2014 ‹ ŠTEVILKA 1 ‹ JAN. FEB. MAR. ‹ LETNIK XXII ‹ 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 sedem organizacij, katerih logotipe objavljamo.

AGORA

LJUDSKA UNIVERZA MURSKA SOBOTA

ŠOLSKI CENTER Novo mesto

spin

ISER

LJUDSKA UNIVERZA CELJE

Micro Team

Spoštovane bralke in spoštovani bralci revije Uporabna informatika,

ugotoviti želimo, kaj menite o vsebinski in izvedbeni kakovosti naše revije, saj smo prepričani, da lahko še izboljšamo njeno uporabno vrednost in s tem tudi vaše zadovoljstvo z njo. Pripravili smo kratek vprašalnik in vas prosimo, da ga izpolnite ter tako prispevate k uspehu prizadevanj za izboljšanje revije.

Izpolnjeni vprašalnik pošljite na naslov:

Slovensko društvo INFORMATIKA – za UI
Litostrojska cesta 54, 1000 Ljubljana

Lahko pa ga izpolnite na spletni strani revije **www.uporabna-informatika.si.**

Že vnaprej hvala za vaše sodelovanje.

Uredništvo revije Uporabna informatika

U P O R A B N A
I N F O R M A T I K A
2014 ŠTEVILKA 1 JAN/FEB/MAR LETNIK XXII ISSN 1318-1882

Znanstveni prispevki

Pregledni znanstveni prispevki

Strokovni prispevki

Razprave

Informacije

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

2014 ŠTEVILKA 1 JAN/FEB/MAR LETNIK XXII ISSN 1318-1882

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

Predstavnik
Niko Schlamberger

Odgovorni urednik
Jurij Jaklič

Naklada
600 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 nadaljni izvod 60,00 EUR, za posameznike 35,00 EUR, za študente in seniorje 15,00 EUR. V ceno je vključen DDV.

Izdajanje revije Uporabna informatika v letu 2014 sofinancira Javna agencija za raziskovalno dejavnost Republike Slovenije.

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 APA sistemu, 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.

Pristop in podporno orodje za delno avtomatski zajem metode razvoja programske opreme

Marko Janković, Slavko Žitnik, Lovro Šubelj, Neli Blagus, Aljaž Zrnec, Marko Bajec
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Tržaška c. 25, 1000 Ljubljana
{ime.priimek}@fri.uni-lj.si

Izvleček

Študije kažejo, da uporaba in sledenje metodam za razvoj programske opreme ter njihova sposobnost prilagajanja zahtevam posameznega projekta in načinu dela razvojne ekipe pomembno vplivajo na uspešnost IT-projektov in prispeva k večji kakovosti razvite programske opreme. Kljub temu je njihova uporaba v praksi redka. Eden izmed razlogov za to je, da obstoječi pristopi zahtevajo znatno sodelovanje razvijalcev. V prispevku opišemo pristop in podporna orodja, ki omogočajo popis osnovne metode dela podjetja in njeno vzdrževanje na podlagi spremljanja dejanskih metod razvoja programske opreme ob minimalnem sodelovanju razvijalcev. Tako bodo predpisane metode odsevale dejanski način dela na projektih, zato pričakujemo, da jih bodo razvijalci sprejeli kot svoje in jim sledili bolj dosledno. Poleg tega bi s tem dosegli višjo stopnjo zrelosti procesa razvoja programske opreme.

Ključne besede: proces razvoja programske opreme, razvoj metod za potrebe specifične situacije, metode za razvoj programske opreme, izboljšave procesa razvoja programske opreme, sistemi za nadzor verzij.

Abstract

Approach and supporting toolset for semi-automatic documentation of software development methods

Studies show that the usage and acceptance of software development methods as well as their ability to adapt to the specific needs of a project and development team have a significant impact on the performance of IT projects, which in turn contributes to a higher quality of the software developed. However, their usage in practice remains low. One of the reasons is the fact that existing approaches require a significant involvement of developers. To overcome this problem we outline an approach and supporting tools which monitor in-action methods during project performance and capture the knowledge needed to supplement the current base method, with only a negligible involvement of developers. This way the prescribed methods will reflect the reality of working on projects, so we expect that the developers will perceive them as a valuable asset and will follow them more rigorously. Furthermore, this will lead to a higher maturity of software development processes.

Key words: software process, situational method engineering, software development methods, software process improvement, revision control systems.

1 UVOD

Številne študije (Bajec, Vavpotič & Krisper, 2007; Bekkers s sod., 2008; Fitzgerald & Hartnett, 2005; Karlsson & Agerfalk, 2004; Van de Weerd s sod., 2006) jasno kažejo, da ima uporaba metod za razvoj programske opreme (angl. software development method – SDM) pozitiven vpliv na proces razvoja programske opreme in prispeva k višji kakovosti produkta, tj. razvite programske opreme. Kljub vsem prednostim pa podjetja v veliki meri še vedno nimajo popisanih in dokumentiranih metod razvoja programske opreme. Tudi podjetja, ki imajo dokumentirane metode, teh ne vzdržujejo ali jim ne sledijo dosledno, kot bi bilo to pričakovano v teoriji. Znanje in izkušnje, pridobljene na posameznih projektih, torej ostajajo v glavah posameznikov. Razlogov, ki pojasnijo nastali položaj, je več (Mohan & Ahlemann, 2011; Mirbel & Ralyte, 2006; Riemenschneider s sod., 2002). Med vsemi izpostavimo predvsem (1) strogost – večina metod za razvoj programske opreme ne omogoča učinkovitega prilagajanja metod zahtevam posameznega projekta, in (2) socialno-tehnično neprimernost – metode pogosto vsili podjetje in niso prilagojene potrebam in znanju razvojne ekipe, zato jih razvijalci ne sprejmejo in jim ne sledijo v želeni meri (Vavpotič & Bajec, 2009).

Predstavljeni položaj splošno priznavajo raziskovalna skupnost in do neke mere tudi posamezniki iz prakse. Vsekakor pomeni velik in resen problem. Glede na raziskavo, ki jo je opravila družba McKinsey v sodelovanju z Univerzo v Oxfordu (Bloch, Blumberg & Laartz, 2012), kar polovica vseh velikih projektov (projekti z začetno ceno, ki presega 15 milijonov dolarjev) preseže načrtovane stroške, se ne dokonča v dogovorjenem času ali pa ne izpolni vseh zahtev, ki so bile dogovorjene. Podobno so ugotovili tudi pri Standish Group,[1] kjer so ugotovili, da se je samo 16 odstotkov opazovanih projektov končalo v skladu s planom, 32 odstotkov jih je bilo prekinjenih, preden so bili končani, in 52 odstotkov jih je bilo končanih kasneje ter z večjimi stroški, kot je bilo predvideno.

V prispevku predstavimo inovativen pristop in podporno orodje za konstruiranje metod, ki bosta vodila k večji uporabi metod razvoja programske opreme v praksi. Za razliko od obstoječih pristopov in rešitev predlagani pristop gradi bazo znanja o razvoju programske opreme znotraj podjetja na podlagi opazovanja dela na projektih. Predpostavljamo, da lahko o tem, kaj razvijalci dejansko delajo na projektu, katere dokumente ustvarjajo ter kakšna sta vrstni red ustvarjanja dokumentov in vrstni red izvajanja aktivnosti, sklepamo na podlagi opazovanja komunikacije med razvijalci in sistemi za nadzor verzij. S tem bomo omogočili, da bodo predpisano osnovno metodo podjetja stalno posodabljali in prilagajali zahtevam projektov in razvojnih skupin z minimalnim sodelovanjem razvijalcev.

V nadaljevanju najprej na kratko predstavimo različne obstoječe rešitve in pristope, ki so se razvili zaradi slabe uporabe predpisanih metod v praksi, ter predstavimo njihove pomanjkljivosti (razdelek 2). V razdelku 3 predstavimo inovativen pristop za konstruiranje metod. V razdelku 4 opišemo orodje, ki je potrebno za podporo predlaganega pristopa, v razdelku 5 pa opišemo postopek vrednotenja. Za konec sledi sklep in predstavitev nadaljnjega dela (razdelek 6).

2 PREGLED OBSTOJEČIH REŠITEV IN PRISTOPOV

V preteklosti je bilo predlaganih več pristopov in rešitev z namenom povečanja uporabe metod razvoja programske opreme v praksi. Pojavile so se različne metode, orodja in procesna ogrodja, ki omogočajo prilagajanje metode potrebam in zahtevam posameznega projekta in razvojne ekipe, npr. IBM Rational Method Composer, Microsoft Solutions Framework (Garcia, Vizcaino & Ebert, 2011). Kljub temu da ta orodja pogosto vključujejo primere dobrih praks, ki temeljijo na dolgoletnih izkušnjah in opazovanju procesa razvoja programske opreme, za učinkovito uporabo zahtevajo specifično znanje. V primeru prilagajanja metode z uporabo orodja IBM Rational Method Composer je treba podrobno poznati elemente procesnega ogrodja RUP (Rational Unified Process).

Priča smo tudi uveljavljanju številnih lahkih in agilnih metod (npr. Scrum, Extreme programming), ki so se pojavile kot odgovor na zapletene in neprilagodljive tradicionalne metode ter v ospredje postavljajo bolj človeško naravnan pristop (Laanti, Salo & Abrahamsson, 2011; Dyba & Dingsøyr, 2008). S tega vidika se zdi uporaba lahkih in agilnih metod dobra alternativa, saj si te prizadevajo približati razvijalcem in ne prinašajo tolikšne obremenitve kot tradicionalne metode. Vseeno pa zaradi poenostavitev, ki jih prinašajo, podjetja redko uporabljajo formalno zapisane metode in raje sledijo viziji posameznikov. To vodi do tega, da načini dela v podjetju niso formalno zapisani in s tem dragoceno znanje in izkušnje, pridobljene na projektih, ostajajo v glavah razvijalcev.

Obsežen sklop znanja se je oblikoval tudi na področju razvoja metod za potrebe specifične situacije (angl. situational method engineering – SME). SME neposredno obravnava togost metod razvoja programske opreme in omogoča prilagajanje in ustvarjanje metod glede na potrebe in lastnosti projekta. Predlagani in razviti so bili številni pristopi (Ralyte & Rolland, 2001; Brinkkemper, Saeki & Harmsen, 1998; Deneckere s sod., 2008), ki so bili načrtovani in izdelani s ciljem, da bi omogočali ustvarjanje novih metod iz osnovnih delov (angl. fragments) že obstoječih metod in prilagajanje že obstoječih metod zahtevam posameznega projekta, vendar empirične študije kažejo, da je njihova uporaba v praksi redka (Mirbel & Rivieres, 2002; Ralyte & Rolland, 2001; Bajec, Vavpotič & Krisper, 2007). Ustvarjanje in prilagajanje metod je časovno zelo potratno, zahteva veliko predanost in vključenost razvijalcev. Poleg tega je treba za učinkovito konstruiranje novih metod poznati vse vrste že obstoječih metod in v večini podjetij nimajo takšnega znanja. Številni pristopi SME prav tako ne upoštevajo tehničnih in socialnih vidikov, kar pogosto vodi do metod, ki so tehnično ali socialno neskladne z delom

[1] http://www.standishgroup.com

razvijalcev ali s potrebami organizacije. Posledično razvijalci predpisane metode zato pogosto dojemajo kot nekoristno in nepotrebno breme in jim ne sledijo v tolikšni meri, kot bi bilo pričakovano v teoriji. Podrobnejši pregled področja SME je na voljo v delu Henderson-Sellers in Ralyte (2010).

Kljub vsem obstoječim rešitvam in pristopom številne študije (Bajec, Vavpotič & Krisper, 2007; Bajec s sod., 2007; Vavpotič & Bajec, 2009; Vlaanderen s sod., 2011) kažejo, da ostaja uporaba metod razvoja programske opreme v praksi nizka. Številna podjetja še vedno ne uporabljajo lastnih, formalno zapisanih metod, zato delujejo v skladu z neformalnimi pravili, ki temeljijo predvsem na znanju in izkušnjah posameznih članov razvojne skupine. Tudi podjetja, ki imajo formalno zapisane metode, tem ne sledijo dosledno. Razlogi za to so predvsem (1) stroški režije, ki pridejo z uporabo teh pristopov, in (2) specifična znanja, ki so potrebna za njihovo učinkovito uporabo.

3 INOVATIVNI PRISTOP ZA KONSTRUIRANJE METOD

Glavna motivacija za naše delo je nizka uporaba in nedosledno sledenje metodam razvoja programske opreme v praksi, kar vodi do številnih neuspešnih IT-projektov in nizke kakovosti razvite programske opreme (Bekkers s sod., 2008; Fitzgerald & Hartnett, 2005). V ta namen predlagamo inovativen pristop za konstruiranje metod in podporno orodje, katerega glavni cilji so a) delno avtomatski zajem znanja, ki ga imajo podjetja in njihovi posamezniki o praksi in pristopih pri procesu razvoja programske opreme, in na podlagi tega oblikovanje in popis dejanskih načinov dela, b) spremljanje in usmerjanje dela razvijalcev na projektih razvoja programske opreme in c) kontinuirano posodabljanje in optimizacija osnovnih metod razvoja programske opreme. Za razliko od drugih pristopov, ki si prizadevajo za dosego enakega cilja, je prednost našega, da zahteva le minimalno sodelovanje razvijalcev. To je znano kot eden izmed glavnih razlogov, zakaj se podobne pobude in pristopi niso uspeli uveljaviti v praksi (Mirbel & Ralyte, 2006; Karlsson & Agerfalk, 2012).

Za doseg ciljev nameravamo opazovati delo razvijalcev in drugih, vključenih v proces razvoja programske opreme. Pri tem nas bo zanimalo, kaj dejansko delajo na projektu, katere dokumente ustvarjajo, kakšne odločitve sprejemajo v določenih okoliščinah ipd. Predpostavljamo, da lahko o slednjem sklepamo na podlagi opazovanja komunikacije med razvijalcem in sistemom za nadzor verzij (angl. revision control system). Za vsak dokument, ki ga bo uporabnik dodal ali spremenil, bomo s pomočjo različnih tehnik, npr. z rudarjenjem po besedilih (angl. text mining), rudarjenjem po procesih (angl. process mining), poskušali ugotoviti, v kateri aktivnosti se nahaja uporabnik in ali je njegovo delo v skladu s predpisano metodo. V primeru odstopanja od predpisane metode bomo s pomočjo uporabnika ugotovili, ali je prišlo do napake (uporabnik je preskočil aktivnost, ki bi jo moral predhodno končati) ali gre za novo znanje, ki ga bomo uporabili za posodobitev osnovne metode podjetja. S tem bi zajeli in dokumentirali znanje podjetja in posameznikov o razvoju programske opreme in tako preprečili, da se znanje o razvoju programske opreme nahaja samo v glavah posameznikov. S popisom dejanskega načina dela na projektih prav tako omogočimo pomoč in vodenje razvijalcev pri drugih projektih s podobnimi lastnostmi. Kot rezultat pričakujemo, da bodo podjetja dosegla višjo raven zrelosti procesa razvoja programske opreme po modelu CMMI (angl. Capability Maturity Model Integration).

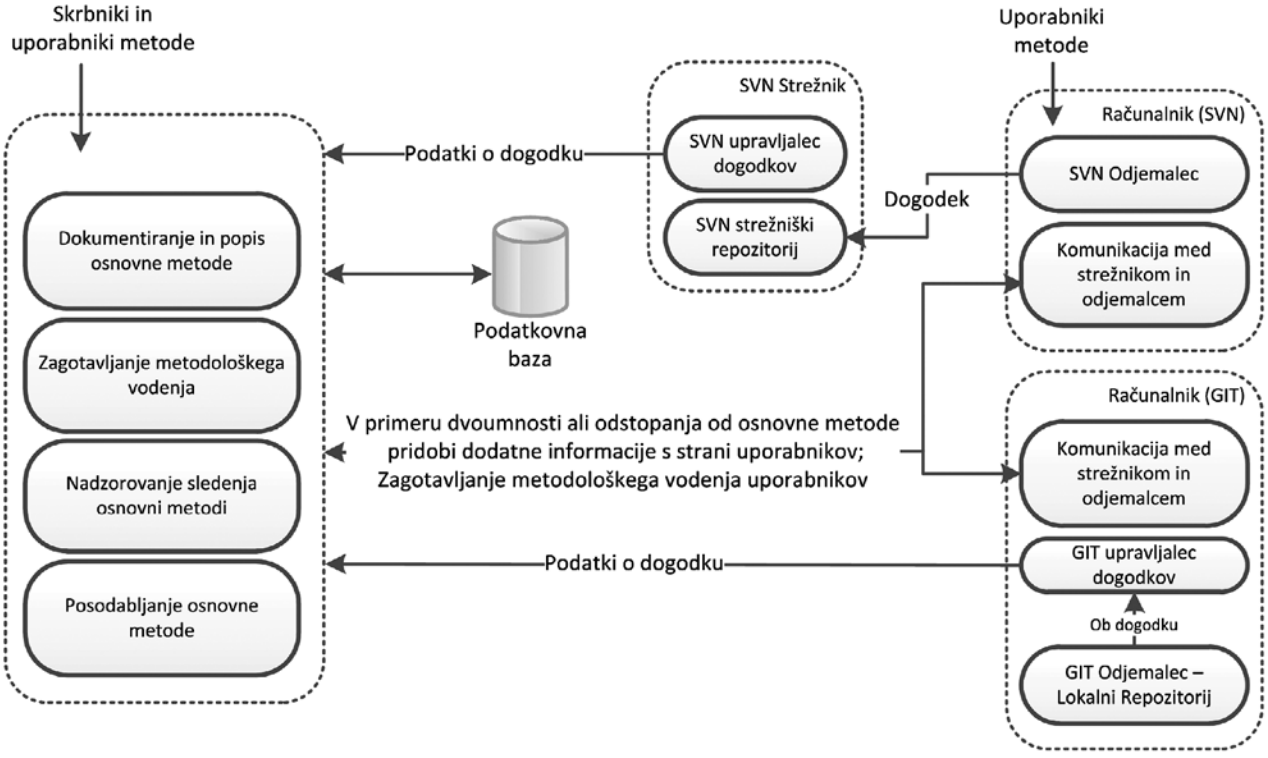
4 ORODJE ZA PODPORO PREDLAGANEGA PRISTOPA

V tem razdelku je predstavljena visokonivojska arhitektura podpornega orodja (slika 1), katerega glavni namen je olajšanje vpeljave predlaganega pristopa v prakso in testiranje postavljenih hipotez. Orodje bo samostojno in ne bo kot komponenta vključeno v razvojno okolje. V nadaljevanju na kratko predstavimo najpomembnejše komponente, njihov namen in vlogo.

4.1 Dokumentiranje in popis osnovne metode

Za podporo, uveljavitev in sledenje predpisanim metodam razvoja programske opreme je treba najprej zajeti trenutni proces razvoja in ga ustrezno dokumentirati. V podjetju, odvisno od vrst projektov, ki jih opravlja, je lahko predpisanih več različnih procesov razvoja – sestavi vseh procesov pravimo osnovna metoda (angl. base method) podjetja.

