koli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen«, pri čemer je posameznik fizična oseba, ki jo je mogoče enolično določiti in identificirati. V svojem 6. členu opredeljuje različne pojme, ki jih uporablja v nadaljevanju, med drugim tudi pojem občutljivih osebnih podatkov, med katere uvršča podatke o zdravstvenem stanju. V 13. členu ZVOP določa primere, ko občutljive osebne podatke lahko obdelujemo. Takšno dovoljenje dobijo zdravstveni delavci, če gre za namen zdravstvenega varstva prebivalstva in

posameznikov ter vodenja ali opravljanja zdravstvenih služb.

Nepooblaščenim osebam mora biti onemogočen dostop do občutljivih osebnih podatkov, kar mora biti zagotovljeno s posebnim načinom njihovega označevanja in zavarovanja (14. člen). ZVOP zahteva uporabo kriptografskih metod in elektronskega podpisa pri prenosu po telekomunikacijskih omrežjih za zagotavljanje nečitljivosti oziroma neprepoznavnosti.

V tretjem poglavju (24. člen) določa ukrepe, ki jih je treba zagotoviti, da se podatki lahko ustrezno varujejo. Zahteva varovanje prostorov, opreme in sistemske programske opreme, v kar spada tudi skupina vhodno-izhodnih enot. Prav tako je treba zagotoviti varno aplikativno programsko opremo, ki se uporablja za obdelavo podatkov. Zakon zahteva preprečevanje nepooblaščenega dostopa do osebnih podatkov pri njihovem prenosu, posebno pri prenosu po telekomunikacijskih omrežjih. Da bi dosegli sledljivost in nezanikanje, ZVOP predpisuje implementacijo možnosti poznejšega ugotavljanja metapodatkov o vnašanju, uporabi in obdelavi podatkov. Vsi zaposleni, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, tako v času zaposlitve kot tudi po njenem prenehanju. (Zakon o varstvu osebnih podatkov RS, 2004)

Zakon o pacientovih pravicah (ZPacP) ureja množico pacientovih pravic, med drugimi tudi pravico do varstva zasebnosti in varstva osebnih podatkov. S tem se podrobno ukvarja 44. člen zakona, ki v svojem prvem stavku pravi: »Pacient ima pravico do zaupnosti osebnih podatkov, vključno s podatki o obisku pri zdravniku in drugih podrobnostih o svojem zdravljenju.« Določa, da morajo zdravstveni delavci in zdravstveni sodelavci s podatki ravnati »v skladu z načelom zaupnosti in predpisi, ki urejajo varstvo osebnih podatkov« (Zakon o pacientovih pravicah RS, 2008).

Zakon o zbirkah podatkov s področja zdravstvenega varstva (ZZPPZ) določa načine obdelave podatkov in upravljanja z zbirkami podatkov na področjih zdravstvenega varstva in storitve eZdravje. Poleg drugih izvajalcev zdravstvene dejavnosti zakon navaja Nacionalni inštitut za javno zdravje (NIJZ) kot »upravljalca zbirk podatkov s področja zdravstvenega varstva«.

Način zbiranja osebnih podatkov je lahko posredni ali neposredni. Pri posrednem zbiranju ZZPPZ pravi, da posameznika ni treba seznaniti z dejstvom, da bodo njegovi podatki pridobljeni iz drugih zbirk podatkov. Prav tako opredeljuje, do katerih podatkov iz Centralnega registra prebivalstva (CRP) imajo upravljalci zbirk pravico brezplačnega dostopa. To so: EMŠO, ime in priimek, kraj rojstva, leto rojstva, spol, prebivališče in vrsta prebivališča, državljanstvo, zakonski stan, šolska izobrazba, EMŠO matere, EMŠO očeta, EMŠO zakonca, EMŠO otrok, datum in podatki o dogodkih, spremembah ali popravkih. Kot primarni ključ oziroma enotni identifikator, po katerem se ti podatki lahko povezujejo med seboj, lahko upravljalci zbirk uporabljajo številko zdravstvenega zavarovanja s kartice zdravstvenega zavarovanja.

S področjem zavarovanja podatkov se ukvarja samo 7. člen zakona, ki pravi: »Tehnične in organizacijske ukrepe za zavarovanje podatkov v zbirkah podatkov predpiše minister, pristojen za zdravje, v soglasju z ministrom, pristojnim za pravosodje, in ministrom, pristojnim za znanost in tehnologijo.« V nadaljevanju se ZZPPZ ukvarja z metodološkimi načeli: predpisuje uporabo enotnih standardov – definicij, klasifikacij in šifrantov, ki jih določi minister, pristojen za zdravje. (Zakon o zbirkah podatkov s področja zdravstvenega varstva RS, 2000)

Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva je nastal na podlagi določb Zakona o varstvu osebnih podatkov in 9. člena Statuta Zbornice zdravstvene in babiške nege Slovenije – Zveze društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije. Pravilnik določa »organizacijske in logično tehnične postopke in ukrepe za varovanje zaupnih in osebnih podatkov« v Zbornici – Zvezi. V svojem 3. členu pravilnik pravi, da morajo biti prostori, v katerih se nahajajo strojna oprema in nosilci zaupnih ali osebnih podatkov, varovani z ukrepi, ki nepooblaščenim osebam onemogočajo dostop. V šestem stavku istega člena govori tudi o izklapljanju in fizičnem ali programskem zaklepanju računalnikov in druge strojne opreme izven delovnega časa. Glede poslovanja s strankami 6. člen zahteva, da so »nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje«.

V nadaljevanju pravilnik opisuje dovoljene načine vzdrževanja in popravila strojne, računalniške in druge opreme. To opremo lahko vzdržujejo samo pooblaščeni servisi in vzdrževalci (8. in 11. člen), ki imajo z Zbornico – Zvezo sklenjeno ustrezno pogodbo. V 9. členu določa, da se zaposleni, ki nimajo dovoljenja

za vpogled v podatke, lahko gibljejo samo v prostorih, kjer je vpogled v podatke onemogočen. Zaposlenim je prepovedano nameščanje programske opreme brez eksplicitnega dovoljenja upravnega odbora.

Z identifikacijo in avtorizacijo se ukvarja 15. člen pravilnika, ki predpisuje uporabo sistema gesel za dostop do podatkov prek aplikativne programske opreme. Razmislek nadaljuje 16. člen, ki govori o generalnih, »supervizorskih« geslih. Ta bi se naj hranila »v zapečatenih ovojnicah« in varovala kot »uradna tajnost – strogo zaupno«.

17. člen zahteva redno izdelavo varnostnih kopij, ki se hranijo na za to določenih in ustrezno varovanih mestih. Prav tako mora biti vsako prenašanje podatkov prek telekomunikacijskih ali drugih omrežij ustrezno varovano (člen 18). Pravilnik se v svojem 19. členu navezuje na 38. člen Ustave RS, ki pravi, da se lahko »zbirajo in obdelujejo samo tisti podatki, ki imajo ustrezno zakonsko osnovo«. Definirano je tudi brisanje podatkov po preteku roka hranjenja (20. člen), in to s tako metodo, »da je nemogoča restavracija vseh ali le dela brisanih podatkov« (21. člen). (Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva, 2005)

3 ZDRAVSTVENO-INFORMACIJSKI SISTEMI V SLOVENIJI

Svetovna zdravstvena organizacija je opredelila zdravstveno-informacijski sistem kot temeljni pogoj za uresničevanje ciljev Zdravja v 21. stoletju (World Health Organization, 1999). Po pregledu domenske zakonodaje smo izvedli pregled zdravstvenih informacijskih sistemov z območja Republike Slovenije. Ti sistemi so komercialni in njihova dokumentacija ni prosto dostopna. Zato smo pregledali dostopne podatke o krovnem sistemu Ministrstva za zdravje.

Ministrstvo za zdravje je leta 2008 začelo z izvedbo podpornih podprojektov nacionalnega projekta eZdravje, leta 2011 pa je ustanovilo tudi sektor eZdravje. Danes v okviru eZdravja deluje 17 aplikacij. Za dostop do nekaterih storitev je za uporabnike zahtevana uporaba digitalnega potrdila. Uporabnikom je na voljo portal zVEM (zdravjeVsenaEnemMestu), ki omogoča dostop do storitev eZdravja. Od pomladi 2016 omogoča dostop do storitev eRecept in eNaročanje. Prvotna investicijska dokumentacija ministrstva je razdelila nacionalni zdravstveni informacijski model na tri komponente: ogrodje slovenskega referenčnega zdravstvenega informacijskega modela, slovenski terminološki slovar zdravstvene informatike in slovenski podatkovni slovar zdravstvene informatike (Ministrstvo za zdravje RS, 2009).

Razen nacionalnih sistemov, za katere skrbi Ministrstvo za zdravje, posamezne bolnišnice razvijajo tudi lastne sisteme, ki so prilagojeni njihovim potrebam in specifikam. Takšni sistemi se pogosto uporabljajo za naročanje bolnikov na posamezne preiskave ali posege. Spletni portal Slo-Tech je 16. marca 2017 poročal o razkritju nevarnosti v sistemu ustanove, ki bolnikom omogoča prijavljanje na preglede po spletu. Razkrili so, da spletna stran ne uporablja zaščitene povezave HTTPS, temveč nezaščiteno povezavo HTTP, kar pomeni, da so pacienti posredovali svoje osebne podatke z uporabo nezaščitene povezave. Prenos podatkov prek povezave HTTPS zagotavlja varnost in zasebnost ter zmanjšuje tveganje, da bi tretja oseba prestregla, spremenila ali zlorabila podatke. Uporaba nezaščitene povezave za prenos osebnih podatkov je v nasprotju z zahtevami Zakona o varstvu osebnih podatkov, ki v svojem 14. členu zahteva uporabo kriptografskih metod in elektronskega podpisa za prenos takšnih podatkov po telekomunikacijskih omrežjih. Po javnem opozorilu je omenjena zdravstvena ustanova namestila varovano povezavo HTTPS (Kovačič, 2017b).