Podjetja se v splošnem strinjajo, da bi morale biti metode razvoja dokumentirane, vendar se med seboj razlikujejo v ravni podrobnosti, ki se jim zdijo uporabne in bi jih bilo smiselno popisati (Garcia s sod., 2011). Zajem, popis in ažuriranje dejanskega



Slika 1: **Visokonivojska arhitektura predlaganega orodja s podporo za Subversion (SVN) in GIT**

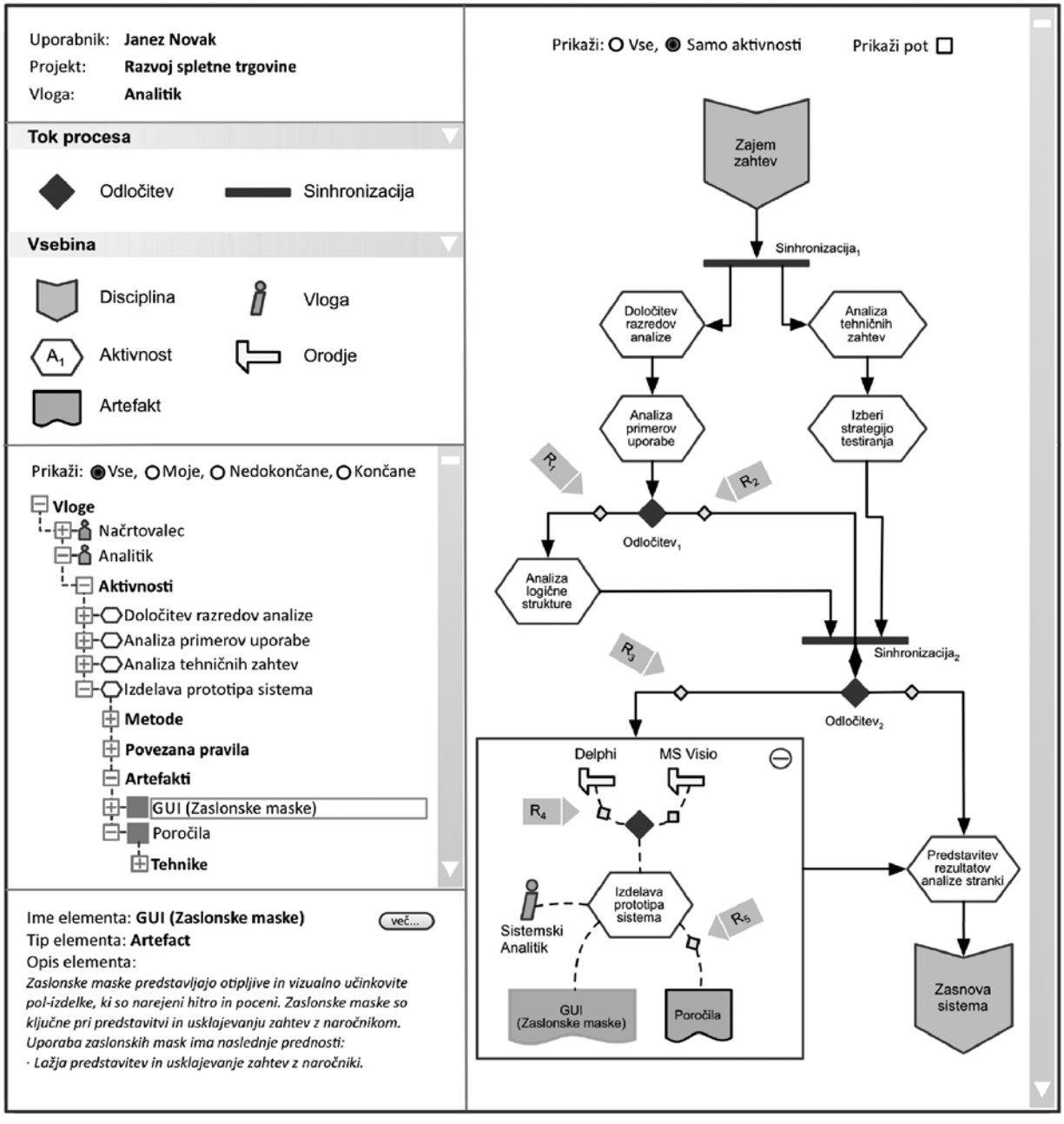
načina dela je običajno zamudno in drago opravilo, zato se podjetja za le redko odločajo za to. Podporno orodje mora tako omogočati zajem in popis osnovne metode podjetja na interaktiven in preprost način ter med drugim omogočiti, da podjetja sama določijo, v kolikšnem obsegu in kateri elementi (npr. aktivnosti, tehnike, orodja) naj se zajemajo. Orodje mora poleg osnovnih metod omogočati tudi zajem podpornih metamodelov (Bajec & Vavpotič, 2008). V prvem koraku vodilni razvijalci, ki so najbolj seznanjeni s trenutnim delom v podjetju in so določeni za skrbnike metode, ustvarijo metamodel, v katerem zajamejo ključna načela osnovne metode (npr. določijo metaelemente, ki lahko nastopajo v osnovni metodi, dovoljene povezave med njimi in druga pravila, kot npr. katere podelemente mora obvezno vsebovati določen element ipd.). Metamodel tako skrbi za konsistentnost osnovne metode in zagotavlja urejenost in celovitost. Skrbniki metode prav tako popišejo začetno osnovno metodo, ki naj bi ji razvijalci sledili pri svojem delu in ki bo uporabljena kot začetni vhod v komponento za nadzorovanje sledenja osnovni metodi.

Orodje mora omogočati vizualizacijo osnove metode. Odločili smo se za prikaz v obliki diagrama in drevesne strukture. Uporabniki metode imajo možnost urejanja (dodajanje, spreminjanje elementov in povezav) osnovne metode podjetja. Primer zaslonske maske uporabniškega vmesnika je prikazan na sliki 2. Posodabljanje metode mora biti omogočeno na interaktiven in uporabniku prijazen način (npr. uporabnik mora imeti možnost izbire elementa iz menija na levi in ga s tehniko povleci in spusti postaviti na želeno mesto v diagramu). Za posamezno aktivnost, orodje in druge elemente metode lahko uporabnik doda kratek opis in predloge za primere dobre prakse.

4.2 Zagotavljanje metodološkega vodenja

Dokumentirana osnovna metoda podjetja vključuje aktivnosti, ki jih je treba izvesti med razvojem različne tehnike in orodja, ki ju lahko uporabijo razvijalci, ter predloge in primere dobre prakse, ki služijo kot opora in vodilo razvijalcem pri njihovem delu. Prav to je še posebno pomembno za nove razvijalce, ki se še spoznavajo s procesom razvoja programske opreme znotraj podjetja.

Vsak razvijalec mora imeti dostop do pregleda osnovne metode podjetja. Razvijalec lahko za posamezni projekt preveri pot skozi predpisano metodo. Interaktivno, s klikanjem na elemente osnovne metode se uporabniku prikaže podrobnejši opis in predstavitev izbranega elementa. Poleg tega so za vsako aktivnost in razvojno orodje na voljo tudi predloge in primeri dobre prakse, ki uporabniku služijo kot vodilo pri delu. Primer zaslonske maske uporabniškega vmesnika je enak zaslonu na sliki 2, pri čemer imajo samo uporabniki z ustreznimi pravicami možnost spreminjanja osnovne metode podjetja (dodajanja novih elementov in povezav). Pri tem želimo predvsem izključiti nove razvijalce, ki se še spoznavajo s procesom razvoja v podjetju in še nimajo dovolj znanja, da bi bili primerni za popis novih načinov dela.



Slika 2: **Primer zaslonske maske komponente za zajem osnovne metode podjetja**

4.3 Nadzorovanje sledenja osnovni metodi

Najpomembnejša funkcionalnost orodja je sposobnost sledenja metodi v praksi (angl. in-action method) in zaznavanje morebitnih odstopanj od predpisane osnovne metode podjetja. Orodje se pri zaznavanju odstopanj lahko zanaša na (1) osnovno metodo podjetja, ki predpisuje, kako je treba izvajati različne vrste projektov, in (2) spremljanje metode v praksi, ki ni dokumentirana, vendar lahko o njej sklepamo na podlagi opazovanja dela razvijalcev in njihove komunikacije s sistemi oz. aplikacijami, ki jih uporabljajo pri izvajanju različnih opravil med razvojem.

Predpostavljamo, da lahko o metodi, ki se uporablja v praksi, sklepamo na podlagi rudarjenja po dnevniku sistema za nadzor verzij (angl. revision control system – RCS) in s skrbnim upoštevanjem osnovne metode, ki določa povezave med elementi metode, kot so aktivnosti, artefakti in vloge. Osnovna metoda nam tako omogoča, da vemo, katere artefakte lahko pričakujemo v posamezni aktivnosti od razvijalcev. Na podlagi artefaktov, ki so že dodani v RCS, lahko sklepamo o poti skozi osnovno metodo in katere aktivnosti so bile že izvedene za posamezni projekt. V primeru, ko je dodani artefakt v skladu z osnovno metodo, lahko nadaljujemo, sicer je treba zajeti razloge in okoliščine za odstopanje. Za Subversion in GIT, ki veljata za dva izmed najbolj uporabljenih RCS, smo za ta namen razvili ustrezne razširitve, ki spremljajo in zajemajo aktivnosti uporabnika. Predlagano orodje predvideva splošni vmesnik za poročanje o delu razvijalcev z namenom naknadnega dodajanja podpore za različne vrste aplikacij, kar bi omogočalo bolj natančno spremljanje dela razvijalcev.

Tipično ločimo dve vrsti razlogov, zaradi katerih metoda v praksi odstopa od predpisane.

- Uporabnik je naredil napako ter npr. dodal artefakt B pred artefaktom A, kar ni v skladu z osnovno metodo. V tem primeru je uporabnik verjetno pozabil izvesti aktivnost, ki je odgovorna za izdelavo artefakta A.
- Posebne okoliščine so uporabnika vodile, da se je odločil drugače, kot je predpisano z osnovno metodo.

V prvem primeru od uporabnika pričakujemo, da bo odpravil oz. kompenziral posledice napake (npr. izdelava manjkajočih artefaktov). V drugem primeru je treba ustrezno posodobiti osnovno metodo (dodajanje novih elementov in povezav), tako da bo zajemala novo znanje, ki ga lahko uporabimo v prihodnjih primerih.

Orodje mora omogočati, da na podlagi podatkov, pridobljenih iz RCS, in z uporabo različnih tehnik, kot so rudarjenje besedil, rudarjenje po procesih ipd., določimo aktivnost, v kateri se nahaja uporabnik, in kateri aktivnosti pripadajo dodani artefakti.

4.4 Upravljavec dogodkov RCS

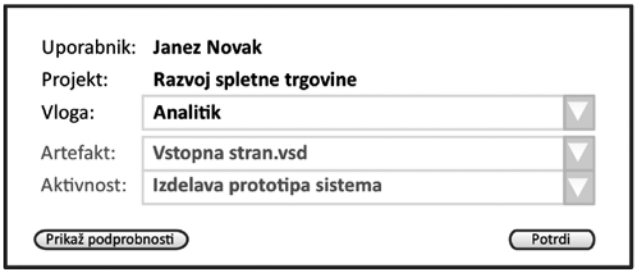
Večina sistemov za nadzor verzij podpira pred- in podogodkovne prožilce (angl. pre/post event hooks), ki omogočajo izvajanje določenih aktivnosti pred določenim dogodkom ali po njem, kot je npr. potrditev (angl. commit). To je pomembno, saj nam omogoča, da prestrezamo vse akcije, ki jih uporabnik izvaja z RCS, in tako dobimo informacije o aktivnostih na projektu. S tem namenom smo razvili razširitve za izbrane RCS, kar nam omogoča zbiranje podatkov, kot so komentar, uporabniško ime, časovni žig, spremenjeni dokumenti, tipi dokumentov ipd. Vsi zbrani podatki so nato poslani na strežnik, na katerem jih obdelamo in uporabimo za ugotavljanje, ali so uporabnikove aktivnosti v skladu s predpisano metodo podjetja.

4.5 Komunikacija med strežnikom in odjemalcem

V določenih primerih informacije, pridobljene na podlagi rudarjenja po dnevniku sistemov za nadzor verzij in na podlagi rudarjenja po vsebini artefaktov, ne bodo omogočile avtomatične določitve, kateri aktivnosti pripada določeni artefakt (tj. aktivnost, v kateri se nahaja razvijalec). Za take primere orodje vsebuje komponento, ki omogoča komunikacijo med strežnikom in uporabnikom. Glavni namen te komponente je, da od uporabnika zajame dodatne informacije, ki so potrebne za umestitev posameznega artefakta v določeno aktivnost. Za potrditev pravilnosti npr. se uporabniku prikaže pogovorno okno (slika 3) z vnaprej izpolnjenimi polji. V primeru, da je sistem pravilno določil aktivnost, kateri pripada artefakt, uporabnik pritisne gumb »Potrdi«, sicer pred tem izbere ustrezne vrednosti.

Komponenta ima pomembno vlogo tudi v primeru odstopanja od predpisane metode. V tem primeru uporabniku posreduje vprašanja, ki so dinamično generirana na strežniški strani in katerih glavni namen je zajem posebnih okoliščin in razlogov, ki so botrovali delovanju, ki ni v skladu s predpisano metodo. Zajete informacije pomenijo znanje o novem

načinu dela na projektih, ki ga uporabimo za posodobitev osnovne metode podjetja. V primerih, ko odstopanje ni namerno, uporabniku lahko zagotovimo metodološko vodenje in mu predstavimo primere dobre prakse za aktivnost, v kateri se nahaja.



Slika 3: **Primer pogovornega okna za zajem informacij o artefaktu, ki je bil dodan v RCS**

4.6 Posodabljanje osnovne metode

Ob ugotovitvi, da se metoda v praksi razlikuje od osnovne, predpisane metode (npr. sistem ugotovi, da je razvijalec dodal dokument, ki ni bil pričakovan v skladu z osnovno metodo), je treba o tem obvestiti razvijalca in ugotoviti, ali je prišlo do odstopanja namerno. V primeru, da odstopanje ni bilo namerno, razvijalcu zagotovimo metodološko vodenje in ga seznanimo s primeri dobre prakse za trenutno aktivnost. Poleg tega od njega zahtevamo, da popravi storjeno napako in vse morebitne posledice. V nasprotnem primeru, ko je odstopanje namerno, je treba zajeti razloge in okoliščine, v katerih je novi način razvoja primeren, ter jih skupaj z novimi povezavami in elementi metode uporabiti za dopolnitev osnovne metode podjetja. Za zajem vseh potrebnih podatkov uporabniku posredujemo obrazec, ki je dinamično ustvarjen na strežniški strani. Obrazec je sestavljen iz različnih tipov vprašanj, ki omogočajo, da od uporabnika na preprost način zajamemo znanje o tem, kateri so novo dodani elementi, kakšne so povezave med novimi in že obstoječimi elementi ter kakšne so okoliščine in razlogi (zapisano v obliki pravil), ki so botrovali k delovanju, ki ni v skladu s predpisano metodo. V primeru odstopanja lahko uporabniki osnovno metodo posodobijo tudi prek grafičnega vmesnika za zajem osnovne metode podjetja. Osnovna metoda podjetja bi se tako stalno prilagajala zahtevam projektov in odražala dejansko delo razvijalcev, ki bi aktivno sodelovali pri njenem oblikovanju. Zaradi tega pričakujemo, da bodo razvijalci predpisano metodo dojemali kot nekaj uporabnega in koristnega in ne le kot dodatno, nepotrebno breme.

5 VREDNOTENJE PRISTOPA

Vrednotenje našega pristopa bo potekalo v dveh korakih. Najprej bomo vrednotenje izvedli v akademskem okolju. Predlagani pristop in podporno orodje bomo uporabili pri predmetu, pri katerem bodo morali študentje razviti informacijski sistem in pri tem slediti točno določeni vnaprej predpisani metodi razvoja. To nam bo omogočilo preveriti, ali se orodje obnaša tako, kot je bilo pričakovano, in izpolnjuje vse predpisane zahteve. Poleg tega bomo lahko ocenili, ali so zajeti podatki zadostni za nadzor in spremljanje sledenja osnovne metode podjetja. Po končanem razvoju informacijskega sistema bomo opravili pogovore z vsemi sodelujočimi z namenom, da pridobimo povratne informacije o mogočih izboljšavah ter percepciji uporabnosti pristopa in podpornega orodja. Na podlagi rezultatov vrednotenja in zbranih informacij bomo optimizirali in izboljšali tako pristop kot tudi podporno orodje.

V drugem koraku bo vrednotenje pristopa in podpornega orodja izvedeno v sodelovanju z industrijo. Glavni namen tega je, da preverimo uspešnost predlaganega pristopa v praksi ter s tem tudi testiramo postavljene hipoteze. Trenutno smo že dogovorjeni za sodelovanje z lokalno industrijo, prav tako pa sodelujemo z raziskovalno skupino univerze v Parizu 1, ki nam bo pomagala vpeljati naš pristop v francoska podjetja. Idealen vzorec podjetij bi vključeval podjetja različnih velikosti (mikro, mala, srednja in velika), ki opravljajo različne projekte in so iz različnih kulturnih okolij. Ko bo predlagani pristop vpeljan v posamezno podjetje in bodo razvijalci seznanjeni z vsemi možnostmi uporabe, bomo na podlagi intervjujev z razvijalci oblikovali trenutno osnovno metodo podjetja, ki bo služila kot izhodiščna točka za nadaljnje opazovanje. Nato bomo s pomočjo podpornega orodja opazovali delovanje razvijalcev in shranjevali vse aktivnosti, ki jih ti opravljajo v povezavi s predlaganim pristopom (npr. potreba po metodološkem vodenju, spreminjanje osnovne metode, spreminjanje opisov posameznih elementov osnovne metode). Prav tako bomo zapisovali, koliko časa razvijalec porabi za uporabo novega pristopa v splošnem in koliko časa za posamezno funkcionalnost. Na podlagi števila odstopanj od predpisane metode, števila zahtev za metodološko vodenje in števila posodobitev

osnovne metode bomo lahko sklepali, ali so razvijalci seznanjeni s predpisano metodo podjetja in ali je ta skladna z metodo, ki jo razvijalci uporabljajo na projektih. Vsi zbrani podatki bodo prav tako uporabljeni za analizo uporabnosti in integracije pristopa v prakso, obenem pa nam bodo omogočili vpogled v sam proces razvoja programske opreme. Za potrditev zbranih podatkov in ugotovitev ter zajem podrobnosti o sami uporabnosti pristopa bomo na mesečni ravni izvajali intervjuje z razvijalci, pri čemer bomo uporabljali inovativne tehnike, kot je npr. »think-aloud experiment«, kar nam bo omogočilo zajem pomembnih in relevantnih informacij v povezavi s predlaganim pristopom.

6 SKLEP

V prispevku smo predstavili inovativni pristop in podporno orodje za konstruiranje metod. Glavna motivacija za to je bila nizka uporaba in nedosledno sledenje metodam razvoja programske opreme v praksi, kar vodi do številnih neuspešnih IT-projektov in nizke kakovosti razvite programske opreme. S pristopom želimo omogočiti zajem in popis znanja o razvoju programske opreme z minimalnim sodelovanjem razvijalcev. Prav tako želimo omogočiti spremljanje uveljavljanja predpisane metode v praksi in zajem znanja ter posodobitev osnovne metode v primerih odstopanja. Pričakujemo, da se bodo z uporabo predlaganega pristopa osnovne metode podjetja bolje prilagajale dejanskemu načinu dela na projektih ter znanju in zahtevam razvojne skupine. S pristopom tako omogočimo, da se znanje o razvoju programske opreme ne nahaja samo v glavah posameznikov, temveč je sistematsko dokumentirano. To omogoča hitrejše uvajanje novih in neizkušenih razvijalcev.

Trenutno se ukvarjamo z razvojem podpornega orodja, ki nam bo omogočilo testiranje hipotez v praksi. Končano orodje in sam pristop nameravamo vrednotiti v okolju fakultete, izboljšano in optimizirano pa kasneje tudi v različnih domačih in tujih podjetjih. Nadaljnje delo vključuje tudi razvoj razširitev za druge sisteme, ki jih razvijalci uporabljajo pri svojem delu (npr. JIRA, Bugzilla, Sharepoint), kar bi omogočilo lažje in bolj celovito spremljanje dela razvijalcev in posledično omogočilo zajem dodatnega znanja o razvoju programske opreme.

7 VIRI IN LITERATURA

[1] Bajec, M., Vavpotič, D., Krisper, M. (2007). Practice-driven approach for creating project-specific software development methods. *Information and Software Technology*, št. 49, zv. 4, str. 345–365.

[2] Bajec, M., Vavpotič, D. (2008). A framework and tool-support for reengineering software development methods. *Informatica, Lith. Acad. Sci.*, št. 19, zv. 3, str. 321–344.

[3] Bajec, M., Vavpotič, D., Furlan, Š., Krisper, M. (2007). Software process improvement based on the method engineering principles. *Situational Method Engineering: Fundamentals and Experiences, ser. IFIP International Federation for Information Processing*, J. Ralyté, S. Brinkkemper, and B. Henderson-Sellers (ur.). Springer Boston, 2007, št. 244, str. 283–297.

[4] Bekkers, W., van de Weerd, I., Brinkkemper, S., Mahieu, A. (2008). The influence of situational factors in software product management: An empirical study. Second International Workshop on Software Product Management. *IWSPM '08*, str. 41–48.

[5] Bloch, M., Blumberg, S., Laartz, J. (2012). *Delivering large-scale it projects on time, on budget, and on value*. http://www.mckinsey.com/client service/business technology.

[6] Brinkkemper, S., Saeki, M., Harmsen, F. (1998). Assembly Techniques for Method Engineering. *Proceedings of the 10th International Conference on Advanced Information Systems Engineering*, London, UK, str. 381–400.

[7] Deneckere, R., Iacovelli, A., Kornyshova, E., Souveyet, C. (2008). From Method Fragments to Method Services. *Proc. of EMMSAD'08*, Montpellier, France, str. 80–96.

[8] Dybå, T., Dingøyr, T. (2008). Empirical studies of agile software development: A systematic review. *Information and Software Technology*, št. 50, zv. 9–10, str. 833–859.

[9] Fitzgerald, B., Hartnett, G. (2005). A study of the use of agile methods within intel. *Business Agility and Information Technology Diffusion, ser. IFIP International Federation for Information Processing*, R. Baskerville, L. Mathiassen, J. Pries-Heje, and J. DeGross (ur.). Springer US, št. 180, str. 187–202.

[10] García, F., Vizcaion, A., Ebert, C. (2011). Process management tools. *IEEE Software*, št. 28, zv. 2, str. 15–18.

[11] García, J., Amescua, A., Sánchez, M., Bermón, L. (2011). Design guidelines for software processes knowledge repository development. *Information and Software Technology*, št. 53, zv. 8, str. 834–850.

[12] Henderson-Sellers, B., Ralyté, J. (2010). Situational method engineering: State-of-the-art review. *Journal of Universal Computer Science*, št. 16, zv. 3, str. 424–478.

[13] Karlsson, F. Ågerfalk, P. J. (2004). Method configuration: adapting to situational characteristics while creating reusable assets. *Information and Software Technology*, št. 46, zv. 9, str. 619–633.

[14] Karlsson, F. Ågerfalk, P. J. (2012). MC Sandbox: Devising a tool for method-user-centered method configuration. *Information and Software Technology*, št. 54, zv. 5, str. 501–516.

[15] Laanti, M., Salo, O., Abrahamsson, P. (2011). Agile methods rapidly replacing traditional methods at nokia: A survey of opinions on agile transformation. *Information and Software Technology*, št. 53, zv. 3, str. 276–290.

[16] Mohan, K., Ahlemann, F. (2011). What methodology attributes are critical for potential users? Understanding the effect of human needs. *Advanced Information Systems Engineering, ser. Lecture Notes in Computer Science*, H. Mouratidis in C. Rolland (ur.). Springer Berlin / Heidelberg, št. 6741, str. 314–328.

[17] Mirbel, I., Rivieres, V. de (2002). Adapting analysis and design to software context: The JECKO approach. *Object-Oriented Information Systems*, Z. Bellahsène, D. Patel in C. Rolland (ur.). Springer Berlin Heidelberg, str. 223–228.
[18] Mirbel, I., Ralyte, J. (2006). Situational method engineering: combining assembly-based and roadmap-driven approaches. *Requirements Engineering*, št. 11, zv. 1, str. 58–78.
[19] Ralyte, J., Rolland, C. (2001). An assembly process model for method engineering. *Advanced Information Systems Engineering*, K. R. Dittrich, A. Geppert in M. C. Norrie (ur.). Springer Berlin Heidelberg, str. 267–283.
[20] Riemenschneider, C., Hardgrave, B., Davis, F. (2002). Explaining software developer acceptance of methodologies: a comparison of five theoretical models. *IEEE Transactions on Software Engineering*, št. 28, zv. 12, str. 1135–1145.
[21] van de Weerd, I., Brinkkemper, S., Souer, J., Versendaal, J. (2006). A situational implementation method for web-based content management system-applications: method engineering and validation in practice. *Software Process: Improvement and Practice*, št. 11, zv. 5, str. 521–538.
[22] Vavpotič, D., Bajec, M. (2009). An approach for concurrent evaluation of technical and social aspects of software development methodologies. *Information and Software Technology*, št. 51, zv. 2, str. 528–545.
[23] Vlaanderen, K., van de Weerd, I., Brinkkemper, S. (2011). The online method engine: From process assessment to method execution. *Engineering Methods in the Service-Oriented Context, ser. IFIP Advances in Information and Communication Technology*, J. Ralyté, I. Mirbel in R. Deneckère (ur.). Springer Boston, št. 351, str. 108–122.

▪

Marko Janković je mladi raziskovalec na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegovo glavno raziskovalno področje je razvoj novih pristopov za izboljšanje metod razvoja programske opreme in njihove uporabe v praksi.

▪

Slavko Žitnik je doktorski študent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani in hkrati zaposlen kot mladi raziskovalec iz gospodarstva v podjetju Optilab, d. o. o. Raziskovalno se ukvarja predvsem s procesiranjem besedil, bolj natančno z razpoznavanjem entitet in povezav med njimi z uporabo metod strojnega učenja in semantičnih tehnologij.

▪

Lovro Šubelj je asistent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Poučuje predvsem predmete s področja podatkovnih baz. Raziskovalno se ukvarja z analizo realnih omrežij, natančneje z odkrivanjem značilnih skupin vozlišč v velikih kompleksnih omrežjih. Je avtor ali soavtor številnih prispevkov v strokovnih in znanstvenih publikacijah.

▪

Neli Blagus je mlada raziskovalka v Laboratoriju za podatkovne tehnologije na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Raziskovalno se ukvarja z analizo omrežij.

▪

Aljaž Zrnec je magistriral leta 2002 na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Leta 2006 je doktoriral s področja konstruiranja metodologij. Zaposlen je v Laboratoriju za podatkovne tehnologije kot asistent za področje podatkovnih baz. Na raziskovalnem področju se ukvarja s konstruiranjem metodologij, podatkovnimi bazami NoSQL in z računalništvom v oblaku. Je avtor ali soavtor številnih prispevkov v strokovnih in znanstvenih publikacijah.

▪

Marko Bajec je izredni profesor na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer poučuje dodiplomske in podiplomske predmete s področja razvoja informacijskih sistemov in podatkovnih baz. Raziskovalno se ukvarja z metodami in pristopi k snovanju in razvoju informacijskih sistemov, obvladovanjem informatike ter v zadnjih letih predvsem s podatkovnimi tehnologijami za predstavitev, analizo in vizualizacijo podatkov. Leta 2009 je ustanovil Laboratorij za podatkovne tehnologije ter prevzel njegovo vodenje. Je član številnih domačih in tujih združenj, komisij in odborov. V okviru fakultete je vodil več aplikativnih in raziskovalnih projektov. Svoje raziskovalne rezultate in dosežke iz prakse redno objavlja v domačih in mednarodnih znanstvenih in strokovnih krogih.

Anonimnost na spletnih medijskih portalih

Martina Lozej, Urša Lutman, Miha Glavač, Jaro Berce
Univerza v Ljubljani, Fakulteta za družbene vede, Kardeljeva ploščad 5, 1000 Ljubljana
martinalozej@gmail.com; ursa.lutman@gmail.com; miha@spletno-oko.si; jaro.berce@fdv.uni-lj.si

Izvleček

Splet – internet – kot nov medij prinaša nove možnosti izražanja mnenj – omogoča participativnost večjega števila ljudi. Ena od lastnosti novega medija je tudi anonimnost, ki dovoljuje drugačne pristope in svobodo izražanja mnenj, vendar pogosto povzroči tudi nestrpno izražanje. Z raziskavo, ki jo predstavljamo v članku, smo ugotovili, da uporabniki spletnih medijskih portalov poleg pozitivnih zaznavajo tudi številne negativne posledice anonimnosti na spletu (sovražni govor, žalitve, nizka kultura komunikacije), kljub temu pa zmanjšanju anonimnosti niso naklonjeni. Menijo namreč, da ima anonimnost še vedno večjo vrednost kot pa zmanjšanje števila sovražnih, neprimernih in neutemeljenih komentarjev. Po mnenju mnogih je premišljeno in dosledno moderiranje komentarjev primernejše in učinkovitejše od zmanjševanja anonimnosti.
Ključne besede: splet, spletni medijski portali, anonimnost, sovražni govor, moderator, komentar.

Abstract

Anonymity on the online media portals

People post and exchange information and express their opinions on the Internet. Its basic attribute is the anonymity of its users which on the one hand promotes diversity and freedom of speech, but on the other it often results in offensive and intolerant speech. Results of our survey show that users perceive both positive and negative effects of anonymity on the internet (hate speech, insults, poor communication etc.). Although survey participants see potential advantages of decreasing anonymity, they are unfavorable to the actual reduction. They believe that the worth of web anonymity is greater and more important than the reduction of hostile or inappropriate speech. The majority of the respondents stated that deliberate and consistent moderation of comments is a more appropriate and effective method than the reduction of user anonymity.
Key words: internet, online media portals, anonymity, hate speech, moderation, comment.

1 UVOD

Članek je rezultat raziskave o anonimnosti v medijih na internetu, ki se je izvajala s pomočjo spletne ankete junija 2012. Mediji namreč omogočajo pridobivanje različnih informacij. S pojavom spleta – interneta[1] – pa se je njihova vloga nekoliko spremenila oz. razširila, saj smo ljudje poleg pasivnega pridobivanja informacij dobili tako rekoč neomejene možnosti za aktivno sodelovanje in izražanje stališč, mnenj ter izmenjavo informacij. Internet je namreč v nasprotju z dosedanjimi mediji postal hipni dvosmerni komunikacijski medij. Vsakdo, če želi, lahko poda svoj komentar, mnenje ali idejo tako prek različnih temu namenjenih internetnih strani (npr. blog, Tumblr itd.) ter spletnih storitev (Twitter, Facebook, Youtube itd.), si ustvari svojo stran ali pa uporabi možnosti, ki jih ponujajo javni mediji na svojih spletnih straneh. S tem se je odprl prostor za različna izredno ažurna in hitra podajanja, vplivanja, izmenjave in spreminjanja mnenj, kakor tudi oblikovanje družbenih predstav posameznika ali celo različnih družbenih skupin.

S svojo preverjeno hipotezo avtorica ideje »teorija spirale molka« Elisabeth Noelle-Neumann (1974) dokazuje, da zaznavanje mnenjskega ozračja vpliva na pripravljenost posameznika za izražanje mnenja. Značilnost spleta je tudi, da lahko uporabniki komunicirajo povsem anonimno, kar omogoča bolj svobodno izražanje mnenj, hkrati pa lahko pripelje do izražanja nestrpnosti in sovražnega govora. Slovenski spletni mediji se prav zaradi sovražnih in žaljivih komentarjev v zadnjih letih soočajo z vse večjimi težavami. V prvi vrsti je za premagovanje le-teh krivo predvsem pomanjkanje sredstev za obvladovanje in preganjanje sovražnega govora (Spletno Oko, 2011a).

[1] Internet ali medmrežje je medsebojno povezana množica računalniških omrežij v splet (svetovni splet, World Wide Web – Web je množica storitev).

Nekateri vidijo rešitev za zmanjšanje sovražnih in neprimernih vsebin v odpravi anonimnosti tistih, ki sodelujejo na forumih ali pri komentiranju spletnih vsebin. Če bi se anonimnost lahko v celoti odpravila, bi to gotovo zmanjšalo primere sovražnega govora. Skrivanje identitete naplavi prikrite strasti, frustracije in sovraštva; kadar se je treba predstaviti s polnim imenom, je samonadzora glede tega gotovo več. Vendar anonimnosti na spletu ni mogoče zapovedati in predpisati. /…/ Strožja tovrstna regulacija bi imela več negativnih kot pozitivnih učinkov. (Rovšek, 2011)

Kaj pravzaprav pomeni pojem anonimnost? Nekdanji Googlov izvršni direktor Eric Schmidt je v intervjuju, objavljenem leta 2010 na spletnem portalu Moj Mikro, razložil, da je treba ločiti med zasebnostjo – ki zagotavlja nadzor nad uporabo, zbiranjem in razširjanjem osebnih podatkov in informacij in je zelo pomembna – in anonimnostjo (Moj Mikro, 2010). Vrst zasebnosti (in njenih definicij) obstaja več, na internetu pa je aktualna predvsem informacijska zasebnost, to je možnost posameznika, da obdrži informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi (Čebulj, 1992), medtem ko je anonimnost v WEB dictionary of Slovene language[2] definirana kot »odsotnost identitete« ali »stanje, v katerem človek ostaja neznan po imenu, navadno, ker tako želi, ali neznan v določenem okolju, bodisi ker tako želi ali ker mu ne uspe zbuditi pozornosti javnosti«. Da gre pri anonimnosti pravzaprav za odsotnost identitete, govori tudi Zakon o varstvu osebnih podatkov, v katerem je anonimiziranje osebnih podatkov definirano kot sprememba oblike osebnih podatkov na tak način, da jih ni več mogoče povezati s posameznikom oz. je to mogoče le z velikimi napori, stroški ali porabo časa (ZVOP-1-UPB1, 2007: 6. čl.).

Ker v praksi obstaja zelo malo raziskav na temo odstranjevanja in vpliva anonimnosti na komentiranje na spletnih medijskih portalih,[3] je bil namen obravnavanega raziskovalnega dela (Lozej idr., 2012) raziskati obstoječe domače in tuje prakse odstranjevanja anonimnosti na novičarskih portalih ter ugotoviti, katere so prednosti in slabosti zmanjšanja anonimnosti. Namen praktičnega dela raziskave je bil s pomočjo spletnega anketiranja ugotoviti, kakšna stališča do anonimnosti in posledično do njenega zmanjšanja obstajajo pri uporabnikih slovenskih spletnih medijskih portalov.

2 ANONIMNOST IN NEPRIMERNI GOVOR NA SPLETU

Anonimnost na spletu igra nadvse pomembno vlogo in je najpogostejša spremljevalna tematika, ko govorimo o neprimerni komunikaciji na internetu, med drugim na javnem forumu o sovražnem govoru v spletnih medijih (Svenšek, 2011), okrogli mizi o etičnem vedenju na internetu (Spletno Oko, 2011b), seminarju Kriminaliteta iz sovraštva na internetu (Spletno Oko, 2011c), v člankih na temo sovražnega govora (Rovšek, 2011; Vehovar idr., 2012) ter v medijih (Verbič, 2012). Kljub temu pa o spletni anonimnosti ne moremo govoriti samo negativno. Bila je katalist za družbene spremembe v Egiptu in Libiji med t. i. »arabsko pomladjo«, v zgodovini pa je pogosto igrala pomembno politično vlogo (če pomislimo samo na uporniške časnike med drugo svetovno vojno) ali kot pravi dr. Igor Verbič: »Anonimnost sama po sebi ne vpliva na grožnje, v zgodovini je igrala pomembno vlogo v političnem življenju in takšno vlogo ima še danes. /…/ Nedavna primera sta Egipt in Iran. Politično delovanje je temeljilo na anonimnosti.« (Verbič, 2012)

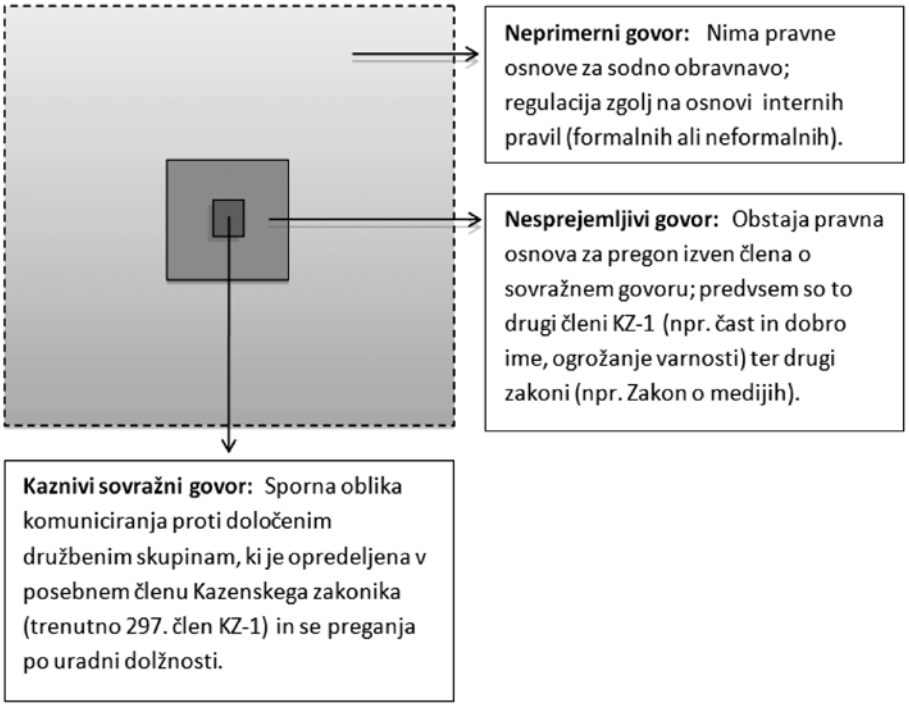
Anonimnost na internetu »omogoča necenzurirano poročanje, neomejeno politično sporočanje, javno in zasebno razpravljanje o žgočih družbenih vprašanjih ali o neprijetnih osebnih težavah« (Bernik & Prislan, 2012, str. 23). Vendar pa ima na spletu lahko tudi izrazito negativen učinek, ki privede k razširjanju spornih in uničevalnih oblik komunikacije, npr. groženj, posmehovanja, laži in razžalitev posameznikov, žaljivih in krutih šal z namenom maščevanja (lažnivi profili na družbenih omrežjih), objestnosti in vandalizma ter sovražnega govora (Spletno Oko, 2011č). Kljub temu da zaradi nadzorovanja (npr. z uporabo piškotkov – »cookies«) o obstoju anonimnosti na internetu danes težko govorimo (Završnik, 2008), pa je zaradi zapletenosti in kompleksnosti tehnologije ter globalnosti odkrivanje storilcev kaznivih dejanj na spletu izredno težavno (Bernik in Prislan, 2012). Anonimnost torej pomeni dvorezen meč in močno sredstvo za koristno in uničevalno dejavnost obenem. Zlorabe so cena, ki jo mora družba plačati za ohranitev koristi, ki jih prinašajo anonimnost, psevdonimnost in pravica do zasebnosti (Bernik in Prislan, 2012).