Omenjeni spletnih portal je 3. aprila objavil članek, v katerem je opozoril na dejstvo, da imajo tudi druge zdravstvene ustanove v Sloveniji težave z informacijsko varnostjo svojih sistemov. Razkrili so, da ena izmed ustanov ne uporablja povezav HTTPS kljub temu, da morajo pacienti v sistem, s katerim se naročajo na preiskave ali posege, vnesti zdravstveno diagnozo poleg drugih osebnih podatkov, kot so ime, priimek, naslov in številka kartice zdravstvenega zavarovanja. Kot primer so navedli še dve drugi ustanovi, ki prav tako nista imeli implementirane povezave HTTPS. Članek je vseboval tudi zaslonske posnetke, iz katerih je razvidno, da povezava HTTPS dejansko ni bila uporabljena (Kovačič, 2017a). Nekaj dni po izidu članka smo preverili stanje na spletnih sistemih omenjenih bolnišnic in ugotovili, da se je stanje nekoliko izboljšalo, saj so vse omenjene bolnišnice implementirale povezavo HTTPS.

Prav tako smo pregledali spletne strani vseh slovenskih bolnišnic in ugotovili, da na svojih spletnih straneh uporablja povezavo HTTPS trinajst bolnišnic, dvanajst pa ne. Poiskali smo tudi spletne obrazce za naročanje na preglede ali posege in ugotovili,

da naročanja na lastnih spletnih straneh omogoča devet bolnišnic, šestnajst pa ne. Poleg tega, da večina bolnišnic bolnike usmerja na centralni portal za eNaročanje (https://narocanje.ezdrav.si/), je pomemben podatek tudi to, da nobena bolnišnica ne omogoča naročanja brez uporabe povezave HTTPS.

4 RAZPRAVA

Veliko podatkov, ki jih trenutno zbirajo in o njih poročajo v okviru zdravstveno-informacijskega sistema, v resnici ni potrebnih za uresničevanje ciljev zdravstvene dejavnosti (Eržen, 2004). Obdelava osebnih podatkov se lahko nanaša na kakršno koli ravnanje s podatki, vključno s samim dostopom do njih. Zato mora zdravstveno-informacijski sistem omogočati sledljivost celotne obdelave osebnih podatkov. Sledljivost lahko razdelimo na tri ravni: sledljivost sprememb, sledljivost dostopa do podatkov in popolno sledljivost z beleženjem dostopov, sprememb podatkov ter beleženjem tako izvornih kot popravljenih podatkov. Na prvi ravni sledljivosti je kasneje mogoče identificirati uporabnika, ki je vnašal, spreminjal ali brisal določeni podatek, ter ugotoviti čas tega dogodka. Druga raven sledljivosti izpolnjuje enake zahteve kot prva, ob tem pa omogoča še sledljivost podatkov o času in identiteti uporabnika, ki dostopa do posameznega podatka. Tretja raven sledljivosti omogoča pregled zgodovine sprememb, kar pomeni, da hrani celotni življenjski cikel podatka z vsemi metapodatki (Informacijski pooblaščenec RS, 2008). Informacijski pooblaščenec RS tolmači, da ZVOP zahteva drugo raven sledljivosti podatkov.

Pri pripravi zakonov se zakonodajalec ne more spuščati v specifike in tehnične podrobnosti, saj morajo biti ti dovolj široki in tehnološko nevtralni, da lahko zajamejo različna realna stanja (Informacijski pooblaščenec RS, 2008). Vendar lahko poudarimo, da potrebna tehnična specifikacija zakonskega okvira ni javno dostopna in zaradi tega ni mogoče ugotavljati skladnosti obstoječih sistemov z zakonodajo. Hkrati ugotavljamo, da je tehnična dokumentacija zdravstveno-informacijskih sistemov prav tako nedostopna. Ker gre za komercialne proizvode, je to razumljivo, saj želimo implementacijske podrobnosti ohraniti zasebne, da ne izpostavljamo morebitnih ranljivosti sistema. Po drugi strani pa pričakujemo, da bi znotraj vladnih institucij moralo obstajati telo, ki bi pripravljalo tehnične specifikacije zakonskega okvira in skrbelo za njihovo ažuriranje glede na svetovne smernice s posameznega področja. Eden izmed možnih primerov bi lahko bilo predpisovanje uporabe konkretnih kriptografskih algoritmov (npr. algoritma AES) za šifriranje občutljivih osebnih podatkov ali obvezna uporaba povezave HTTPS. Prav tako bi morali odgovoriti na vprašanje, kdo ima lahko dostop do šifrirnega ključa (npr. osebni zdravnik, specialist, zdravstveni tehnik, bolnik), in tako pokriti področje zaupnosti osebnih podatkov. Tako pripravljene tehnične specifikacije bi morale biti javno dostopne. S tem bi omogočili validacijo zdravstveno-informacijskih sistemov in zagotavljali primerno raven kakovosti, kar je v končni fazi v interesu javnosti.

5 SKLEP

Zdravstveni delavci so tisti, ki se morajo držati visokih etičnih standardov, primernih za njihov poklic, saj v nasprotnem primeru izgubijo zaupanje svojih bolnikov. Pri kroničnih bolnikih ter pripadnikih rasnih in etničnih manjšin obstaja še večja skrb glede zasebnosti njihovih zdravstvenih podatkov, zato se bolj pogosto dogaja, da zadržijo informacije, ker se bojijo njihove neustrezne uporabe. Za vzpostavitev večjega javnega zaupanja v informacijske tehnologije na področju zdravstva in olajšanje hitrejšega sprejetja obetavnih novih tehnologij je treba obravnavati varnostna in zasebnostna tveganja.

Ugotovili smo, da evropska in slovenska zakonodaja postavljata podlage za varno delovanje zdravstveno-informacijskih sistemov, kar pomeni zgolj temelj za zagotavljanje ustrezne ravni varnosti. Tudi če obstajajo tehnične specifikacije zakonskih okvirov, ki bi omogočale doseganje in zagotavljanje primerne ravni varnosti, niso javno dostopne. Prav tako ni dostopna dokumentacija o zdravstveno-informacijskih sistemih, zaradi česar nismo uspeli analizirati stopnje prileganja obstoječi zakonodaji. To študijo bomo izvedli na podlagi osebnih stikov z odgovornimi za implementacijo zdravstveno-informacijskih sistemov v slovenskem zdravstvu. Prav tako želimo izvesti primerjalno študijo, v kateri bomo pregledali stanje v bolnišničnih informacijskih sistemih sosednjih držav, saj bo takšna študija podala širši in kompleksnejši pogled na trenutno stanje informatike v slovenskih bolnišnicah in pokazala morebitne smernice za prihodni razvoj.

6 LITERATURA

[1] Adamski, D. (2014). *Overview of the National Laws on Electronic Health Records in the EU Member States. National Report for Poland.* Brussels, Belgium: Milieu Ltd & Time. lex. Retrieved from http://ec. europa. eu/health/ehealth/docs/laws_poland_en. pdf.

[2] Eržen, I. (2004). Zdravstveno informacijski sistem v Sloveniji na razpotju – potrebe in praksa. V *Informatica medica slovenica, 9*, 3–8.

[3] Gunter, T. D., Terry, N. P. (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. *Journal of Medical Internet Research, 7*(1).

[4] Hough, M. G. (2009). Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society, 31*(4), 406–413.

[5] Informacijski pooblaščenec RS. (2008). Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic.

[6] Kovačič, M. (2017a, april). Piškotki kot dimna zavesa spletne varnosti in zasebnosti. *Slo-Tech | Tehnoloski koticek spleta*. Pridobljeno s https://slo-tech.com/novice/t697519.

[7] Kovačič, M. (2017b, marec). Odgovorno razkritje ali neodgovorno nerazkritje. *Slo-Tech | Tehnoloski koticek spleta*. Pridobljeno s https://slo-tech.com/novice/t696199.

[8] Miller, A. R., Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. *Management Science, 55*(7), 1077–1093.

[9] Ministrstvo za zdravje Republike Slovenije. (2009). Študija izvedljivosti projekta eZdravje – predinvesticijska zasnova in investicijski program s študijo izvedbe.

[10] World Health Organization. (1999). Health21: The health for all policy framework for the who european region. *Health21: The Health for All Policy Framework for the WHO European Region.*

[11] Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva. (2005).

[12] Ustava Republike Slovenije. (2006).

[13] Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25(1)*, 166.

[14] Zakon o pacientovih pravicah RS. (2008).

[15] Zakon o varstvu osebnih podatkov RS. (2004).

[16] Zakon o zbirkah podatkov s področja zdravstvenega varstva RS. (2000).