[2] Vir: http://eng.slovenscina.eu/spletni-slovar?dictId=79&entryId=21730&key=A.

[3] Mediji in novice, tiskarske storitve in podjetja, združeni na enem mestu na internetu.

Zavedati se moramo tudi, da je svoboda izražanja v demokratičnih državah zaščitena vrednota (Matteucci v Teršek, 2005). Poleg pomembnosti za demokratično delovanje je pomembna »tudi zaradi možnosti za posameznikovo samoizpopolnitev (self-fulfillment) oziroma zaradi omogočanja posameznikove osebnostne rasti (personal growth) in samoizpolnitve (self-realisation)« (Teršek, 2005, str. 23). Čeprav je svoboda izražanja v zakonodaji in sodni praksi ZDA, kjer je s prvim amandmajem prepovedano sprejetje zakonov, ki omejujejo svobodo govora (Teršek, 2005), bolj absolutna kot v Evropi, pa je tudi Evropsko sodišče za človekove pravice (v primeru Handyside proti Združenemu kraljestvu, 1976) zavzelo stališče, da je treba ščititi tudi ideje, ki žalijo ali šokirajo celotno populacijo ali njen del (Teršek, 2005). Nadalje, Deklaracija o človekovih pravicah v 19. členu določa, »da ima vsakdo pravico do svobode mišljenja, vštevši pravico, da nihče ne sme biti nadlegovan zaradi svojega mišljenja, in pravico, da lahko vsak širi informacije in ideje s kakršnimi koli sredstvi in ne glede na meje« (Berden, 1999). Svoboda govora je v Sloveniji ustavno zagotovljena z 39. členom Ustave Republike Slovenije, ki pravi: »Zagotovljena je svoboda izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja.« (Ustava Republike Slovenije, 1991: 39. čl.)

Seveda pa zakonski prag, ki ima za kaznivost izražanja visoka merila (sodeč po noveli kazenskega zakonika KZ-1B le tista dejanja (govor), ki privedejo do kršenja javnega reda in miru) (Spletno Oko, 2013), ne preprečuje lastnikom spletnih mest (zasebna lastnina), da sami določijo merila za še sprejemljiv govor na svojem spletnem mestu (po sistemu »moja hiša, moja pravila«) in sankcionirajo morebitne kršitelje (s prepovedjo dostopa, začasnim izklopom itd).



Slika 1: **Sovražni govor na slovenskem spletu** (Vir: Vehovar idr., 2012, str. 173)

Največ spornih komentarjev v slovenskem spletu spada v kategorijo neprimernih in nesprejemljivih oblik govora, ki v večji meri niso kaznive ali preganjane po uradni dolžnosti (Vehovar idr., 2012). Na sliki 1 je prikazana groba razčlemba oblik neprimernih komunikacij v slovenskem spletu, prav tako pa lahko razberemo tudi, da bi večino neprimernih oblik komuniciranja na spletu lahko zajezilo že hitro in dosledno moderiranje uporabniških vsebin.

Omeniti je treba, da se v poljudni in bistveno razširjeni določitvi sovražnega govora, v medijih in javnosti (razvidno iz preglednice 2) pojavljata tudi »neprimerni« in »nesprejemljivi govor«, čeprav pravno ne spadata v kategorijo kaznivega sovražnega govora.[4,5]

Preglednica 2: **Na kaj pomislite, ko nekdo omeni izraz sovražni govor?**

Navedba	**Odstotek (%)**	
	Splet	Telefon
Nekdo je javno spodbujal nasilje zoper določeno skupino ljudi.	69	43
Nekdo je javno izražal sovraštvo do druge osebe.	60	35
Nekdo je žalil drugo osebo.	36	23
Nekdo je grozil drugi osebi.	32	20
Uporaba neprimernega besednjaka, ki sicer ni uperjen zoper druge osebe.	20	16

(Vir: Glavač in Vehovar, 2011)

Omejevanje oblik govora pogosto trči ob ustavno in mednarodno priznano pravico do svobode izražanja, ki ima velik pomen v demokratičnih družbah. Evropsko sodišče za človekove pravice (ESČP) v svoji sodni praksi pogosto navaja, da se svoboda izražanja ne nanaša le na informacije ali ideje, ki jih sprejemamo naklonjeno ali se do njih ne opredeljujemo, temveč zajema tudi tiste, ki prizadenejo, šokirajo ali vznemirjajo.6 Ob tem velja omeniti tudi primer Vejdeland proti Švedski (Interights, 2012), v katerem so pri ESČP ustvarili doktrino za kaznivost »resnih obtožb na podlagi predsodkov, ki neposredno ne pozivajo k dejanjem iz sovraštva«. Ob tem se nekaterim strokovnjakom postavlja vprašanje, ali sta homofobija in diskriminatorni govor v praksi ESČP enačena s sovražnim govorom (Teršek, 2012). Odgovor na to vprašanje bo razkrila sodna praksa evropskega sodišča v prihodnosti. Vendar ESČP ob tem hkrati poudarja, da izvrševanje svobode v demokratični družbi predpostavlja tudi dolžnosti in odgovornosti. Tudi svoboda izražanja je varovana le do meja varstva drugih človekovih pravic ter svoboščin in pravic drugih (Rovšek, 2011).

2.1 Zmanjšanje stopnje neprimernega govora na spletu

Spletni novičarski portali morajo najti pravo ravnovesje, ko se odločajo o tem, ali naj tisti, ki komentirajo, ostanejo tudi anonimni. Da bi pritegnili uporabnike, morajo svoje spletne strani narediti čim bolj nezahtevne za uporabo, dopustiti pa morajo tudi anonimnost, saj ta daje uporabnikom večjo svobodo pri komentiranju. S tem privabljajo na svoje strani večje število uporabnikov, posledično so bolj znane. Ljudje na spletu povejo stvari, ki jih v živo nikoli ne bi. V najboljši luči lahko ta svoboda prinaša odprto razpravo in izmenjavo mnenj, v najslabšem primeru pa sovražno nastrojen govor. Veliko spletnih medijskih portalov se boji, da z ukrepi, kot je uvedba obvezne registracije za uporabnike, ljudi lahko odtegnejo od komentiranja. Dejavnik za neprimerne objave oz. komentarje je v večini primerov tudi anonimnost, registracija uporabnikov pa ne zagotavlja popolne odprave le-teh. Sovražni komentarji in neželena sporočila (spam) se pojavljajo tudi na straneh, na katerih je zahtevana popolna registracija uporabnikov. Težava se pojavlja tudi pri samem moderiranju vsebin, kajti medijske hiše ne želijo dajati občutka »velikega brata«, temveč želijo spodbuditi prost pretok informacij in idej. Hkrati pa tudi ne želijo, da bi njihovi spletni portali postali igrišča brez pravil, na katerih bi prevladovali nasilneži, ki onemogočajo vsakemu novemu članu, da bi se priključil razpravi. Empirično je dokazano, da deljenje osebnih informacij odvrne določen odstotek uporabnikov, odprto je le vprašanje, ali lahko to pripomore k višji kakovosti vsebin v komentarjih (Gsell, 2009). Ob tem ne moremo mimo (splošne) ravni novinarstva v slovenskem prostoru, za katero je značilna nizka stopnja objektivnosti, politična pripadnost in medsebojno obračunavanje. O tem govori tudi predsednica novinarskega častnega razsodišča Ranka Ivelja (Verbič, 2012). Po njenem mnenju so razne kolumne na spletnih medijih poligon za obračunavanje s političnimi nasprotniki, ob tem pa poziva, da se »upremo vsakršnemu odmiku od profesionalnih in etičnih norm, ki so jasno zapisane v zakonih, kot tudi novinarskemu ko-

[4] Kar je, denimo, razvidno iz članka na temo groženj proti predsedniku vlade in varuhinji človekovih pravic (avgusta 2012), npr: Č/…/ tudi varuhinja človekovih pravic, ko ni bila sposobna javno obsoditi tako evidentnega sovražnega govora, kot je sovražni govor s pozivi k uboju nekoga, pa naj bo to Janez Janša, Zoran Janković ali neznani Janez Novak« (Urbanija, 2012).

[5] V še ne izdani publikaciji Sovražni govor na slovenskem spletu (2011) je na vzorcu 2140 uporabnikov spleta 60 odstotkov anketirancev odgovorilo (lahko so izbrali več odgovorov), da ob izrazu sovražni govor pomislijo na javno izražanje sovraštva do druge osebe, 32 odstotkov jih pomisli na grožnje, medtem ko jih je 69 odstotkov odgovorilo, da gre za javno spodbujanje nasilja zoper določeno skupino ljudi (edina pravnoformalno pravilna definicija) (Glavač in Vehovar, 2011). Sovražni govor je v javnosti torej izraz Čcatch-all«, ki obsega različne vrste družbeno nesprejemljivega govora.

[6] V primeru Handyside proti VB (1974) (Teršek, 2005).

deksu« (ibid). Na koncu se postavlja vprašanje, ali od novinarskih člankov, katerih namen je podžiganje političnih strasti, lahko pričakujemo kakovostne komentarje.

2.1.1 Prakse iz tujine

V tujini že imajo nekaj prakse z omejevanjem in odstranjevanjem anonimnosti na spletnih novičarskih portalih. Trije švedski portali[7] so v času po morilskem pohodu Andersa Breivika prepovedali anonimne komentarje. Komentiranje so dovolili samo osebam, ki so se prijavile prek Facebooka ali podobnega portala. Poleg tega so pri portalih ugotovili, da rasistični govor širi majhna, vedno ista skupina posameznikov. Po tem ko je podoben sistem prijavljanja prek socialnih omrežji uvedel časnik Verdens Gang, je v kratkem času izgubil 15-odstotni delež obiskanosti (RTV SLO, 2011), kar priča o negativni plati deanonimizacije. Uredniki portalov se morajo namreč soočiti z dilemo, ali jim je pomembnejše večje število komentarjev in nižja raven komunikacije ali pa manjše število kakovostnejših komentarjev.

Leta 2012 je britanska vlada predlagala »Defamation bill«, zakon usmerjen proti t. i. »internetnim trolom« (spletnim zbadljivcem). Po predlogu zakona bodo imele, če bo zakon sprejet, žrtve pravico vedeti, kdo je pisec komentarjev, ki so usmerjeni proti njim, poleg tega pa bi moral portal, na katerem se je pojavljal obrekljivi, žaljivi ali sovražni komentar, razkriti identiteto piscev (Sky News, 2012). Zaradi hitrejših sodnih postopkov v primeru razžalitev, ki jih predvideva zakon, in odstranjevanja anonimnosti ga nekateri označujejo kot »katastrofalnega za svobodo govora« (O'Neill, 2012).

Jack Rosenberry je v svoji raziskavi o anonimnosti in komentiranju na spletnih forumih osemdesetih ameriških časopisnih hiš ugotovil, da udeleženci vzrok za vse pogostejšo uporabo negativnih in žaljivih komentarjev vidijo v anonimnosti, vendar so kljub temu proti deanonimizaciji. Dve tretjini respondentov sta se močno strinjali s trditvijo, da so pogovori na forumih večinoma nastrojeni negativno, udeleženci v diskusijah pa napadajo druge ljudi in njihove ideje. Takšno vedenje in komentiranje onemogoča produktivno razpravo. Na drugi strani pa občutna manjšina (le slabih 27 %) respondentov podpira idejo o samoidentifikaciji udeležencev (Rosenberry, 2011).

[7] Aftonbladet, Expressen in Dagens Nyheter.

Z začetkom leta 2013 je na Hrvaškem začel veljati novi kazenski zakonik, ki kot kaznivo dejanje sovražnega govora opredeljuje tudi pozivanje k nasilju ali sovraštvu prek računalniškega sistema ali mreže, za kar je zagrožena kazen do tri leta zapora (Šurina, 2013).

2.1.2 Prakse v Sloveniji

Kot omenja Rovšek, je pomemben ukrep samoregulacije vsebin v Sloveniji *Kodeks regulacije sovražnega govora na slovenskih spletnih medijskih portalih* (2010), katerega podpisniki so poleg prijavne točke Spletno Oko večji slovenski spletni medijski portali – *multimedijski portal RTV SLO, delo.si, dnevnik.si, vecer.com, siol.net* in *zurnal24.si* (Rovšek, 2011). Leta 2012 sta se kodeksu pridružila tudi portala *24ur.com ter slovenskenovice.si* (Spletno Oko, 2012a; Spletno Oko, 2012b). Kodeks je bil oblikovan z namenom vzpostavitve enotnih elementov za regulacijo sovražnega govora na slovenskih spletnih medijskih portalih. Splošna določila kodeksa pravijo, da le enotno delovanje zoper sovražni govor lahko učinkovito zmanjša ta pojav na slovenskem spletu, podpisniki pa so se zavezali, da pri upravljanju svojega spletnega portala dosledno upoštevajo ukrepe, kot so obvezna registracija uporabnikov, ki želijo oddajati komentarje na spletnih portalih, dosledno moderiranje uporabniških vsebin, poenotenje obrazca za oddajo komentarjev, na katerem mora biti jasno vidno določilo iz kazenskega zakonika (297. člen KZ-1b) o posameznikovi kazenski odgovornosti za javno spodbujanje sovraštva, nasilja ali nestrpnosti. Ne nazadnje je kodeks tudi podlaga za ustanovitev delovne skupine za regulacijo sovražnega govora na slovenskih spletnih medijskih portalih (Spletno Oko, 2011a). Podpisniki kodeks vidijo kot dober ukrep za preprečevanje sovražnega govora in razbremenitev administratorjev ter moderatorjev (RIS, 2010).

Na spletnem portalu časopisne hiše Delo (delo.si) so ugotovili, da sama registracija uporabnikov še ne zagotavlja večje kakovosti komentarjev, menijo pa, da bi manjša stopnja anonimnosti (npr. prijava prek Facebooka) vplivala na kakovost komentarjev. Tudi dr. Marko Milosavljević je mnenja, da je na Facebooku manj sovražnega govora prav zaradi manjše stopnje anonimnosti. Na spletnem portalu Žurnala (zurnal24.si) so po uvedbi obvezne registracije najprej opazili upad števila komentarjev. Sčasoma se

je število komentarjev ponovno vrnilo na prejšnjo vrednost, vendar se skrajne oblike sovražnega govora niso več pojavljale (RIS, 2010).

Sovražni govor v medijih v Sloveniji regulirata tudi 8. člen Zakona o medijih ter 21. člen Kodeksa novinarjev Slovenije. Prvi prepoveduje spodbujanje k rasni, spolni, verski ali drugi neenakopravnosti in nestrpnosti ter nasilju, drugi pa kot nedopustno označuje novinarsko spodbujanje k nasilju, širjenju sovraštva in nestrpnosti ter druge oblike sovražnega govora, hkrati pa predpisuje, da se mora novinar v primeru njihove pojavitve nemudoma odzvati in jih obsoditi. (Zakon o medijih, 2006: 8. čl.; Kodeks novinarjev Slovenije, 2002: 21. čl.)

3 METODOLOGIJA

3.1 Zbiranje podatkov in vzorec

Udeležence raziskave predstavlja priložnostni vzorec obiskovalcev spletnih medijskih portalov ter forumov, ki so junija 2012 izpolnili spletno anketo. Skupno je na povezavo do ankete kliknilo 1473 oseb, končni vzorec izpolnjene spletne ankete pa predstavlja 762 respondentov. Kot ustrezne udeležence smo upoštevali le tiste, ki obiskujejo spletne medijske portale in so odgovorili na vsaj eno od vprašanj v sklopih o anonimnosti.

Med anketiranci je bilo 58 odstotkov moških in 42 odstotkov žensk. Starostni razpon vzorca je bil od 12 do 85 let, povprečna starost pa 37 let. Malo manj kot 50 odstotkov vzorca ima srednješolsko izobrazbo ali manj, četrtina pa univerzitetno izobrazbo ali več. Z vidika dejavnosti na spletnih medijskih portalih smo udeležence razdelili v tri skupine: 1 – bralci novic (8 %), 2 – bralci novic in komentarjev (59 %) ter 3 – udeleženci, ki berejo novice, komentarje ter tudi sami komentirajo (33 %). V nadaljevanju bomo anketirance skupin 1 in 2 imenovali bralci, anketirance skupine 3 pa komentatorji.

3.2 Merski instrument

Za merski instrument smo uporabili lastni spletni anketni vprašalnik, sestavljen iz 18 vprašanj, od tega je bilo trinajst zaprtih, štiri odprta in eno polodprto vprašanje. Vsebinsko je vprašalnik obsegal področja: vedenje obiskovalcev na spletnih medijskih portalih, splošna stališča o anonimnosti na spletu ter stališča o anonimnosti in načine ter posledice zmanjšanja le-te v kontekstu spletnih medijskih portalov.

Prvi sklop vprašalnika je vseboval pet vprašanj zaprtega in eno vprašanje polodprtega tipa. Zanimalo nas je, ali anketiranci sploh obiskujejo slovenske spletne medijske portale, kakšne so njihove aktivnosti na portalih, kdaj so nazadnje objavili komentar pod novico/člankom in kako pogosto to počnejo ter katere spletne medijske portale vsaj občasno obiskujejo. Pri zadnjem vprašanju sklopa pa so anketiranci na petstopenjski lestvici ocenjevali strinjanje z osmimi trditvami, ki so se nanašale na komentiranje novic in člankov.

V drugem sklopu so anketiranci najprej odgovarjali na dve odprti vprašanji o pozitivnih in negativnih vidikih anonimnosti na spletu, tretje vprašanje pa je bilo zaprtega tipa, pri katerem so na petstopenjski lestvici ocenjevali strinjanje s petimi trditvami o anonimnosti na spletu.

Tretji sklop je bil sestavljen iz treh vprašanj zaprtega in enega vprašanja odprtega tipa. Pri prvem vprašanju so anketiranci na petstopenjski lestvici ocenjevali primernost različnih načinov zmanjševanja stopnje anonimnosti uporabnikov ob registraciji na spletnih medijskih portalih. Pri drugem vprašanju, ki je bilo odprtega tipa, so imeli anketiranci možnost podati pripombe oz. predloge na navedene načine zmanjševanja anonimnosti. Pri tretjem vprašanju pa so anketiranci na petstopenjski lestvici ocenjevali pet trditev o tem, kako bi zmanjšanje anonimnosti vplivalo na način oz. spremembo pri pisanju komentarjev – v primeru, da bi njihove osebne podatke (ime, priimek) videl administrator, ter v primeru, da bi njihove podatke videli vsi uporabniki. Tudi zadnje vprašanje tega sklopa je sestavljalo pet trditev, pri katerih so anketiranci svoje strinjanje ocenjevali na petstopenjski lestvici, trditve pa so se nanašale na vpliv zmanjšanja anonimnosti na komentarje in komentatorje.

Zadnji sklop je bil sestavljen iz štirih demografskih vprašanj zaprtega tipa (spol, letnica rojstva, izobrazba, zaposlitveni status) ter iz odprtega vprašanja, pri katerem so imeli anketiranci možnost podati sklepno misel, pripombo, dopolnilo, pojasnilo ali predlog.

Šlo je za raziskavo preliminarne in eksploratorne narave, katere cilj je bil pridobiti čim širši vpogled v percepcijo anonimnosti uporabnikov spletnih medijskih portalov in stališč do zmanjšanja le-te. V raziskavi smo zato uporabili večje število odprtih vprašanj in s tem pridobili tudi kvalitativne odgovore, v katerih so udeleženci prosto opisovali svoja stališča in izrazili mnenje.

3.3 Omejitve raziskave

V raziskavi je poudarek na stališčih in percepciji anonimnosti, naš vprašalnik pa vsebuje tudi vprašanja, ki zahtevajo samoocenjevanje vedenja uporabnikov. Ob rezultatih tovrstnih vprašanj se je treba zavedati, da pri ocenjevanju lastnih vedenj anketiranci nikoli ne morejo biti povsem objektivni. V anketnem vprašalniku nista bila definirana pojma anonimnost in zmanjšanje anonimnosti, kar je sicer pri anketirancih povzročilo subjektivno dojemanje in odgovarjanje na vprašanja, vendar je ravno to omogočilo širok vpogled v raziskovano področje in dojemanje anonimnosti med uporabniki.

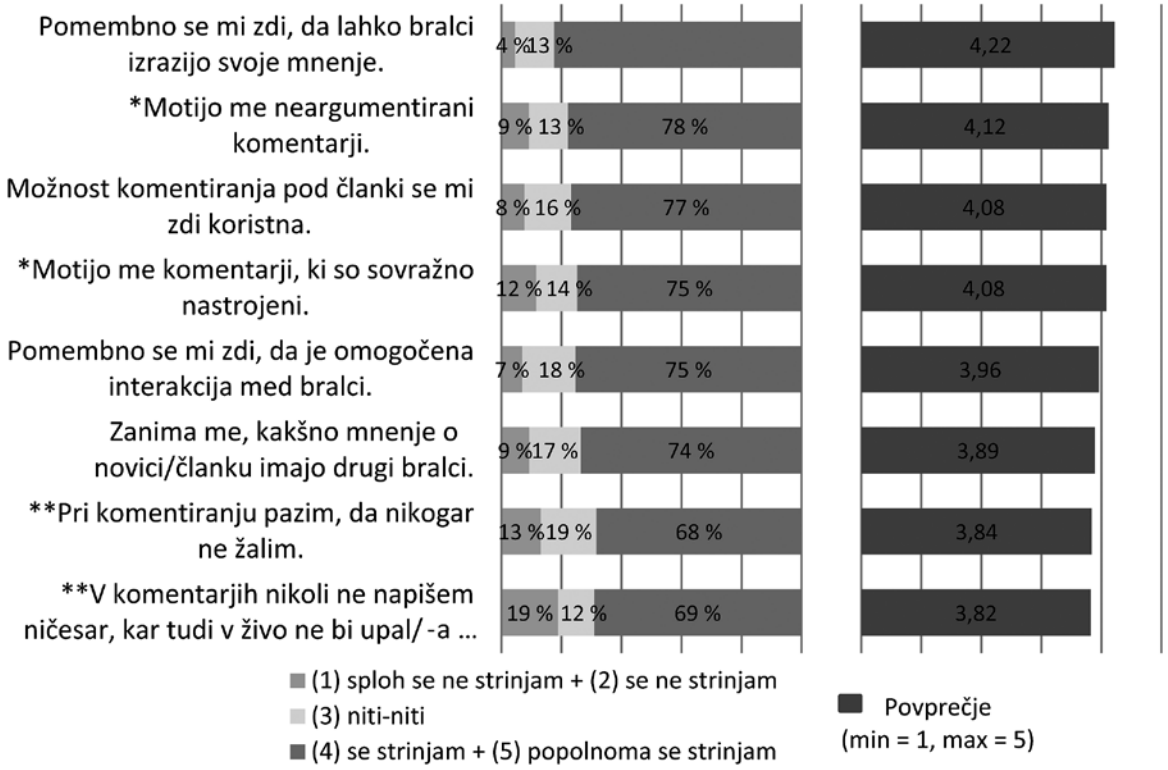
Kot potencialno omejitev raziskave bi lahko omenili tudi vprašljivo reprezentativnost vzorca, ki onemogoča prenašanje ugotovitev na celotno populacijo, vendar avtorji menimo, da zaradi izrazito eksploratorne narave raziskave to niti ni omejitev.

4 REZULTATI

4.1 Komentiranje novic in člankov

Anketirance smo prosili, da ocenijo strinjanje s trditvami, ki se nanašajo na komentiranje novic in člankov. Svoje strinjanje s trditvami so ocenjevali na petstopenjski lestvici (1 = sploh se ne strinjam, 5 = popolnoma se strinjam). Iz slike 3 je razvidno, da se je večina vprašanih anketirancev strinjala z vsemi trditvami. Najbolj so se strinjali, da je pomembno, da lahko bralci izrazijo svoje mnenje (M = 4,22) ter da jih motijo neargumentirani komentarji (M = 4,12). Možnost komentiranja pod članki se jim zdi koristna (M = 4,08), motijo pa jih sovražno nastrojeni komentarji (M = 4,08).

Komentatorji se v primerjavi z bralci v večji meri strinjajo, da je možnost komentiranja koristna, da je pomembno, da lahko bralci izrazijo svoje mnenje,



* Odgovarjali so le bralci novic in komentarjev (skupina 2) in komentatorji (skupina 3).
** Odgovarjali so le komentatorji (skupina 3).

N = 259–761

Slika 3: **Strinjanje s trditvami o komentiranju novic in člankov**

zanima pa jih tudi, kakšno mnenje o novici/članku imajo drugi bralci. Bralce bolj kot komentatorje motijo sovražno nastrojeni komentarji.

4.2 Vidik anonimnosti

Tako kot pri trditvah o komentiranju so tudi pri trditvah o anonimnosti na spletu anketiranci svoje strinjanje ocenjevali na petstopenjski lestvici. Anketiranci so se najbolj strinjali s trditvijo, da bi moral biti tudi na spletu vsak odgovoren za svoja dejanja in besede (M = 4,05), kljub temu pa menijo, da bi moral imeti na spletu vsak pravico do popolne anonimnosti (M = 3,65) ter da anonimnost uporabnika varuje pred zlorabo podatkov (M = 3,63). Dobra tretjina anketirancev (39 %) je bila mnenja, da ima anonimnost na spletu predvsem pozitivne lastnosti.

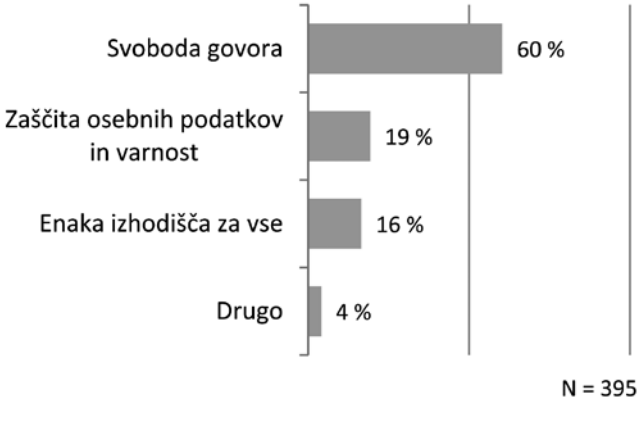
Bralci se v večji meri kot komentatorji strinjajo, da bi moral biti tudi na spletu vsak odgovoren za svoja dejanja ter da anonimnost negativno vpliva na vedenje uporabnikov.

4.2.1 Pozitivni vidiki anonimnosti

Anketirancem smo postavili odprto vprašanje o pozitivnih vidikih anonimnosti. Odgovore smo vsebinsko kodirali, pri čemer je bil posamezen odgovor lahko uvrščen v več kot eno od kategorij:

1. svoboda govora,
2. zaščita osebnih podatkov in varnost,
3. enaka izhodišča za vse,
4. drugo.

Frekvenčna porazdelitev odgovorov je prikazana na sliki 4.



Slika 4: **Pozitivni vidiki anonimnosti**

Največ anketirancev meni, da je pozitivni vidik anonimnosti **svoboda govora**, saj *»svoboda govora res postane svoboda«*. Zaradi anonimnosti lahko izrazijo svoje mnenje (ki je lahko drugačno od večine), mnenja so bolj verodostojna, pri izražanju mnenj so bolj odprti, povejo, kar mislijo, *»podobno kot In vino veritas«*. Zavedajo se, da je anonimnost le iluzija, vendar *»ta iluzija omogoča, da se človek izpove, tako kot bi se recimo župniku v cerkvi, gre za psihologijo za množice«*.

Pozitivni vidik anonimnosti vidijo tudi v **zaščiti osebnih podatkov in varnosti**. Ni mogoča zloraba osebnih podatkov, prav tako tudi ne kraja identitete. Anonimno komentiranje je bolj varno, saj nihče ne ve, kdo si, ne morejo te nadlegovati, se ti maščevati, *»nikomur se ne more groziti, nikogar se ne more tožiti, preganjati ali ga ustrahovati zaradi anonimne izjave«*.

Anonimnost omogoča tudi **enaka izhodišča za vse**, saj imajo možnost oglašanja »tudi kakor *koli izpostavljeni ali pa manj samozavestni ljudje«*. Vsi so enaki, ne glede na raso, nacionalnost, izgled, *»šteje mnenje, ne ime in priimek«*. Anonimnost omogoča, da pisec ni izpostavljen in ga prijatelji, znanci, družina in sodelavci ne morejo prepoznati. Slovenija je namreč tako majhna, »da se ljudje instinktivno in stalno *samocenzurirajo,'kaj bi mama rekla, kaj bi sosedje rekli …', treba je slediti uglednemu splošnemu trendu in bog ne daj odstopati, to bi mamo uničilo, tega pa res ni zaslužila …«*.

Kot **drugo** so anketiranci omenjali še, da se z anonimnostjo oblikuje realna slika stanja duha družbe, sliši se glas ljudstva, *»pri reševanju osebnih stisk in težav je anonimnost nujna«*.

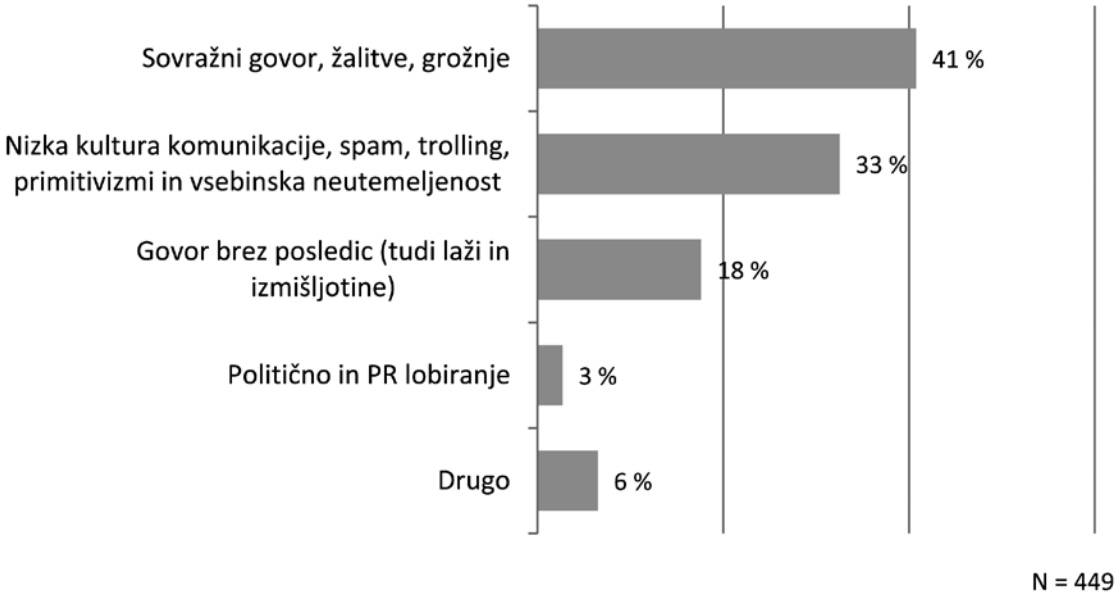
4.2.2 Negativni vidiki anonimnosti

Enako kot o pozitivnih smo udeležence povprašali tudi o negativnih vidikih anonimnosti. Na podlagi odgovorov smo oblikovali pet kategorij:

1. sovražni govor, žalitve, grožnje,
2. nizka kultura komunikacije, spam, trolling, primitivizmi in vsebinska neutemeljenost,
3. govor brez posledic (tudi laži in izmišljotine),
4. politično in PR lobiranje,
5. drugo.

Razporeditev odgovorov po kategorijah je prikazana na sliki 5.

Kot negativni vidik anonimnosti anketiranci opažajo **sovražni govor, žalitve in grožnje** (včasih gre tudi za kazniva dejanja, kot so opredeljena v kazenskem zakoniku (Kazenski zakonik, 2012)). Nekateri si zaradi anonimnosti preveč dovolijo, sovraž-



Slika 5: **Negativni vidiki anonimnosti**

no komunicirajo, grozijo. Anonimnost predstavlja »*ventil za sproščanje frustracij*«, preveč ljudi jo izkoristi za »žaljenje in poniževanje drugih ljudi, člankov, napisanega«.

Anonimnost po mnenju anketirancev povzroča **nizko kulturo komunikacije, spam,[8] trolling,[9] primitivizme in vsebinsko neutemeljenost**. Pod krinko anonimnosti so nastrojeni proti vsemu, vulgarni, presežejo meje dobrega okusa, »*raven debat in objav je mestoma nižja od ravni kanalizacije pod ulicami …*«. Nekateri uporabniki »prestopajo meje in objavljajo nepremišljene in neargumentirane komentarje«, komentarji velikokrat nimajo nobene povezave z vsebino članka, nekateri pa objavljajo tudi reklamne komentarje.

Negativni vidik anonimnosti je tudi **govor brez posledic, laži in izmišljotine**. Nekateri namreč preveč sproščeno izražajo mnenja, so predrzni in si dovolijo več, kot bi si v resnici, »*vsak bedak lahko objavlja neumnosti in s tem otežuje iskanje resnice*«. »Anonimnež lahko namenoma provocira, ker ve, da ne bo trpel posledic«, vendar anketiranci menijo, da »*ker si bil junak ušpičiti, bodi še junak priznati*«.

Nekateri anonimnost izkoriščajo za **politično in PR lobiranje**. Mogoča je zloraba »s strani organiziranih interesnih skupin – plačani aktivizem« ter manipulacija in zloraba medijev v namene promocije.

Kot **drugo** so anketiranci omenjali, da ima zaradi anonimnosti napisano manjšo težo, pri bralcih komentarjev spodbuja negativizem in omogoča »*krepitev brezjajčnosti*«.

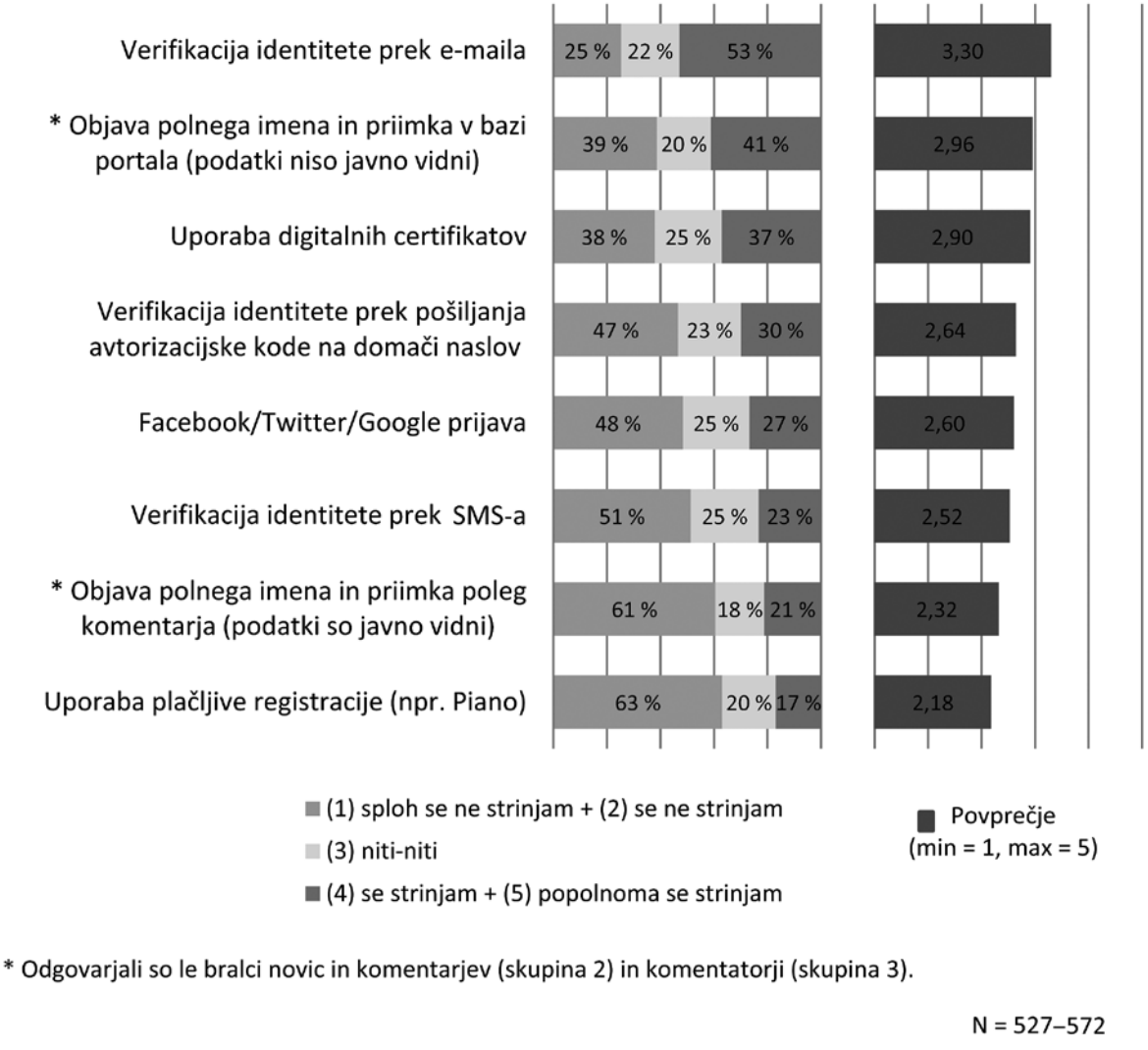
4.3 Zmanjšanje stopnje anonimnosti

Zanimalo nas je, kakšen način zmanjševanja anonimnosti (komu so vidni osebni podatki komentatorja in posledično povezava z njegovim spletnim komentarjem) na spletnih medijskih portalih bi se zdel anketirancem najbolj primeren. Prosili smo jih, da ocene podajo ob predpostavki, da bi ob registraciji morali vnesti resnične osebne podatke. Iz slike 6 je razvidno, da so se najbolj strinjali z verifikacijo identitete po elektronski pošti (M = 3,30), z objavo polnega imena in priimka v bazi portala, pri čemer podatki ne bi bili javno vidni (M = 2,96) in z uporabo digitalnih certifikatov (M = 2,90). Le z verifikacijo identitete po elektronski pošti se je strinjala več kot polovica anketirancev.