▪

Luka Hrgarek je magister informatike in tehnologij komuniciranja. Diplomiral je leta 2015 na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru na študijskem programu Računalništvo in informacijske tehnologije. Leta 2017 je magistriral z magistrsko nalogo Zbiranje podatkov in profiliranje uporabniških naprav s pomočjo spletnih brskalnikov. Zaposlen je na Fakulteti za elektrotehniko, računalništvo in informatiko kot tehniški sodelavec. Njegovo raziskovalno področje vključuje sodobne spletne tehnologije, informacijsko varnost ter medicinske sisteme.

▪

Leon Bošnjak je asistent in raziskovalec na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Leta 2014 je magistriral s področja informatike in je trenutno doktorski študent na računalništvu in informatiki. Njegova raziskovalna področja obsegajo sistemsko varnost, tekstovna in grafična gesla ter metode dvofaktorskega overjanja.

▪

Tatjana Welzer Družovec je redna profesorica in vodja Laboratorija za podatkovne tehnologije na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Njena glavna raziskovalna področja so konceptualno oblikovanje podatkovnih baz, podatki v podatkovnem skladiščenju in rudarjenju, ponovna uporaba in vzorci, varnost ter izobraževanje na področju informatike in mobilnosti. Svoje raziskovalne ugotovitve objavlja v znanstvenih revijah in knjigah ter na domačih in mednarodnih konferencah.

▪

Aida Kamišalić je asistentka in raziskovalka na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Doktorirala je leta 2014 na računalništvu in informatiki. Njena raziskovalna področja vključujejo podatkovne tehnologije, modeliranje medicinskih postopkov za kronične bolnike in pridobivanje znanja iz podatkov za medicinske postopke.

Odpiranje podatkov javnega sektorja in omogočanje njihove ponovne uporabe

Mateja Prešern, Aleš Veršič,
Ministrstvo za javno upravo, Tržaška cesta 21, 1000 Ljubljana
mateja.presern@gov.si; aversic@gov.si

Izvleček

Direktiva EU o ponovni uporabi podatkov javnega sektorja je postavila podlago za enakopravno in vsem zainteresiranim subjektom omogočeno ponovno uporabo informacij javnega značaja, zadnje zakonodajne spremembe pa prinašajo težnjo pospešenega odpiranja podatkov. Ministrstvo za javno upravo želi izboljšati dostop do odprtih podatkov javnega sektorja, zato je vzpostavilo nov sistem za objavo odprtih podatkov javnega sektorja, ki deluje na odprtokodnih rešitvah. Poleg tehnološke prenove pomeni poseben izziv tudi vzpostavitev omrežja objaviteljev podatkov. Odprti podatki javnega sektorja bodo (po posameznih področjih) skladno s strateškimi usmeritvami in zakonodajo objavljeni na nacionalnem portalu odprtih podatkov (OPSI). Vzpostaviti bo treba ekosistem, v katerem bi se srečevali ponudniki podatkov, podatkovni analitiki, razvijalci aplikacij, ki bodo uporabili odprte podatke in nad njimi razvili različne aplikacije, ki bodo ponujale različne storitve za državljane.

Ključne besede: zakonodaja, odprti podatki, ponovna uporaba, javni sektor, portal, CKAN, ekosistem.

Abstract

Open public sector information and its reuse

The EU Directive on the re-use of public sector information has set the foundation for equal rights of every potential user of public information while the latest amendments are resulting in the accelerated opening up of public information. The Ministry of Public Administration aims to improve access to open public sector information by setting up a new system for the publication of open public sector information, built on open source solutions. Alongside technological overhaul, another special challenge is the deployment of a data publisher network. In line with strategic goals and legislation, open public sector information will be published via the national open data portal (OPSI). In the future, what needs to be established is an open data ecosystem where data providers can meet with data analysts and application developers, and where innovative applications are developed on top of open data offering various quality services to citizens.

Keywords: law, open data, re-use, public sector, portal, CKAN, ecosystem.

1 UVOD

V zadnjih letih se je količina podatkov na svetu znatno povečala, hkrati se nenehno razvijajo tehnologije za analiziranje in obdelavo podatkov, kar omogoča oblikovanje novih proizvodov in storitev, ki temeljijo na združevanju ali kombiniranju podatkov. Dostop do znanja in informacij je bistven za razvoj posameznikov in družbe kot celote, zato se mora pomena in vrednosti informacij zavedati tudi javni sektor, saj ta pri svojem delu ustvarja veliko količino podatkov in upravlja z njimi. Javne institucije zbirajo najrazličnejše podatke – od prostorskih in okoljskih do statističnih in finančnih. Določena javna institucija podatke ustvari ali zbere enkrat, zasebni sektor ali druga institucija javne uprave te podatke lahko uporabi ponovno, kot podlago za nove informacije, informacije z dodano vrednostjo ali v okviru najraznovrstnejših storitev zasebnega sektorja. Ob upoštevanju navedenih izhodišč in v prizadevanju, da bi zagotovili enotni evropski trg javnih podatkov ter da bi javne institucije podatke v čim večji meri in brez večjih stroškov odprle za potencialne uporabnike, je bila leta 2003 sprejeta direktiva EU o ponovni uporabi podatkov javnega sektorja (v nadaljevanju direktiva PSI), ki je postavila podlago za enakopravno in vsem zainteresiranim subjektom omogočeno ponovno uporabo informacij javnega značaja, saj prepoveduje podeljevanje ekskluzivnih pravic uporabe podatkov in druge dejavnosti, ki lahko preprečujejo konkurenčnost na ravni EU. Spremembe direktive PSI iz 2013 so šle še korak dlje, saj poudarjajo potrebo po proaktivnem odpiranju podatkov v institucijah in uvajajo nov pojem »odprti podatki« (angl. Open Data).

Pojem ponovna uporaba (angl. re-use) pomeni takšne vrste uporabo, ki presega glavni razlog, zaradi katerega javni organ sploh zbira ali proizvaja podatke. Zbiranje določenih podatkov pri organu je predvideno in zakonsko določeno zaradi izvajanja določene javne naloge. Na tej podlagi je predvideno tudi financiranje organa za potrebe zbiranja podatkov. Obveznost ponudbe podatkov za »ponovno« uporabo pa ima za cilj, da postanejo podatki, ki se tako ali tako že zbirajo pri javnih organih in katerih financiranje je zagotovljeno z javnim denarjem, v čim večji meri odprti (če ni zadržkov glede dostopa javnosti do podatkov) za raznovrstno ponovno (torej nadaljnjo) uporabo, bodisi v javnem bodisi v zasebnem sektorju. Uporaba odprtih podatkov pomeni tudi brezplačno uporabo za nekomercialno ali komercialno rabo. Ob tem je vseeno treba poudariti, da podatki niso zastonj, brezplačna je le njihova uporaba.

Poleg zasledovanja transparentnega in učinkovitega delovanja javnega sektorja je še posebno pomemben tudi gospodarski vidik, saj odprti podatki pomenijo spodbudo za razmah digitalnega gospodarstva, kot so storitve, povezane z izdelavo spletnih aplikacij, navigacijskih sistemov, zemljevidov, vremenskih napovedi itd.

2 STRATEŠKE USMERITVE IN ZAKONODAJA ODPIRANJA PODATKOV JAVNEGA SEKTORJA

V Sloveniji smo z aktivnostmi, usmerjenimi v pospešeno odpiranje podatkov javnega sektorja, začeli v lanskem letu. Aprila 2015 je bila sprejeta *Strategija razvoja javne uprave 2020* (v nadaljevanju strategija),[1] ki kot eno temeljnih načel poudarja odprtost in transparentnost delovanja javne uprave ter v tem okviru kot enega temeljnih ciljev določa objavo zbirk podatkov iz pristojnosti ministrstev v strojno berljivih in odprtih formatih na nacionalnem portalu odprtih podatkov. V strategiji je posebej omenjeno, da dobre prakse ponovne uporabe podatkov javnega sektorja tudi pri nas kažejo, da je mogoče na podlagi surovih javnih podatkov ustvariti inovativne aplikacije. Kot primer so navedene ponovna uporaba podatkov o podzemskih jamah v Sloveniji, na podlagi katere je Društvo za raziskovanje jam Ljubljana leta 2005 izdelalo prvi spletni kataster jam na svetu,[2] in mnoge vizualizacije na spletni strani virostatiq.si, kot na primer prikaz udeležbe poslancev na sejah državnega zbora ali prikaz izdanih parkirnih kazni v Ljubljani med letoma 2012 in 2014.[3] Na podlagi strategije je bil pripravljen *Dvoletni akcijski načrt izvedbe Strategije razvoja javne uprave 2015–2020* (Vlada Republike Slovenije ga je sprejela julija 2015, prenovljen pa je bil aprila 2016),[4] ki kot cilj do leta 2020 določa znatno povečanje števila podatkovnih zbirk, objavljenih na nacionalnem portalu odprtih podatkov.