V primerjavi s komentatorji bralci izražajo višjo podporo uvedbi digitalnih certifikatov, verifikaciji identitete prek pošiljanja avtorizacijske kode na domači naslov ter uporabi plačljive registracije. Glede drugih načinov med bralci in komentatorji ni statistično značilnih razlik.

Anketirancem smo ponudili tudi možnost dodatnih komentarjev in pripomb na navedene načine deanonimizacije. Omenjali so, da za doseganje ka-

[8] Nezaželene, nenaročene reklame in nadležna pošta.
[9] Namerno zavajanje s ciljem provociranja in draženja uporabnikov.

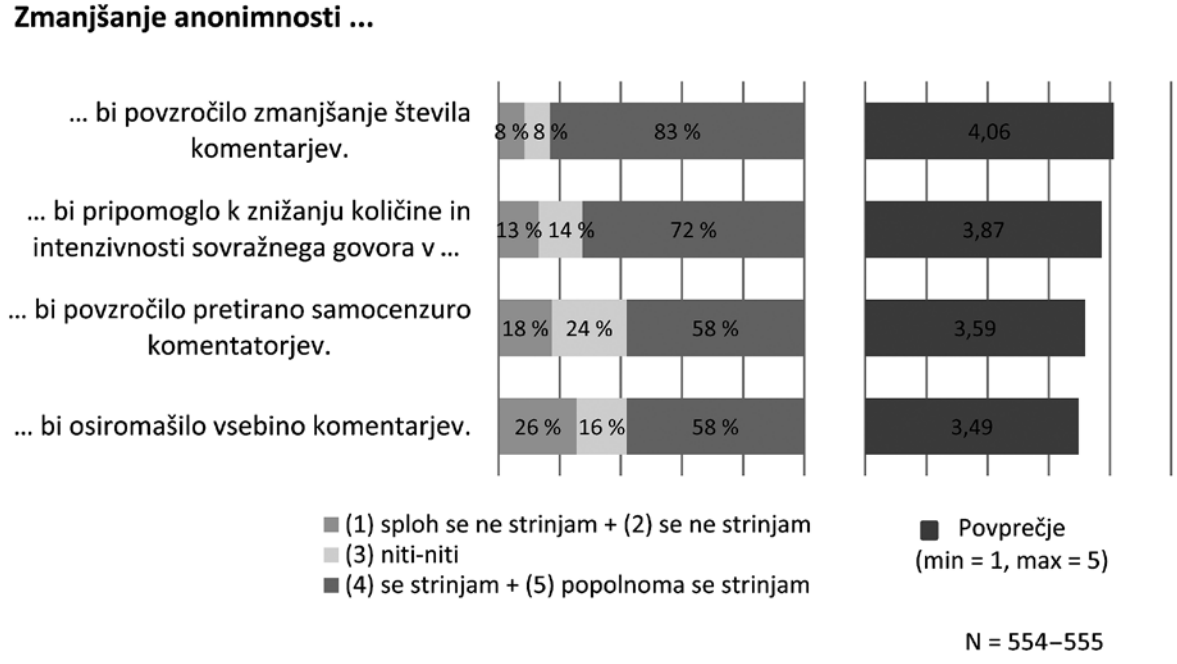


Slika 6: **Strinjanje z načini zmanjševanja anonimnosti na spletnih medijskih portalih**

kovostnejše komunikacije ni potrebno zmanjšanje anonimnosti, saj *»vse, kar zahteva od uporabnika vnos njegovih osebnih podatkov, je nepotrebno in ne pripomore h kakovosti komentiranja«*. Skrbi jih varnost podatkov, ki jih morajo vpisati pri registraciji, *»težava je možna zloraba in prodaja podatkov s strani uredništev«*, menijo pa tudi, da bi ustrezno moderiranje komentarjev izboljšalo komunikacijo, saj je administriranje *»edini način za zagotavljanje forumske higiene«*.

4.4 Posledice zmanjšanja anonimnosti

Strinjanje s trditvami o posledicah zmanjšanja anonimnosti je prikazano na sliki 7. Anketiranci se najbolj strinjajo s trditvijo, da bi zmanjšanje anonimnosti povzročilo zmanjšanje števila komentarjev (M = 4,06). Prav tako pa se strinjajo tudi, da bi zmanjšanje anonimnosti pripomoglo k znižanju količine sovražnega govora (M = 3,87).



Slika7: **Posledice zmanjšanja anonimnosti**

Bralci se, v primerjavi s komentatorji, bolj strinjajo, da bi zmanjšanje anonimnosti pripomoglo k znižanju količine sovražnega govora, komentatorji pa v večji meri menijo, da bi zmanjšanje anonimnosti osiromašilo vsebino komentarjev.

5 SKLEP

Anonimnost na spletnih medijskih portalih se je med uporabniki izkazala kot zelo aktualna tematika, tako z vidika posledic kot tudi njenega zmanjševanja.

Mnenja uporabnikov spletnih medijskih portalov o anonimnosti so deljena. Kot pozitivne vidike anonimnosti najpogosteje navajajo lažje izražanje lastnega iskrenega mnenja, ki je lahko drugačno od mnenja večine, ter zaščito osebnih podatkov pred zlorabami in varnost v fizičnem svetu, v katerem bi se ob ukinitvi anonimnosti počutili ogrožene od nasprotujočih posameznikov in (predvsem političnih) organizacij. Negativno plat anonimnosti udeleženci zaznavajo predvsem kot sovražni govor, žalitve in grožnje, pa tudi nizko kulturo komunikacije na forumih, napolnjeno z nesramnostmi, žalitvami ter vsebinsko neutemeljenimi komentarji.

»Kljub nekaterim neprimernim, žaljivim, sovražnim govorom v komentarjih je neprimerno večja vrednota možnost svobodno in anonimno povedati svoje mnenje.« (Anketiranec)

V povprečju uporabniki niso naklonjeni nobeni od navedenih metod zmanjševanja anonimnosti, najbolj naklonjeni pa so bili med spletnimi medijskimi portali najbolj razširjeni verifikaciji identitete prek elektronske pošte. Močno deljena mnenja so bila glede objave polnega imena in priimka v bazi portala ter uporabe digitalnih certifikatov. Drugih načinov uporabniki večinoma ne podpirajo, velika večina uporabnikov – predvsem tistih, ki komentirajo – pa je bila močno nenaklonjena uporabi plačljive registracije in javne objave imena in priimka uporabnika. Kljub zaznavanju negativnih vidikov anonimnosti na spletnih medijskih portalih udeleženci tako v večji meri ne podpirajo nobenega izmed predlaganih načinov zmanjševanja anonimnosti. Nekateri udeleženci raziskave so mnenja, da bi bilo negativne posledice anonimnosti mogoče odpraviti z doslednim moderiranjem komentarjev.

»Sovražni govor ni težava komentatorjev, ampak moderatorjev. Z doslednim moderiranjem, ki seveda zahteva veliko dela in tudi razumnega človeka, se tudi kakovost komentarjev izboljša. Zmanjševanje anonimnosti na spletu ni rešitev.« (Anketiranec)

Z raziskavo so se potrdile ugotovitve preteklih študij, da kljub precejšnjemu zmanjšanju dejanske anonimnosti v zadnjih letih uporabniki spleta še vedno v veliki meri verjamejo, da so na spletu anonimni

in neprepoznavni (Demetriou in Silke, 2003), prav občutek zakrite oz. drugim nepoznane identitete pa povzroča večjo verjetnost, da se bodo na spletu vedli agresivno in kaznovalno (Peršak, 2009). Izsledki raziskave nakazujejo, da se uporabniki spletnih medijskih portalov vsaj na deklarativni ravni zavedajo, da na spletu niso povsem anonimni. Domnevajo, da administratorji lahko pridobijo vpogled v njihovo identiteto, vendar jim to ne povzroča občutka zmanjšane anonimnosti. Možnost uporabe vzdevkov ob komentiranju namreč poskrbi, da ohranjajo za njih bistveno značilnost spletne anonimnosti – anonimnost do znancev, sorodnikov, sodelavcev; t. i. navidezna anonimnost jim tako še vedno omogoča prostor za iskreno ter nezadržano izražanje lastnega mnenja, brez neželenih posledic v prihodnosti – obsojanja in vrednotenja od drugih, njim poznanih ljudi.

»*Lahko poveš tisto, kar misliš, ne da bi te kasneje nekdo, ki te pozna, spraševal glede napisanega oz. te zasliševal v smislu 'Kako pa lahko tako razmišljaš?' in te po možnosti še prepričeval v svoj prav.*« (Anketiranec)

6 LITERATURA

[1] Berden, A. (1999, 25. maj). *Svoboda izražanja in zaščita posameznikov pred njeno zlorabo.* Dostopno na http://www.media-forum.si/slo/pravo/strokovna-mnenja/svoboda-izrazanja.

[2] Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede.

[3] Čebulj, J. (1992). *Varstvo informacijske zasebnosti v Evropi in v Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti.

[4] Demetriou, C. in Silke, A. (2003). A Criminological Internet »Sting« - Experimental Evidence of Illegal and Deviant Visits to a Website Trap. *British Journal of Criminology, 43*(1), 213–222.

[5] Glavač, M. in Vehovar, V. (2011). *Sovražni govor na slovenskem spletu.* Fakulteta za družbene vede, Ljubljana: interno gradivo.

[6] Gsell, L. (2009, n. d.). *Comments Anonymous.* Dostopno na http://www.ajr.org/article.asp?id=468.

[7] Interights. (2012, n. d.). *Vejdeland v Sweden.* Dostopno na http://www.interights.org/vejdeland/index.html.

[8] Kazenski zakonik (KZ-1-UPB2). Ur. l. RS 50/2012. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=201250&stevilka=2065.

[9] Kodeks novinarjev Slovenije. (2002). Dostopno na http://www.razsodisce.org/razsodisce/kodeks_ns_txt.php.

[10] Lozej, M., Lutman, U. in Vinkovič, M. (2012). *Anonimnost na novičarskih portalih – poročilo raziskave.* Fakulteta za družbene vede, Ljubljana: interno gradivo.

[11] Moj Mikro. (2010, 12. avgust). *Anonimnosti na internetu ni?* Dostopno na http://www.mojmikro.si/news/anonimnosti_na_internetu_ni.

[12] Noelle-Neumann, E. (1974). The Spiral of Sillence. A theory of Public Opinion. *Journal of Communication, 24*(2), 43–51.

[13] O'Neill, B. (2012, 13. junij). *This defamation bill is a disaster for free speech.* Dostopno na http://blogs.telegraph.co.uk/news/brendanoneill2/100164840/this-defamation-bill-is-a-disaster-for-free-speech/.

[14] Peršak, N. (2009). Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. *Revija za kriminalistiko in kriminologijo 60*(3),191–198.

[15] Raba interneta v Sloveniji – RIS. (2010, 15. december). *6 večjih medijev podpisalo Kodeks za regulacijo sovražnega govora na spletnih portalih.* Dostopno na http://www.ris.org/db/27/11885/Raziskave/6_ve%C4%8Djih_medijev_podpisalo_Kodeks_za_regulacijo_sovra%C5%BEnega_govora_na_spletnih_portalih/?&p1=276&p2=285&p3=1318&db=79.

[16] Rosenberry, J. (2011). Users Support Online Anonymity Despite Increasing Negativity. *Newspaper Research Journal 32*(2), 6–19.

[17] Rovšek, J. (2011, n. d.). *Ali je sovražni govor sploh mogoče omejiti?* Dostopno na http://mediawatch.mirovni-institut.si/bilten/seznam/39/sovrazni/.

[18] RTV SLO. (2011, 1. september). Švedski časniki ukinjajo anonimne spletne komentarje. Dostopno na http://www.rtvslo.si/svet/svedski-casniki-ukinjajo-anonimne-spletne-komentarje/265275.

[19] Sky News (2012, 12. junij): *Websites will be forced to identify trolls.* Dostopno na http://news.sky.com/story/947933/websites-will-be-forced-to-identify-trolls.

[20] Spletno oko. (2010). *Kodeks regulacije sovražnega govora na slovenskih spletnih portalih.* Dostopno na http://www.spletno-oko.si/uploadi/editor/1292489478Kodeks.pdf.

[21] Spletno Oko. (2011a, n. d.). *Spletno oko in spletni medijski portali podpisali Kodeks regulacije sovražnega govora.* Dostopno na https://www.spletno-oko.si/r/3/33/ Aktualno/Spletno_oko_in__spletni_medijski_portali_podpisali_Kodeks_regulacije_sovraznega_govora/.

[22] Spletno Oko. (2011b, 3. februar). *Kako zmanjšati sovražni govor na internetu? Utrinki iz okrogle mize.* Dostopno na https://www.spletno-oko.si/r/9/123/Novice/Kako_zmanjsati_sovrazni_govor_na_internetu_Utrinki_iz_okrogle_mize_/?offset=51&p1=603&p2=702.

[23] Spletno Oko. (2011c). *Poročilo o seminarju Kriminaliteta iz sovraštva na internetu.* Ljubljana: interno gradivo.

[24] Spletno Oko. (2011č). *Ugotovitve okrogle mize o etičnem vedenju na internetu.* Ljubljana: interno gradivo.

[25] Spletno Oko. (2012a, 3. januar). *24ur.com se je pridružil Kodeksu regulacije sovražnega govora.* Dostopno na https://www.spletno-oko.si/r/3/53/Aktualno/24urcom_se_je_pridruzil_Kodeksu_regulacije_sovraznega_govora/.

[26] Spletno Oko. (2012b, 17. januar). *Slovenskenovice.si so se pridružile Kodeksu regulacije sovražnega govora.* Dostopno na https://www.spletno-oko.si/r/3/54/Aktualno/Slovenskenovicesi_so_se_pridruzile_Kodeksu_regulacije_sovraznega_govora/?offset=11&p1=603&p2=573&p2=702.

[27] Spletno Oko. (2013, n. d.). *Kdaj je sovražni govor kazniv? Prakse in odzivi pristojnih organov.* Dostopno na https://www.spletno-oko.si/c/788/Kdaj_je_sovrazni_govor_kazniv/?preid=0.

[28] Svenšek, A. (2011, 13. december). »Splet je razkril, koliko sovraštva še vedno obstaja v družbi«. Dostopno na http://www.rtvslo.si/slovenija/splet-je-razkril-koliko-sovrastva-se-vedno-obstaja-v-druzbi/272712.

[29] Šurina, M. (2013, 2. januar). *Od jučer su uvrede na internetu – kaznjeno djelo!* Dostopno na http://www.tportal.hr/vijesti/hrvatska/234882/Od-jucer-su-uvrede-na-internetu-kazneno-djelo.html#.USTDdWe3rBj.

[30] Teršek, A. (2005, n. d.). Svoboda javnega komuniciranja. V P. Pičman Štefančič in A. Teršek (ur.), *Preludij demokracije:*

Civilna družba in svoboda javnega komuniciranja (1–154). Ljubljana: Pravna fakulteta. Dostopno na https://www.ip-rs.si/fileadmin/user_upload/Pdf/clanki/Svoboda_javnega_komuniciranja_-_Tersek_Andraz.pdf.

[31] Teršek, A. (2007). *Svoboda izražanja v sodni praksi Evropskega sodišča* za človekove pravice in slovenski *ustavnosodni praksi.* Ljubljana: Informacijsko dokumentacijski center Sveta Evrope pri NUK.

[32] Teršek, A. (2012). Je homofobija sovražni govor? *Pravna praksa, 28*(14), 25–29.

[33] Urbanija, U. (2012, 16. avgust). *Kako dolgo še grožnje s smrtjo – tokrat tarča tudi naš novinar.* Dostopno na http://www.siol.net/novice/slovenija/2012/08/grozenje_s_ smrtjo_tokrat_tarca_tudi_nas_novinar.aspx.

[34] Ustava Republike Slovenije (URS). Ur. l. RS 33/1991. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=199133&stevilka=1409.

[35] Vehovar, V., Motl, A., Mihelič, L., Berčič, B. in Petrovčič, A. (2012). Zaznava sovražnega govora na slovenskem spletu. *Teorija in praksa, 49*(1), 170–188.

[36] Verbič, J. (2012, 21. avgust). *Grozim, groziš, grozimo ...* Dostopno na http://www.val202.si/2012/08/vroci-mikrofon-do-kdaj-se-bomo-zalili.

[37] Zakon o medijih (Zmed-UPB-1). Ur. l. RS 110/2006. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=2006110&stevilka=4666.

[38] Zakon o varstvu osebnih podatkov, uradno prečiščeno besedilo (ZVOP-1-UPB1). Ur. l. RS 94/2007. Dostopno na http://www.uradni-list.si/1/content?id=82668.

[39] Završnik, A. (2008). Boj za prevlado nad internetom – internetno upravljanje in nadzorovanje. *Revija za kriminalistiko in kriminologijo 59*(4), 321–338.

▪

Martina Lozej je študentka druge bolonjske stopnje programa Družboslovna informatika na Fakulteti za družbene vede Univerze v Ljubljani.

▪

Urša Lutman končuje magistrski študij družboslovne informatike na Fakulteti za družbene vede Univerze v Ljubljani. Njeno sedanje raziskovalno delo se nanaša na področje tržnega raziskovanja in statističnih analiz.

▪

Miha Glavač je zunanji sodelavec pri projektu Spletno oko na Fakulteti za družbene vede. Od leta 2010 je sodeloval pri prijavni točki za nezakonite vsebine na spletu Spletno oko. Je soavtor ali avtor strokovnih in poljudnih člankov na temo sovražnega govora na spletu. V letih 2011 in 2012 je klasificiral prijave sovražnega govora na spletu, pripravil vodič za soočanje s sovražnim govorom za moderatorje in se udeleževal nacionalnih ter mednarodnih konferenc na področju sovražnega govora. Od marca 2013 je član slovenske nacionalne koordinacije za gibanje Sveta Evrope »No HateSpeech«.

▪

Jaro Berce izredni profesor za področje družboslovne informatike na Fakulteti za družbene vede Univerze v Ljubljani, kjer je nosilec več predmetov na dodiplomskem in podiplomskem študiju. Je strokovnjak z mnogimi izkušnjami v različnih sektorjih družbe (zasebnem, državnem in akademskem). Študij je začel na Fakulteti za elektrotehniko Univerze v Ljubljani, magistriral iz računalniških znanosti v ZDA ter doktoriral na Fakulteti za družbene vede Univerze v Ljubljani na področju družboslovne informatike.

Pomembni spletni naslovi

- IFIP News: http://www.ifip.org/images/stories/ifip/public/Newsletter/news ali www.ifip.org – Newsletter
- IT Star Newsletter: www.itstar.eu
- ECDL: www.ecdl.com
- CEPIS: www.cepis.com

Dostop do dveh tujih strokovnih revij

- Revija Upgrade (CEPIS) v angleščini (ISSN 1684-5285) je dostopna na spletnem naslovu http://www.upgrade-cepis.org/issues/2008/4/upgrade-vol-IX-4.html
- Revija Novática (CEPIS) v španščini (ISSN 0211-2124) je dostopna na spletnem naslovu http://www.ati.es/novatica/

Trendi informacijske varnosti v sodobni organizaciji

Kaja Prislan, Igor Bernik
Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova 8, 1000 Ljubljana
kaja.prislan@fvv.uni-mb.si; igor.bernik@fvv.uni-mb.si

Izvleček

Trenutne gospodarske razmere in finančna kriza so z varnostnega, razvojnega in konkurenčnega vidika ustvarile neugodno izhodišče za vsako sodobno organizacijo. Kritična odvisnost operativnih ter taktičnih poslovnih ciljev od tehnologije povečuje organizacijske ranljivosti, tveganja in varnostne potrebe. Raziskave o stanju informacijske varnosti in kibernetskih grožnjah kažejo, da so organizacije neučinkovite pri sledenju varnostnim trendom ter neracionalne pri vzpostavljanju zaščite pred tveganji, ki jih prinaša najnovejša tehnologija. Ugotavljajo tudi, da je učinkovitost omenjene varnostne funkcije vse pogosteje povezana z netehničnimi upravljavskimi funkcijami. Ob predpostavki, da organizacije razpolagajo z osnovnimi tehničnimi rešitvami, so razvit varnostni menedžment, multidisciplinarni pristop, vodstveni odnos in ustrezna organizacijska kultura ključni dejavniki zanesljive in celovite informacijske varnosti.

Ključne besede: informacijska varnost, organizacije, učinkovitost, varnostni trendi, varnostni menedžment.

Abstract

Information Security Trends in a Modern Organisation

The current economic situation and the financial crisis have created an unfavourable starting point for any modern organisation in terms of their security, development and competitiveness. The critical dependence of their operational and tactical business goals on technology increases organisations' vulnerability, risks and security needs. Research studies focusing on information security situations and cyber threats demonstrate organisations' inefficiency in following security trends and their irrational decisions related to the adoption of protection measures against risks generated by the latest technology. These studies also find that the efficiency of security-related functions is ever more frequently linked to non-technical managerial functions. If one presumes that organisations have basic technical solutions at their disposal, it becomes obvious that well-developed security management, multidisciplinary approach, management's attitude and adequate organisational culture represent key factors for a reliable and comprehensive information security.

Key words: information security, organisations, efficiency, security trends, security management.

1 UVOD

Zadnje desetletje je zaznamovano z eksponentno integracijo informacijsko-komunikacijske tehnologije v vsakodnevno življenje razvitih družbenih struktur. Tehnološki napredek in njegove prednosti (npr. hitrejša komunikacija in stalen dostop do podatkov) so povzročili veliko odvisnost organizacij od nemotenega in zanesljivega delovanja informacijskih sistemov. Izpolnjevanje organizacijskih ciljev in doseganje konkurenčnosti v poslovnem okolju je vse pogosteje pogojeno z uporabo učinkovitih varnostnih rešitev na področju informacijske varnosti, saj informacijski sistemi v organizacijskih strukturah postajajo vse bolj kompleksen in integriran del delovnih (poslovnih) aktivnosti. So tudi temelj kibernetskega okolja, ki podpira shranjevanje, prenos in obdelavo zaupnih informacij. To pomeni, da je informacijsko-komunikacijska tehnologija znotraj organizacij razvila posebno okolje, ki je sestavljeno iz njihovega najpomembnejšega premoženja, hkrati pa omogoča zunanje in notranje vstope v virtualno organizacijsko strukturo. Z varnostnega vidika je to povzročilo nova tveganja.

Z zagotavljanjem učinkovite informacijske varnosti, ki prispeva k razvoju sodobne organizacije, so v praksi povezane številne dileme. Teoretično sicer obstajajo idealne okoliščine, v katerih so izvedeni vsi ustrezni postopki: varnostni menedžment je razvit in ozaveščen, tehnični oddelek je usposobljen in na voljo, zaposleni so ozaveščeni in motivirani, tehnologija je posodobljena, izvajajo se ustrezne meritve učinkovitosti, postopki so dokumentirani, predpisani in nadzorovani, kibernetske grožnje so na sprejemljivi ravni, ukrepi pa upoštevajo zahteve in potrebe uporabnikov ter poslovnih procesov. V resnici pa so takšne okoliščine

v realnem poslovnem okolju težko dosegljive, saj se poslovne razmere nenehno spreminjajo, naklonjenost vodstva varnostnemu področju stalno niha, spreminjajo pa se tudi struktura tehničnih oddelkov in njihove pristojnosti oz. odgovornosti. Tudi teoretične predpostavke in aktualne študije dokazujejo, da je trenutno stanje informacijske varnosti v organizacijskem okolju parcialno in le redko urejeno celovito oz. učinkovito.

Neustrezno stanje varnosti informacijskih sistemov ogroža splošno stanje varnosti poslovnega okolja, preživetje posameznih poslovnih entitet, v primeru uresničenih groženj pa se povečuje nestabilnost (nacionalnega) gospodarstva in zmanjšujejo možnosti za njegovo hitrejše okrevanje. Da bi v kontekstu trenutnih gospodarskih razmer in varnostnih trendov informacijsko varnost urejali v skladu s potrebami in z zmožnostmi organizacij ter prispevali k bolj varnemu poslovanju, je treba proučiti in razumeti pogoje, ki določajo, kdaj je (informacijska) varnost učinkovita.

2 UČINKOVITOST VARNOSTNE FUNKCIJE

Učinkovitost organizacijskih aktivnosti je temeljna poslovna potreba in cilj vsake sodobne organizacije (Mouzas, 2006; Computer crime and security survey,[1] 2011). Termin učinkovitost je tesno povezan s pojmoma uspešnost in odličnost, zaradi česar v praksi tovrstne izraze pogosto obravnavajo kot sinonime, z vidika organizacijskega okolja pa se pojavljajo v različnih kontekstih.

Evropska centralna banka navaja, da je ugotavljanje učinkovitosti upravljavskih nalog zelo zahtevna naloga, ki jo je veliko lažje izvesti in oceniti subjektivno kakor objektivno v obliki natančnih podatkov (Afonso, Schuknecht in Tanzi, 2006). Uspešnost z organizacijskega vidika pomeni stopnjo doseganja zastavljenih organizacijskih ciljev. Pri tem velja, da uspešno podjetje stalno napreduje in se razvija zaradi izpolnjevanja ciljev oz. interesov vodstvenega kadra. Učinkovitost v istem kontekstu pomeni povečevanje poslovne koristi oz. rezultata ob hkratnem zmanjševanju skupnega vložka oz. porabljenih virov (Vila, 1994). Organizacija je torej učinkovita, kadar poslovne rezultate ustvarja z najmanjšimi stroški, viri pa so učinkovito izkoriščeni, kadar z njihovo drugačno rabo ni mogoče bolje narediti niti ene dobrine, ne da bi pri tem naredili vsaj eno dobrino slabše[2] (Rebernik, 1994). Za ocenjevanje učinkovitosti morajo organizacije izpolniti tri pogoje: ocena stroškov, ocena koristi, primerjava stroškov in koristi. Iz tega sledi, da je za ocenjevanje učinkovitosti treba določiti izhodiščni položaj, ki ga lahko nadalje primerjamo s končnim stanjem (Afonso, Schuknecht in Tanzi, 2006). Pri analiziranju učinkovitosti je treba upoštevati, da sta pojma uspešnost in učinkovitost medsebojno neločljivo povezana in ju v organizacijskem okolju ni mogoče dosegati ali obravnavati ločeno.

Z uspešnostjo in učinkovitostjo lahko povežemo tudi koncept odličnosti podjetja, ki poleg stroškov in finančnih vidikov upošteva še druge odlike podjetja. Odličnost pomeni, da je podjetje pri poslovanju uspešno in ugledno v tolikšni meri, da postane močno konkurenčno in primer dobre prakse. Pri tem je treba upoštevati predvsem odnose med zaposlenimi, odnose do strank, vodstveno ozračje, vrednote podjetja in podjetniške taktike oz. inovativnost podjetja. Pri tem kot odlična podjetja označujemo tista, ki so sposobna v kompleksnem sistemu in okolju razviti preproste modele upravljanja in sprejemati hitre odločitve (Peters in Waterman, 1982). Če posplošimo, ukrepi so uspešni, kadar pripomorejo k doseganju organizacijskih ciljev, učinkoviti, kadar jih izpolnimo z minimalnimi investicijami, in odlični, kadar jih dosegamo preprosto in hitro, kar pripomore k razvoju, stabilnosti in ugledu organizacije. Težava, ki se pojavlja v organizacijah, je uskladitev zahtev po uspešnosti, učinkovitosti in odličnosti hkrati. V praksi organizacije pogosto stremijo samo k uspešnosti, torej doseganju zastavljenih ciljev, pri čemer velikokrat pozabljajo na dodano vrednost organizacijskega ugleda, zanemarjajo pa tudi merilo učinkovitosti oz. racionalno izpolnjevanje zahtev po uspehu (Mouzas, 2006).

Velike dileme pri ocenjevanju implementiranih ukrepov se pojavljajo predvsem v kontekstu varnosti, saj je varnost specifična organizacijska veja in področje, ki ga ni mogoče obravnavati in ocenjevati enako kot druge poslovne aktivnosti. O tem, kdaj je organizacija varna v celoti ali kdaj je varno njeno določeno področje, je zelo težko govoriti, saj je varnost abstraktno stanje, ki ga ni mogoče izraziti v natančnih in popolnoma objektivnih rezultatih. Trček (2006) navaja, da je varnost stanje minimalnih tveganj in da stanje absolutne varnosti ne obstaja, saj bodo vedno prisotna določena tveganja, ki jih ne moremo obvladati ali predvideti. Varnostna funkcija je v organizaciji podporne narave, saj omogoča nemo-

[1] Raziskava opravljena med 351 varnostnimi strokovnjaki, zadolženimi za informacijsko varnost v organizacijah.

[2] Z drugimi besedami: neki poslovni (lahko tudi varnostni) proces je učinkovit, kadar ne obstaja noben drug proces, ki bi ga lahko uporabili za proizvodnjo iste stopnje rezultata po nižjih stroških.

teno izvajanje vsakodnevnih poslovnih aktivnosti. Vsaka organizacija – še posebno v času gospodarske nestabilnosti – zahteva racionalnost pri razporejanju razpoložljivih virov za podporna področja, ki morajo prispevati k doseganju organizacijskih ciljev. Iz tega razloga mora biti varnost tako uspešna kakor tudi učinkovita.

Uspeh oz. izpolnjevanje postavljenih ciljev se na področju varnosti zato v relativno veliki meri povezuje z menedžersko-upravljavskimi funkcijami, kot so razvoj organizacije, načrtovanje in opredeljevanje organizacijskih ciljev, odzivanje na nepričakovane okoliščine, način in sposobnost vodenja, upravljanje s kadrovskimi viri, njihov razvoj in nadzor ter organizacijske vrednote. Pri tem je zelo pomembno, da organizacija določi in izbere pravo strategijo, kajti ukrepi so lahko uspešni, vendar še vedno neracionalni in neučinkoviti, kadar jih organizacija ne potrebuje in si pri tem zastavlja napačne cilje (Afonso, Schuknecht in Tanzi, 2006). Tudi Stewart (2012) navaja, da je upravljanje organizacije uspešno, kadar ima natančno določeno strategijo razvoja, načrt zagotavljanja varnosti pa je skladen z organizacijskimi cilji. Iz tega je razvidno, da so pogoji oz. merila ocenjevanja uspešnosti in učinkovitosti relativno nedoločeni in povezani z zelo abstraktnimi stanji, kar ustvarja veliko nejasnosti. Če zahteve po uspešnosti in učinkovitosti varnosti prenesemo na področje informacijske varnosti, je pri njunem pojasnjevanju in ocenjevanju treba upoštevati še nekatere specifične značilnosti omenjene funkcije.

2.1 Učinkovitost informacijske varnosti

Univerzalna in klasična definicija informacijske varnosti je zelo jedrnata in preprosta, saj po NIST-u (2013) »informacijska varnost pomeni zaščito informacij in informacijskih sistemov pred neavtoriziranim dostopom, uporabo, razkritjem, onemogočanjem ali uničenjem, z namenom zagotoviti njihovo zaupnost, celovitost in dostopnost«. Tudi organizacija ISO/IEC proces varovanja informacij opredeljuje kot ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij kakor tudi zagotavljanje drugih lastnosti, kot so verodostojnost, odgovornost, neovrgljivost in zanesljivost (ISO/IEC 27000: 2012).

V praksi si lahko organizacije pri doseganju omenjenih odlik informacijskega premoženja pomagajo z različnimi priročniki, navodili in standardi za organizacijsko upravljanje informacijske varnosti. V evropskem (in tudi svetovnem) prostoru so se uveljavila priporočila iz serije standardov ISO/IEC 27000 (Information security management system – ISMS), ki skupaj zajemajo celovit pristop k vzpostavljanju sistema upravljanja (ali vodenja) varovanja z informacijami (SUVI ali SVVI). Procesni model SUVI je natančno definiran in opisan v mednarodnem standardu ISO/IEC 27001: 2013,3 kontrole in praktična navodila za izpolnitev ciljev SUVI pa v standardu ISO/IEC 27002: 2013 (na voljo so npr. še ISO/IEC 27003: 2010 – vodnik za načrtovanje implementacije ISMS; ISO/IEC 27004: 2009 – metodologija za merjenje učinkovitosti SUVI; ISO/IEC 27005: 2011 – vodnik za proces upravljanja z informacijskimi tveganji, ISO/IEC 27006: 2011 – pogoji za izvajalce revizij in postopkov certificiranja, ISO/IEC 27007: 2011 – vodnik za ocenjevanje in revizijo upravljavskih procesov, ISO/IEC 27008: 2011 – vodnik za ocenjevanje ter revizijo varnostnih kontrol, ISO/IEC 27010: 2012 – vodnik za ocenjevanje kontrol medsektorskih in medorganizacijskih informacijskih sistemov, ISO/IEC 27011: 2008 – vodnik za informacijsko varnost telekomunikacijskih organizacij, ISO/IEC 27033: 2011 – priporočila pri načrtovanju in zagotavljanju varnosti omrežij idr.). Omenjeni standardi (v obliki priročnikov, kodeksov ali vodnikov) so namenjeni organizacijam in podjetjem, da z njihovo pomočjo dosežejo primerno informacijsko varnost in varnost poslovanja.

Področja, ki jih zajema in od organizacij zahteva krovni standard informacijske varnosti ISO/IEC 27000: 2013, so zaradi kompleksnosti poslovanja in vpliva mnogoterih dejavnikov na organizacijsko (informacijsko) varnost, številna in raznovrstna. To pomeni, da je tehnične kontrole nujno treba dopolnje-

[3] Oktobra 2013 je izšla prenovljena in posodobljena verzija standarda ISO/IEC 27001: 2013 (pred tem ISO/IEC 27001: 2005), ki je vsebino prilagodila najnovejšim tehnološkim in varnostnim trendom (spremembe in posodobitve se vsebinsko nanašajo na upoštevanje varnostnih vprašanj glede računalništva v oblaku, zunanjega izvajanja storitev, sodelovanja s tretjimi strankami – poudarek na dobaviteljih informacijsko-komunikacijske tehnologije, upoštevanje informacijske varnosti pri projektnem menedžmentu, omejitve pri nalaganju in uporabi programske opreme, varnostna načela pri sistemskem inženiringu, dostopnosti kritičnih poslovnih procesov itd.). Z organizacijskega vidika je sedaj obveznih 148 kontrolnih točk (pred tem 102), pri čemer so bolj poudarjeni postopki upravljanja – menedžment. Kljub temu je posodobljeni standard manj rigiden in bolj fleksibilen – organizacijam daje več manevrskega prostora pri sprejemanju odločitev o načinih izpolnjevanja obveznih kontrol. Nova verzija tako vsebuje 14 vsebinskih sklopov in 114 kontrol (stara 11 sklopov in 133 kontrol). Vsebinski sklopi v prenovljeni verziji standarda so: 1) menedžment informacijske varnosti, 2) organizacija informacijske varnosti, 3) varovanje človeških virov, 4) upravljanje s premoženjem, 5) nadzor dostopa, 6) kriptografija, 7) fizična in okoljska varnost, 8) varnost računalniških operacij, 9) komunikacijska varnost, 10) pridobivanje, razvoj in vzdrževanje informacijskih sistemov, 11) odnosi z dobavitelji, 12) upravljanje z incidenti, 13) neprekinjeno poslovanje, 14) skladnost (BSI Group, 2013).

vati z netehničnimi oz. upravljavskimi procesi, ustrezen menedžment pa je zato nujni pogoj učinkovitosti informacijske varnosti. ISO 27000: 2012 določa, da je organizacija pri zagotavljanju informacijske varnosti učinkovita, kadar so kontrole standarda (cilji) izpolnjene, obenem pa je zagotovljena sorazmernost med načinom doseganja ciljev in uporabljenimi viri.

Pomen upravljanja, nadzora in racionalnosti pri zagotavljanju informacijske varnosti izpostavlja tudi Ponemon Institute (Security effectiveness framework study, 2010), ki v primerjavi z ISO/IEC bolj splošno opredeljuje pogoje, ki morajo biti izpolnjeni za učinkovito informacijsko varnost v organizacijskem okolju. Organizacija mora:

1. biti sposobna preprečiti in hitro odkriti zunanje zlonamerne grožnje ter notranje zlorabe in napake,
2. biti odporna na varnostne incidente v obliki hitrega okrevanja in zagotavljanja neprekinjenega poslovanja,
3. zagotoviti skladnost postopkov in ukrepov z zahtevami zakonodaje in regulatorjev,
4. racionalno razporejati kadrovske in finančne vire,
5. izvajati dosleden nadzor nad upoštevanjem notranjih varnostnih pravil in postopkov.

Da bi lahko organizacije racionalno oz. gospodarno zagotovile čim bolj celovito obravnavo informacijske varnosti, morajo izpolniti enega izmed glavnih pogojev učinkovitosti – poznavanje dejanskega stanja ogroženosti in določanje prioritetnih varnostnih potreb, ki jih je treba nasloviti. Učinkovit pristop zavarovanja zaupnih informacij mora temeljiti na rezultatih analize tveganj in nadaljnjih analizah stroškov ter racionalnosti zaščitnih ukrepov. To najprej vključuje identifikacijo kritičnega informacijskega premoženja, njegove ranljivosti in grožnje. Na podlagi rezultatov takšne analize lahko organizacija v nadaljevanju izbira racionalne in učinkovite varnostne ukrepe glede na realno stanje ogroženosti (Sethuraman in Adaikkappan, 2009; Peláez, 2010). Pri tem bi morale organizacije, ki želijo zagotoviti optimalno varnost in racionalno razporejanje virov, najprej presoditi, katera področja je treba zaščititi ali varnostno posodobiti, in šele nato sprejemati odločitve, koliko virov bodo namenile za njihovo zaščito. V nasprotnem primeru, ko organizacije vnaprej določajo razpoložljive vire in jih šele nato razporejajo, so neracionalne odločitve zelo pogosta posledica. Varnostni ukrepi, ki jih ni mogoče upravičiti in pojasniti – torej argumentirati z zanesljivimi informacijami, so neracionalni in neučinkoviti (Stewart, 2012).