Za implementacijo sprememb direktive PSI iz leta 2013 je bila pripravljena in decembra 2015 sprejeta novela *Zakona o dostopu do informacij javnega značaja* (v nadaljevanju ZDIJZ-E),[5] katere določbe so se začele uporabljati 8. maja 2016. Na podlagi prenovljenih zakonskih pravil je bila aprila 2016 sprejeta tudi nova *Uredba o posredovanju in ponovni uporabi informacij javnega značaja* (v nadaljevanju uredba).[6] ZDIJZ je temeljni zakon, ki zagotavlja transparentnost delovanja organov javnega sektorja. Organi so skladno z ZDIJZ prvenstveno zavezani zagotavljati dostop do informacij javnega značaja, s katerimi razpolagajo. Dostop se omogoča tako proaktivno, npr. z možnostjo vpogleda v dokumente ali podatke preko spleta kot tudi na podlagi individualnih zahtev, na katere mora organ odgovoriti v dvajsetih delovnih dneh. Bistvo »dostopa« je v omogočanju seznanitve z vsebino dokumenta. Za razliko od dostopa je bistvo »ponovne uporabe« v tem, da lahko uporabnik določen dokument, zbirko ali surove podatke preprosto prenese s spleta ter jih na svojem računalniku nadalje obdeluje, analizira, vključuje v nove aplikacije, storitve ali produkte ipd. V zadnjih letih je bilo v Sloveniji veliko storjenega za omogočanje spletnega dostopa javnosti do javnih podatkov iz evidenc. Poudariti je treba, da spletni servisi organov v pretežni meri zagotavljajo zgolj *dostop* do spletno objavljenih podatkov *preko možnosti vpogleda oziroma seznanitve* s podatki. Da zagotovimo cilj v smeri enostavne ponovne uporabe, je treba omogočiti objavo surovih (odprtih) podatkov v strojno berljivih formatih. Za objavo odprtih podatkov je treba zagotoviti enotno platformo, kar se zagotovi preko nacionalnega portala odprtih podatkov.

[1] SJU 2020, glej poglavje 6.4.1.
[2] Glej spletno aplikacijo www.katasterjam.si.
[3] Glej vizualizacije, dostopne na http://virostatiq.com/voting-attendance-slovenian-parliament-2004-current-term/ ali http://virostatiq.com/analysis-traffic-violations-slovenia-beginning-2012-end-2014/.
[4] Dvoletni akcijski načrt izvedbe Strategije razvoja javne uprave 2015–2020 za leti 2016 in 2017 (sprejet 2. 6. 2016) nadomešča aktualni akcijski načrt za obdobje 2015–2016, ki ga je Vlada Republike Slovenije sprejela s sklepom št. 01000-2/2015/13 z dne 29. 7. 2015.
[5] Zakon o spremembah in dopolnitvah Zakona o dostopu do informacij javnega značaja (Uradni list RS, št. 102/15).
[6] Uradni list RS, št. 24/16.

Za razliko od določb novele ZDIJZ-A,[7] s katerimi je bila pred več kot desetimi leti prenesena prvotna direktiva PSI iz leta 2003, določbe ZDIJZ-E nalagajo javnim organom, da morajo ne le omogočati javne podatke za ponovno uporabo na podlagi prejetih zahtev za ponovno uporabo, temveč jim nalaga proaktivni angažma, torej *proaktivno odpiranje javnih podatkov na način (vnaprejšnje) objave v svetovnem spletu*. ZDIJZ namreč po uveljavitvi novele ZDIJZ-E v prvem odstavku 10.b člena vsebuje pomembno priporočilo, ki določa, naj bi organi zavezanci povsod, kjer to ne pomeni prevelikega in nesorazmernega napora (predvsem na prioritetnih področjih javnega sektorja), odprli podatke v strojno berljivih formatih in jih torej dali na voljo za nadaljnjo uporabo komur koli za kateri koli namen, in sicer preko objave na spletu (nacionalni portal odprtih podatkov ali lastna spletna stran organa).[8] Definicija odprtega podatka temelji na treh bistvenih elementih:

- podatek je po vsebini prosto javno dostopen (torej ni omejitev glede obstoja izjem po 6. členu ZDIJZ),
- podatek je objavljen v strojno berljivem in odprtem tehničnem formatu,
- podatek je na voljo pod t. i. odprto licenco – brezplačno, za kateri koli namen, edini pogoj za (ponovno) uporabo je navedba avtorstva oziroma vira.[9] Odprti podatki morajo biti na voljo vsem pod enakimi pogoji; to pomeni, da ne sme biti diskriminacije za posamezna področja, posameznike ali skupine (npr. omejitve glede komercialne rabe ali omejitve uporabe iz določenih razlogov, npr. le v izobraževanju, le za nekomercialni namen ipd.).

Odpiranje podatkov za namen enostavne ponovne uporabe je smiselno predvsem za zbirke, za katere je znano večje povpraševanje tako drugih organov javnega sektorja kot tudi fizičnih ali pravnih oseb ne glede na namen. Ne gre pričakovati, da bodo popolnoma vse zbirke podatkov, ki jih organi vodijo na podlagi javnih nalog, objavljene v obliki odprtega formata in spletno dostopne za ponovno uporabo. Pri nekaterih obstajajo zakonske (npr. varovani osebni podatki), pri drugih pa lahko tudi tehnične ovire. Če je mogoče varovane osebne podatke anonimizirati, še vedno obstaja možnost odpiranja določenega dela baze podatkov, ki bi bila zanimiva za ponovno uporabo. Prioritetna področja, na katerih bi bilo treba ponuditi največ zbirk odprtih podatkov, so objavljena v priporočilih Evropske komisije in tudi drugih strateških dokumentih, ki so podlaga za mednarodne primerjave uspešnosti držav na omenjenem področju.

V skladu s priporočilom organom, da javne podatke v čim večji meri objavljajo kot odprte podatke, zakon minimalizira možnosti za zaračunavanje stroškov pri zagotavljanju podatkov za ponovno uporabo. Po novem lahko organi za namen ponovne uporabe prosilcem zaračunavajo zgolj t. i. mejne (materialne) stroške.[10] To v splošnem pomeni možnost zaračunavanja najbolj osnovnih materialnih stroškov v skladu s pravili, ki veljajo pri dostopu (torej 16. in 17. člen uredbe).[11] Specialna ureditev velja za nove zavezance, to je knjižnice, muzeje in arhive, pri katerih se lahko upoštevajo tudi stroški razširjanja podatkov, to so predvsem stroški reprodukcije, stroški obdelave oziroma priprave naročila, stroški dostave in stroški posebnih zahtev (npr. priprava in formatiranje podatkov na zahtevo, digitalizacija). Poudariti je treba, da so novi zavezanci podvrženi režimu ponovne uporabe zgolj v zvezi z gradivom, na katerem nobena tretja oseba ni imetnik pravic intelektualne lastnine. Knjižnice, muzeji in arhivi bodo tako zavezani zagotavljati prvenstveno ponovno uporabo gradiva, ki je v javni domeni.[12]

Nova zakonodaja z vidika spodbujanja odpiranja podatkov daje večji poudarek pomenu metapodatkov v zvezi s podatkovnimi zbirkami. Izraz metapodatek pomeni informacije, ki opisujejo zbirko podatkov in storitve v zvezi s podatki ter omogočajo njihovo iskanje, evidentiranje in uporabo.[13] Kar zadeva status metapodatkov, ZDIJZ določa, da se šteje, da so metapodatki besedilo z upravnega področja po

[7] Uradni list RS, št. 61/05 z dne 30. 6. 2005.

[8] Glej tudi Priročnik za odpiranje podatkov javnega sektorja, 2016, str. 13.

[9] Glej peti odstavek 3. člena ZDIJZ: Izraz odprti podatek pomeni, da je podatek v datotečnem formatu, katerega struktura je določena v dogovorjenih odprtih standardih, ki jih je sprejela organizacija za standarde in ki se lahko uporabijo ter implementirajo brez tehničnih omejitev. Poleg tega je prosto dostopen ter na voljo za uporabo in razširjanje brez omejitev po zakonu, ki ureja avtorsko in sorodne pravice, razen navedbe avtorstva ali vira.

[10] Izjemoma je mogoče pridobiti dovoljenje za zaračunavanje, če organ nima zagotovljenih javnih sredstev za izvajanje javnih nalog. Za dve leti je dovoljenje pridobila Agencija za javnopravne evidence (AJPES). Skladno s prehodno določbo ZDIJZ-E pa sta tudi GURS in ARSO za določene zbirke lahko zaračunavala ponovno uporabo do konca leta 2017. V navedenih primerih je zaračunavanje mogoče samo v primeru, ko gre za ponovno uporabo v pridobitne namene.

[11] Glej 20. člen uredbe.

[12] Za gradivo, na katerem imajo navedene institucije pravice intelektualne lastnine, bo režim pravil za ponovno uporabo veljal, kadar se bo institucija odločila ponuditi gradivo za ponovno uporabo; šteje se, da se je institucija tako odločila, kadar je najmanj enemu prosilcu omogočila ponovno uporabo zahtevanega gradiva ali kadar sama ponovno uporablja gradivo.

[13] V skladu z novim sedmim odstavkom 3.a člena ZDIJZ.

zakonu, ki ureja avtorsko in sorodne pravice, kar pomeni, da metapodatki niso avtorskopravno varovani in za njih na podlagi samega zakona velja brezplačna in prosta ponovna uporaba. V skladu z ZDIJZ imajo torej metapodatki podoben status kot besedila zakonov, njihova uporaba je prosta. Nova uredba prinaša dopolnjene določbe glede metapodatkov, opisi posameznih metapodatkov pa so natančneje razdelani v prilogi 1 k uredbi. Ministrstvo za javno upravo (v nadaljevanju MJU) je na svojih spletnih straneh objavilo tudi vzorčni primer metapodatkovnega opisa zbirke in vzorčno datoteko za vnos metapodatkov, ki bo služila organom kot podlaga za pripravo in spletno objavo metapodatkov (rok za popis metapodatkov v zvezi z zbirkami podatkov je bil konec leta 2016).[14]

3 PRENOVA SISTEMA ZA OBJAVO ODPRTIH PODATKOV JAVNEGA SEKTORJA

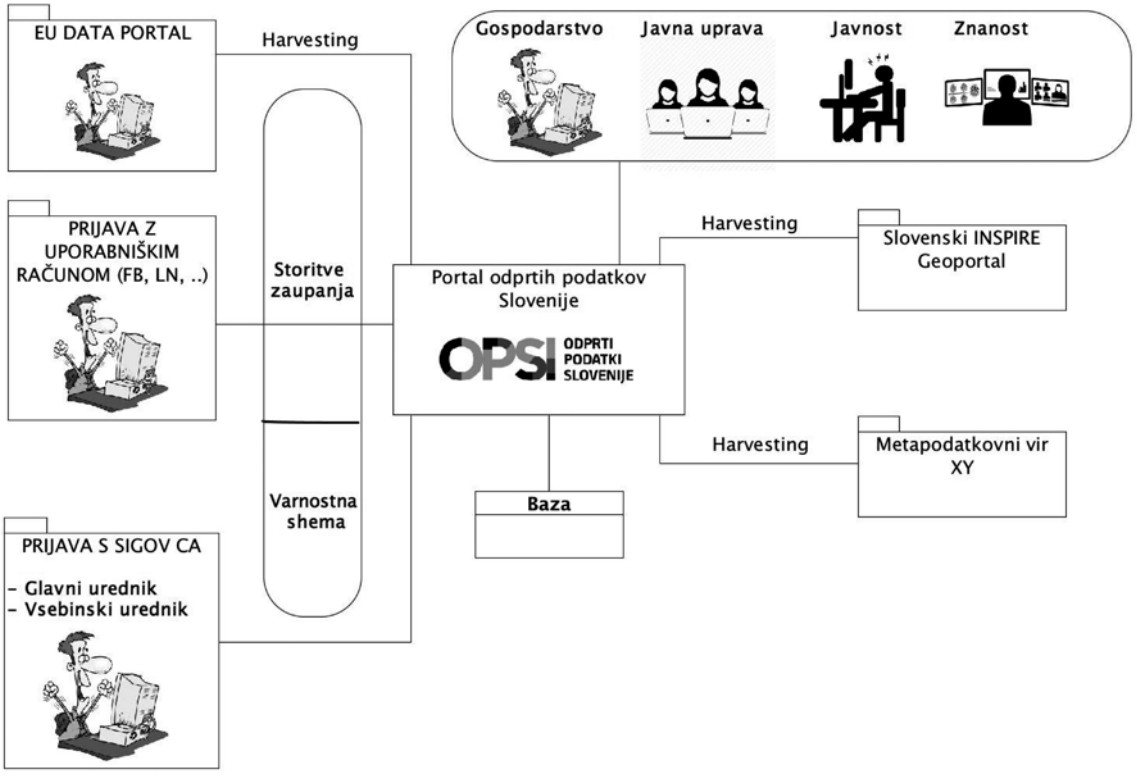
3.1 Prakse odpiranja podatkov javnega sektorja

V splošnem imajo danes uporabniki spletnih strani institucij javnega sektorja še vedno precej razpršen in otežen dostop do vira podatkov, ki jih vodita državni in javni sektor. Praviloma ima uporabnik zgolj možnost vpogleda v podatkovne zbirke (dostop), nima pa možnosti prenosa zbirk podatkov v strojno berljivem formatu za namen ponovne uporabe. Obstajajo tudi primeri dobrih praks. Dober primer spletne objave javnih podatkov je npr. AJPES, ki v datotekah strojno berljivega formata xml oziroma csv za ponovno uporabo objavlja seznam zavezancev za informacije javnega značaja (seznam subjektov javnega sektorja).[15] AJPES seznam objavlja in ažurira vsakodnevno, poleg javnosti pa je seznam namenjen tudi bankam za izvajanje njihovih zakonskih obveznosti v razmerju do Uprave RS za javna plačila na podlagi 10.a člena ZDIJZ.[16] Tako so podatki enostavno, učinkovito in z najmanj stroški za organ na voljo različnim uporabnikom, kar pomeni, da odpiranje podatkov preko objave na spletu dejansko lahko pomeni administrativno razbremenitev za organ. Zaradi različnih omejitev v zvezi s podatki ali drugih razlogov je včasih smiselno tudi parcialno odpiranje, tj. da organ odpre le del večje podatkovne zbirke. Tako na primer AJPES iz Poslovnega registra Slovenije objavlja seznam vseh poslovnih subjektov na vsake četrt leta.[17] Dodana vrednost je lahko že tudi zgolj objava osnovnih podatkov iz določene zbirke. MJU je pristojno za upravljanje portala javnih naročil, v sklopu katerega naročniki objavljajo osnovne podatke o posameznem izvedenem javnem naročilu vključno z besedilom podpisane pogodbe. MJU zbirko osnovnih podatkov o vseh oddanih javnih naročilih objavlja v eni datoteki za namen ponovne uporabe ter jo ažurira na četrt leta.[18]

Pri odpiranju podatkov preko spletnih storitev je pomembno, da se posamezna institucija zaveda finančnih prihrankov, ki jih lahko doseže pri distribuciji podatkov. Na Agenciji RS za okolje je bila pred leti vzpostavljena spletna objektna storitev (WFS), ki uporabnikom omogoča prenos prostorskih podatkov. Glede na število prenesenih podatkov in vrednost investicije se je ta povrnila v osmih mesecih. Za isto število izdanih podatkov bi potrebovali dva do tri zaposlene. Zato bi lahko institucije ob vzpostavitvi distribucije podatkov preko portala odprtih podatkov obstoječi kader usmerile v izboljševanje kakovosti zbirk podatkov, ki jih vodijo.

Nekateri organi (AJPES, GURS, ARSO) ponovno uporabo podatkov (na podlagi ZDIJZ) zaračunavajo (GURS in ARSO le še do konca leta 2017). Nekateri državni organi imajo vzpostavljene lastne sisteme odprtih podatkov (SURS, ARSO, NIJZ, GURS idr.), ki niso popolnoma odprti v skladu s predpisi in načeli ponovne uporabe; nekaj je tudi takih, ki so odprte podatke objavljali na portalu NIO, ki pa je namenjen zlasti objavi interoperabilnostnih izdelkov javnega sektorja. Predvsem pa država ni imela namenskega portala, ki bi omogočal uporabo odprtih podatkov tako, kot predvideva ZDIJZ. Zato je MJU vzpostavilo projektno skupino, ki bo prenovila sistem za objavljanje odprtih podatkov javnega sektorja. Prva faza prenove, ki je vzpostavila portal z glavnimi funkcijami dostopa do odprtih podatkov, je bila končana v začetku decembra 2016.

[14] Dostopno na http://www.mju.gov.si/si/delovna_podrocja/transparentnost_in_dostop_do_informacij_javnega_znacaja/aktualno/, glej pod »Metapodatkovni opis evidenc in zbirk podatkov – NOVO«.
[15] Dostopno na: http://www.ajpes.si/Registri/Drugi_registri/Zavezanci_za_informacije_javnega_znacaja).
[16] Tretji odstavek 10.a člena ZDIJZ.
[17] Dostopno na: http://www.ajpes.si/Registri/Poslovni_register/Ponovna_uporaba.
[18] Dostopno na: http://www.enarocanje.si/objavaPogodb/Izvozi.aspx . V obliki .csv so na voljo letni izvozi osnovnih podatkov o javnih naročilih v Republiki Sloveniji za leta 2012, 2013, 2014 in 2015.



Slika 1: **Poslovne zahteve delovanja portala glede na zunanje dejavnike**

3.2 Prenova nacionalnega portala odprtih podatkov

Pri prenovi sistema smo sledili nekaterim primerom dobrih praks. Med njimi je treba posebej omeniti portale odprtih podatkov iz ZDA,[19] Velike Britanije[20] in EU.[21] Vsi trije tudi delujejo na podobni tehnološki platformi, kot deluje slovenski portal odprtih podatkov. Pred začetkom prenove je bila opravljena analiza poslovnih procesov in zahtev, ki jih bo moral podpirati novi sistem. Sledimo načelu »enkrat zapisano«, to pomeni, da se metapodatki in podatki, ki se vodijo pri sektorsko specifičnih portalih, prevzemajo ali posredujejo preko sistema »harvesting«. Tak primer prevzemanja podatkov so prostorski podatki, ki jih na podlagi direktive INSPIRE in Zakona o infrastrukturi za prostorske informacije[22] vodi Geodetska uprava RS na Slovenskem INSPIRE Geoportalu. Preko »harvestinga« se bodo podatki posredovali s slovenskega portala odprtih podatkov na evropski portal odprtih podatkov.

Na sliki 1 je prikazan koncept vodenja vsebine Portala odprtih podatkov Slovenije (v nadaljevanju portal), ki je del blagovne znake OPSI (Odprti podatki Slovenije).

Na podlagi uredbe je vzpostavljena standardizirana struktura metapodatkovnih opisov zbirk podatkov. Tako bodo vse zbirke enotno opisane, kar bo uporabnikom olajšalo iskanje in uporabo zbirk podatkov. Pri popisu poslovnih zahtev so bile posebej obravnavane splošne in tehnične zahteve portala.

Od splošnih zahtev omenimo strojno prevajanje vsebine portala, možnost komunikacije s socialnimi omrežji, naročanje na različne vsebine portala preko protokola RSS. Poseben poudarek je na možnosti komunikacije uporabnikov s skrbnikom posamezne zbirke podatkov. Portal bo omogočal, da uporabnik skrbniku zbirke podatkov predlaga popravek podatka. Portal bo tudi prilagojen uporabi za slepe in slabovidne uporabnike po smernicah WCAG.[23]

Od tehničnih zahtev omenimo samodejni nadzor delujočih naslovov URL, samodejno ocenjevanje odprtosti podatkov. Portal bo omogočal, da si bo lahko

[19] https://data.gov/
[20] https://data.gov.uk/
[21] http://www.europeandataportal.eu/
[22] Uradni list RS, št. 61/05 z dne 30. 6. 2005.
[23] https://www.w3.org/WAI/intro/wcag

uporabnik pred prenosom pogledal podatke in preveril, ali je to tisto, kar išče.

Pomemben napredek nacionalnega portala kot enotne točke za odprte podatke javnega sektorja je katalog zbirk podatkov, ki jih vodi javni sektor, kar pomeni, da so na enem mestu zbrani opisi vseh zbirk javnega sektorja. Preko opisa bo uporabniku preprosto na voljo informacija o vsebini zbirke in načinu pridobitve podatkov za ponovno uporabo (bodisi v odprtih podatkih bodisi na način konkretne zahteve pri določenem organu).

3.2.1 Tehnične lastnosti portala

Portal je v celoti narejen z odprtokodno programsko opremo in deluje na državnem računalniškem oblaku. Na sliki 2 je prikazana arhitektura celotnega sistema. Pri vzpostavitvi je bila uporabljena izvorna koda angleškega portala odprtih podatkov, ki je dostopna preko repozitorija Github.

Zaradi zagotavljanja visoke razpoložljivosti ima portal podvojena spletna in aplikativna strežnika. Urejanje vsebine je ločeno na dva dela. Osnovne vsebine, kot so novice o portalu, se urejajo v spletnem strežniku, preko sistema za upravljanje vsebin Drupal. Urejanje metapodatkovnih opisov poteka v aplikativnem zalednem delu, in sicer na platformi CKAN, ki je sistem za upravljanje podatkov. Vsi podatki se hranijo v dveh bazah ter na datotečnem sistemu.

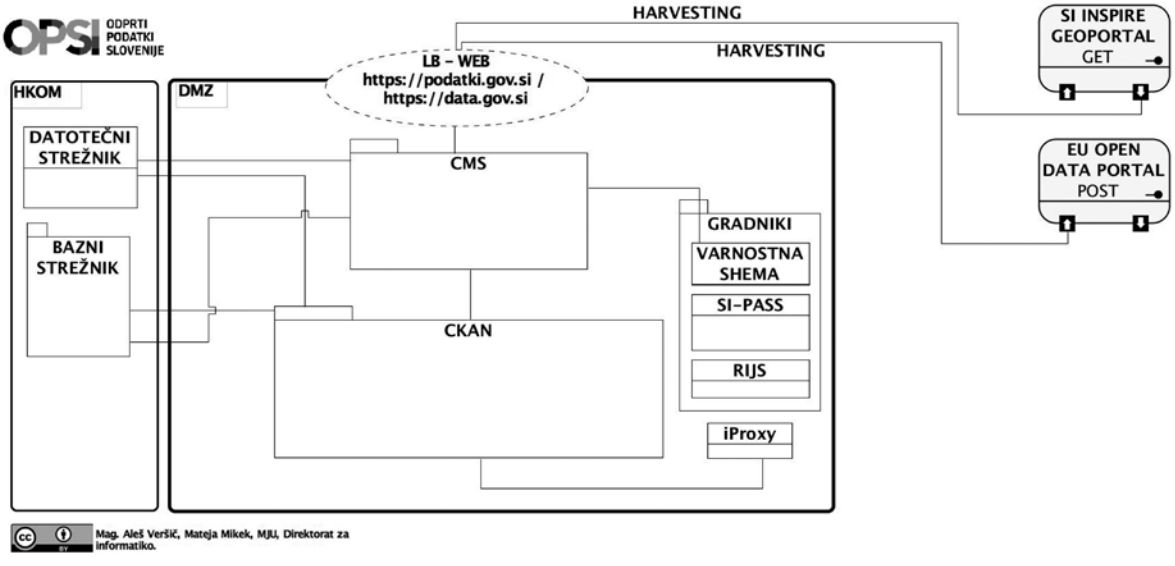
3.2.2 Urednikovanje portala

Za vodenje vsebin na portalu so predvideni glavni, področni in vsebinski uredniki. Vsebinski uredniki bodo napisali metapodatkovne opise ter objavili zbirke podatkov, za katere so odgovorni. Vsi tipi urednikov bodo lahko objavljali novice. Glavni uredniki bodo potrjevali objave, področni uredniki pa bodo skrbeli, da bodo objavljene vsebine s področja, za katerega so odgovorni. Poseben poudarek bo na kakovosti metapodatkovnih opisov, saj je dosedanja praksa pokazala, da so ti opisi večinoma zelo skopi in uporabniku ne dajejo ustrezne informacije o sami zbirki podatkov.

4 SPODBUJANJE (PONOVNE) UPORABE – VZPOSTAVLJANJE EKOSISTEMA ODPRTIH PODATKOV JAVNEGA SEKTORJA

V večini držav že nekaj časa ni več vprašanje, ali naj javne podatke odprejo in kako naj bodo ti odprti. Tehnološki pogled je večinoma že rešen. Največji izziv, ki sledi po tem, ko smo vzpostavili namenski portal za odprte podatke, je spodbujati institucije javnega sektorja, da začnejo objavljati svoje podatke, na drugi strani pa se je treba povezovati z uporabniki, da pridobimo povratne informacije o tem, kaj si dodatno želijo in kaj jih moti pri pridobljenih podatkih javnega sektorja.

V skladu z navedenim je zato poleg aktivnosti, povezanih s pripravo zakonodaje, posebna pozornost



Slika 2: **Arhitektura sistema portala odprtih podatkov**

MJU namenjena seznanitvi tako organov zavezancev kot tudi potencialnih uporabnikov, kot so npr. nevladne organizacije, novinarji in podjetniki, s pravicami in priložnostmi, ki jih ponuja spremenjena zakonodaja. S tem namenom je bil v sodelovanju s Fakulteto za računalništvo in informatiko Univerze v Ljubljani organiziran *Festival odprtih podatkov,*[24] ki je potekal jeseni 2015 in spomladi 2016. V okviru navedenega so študenti informatike v jesenskem semestru analizirali in obdelovali podatke o proračunu, turizmu, motornih vozilih ipd., ki so jih zagotovila pristojna ministrstva, ter na tej podlagi ustvarili najrazličnejše vizualizacije in inovativne prikaze. V študijskem letu 2016/17 je k sodelovanju poleg Fakultete za računalništvo in informatiko pristopila tudi Fakulteta za upravo.

V okviru mednarodnega projekta Share PSI 2.0, pri katerem je sodelovalo 44 partnerjev iz Evrope in ki ga vodi organizacija W3C, katere ustanovitelj je sir Tim Berners Lee, utemeljitelj odprtih podatkov, je MJU v sodelovanju z Geodetskim inštitutom Slovenije pripravilo spletni *Priročnik za odpiranje javnih podatkov (t. i. OPSI priročnik)*. Namenjen je državnim organom, občinam in drugim subjektom javnega sektorja in vsebuje napotke, kako se lotiti odpiranja javnih podatkov. Odgovarja na vprašanja, kot so: kaj je informacija javnega značaja, kaj je podatkovna zbirka, kdaj govorimo o odprtih podatkih, kaj je odprta licenca, kaj so metapodatki itd. Do konca leta ima MJU namen pripraviti tudi smernice za nove zavezance za ponovno uporabo (kulturne institucije – arhive, muzeje in knjižnice). V okviru istega projekta je Transparency International Slovenia v sodelovanju z Inštitutom Jožef Stefan in Virostatiq pripravil dve izredno zanimivi vizualizaciji: prvo na temo projektov, financiranih iz državnega proračuna (projekti, ki so bili del rebalansa proračuna za leto 2015), ter analizo proračunskih prihodkov in odhodkov slovenskih občin v letu 2015**.** Vizualizaciji omogočata primerjavo med projekti oziroma proračuni občin in nadaljnjo podrobnejšo analizo prečiščenih in obdelanih podatkov, ki jih je zagotovilo Ministrstvo za finance.[25]

Aplikacij, ki so nastale kot podjetniške pobude in uporabljajo odprte podatke, je po svetu že zelo veliko. Dostikrat slišimo pomisleke pri odpiranju podatkov, da bodo od tega imele koristi (zgolj) velike multinacionalke. Vendar se v praksi pokaže, da ni tako. Na angleškem portalu odprtih podatkov je dve tretjini aplikacij objavil zasebni, petino aplikacij pa javni sektor. Tudi pri objavah iz zasebnega sektorja se najdejo primeri, ko to objavijo posamezniki. Če so podatki na voljo za vse uporabnike pod enakimi pogoji, je to lahko priložnost, da tudi manjše podjetje pride do osnovnih podatkov in iz njih lahko naredi aplikacijo, ki jo ponuja tudi po svetu. Tako imamo primer aplikacije Razglednice iz vesolja, ki jo je razvilo slovensko podjetje Sinergise, d. o. o., na podlagi uporabe satelitskih posnetkov iz satelita Sentinel, ki jih ponuja Evropska vesoljska agencija kot odprte podatke. Drug primer je aplikacija Open corporates,[26] ki jo je razvilo podjetje Chrinon Ltd., ki ponuja dostop do osnovnih podatkov o posameznemu podjetju iz baze, v kateri so zbrani podatki z vsega sveta. Zavedamo se tudi pomena občinskih podatkov, zato so z občinami že stekle aktivnosti za pospešitev odpiranja njihovih podatkov. Pri tem je treba omeniti zanimive povezave z iniciativo Smartcities. Odprti podatki so temelj za razvoj »pametnih« rešitev, storitev in produktov za razvoj mest.

5 SKLEPNE UGOTOVITVE

Odpiranje podatkov javnega sektorja pomeni velik potencial za povečanje transparentnosti delovanja družbe in gospodarskega napredka. Z razvojem različnih storitev in aplikacij, ki bodo med drugim tudi olajšale življenje marsikateremu posamezniku, se bo povečalo tudi zadovoljstvo ljudi, ki jih bodo uporabljali. Pomembni koraki, ki omogočajo odpiranje podatkov, segajo v leto 2003, ko je prvotna direktiva EU o ponovni uporabi nakazala smer, v katero bo šel javni sektor na področju odpiranja podatkov. Z dopolnitvijo direktive leta 2013 ter ob pritisku javnosti, da želi imeti celovit dostop do podatkov javnega sektorja, so se ovire pri ponovni uporabi začele počasi podirati. Razmere še vedno niso idealne, vendar je zakonska podlaga dovolj ustrezno zapisana; še vedno obstaja določen strah pred odpiranjem podatkov, ki pa je vedno manjši. Zelo pomembno je tudi, da znamo ločiti med dostopom in ponovno uporabo

[24] Festival, namenjen ponovni uporabi podatkov,se je začel s prvim dogodkom 1. oktobra 2015 in se nadaljeval s sodelovanjem s Fakulteto za računalništvo in informatiko Univerze v Ljubljani. Več o festivalu na spletni strani MJU http://www.mju.gov.si/si/delovna_podrocja/transparentnost_in_dostop_do_informacij_javnega_znacaja/spletni_dostop_do_javnih_evidenc_ponovna_uporaba_in_odprti_podatki/.

[25] Več o tem dostopno na https://pravokator.si/index.php/2016/06/19/dve-vizualizaciji-odprtih-podatkov/ (avtor dr. Matej Kovačič).

[26] https://opencorporates.com/

podatkov javnega sektorja. Ta kvalitativna razlika marsikomu še ni dovolj jasna. Na tem področju bo treba usmeriti vse sile v ozaveščanje vseh deležnikov.

S prenovo sistema za objavo odprtih podatkov javnega sektorja je narejen tudi korak naprej v tehnološki podpori uporabnikom pri ponovni uporabi podatkov. Da je bil storjen precejšen napredek na tem področju, je zaznala tudi Evropska komisija, ki je v primerjalni analizi držav članic ocenila, da je Slovenija v zadnjem letu izredno napredovala na področju odprtih podatkov javnega sektorja in se tako uvrstila med t. i. »hitre sledilce«.[27] Pred nami je največji izziv, vzpostavitev ekosistema odprtih podatkov, preko katerega se bo aktivno spodbujala uporaba odprtih podatkov ter izmenjava informacij in izkušenj. Prvi korak k vzpostavitvi takšnega ekosistema je v sklopu Festivala odprtih podatkov sodelovanje MJU in Fakultete za računalništvo in informatiko. V letu 2016 smo to dopolnili še s sodelovanjem Fakultete za upravo. Tovrstno sodelovanje bo treba razširiti z gospodarskimi družbami, zagonskimi podjetji, raziskovalnimi novinarji, raziskovalci itd. Dolgoročno bo treba vzpostaviti ekosistem, v katerem bi se srečevali ponudniki podatkov, podatkovni analitiki in razvijalci aplikacij, ki bodo uporabili odprte podatke ter nad njimi razvili različne aplikacije s ponudbo uporabnih storitev za državljane. Šele ko se bodo odprti podatki začeli bolj množično uporabljati in bo na podlagi tega nastalo veliko storitev, ki bodo prinesle koristi državljanom, bomo lahko rekli, da smo dosegli cilj. Do takrat nas čaka še dolga in trnova pot s številnimi izzivi. Vendar je vredna, da gremo po njej. Kajti cilj je, da bodo imeli od tega največ koristi državljani Republike Slovenije.

[27] Več informacij o primerjalni analizi Evropske komisije: http://www.mju.gov.si/si/novinarsko_sredisce/novica/article/1328/7744/.

6 LITERATURA IN VIRI

[1] (2015). Strategija razvoja javne uprave 2020, sprejela Vlada Republike Slovenije, objavljeno na http://www.mju.gov.si/si/delovna_podrocja/razvoj_projektov_kakovost_javne_uprave_in_kohezijska_politika/strategija_razvoja_javne_uprave/ (30. 7. 2016).

[2] (2016). Dvoletni akcijski načrt izvedbe Strategije razvoja javne uprave 2015–2020 za leti 2016 in 2017, sprejet 2. 6. 2016, objavljeno na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/SOJ/STRATEGIJA_JU2020_IN_AKCIJSKI_PLAN/Dvoletni_akcijski_nacrt_SJU_16-17.pdf (30. 7. 2016).

[3] Direktiva 2003/98/ES Evropskega parlamenta in Sveta z dne 17. novembra 2003 o ponovni uporabi informacij javnega sektorja, *UL L 345, 31. 12. 2003,* objavljeno na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:SL:NOT (30. 7. 2016).

[4] Konsolidirano besedilo Direktive EU o ponovni uporabi informacij javnega sektorja, objavljeno na http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02003L0098-20130717 (30. 7. 2016).

[5] (2015) Skupno letno poročilo (državnih organov in organov lokalnih skupnosti) o izvajanju ZDIJZ v 2014, objavljeno na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/SOJ/2015/Letno_porocilo_ZDIJZ_2014.pdf (30. 7. 2016).

[6] Predlog Zakona o spremembah in dopolnitvah zakona o dostopu do informacij javnega značaja, gradivo za javno razpravo z dne 21. 4. 2015, objavljeno na https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=5887 (30. 7. 2016).

[7] Predlog Uredbe o posredovanju in ponovni uporabi informacij javnega značaja, gradivo za javno razpravo z dne 26. 2. 2016, objavljeno na https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=6558 (30. 7. 2016).

[8] (2014). Smernice Evropske komisije o priporočenih standardnih licencah, podatkovnih zbirkah in zaračunavanju za ponovno uporabo dokumentov (UL EU C 240, 24. 7. 2014), objavljeno na http://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52014XC0724(01)&from=EN (30. 7. 2016).

[9] (2016). Priročnik za odpiranje podatkov javnega sektorja, objavljen na http://www.mju.gov.si/en/media_room/news/article/1328/7539/ (30. 7. 2016).

▪

Mateja Prešern je zaposlena na Ministrstvu za javno upravo kot vodja Službe za transparentnost, integriteto in politični sistem. Zadolžena je za sistemsko zakonodajo s področja dostopa do javnih informacij, ponovne uporabe in odprtih podatkov javnega sektorja in je sodelovala pri pripravi EU direktiv s tega področja. Je avtorica strokovnih del in predavateljica s področja transparentnega delovanja javnega sektorja, integritete in odprtih podatkov. Magisterij pravnih znanosti s področja prava intelektualne lastnine in varstva osebnih podatkov je pridobila na Univerzi v Londonu, UCL.

▪

Aleš Veršič je zaposlen v Direktoratu za informatiko na Ministrstvu za javno upravo kot vodja projektov v Sektorju za razvoj aplikativnih rešitev. Glavna področja njegovega dela so geografski informacijski sistemi, standardizacija in odprti podatki. Je član tehničnega odbora za geografske informacije pri Slovenskem inštitutu za standardizacijo. Je avtor strokovnih del s področja geografskih informacijskih sistemov. Raziskoval je na področju volilne geografije ter e-storitev javne uprave s pomočjo geografskih informacijskih sistemov.

Iz Islovarja

Islovar je spletni terminološki slovar informatike, ki ga ureja jezikovna sekcija Slovenskega društva Informatika na naslovu http://www.islovar.org. Tokrat objavljamo izbor izrazov, ki smo jih urejali v zadnjem času. Vabimo vas, da v Islovar prispevate nove izraze.

gradník[1] -a m *(angl. widget, control)* sličica, polje[1] (1), simbol na zaslonu za prikaz, spreminjanje vrednosti atributa, zagon (1)

gráfični uporábniški vmésnik -ega -ega -a m *(angl. graphical user interface, GUI)*uporabniški vmesnik, s katerim komuniciranje (1) med človekom in računalnikom poteka s klikanjem, premikanjem gradnikov[1] na zaslonu (1); sin. slikovni uporabniški vmesnik; prim. WIMP

indikátor dostôpa do díska -ja -- -- -- m *(angl. hard-disk drive access indicator)* znak (3), ki kaže, kdaj je disk aktiven

indikátor odpôvedi -ja -- m *(angl. failure indicator)* znak (3), ki se sproži ob odpovedi sistema

kazálec -lca m *(angl. cursor, pointer)* gradník[1], ki kaže mesto za naslednji vnos

kazálec aktívnosti -lca -- m *(angl. activity indicator, waiting indicator)* znak (3), ki nakazuje delovanje sistema v ozadju

kazálna napráva -e -e ž *(angl. pointing device)* vhodna naprava, s katero lahko uporabnik premika žarišče (1), izbira in premika gradnike[1] v grafičnem uporabniškem vmesniku, npr. miška, grafična tablica

kazálnik -a m *(angl. indicator)* številski podatek, ki kaže stanje, razvoj kakega pojava; sin. indikator

kazálnik potéka -a -- m *(angl. progress indicator)* gradnik[1], ki sporoča uporabniku, da obdelava poteka; prim. vrstica napredovanja

kazálnik razpoložljívosti -a -- m *(angl. availability ratio)* razmerje dejansko razpoložljivega časa v primerjavi z dogovorjenim časom razpoložljivosti

ključni kazálnik uspéšnosti -ega -a -- m *(angl. KPI, key performance indicator)* kazalnik uspešnosti postopka, procesa, sistema, s katerim je mogoče spremljati in meriti doseganje cilja; sin. KPI

križni kazálec -ega -lca m *(angl. cross pointer)* kazalec v obliki križa

puščični kazálec -ega -lca m *(angl. arrow pointer)* kazalec v obliki puščice

sistém uravnotéženih kazálnikov -a -- -- m *(angl. balanced scorecard, BSC)* vrednotenje poslovne uspešnosti z uporabo vsebinsko povezanih kazalnikov

skladóvni kazálec -ega -lca m *(angl. stack pointer)* naslov zadnjega zahtevanega podatka v skladu

vrstíca napredovánja -e -- ž *(angl. progress bar)* kazalnik poteka, ki prikazuje potek računalniške obdelave, npr. posodobitev, prenos datoteke; sin. vrstica napredka

WIMP WIMP-a krat. m *(angl. window, icon, menu, pointing device)* uporabniški vmesnik, ki uporablja okna, ikone, menije in kazalne naprave, npr. Windows; prim. grafični uporabniški vmesnik

zastávica prekoračítve -e -- ž *(angl. overflow flag)* del kontrolnega registra, ki opozarja na prekoračitev obsega registra, akumulatorja

znák -a m *(angl. 1.sign, 2.character, 3.signal)*
1. dogovorjen lik, ki ima dogovorjen pomen
2. vsak od elementov besedila, ki v določeni sestavi oblikuje pomen, npr. črka, številka, ločilo
3. gib, zvok, oddajanje svetlobe, ki kaj sporoča ali na kaj opozarja

Izbor pripravlja in ureja Katarina Puc s sodelavci.

Spoštovani bralci revije,

Z letom 2018 je prišlo v reviji Uporabna informatika Slovenskega društva INFORMATIKA do nekaterih sprememb. Sam sem prevzel vlogo glavnega urednika revije, tehnični urednik pa je postal dr. Slavko Žitnik.

Naj se najprej sam na kratko predstavim. Sem zaslužni profesor na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Svojo pot sem začel najprej na Institutu Jožef Stefan, kjer sem bil načelnik oddelka za elektroniko. Kasneje sem postal pomočnik direktorja Iskre Delte, zadolžen za področje izobraževanja. Ves čas svoje akademske kariere sem bil zaposlen najprej na Fakulteti za elektrotehniko in kasneje na Fakulteti za računalništvo in informatiko. Bil sem 6 let prodekan za raziskovalno delo in 4 leta dekan. Več let sem tudi predaval na Univerzi v Vidmu v Italiji. Bil sem nosilec ali sodelavec v različnih nacionalnih, pa tudi mednarodnih projektih. Moje strokovno področje je bilo najprej avtomatizacija industrijskih procesov in robotika, kasneje pa uporaba IKT v izobraževanju. Bil sem član različnih mednarodnih združenj ali njihovih nacionalnih sekcij (IEEE, ACM Slovenija, CoLoS, HSci, EURASC). Občasno sem bil tudi član odborov ali predsednik v nekaterih od teh združenj.

Povrnimo se k naši reviji. Poskušamo uvesti tudi nekaj sprememb v obliki in v vsebini revije. Z letošnjim letom je revija postala spletna, tako kot njena sestrska revija Informatica, ki jo društvo objavlja v angleščini. Prehod na novo obliko pomeni, da bodo na spletu objavljeni vsi prispevki v celoti, ne le njihovi povzetki. Tudi samo upravljanje revije teče sedaj po istih postopkih, ki veljajo za revijo Informatica. V obeh primerih uporabljamo mednarodno uveljavljeni sistem OJS (Open Journal Systems), ki ga v različnih jezikih uporablja več kot 32000 revij. Sedaj ga imamo lokaliziranega tudi v slovenščino.

Novi koncept pomeni spremembo tudi v dostopnosti revije. Člani društva bodo o objavi novih številk obveščeni po elektronski pošti. Imeli bodo prost dostop do vseh številk. Tiskani izvod bodo odslej prejemali le naročniki revije in tiste fakultete slovenskih državnih univerz, ki imajo v programu informatiko ali računalništvo. Elektronska oblika revije je tudi bolj primerna za razne iskalnike na spletu pa tudi za brskanje na lastnem računalniku.

Dostop bo spletnih številk revije bo na voljo članom društva, drugim bralcem pa bo omogočen šest mesecev po objavi vsake številke.

Poskušali bomo uvesti vsebine, ki bi revijo naredile še bolj uporabno in morda všečno. Trenutno ima revija tri rubrike: znanstvene prispevke, strokovne prispevke in informacije. Elektronska oblika bi omogočala večjo interaktivnost. Tako bi lahko na primer uvedli Pisma uredniku, seveda omejena na strokovno področje revije. Lahko bi objavljali krajše prispevke z zanimivimi dosežki. Tipični članki v reviji obsegajo sedaj približno 10 strani, nova oblika pa bi lahko omogočala tudi krajše novice, dolge morda stran ali dve.

In ne nazadnje, elektronska oblika revije omogoča tudi uvajanje multimedijskih vsebin, na primer videoposnetkov, podobno kot to zasledimo na spletnih straneh raznih časopisov in revij. To bi lahko bili posnetki s konferenc, z dogodkov ipd. Razmisliti velja tudi o novih možnostih objave oglasov, ki jih omogoča spletna oblika revije. To je le nekaj neobvezujočih zamisli.

Pa končajmo s stavki, s katerimi bi morali pravzaprav nagovor začeti. Uporabna informatika je in ostaja edina slovenska revija, ki objavlja strokovne in znanstvene članke in tako prispeva k razvoju in ohranjanju slovenskega strokovnega jezika na področju informatike, informacijsko komunikacijskih tehnologij. Skrb za odličnost jezika potrjuje tudi z rednim objavljanjem izbora sestavkov iz spletnega terminološkega slovarja Islovar.

To so naloge in včasih izzivi, ki jih lahko uresničimo z uredniškim odborom revije pa tudi skupaj z vami, bralci.

Prof. dr. Saša Divjak, glavni urednik revije

Včlanite se v Slovensko društvo INFORMATIKA

Pristopna izjava

za članstvo v Slovenskem društvu INFORMATIKA

Pravne osebe izpolnijo samo drugi del razpredelnice

Ime in priimek	
Datum rojstva	
Stopnja izobrazbe	srednja, višja, visoka
Naziv	prof., doc., spec., mag., dr.
Domači naslov	
Poštna št. in kraj	
Ulica in hišna številka	
Telefon (stacionarni/mobilni)	

Zaposlitev člana oz. člana - pravna oseba	
Podjetje, organizacija	
Kontaktna oseba	
Davčna številka	
Poštna št. in kraj	
Ulica in hišna številka**	
Telefon	
Faks	
E-pošta	

Zanimajo me naslednja področja/sekcije*

- ☐ jezik
- ☐ informacijski sistemi
- ☐ operacijske raziskave
- ☐ seniorji
- ☐ zgodovina informatike
- ☐ poslovna informatika
- ☐ poslovne storitve
- ☐ informacijske storitve
- ☐ komunikacije in omrežja
- ☐ softver
- ☐ hardver
- ☐ upravna informatika
- ☐ geoinformatika
- ☐ izobraževanje

podpis

kraj, datum

Pošto društva želim prejemati na domači naslov / v službo.

Članarina znaša: 18,00 € - redna
7,20 € - za dodiplomske študente in seniorje (ob predložitvi dokazila o statusu)
120,00 € - za pravne osebe

Članarino, ki vključuje glasilo društva – revijo **Uporabna informatika**, bom poravnal sam / jo bo poravnal delodajalec.

DDV je vključen v članarino.

✂

Naročilnica na revijo UPORABNA INFORMATIKA

Naročnina znaša: 35,00 € za fizične osebe
85,00 € za pravne osebe – prvi izvod
60,00 € za pravne osebe – vsak naslednji izvod
15,00 € za študente in seniorje (ob predložitvi dokazila o statusu)

DDV je vključen v naročnino.

ime in priimek ali naziv pravne osebe in ime kontaktne osebe

davčna številka, transakcijski račun

naslov plačnika

naslov, na katerega želite prejemati revijo (če je drugačen od naslova plačnika)

telefon/telefaks

elektronska pošta

Podpis

Datum

Znanstveni prispevki

Strokovni prispevki

Informacije

ISSN 1318-1882