Med pogoje učinkovitosti informacijske varnosti spada tudi zahteva po sprejemanju dobrih kompromisov med varnostnimi in poslovnimi funkcijami oz. po ravnovesju med varnostjo in uporabnostjo informacijsko-komunikacijske tehnologije, ob hkratnem zagotavljanju zadostne stopnje zasebnosti uporabnikov. Koncept »organizacijski kompromis« se pri zagotavljanju informacijske varnosti nanaša na idejo, da je za pridobitev določene odlike sistema treba žrtvovati ali zmanjšati drugo odliko istega oz. drugega sistema/procesa (Wolter in Reinecke, 2010). Informacijskovarnostni ukrepi, ki so sicer uspešni pri preprečevanju groženj, ne morejo biti učinkoviti, kadar onemogočajo izvajanje poslovnih aktivnosti oz. kadar varnostni mehanizmi pretirano omejujejo funkcionalnost informacijsko-komunikacijske tehnologije in njenega namena (Johansson, 2004). Prav tako mora biti uporaba informacijskih sistemov omogočena na način, ki uresničuje pravice zaposlenih in varuje njihovo zasebnost, saj kršitve pravic uporabnikov nasprotujejo ciljem organizacije in splošnim zakonskim zahtevam (Conklin, White, Williams, Davis in Cothren, 2011). Kot pravi Anderson (2006), morajo organizacije določiti poslovne prioritete in nadrejene varnostne zahteve, ki jih je treba izpolniti, hkrati pa oceniti, katere odlike je zaradi tega mogoče zmanjšati in v kolikšni meri. Učinkovitost informacijske varnosti torej ni odvisna samo od uspeha posameznih varnostnih ukrepov (onesposobitev ali onemogočenje groženj), ki jih izbere organizacija, temveč od sprejemanja (dobrih) odločitev in kompromisov. Določeni ukrepi so lahko sicer uspešni in preprečujejo uresničitev neke grožnje, vendar so v določenem organizacijskem okolju nepotrebni. Ker je glede na nizko stopnjo ogroženosti organizacije njihova implementacija lahko moteča, se grožnja upravlja manj invazivno. V drugačnem, varnostnem okolju pa bi bila uporaba enakih ukrepov edini način zaščite oz. upravljanja tveganj (Schneier, 2008).

Iz vsega zapisanega je razvidno, da je informacijska varnost v organizacijskem okolju zelo obsežno področje, ki zahteva multidisciplinaren in timski pristop ter različne kompetence in sposobnosti varnostnih strokovnjakov (Thomson in Solms, 2006; Whitman in Mattord, 2008; Ivanc, 2013). V praksi se organizacije ravno zaradi kompleksnosti in heterogenosti področja pri optimizaciji varnosti informacij

in odpravljanju groženj srečujejo z različnimi dilemami. K temu močno pripomorejo tudi varnostni in poslovni trendi, s katerimi se soočajo vse sodobne organizacije.

3 VPLIV GOSPODARSKE KRIZE NA VARNOST

Organizacije v zadnjem desetletju ni zaznamoval samo tehnološki razvoj. Poslovne entitete se soočajo s splošno neugodnimi razmerami oz. s finančno krizo, ki vpliva na varnostne razmere in organizacijski obstoj v poslovnem okolju. Glede na trenutni gospodarski položaj je pri zagotavljanju učinkovitosti informacijske varnosti poleg varnostnih potreb treba upoštevati tudi zmogljivosti organizacij. Viri, ki jih ima trenutno na voljo povprečna organizacija, so omejeni. Peláez (2010) ugotavlja, da je ravno proračun informacijske varnosti glavna ovira učinkovitega urejanja tega področja.

Na splošno se vpliv finančne krize na varnost kaže v pomanjkanju finančnih virov, zmanjševanju stopnje varnosti, manjši stopnji splošne učinkovitosti organizacij in slabšem upravljanju procesov (TMT Global security study, 2011).[4] Analize vpliva krize na poslovno okolje kažejo, da sta bili s finančno krizo najbolj prizadeti likvidnost in finančna zmogljivost podjetij (OECD, 2009), zaradi česar se zmanjšujejo razpoložljivi finančni viri za zagotavljanje varnosti (Melese, 2009). Tudi slovensko poslovno okolje se je zaradi omenjene finančne krize znašlo v zelo neugodnem položaju. Leta 2011 je 43 odstotkov podjetij, ki je v tem času prenehalo s poslovanjem, to storilo iz finančnih razlogov (Rebernik, Tominc in Crnogaj, 2012). Leta 2012 se je Slovenija uvrstila na 58. mesto (od skupno 67) glede poslovnih in razvojnih priložnosti ter sposobnosti podjetij (Xavier, Kelley, Herrington in Vorderwulbecke, 2013), kar nakazuje na to, da se tudi slovenska podjetja srečujejo z visokimi finančnimi in poslovnimi omejitvami.

Čeprav ima trenutna kriza v ekonomskem, političnem in poslovnem okolju negativen vpliv na varnostne sposobnosti organizacij, pa prav zaradi nje naraščajo varnostne potrebe le-teh. Stranke in poslovni partnerji zahtevajo vse večjo zaupnost pri poslovanju, vse večja pa je tudi potreba po informacijah oz. želja po konkurenčni prednosti (Allen in Westby, 2007; Figliuzzi, 2012), kar povečuje agresivnost v medorganizacijski tekmovalnosti (Economic Intelligence Unit, 2012).[5] Raziskave ugotavljajo (PWC, 2009;[6] Global information security survey, 2012;[7] TMT Global security study, 2011; Global state of information security survey, 2013), da je informacijska varnost zaradi vpliva na finančno stabilnost organizacij postala ena izmed glavnih skrbi in prioritet organizacij, saj tveganja na tem področju stalno naraščajo. Nasprotno pa iste raziskave ugotavljajo, da se varnostne pomanjkljivosti oz. razhajanja med dejanskimi in želenimi varnostnimi razmerami poglabljajo, kar pretežno pripisujejo slabi varnostni zasnovi informacijsko-komunikacijske tehnologije, neustreznim postopkom in pomanjkljivim upravljanjem s človeškimi viri – uporabniki. Rezultati raziskave vpliva gospodarske krize na delovni odnos ljudi, njihovo etiko in splošno stanje informacijske varnosti so pokazali, da so v tem času močno narasle grožnje, povezane z industrijskim vohunjenjem in krajo zaupnih podatkov. Motivacija in priložnosti naraščajo med zaposlenimi in hekerji, ki jim pomanjkanje virov za zagotavljanje varnosti v organizacijah odpira nove možnosti za zlorabe (Fullbrook, 2009; Global state of information security survey, 2012[8]). Raziskave ugotavljajo, da je v težkih ekonomskih časih človek najpogostejši vzrok informacijskovarnostnih incidentov, saj povečan stres in občutek strahu pred izgubo službe povzroči, da se zaposleni pogosteje obnašajo deviantno (TMT Global security study, 2011). Pri tem zaposleni kot uporabniki postajajo glavna tarča storilcev kibernetske kriminalitete, saj ljudje pomenijo najšibkejši člen varnostnega sistema, prek katerega je mogoče zaobiti tehnično zaščito in najhitreje pridobiti dostop do zaupnih in varovanih organizacijskih področij.

Zaradi povečevanja tveganj in omejenih organizacijskih virov podjetja zahtevajo vse večjo učinkovitost varnostnih ukrepov (PWC, 2009; Vaish in Varma, 2010; Hall, Sarkani in Mazzuchi, 2011), investicije, vložene v področje varnosti pa morajo odgovorni prikazati s hitrimi in konkretnimi rezultati (Ashraf, 2005; Pironti, 2007). Ker informacijska varnost v primeru učinkovitosti daje rezultate v obliki neuresničenih groženj, jo je težko dokazati s konkretnimi

[4] Mednarodna raziskava, opravljena v 138 organizacijah.

[5] Mednarodna raziskava, izvedena med 352 pripadniki varnostnega menedžmenta o grožnjah podatkom.

[6] Raziskava, opravljena med 7.200 pripadniki najvišjega menedžmenta v 130 državah.

[7] Raziskava, izvedena med 1.836 pripadniki informacijskovarnostnega menedžmenta v 64 državah.

[8] Raziskava, opravljena med 9.600 pripadniki varnostnega menedžmenta iz 138 držav.

(finančnimi) podatki (Stewart, 2012). Iz tega razloga je varnost pogosto tisto organizacijsko področje, pri katerem najprej uvajamo in sprejemamo varčevalne ukrepe. Na drugi strani pa ravno varčevalni ukrepi v smislu zmanjševanja finančnih in kadrovskih virov slabšajo splošno stanje varnosti, saj se s tem povečujejo možnosti za uresničitev kibernetskih groženj (Burton in Stewart, 2009; Knopik in Zhan, 2010). To dokazujejo tudi aktualne raziskave, ki kljub visokemu pomenu informacijske varnosti potrjujejo visoko stopnjo prisotnosti kibernetskih groženj v organizacijskem okolju in neučinkovitost organizacij pri njihovem upravljanju.

4 TRENUTNO STANJE INFORMACIJSKE VARNOSTI

Finančna kriza in gospodarska nestabilnost sta z vidika informacijske varnosti za večino organizacij ustvarili paradoksalen položaj. Podjetja zaradi naraščajočih in vse bolj sofisticiranih kibernetskih groženj potrebujejo visoko stopnjo informacijske varnosti ob hkratnem zmanjševanju razpoložljivih virov, namenjenih za njeno zagotavljanje. Zahtevamo torej uspeh informacijsko varnostnih ukrepov z minimalnimi investicijami. Nasprotno pa je zaradi omenjenih izzivov to področje v poslovnem okolju pogosto neurejeno in tudi v stroki ni konsenza o tem, kaj sploh pomeni učinkovitost (informacijske) varnosti in kako jo optimalno ter racionalno urediti. Tako Vršec (2013) navaja, da je v gospodarskih družbah in organizacijah nasploh premalo znanja, volje, zavedanja, vnašanja primerov dobrih praks in finančnih virov, zaradi česar v praksi ne uporabljamo učinkovitih varnostnih mehanizmov. Enako ugotavljajo tudi raziskave o trenutnem globalnem stanju informacijske varnosti.

Raziskave kažejo močne razlike med stopnjo učinkovitosti informacijske varnosti v različnih poslovnih okoljih. Pri tem ocenjujejo, da je učinkovitost informacijske varnosti najbolj ogrožena in najslabša v manjših podjetjih in v organizacijah, ki ne razvijajo varnostnega menedžmenta, medtem ko na bi bilo v splošnem približno 35 odstotkov organizacij neučinkovitih pri zagotavljanju informacijske varnosti (Security effectiveness framework study, 2010).[9] V praksi 52 odstotkov organizacij neučinkovito razporeja tudi obstoječe vire (TMT Global security study, 2011), le osem odstotkov podjetij oz. varnostnega menedžmenta pa se vede varnostno odlično (Global state of information security survey, 2013). Splošno neučinkovitost organizacij pri vzpostavljanju informacijske varnosti najpogosteje povezujejo z neučinkovitim menedžmentom oz. neustrezno miselnostjo o odgovornosti za zagotavljanje varnosti, ki ostaja zelo tradicionalna, tehnično usmerjena (Pironti, 2007; Peláez, 2010). V organizacijah, ki nimajo ustreznega strokovnega znanja, velikokrat prevladuje mnenje, da je informacijska varnost pretežno odgovornost IT-oddelka v organizaciji (Ashraf, 2005). To dokazujejo tudi raziskave, ki ugotavljajo zanemarjanje področje varnostnega menedžmenta. Analiza 9.300 podjetij v 128 državah je pokazala, da ima le 42 odstotkov organizacij proaktivno informacijskovarnostno strategijo, medtem ko imajo preostale pomanjkljive varnostne načrte (ali pa jih sploh nimajo) in se na grožnje odzivajo pretežno reaktivno (Global state of information security survey, 2013). Še bolj zaskrbljujoč je sklep raziskave, ki ugotavlja, da bi 97 odstotkov od 855 zaznanih incidentov v letu 2011 lahko preprečili s preprostimi oz. z osnovnimi varnostnimi rešitvami (Data breach investigation report, 2012), ki pa jih organizacije ne razvijajo.

Opisani problemi in predstavljene varnostne dileme dokazujejo, da je učinkovitost informacijske varnosti najpogosteje ogrožena zato, ker organizacije v poizkusih sledenja hitremu razvoju informacijsko-komunikacijske tehnologije in tehničnim ukrepom pozabljajo na osnovne varnostne predpostavke in prispevek človeškega faktorja k varnostnemu stanju v organizaciji (Ashraf, 2005). Tehnični ukrepi ne morejo biti učinkoviti, kadar jih uporabniki ne upoštevajo in ne razumejo varnostnih pravil (Herath in Rao, 2009), zaradi česar sta potrebna varnostno ozaveščanje in vpletenost uporabnikov v varnostne procese organizacije. Spears in Barkhi (2010) sta ugotovila, da aktivna udeležba zaposlenih pri vzpostavljanju varnostnih ukrepov skupaj s programi ozaveščanja pomembno vpliva na dvig dejanske stopnje informacijske varnosti v organizaciji. Tudi NIST (Wilson in Hash, 2003) v svojih priporočilih navaja, da stanje ozaveščenosti zaposlenih vpliva na manjšo stopnjo informacijskih incidentov. Medtem so Talib, Clarke in Furnell (2010) s pomočjo raziskave prišli do ugotovitve, da ljudje večino znanja, povezanega z varno uporabo informacijsko-komunikacijske tehnologije pridobimo ravno v delovnem okolju.

[9] Mednarodna raziskava, opravljena na vzorcu 101 organizacije.

Programi izobraževanja in usposabljanja so torej še toliko bolj pomembni, saj v delovnem okolju pridobljeno znanje prenašamo na druga okolja zunaj organizacije. Bernik in Meško (2011) sta ob analizi zavedanja in dojemanja kibernetskih groženj med uporabniki interneta v Sloveniji ugotovila, da na splošno obstaja pomanjkanje ozaveščenosti o kibernetskih grožnjah in zakonodaji na tem področju.

Pri proučevanju trenutnega stanja informacijske varnosti v organizacijskem okolju je problematična tudi ugotovitev, da informacijsko varnost v organizacijah pogosto najbolj ogrožajo tisti, ki so odgovorni za njeno učinkovitost in so zgled vsem zaposlenim. To potrjujejo intervjuji s tristotimi strokovnjaki, odgovornimi za menedžment (informacijske) varnosti v različnih organizacijah, pri čemer je bilo ugotovljeno, da jih 42 odstotkov meni, da zanje ne veljajo varnostna pravila in postopki. Pri opravljanju svojih aktivnosti ne upoštevajo procesnih ukrepov zagotavljanja varnosti oz. jih ignorirajo, hkrati pa imajo dostop do zaupnih informacij (Perception of security awareness study, 2012). V primeru neupoštevanja pravil in neodgovornega vedenja vodstva takšnemu zgledu navadno sledijo tudi drugi zaposleni, zaradi česar varnostni ukrepi ne morejo doseči svojega namena. Ob predpostavki, da za zagotavljanje informacijske varnosti organizacije razpolagajo s povprečnimi tehničnimi rešitvami in da lahko na dejavnike iz zunanjega okolja vplivamo le v manjši meri, sta posameznik in njegovo vedenje med ključnimi dejavniki učinkovitosti informacijske varnosti v organizacijah.

Iz ugotovitev prikazanih raziskav lahko predpostavljamo, da organizacije na splošno niso učinkovite pri zagotavljanju celovite organizacijske varnosti, prav tako pa pogosto sprejemajo neracionalne odločitve in slabe organizacijske kompromise. V trenutnih gospodarskih razmerah, ko je propadanje organizacij vsesplošen trend, sta njihov obstoj in preživetje odvisna od preudarnih in učinkovitih odločitev. Te so na področju informacijske varnosti najbolj ogrožene zaradi paradoksalnega stanja na področju upravičevanja investicij in upravljanja varnostnih tveganj.

Odločitve o investicijah v varnostno področje so v domeni vodstvenega kadra, ki (tudi) informacijsko varnost zelo pogosto povezuje s finančno koristjo varnostnih ukrepov in z idejo, da je varnost strošek. Zaradi dejstva, da je težko oceniti korist in učinkovitost implementiranih varnostnih ukrepov oz. ugotoviti, koliko je organizacija pridobila s tem, da se nepoznane grožnje niso uresničile, redko izvajajo ustrezne postopke ugotavljanja dejanskega stanja (Centre for Internet Security [CIS], 2010). Ocenjevanje informacijske varnosti je temeljni pogoj, ki ga mora izpolniti vsaka organizacija, ki želi zagotoviti učinkovito informacijsko varnost. Gre za proces, s katerim ugotavljamo, v kolikšni meri so izpolnjeni cilji informacijskovarnostne politike (ki je tudi prvi pogoj za izvajanje merskih postopkov) in koliko ti cilji pripomorejo k celovitem stanju varnosti v organizaciji (SANS Institute, 2007). Slagell (2010) ugotavlja, da je analiziranje tveganj zelo redka organizacijska praksa, na podlagi katere bi organizacije sprejemale odločitve. Če pa že izvajajo tovrstne analize, so pri tem prepuščene same sebi in lastnemu (pogosto omejenemu) znanju, analize pa so medsebojno neenotne nedosledne in neprimerljive. Glede na dejstvo, da organizacije pogosto trpijo pomanjkanje strokovnega znanja, volje in finančnih virov, medtem ko so storitve varnostnih svetovalcev pogosto finančno prezahtevne, je omejeno poznavanje stanja logična posledica. To potrjujejo tudi študije, ki poročajo o stagnaciji poizkusov ocenjevanja informacijske varnosti v praksi (Mimoso, 2009). Raziskave ugotavljajo, da podjetja sicer aktivno razvijajo informacijsko varnost, vendar varnostne zmogljivosti podjetij nazadujejo od leta 2008, saj 65 odstotkov organizacij ne analizira stanja informacijske varnosti oz. je to ocenjevanje neučinkovito in neustrezno razvito (Global state of information security survey, 2012; Info Security, 2011). Pomanjkanje točnih in aktualnih informacij o trenutnem stanju varnosti in ogroženosti ali napačne informacije, ki so posledica neustreznih postopkov ugotavljanja dejanskega stanja, vodijo v nepravilne odločitve, ki temeljijo na predvidevanjih (Pironti, 2007). Zaradi pomanjkanja informacij o dejanskem stanju varnosti se podjetja na viktimizacijo v praksi najpogosteje odzivajo z odpravo posledic prvotne viktimizacije; s povečanjem fizične varnosti, zmanjšanjem privlačnosti tarče in nadzorom dostopa (Lamm Weisel, 2005; Global state of information security survey, 2013). Najpogosteje torej uporabljajo situacijsko prevencijo, najmanj pa v praksi uporabljajo socialno strategijo, s katero bi ugotavljali dejanske vzroke viktimizacije in poskušali uvajati dolgoročne spremembe, saj to zahteva veliko časa in truda.

4.1 Stanje kibernetske kriminalitete v organizacijskem okolju

Na splošno se organizacije nenehno srečujejo z različnimi notranjimi in zunanjimi tveganji, ki zajemajo grožnje poslovnemu uspehu, finančni stabilnosti in varnosti nasploh. Določene grožnje so v poslovnem okolju prisotne že dolgo časa, zaradi česar so se nekaterim bolj ali manj uspešno prilagodile in standardizirale postopke njihovega upravljanja. V primeru hitrega in nepričakovanega razvoja informacijsko-komunikacijske tehnologije in kibernetskih groženj pa veliko organizacij ni imelo časa ali znanja, da bi se ustrezno zaščitile in dosledno sledile trendom razvoja. Zaradi tega so se na različnih točkah organizacijske strukture pojavile številne varnostne vrzeli oz. ranljivosti (na ravni strojne in programske opreme, uporabnikov, podatkov in omrežja), prek katerih lahko dostopamo do najpomembnejšega organizacijskega premoženja. Kibernetske grožnje so postale sodobni vidik ogrožanja varnosti organizacij, saj ob njihovem uresničenju vsi drugi (klasični) varnostni ukrepi nimajo učinka. Pri tem je še posebno problematična kibernetska kriminaliteta, ki lahko z visoko stopnjo znanja in motivacije storilcev zaobide vse tehnične varnostne ukrepe in pridobi neposreden dostop do najpomembnejšega organizacijskega premoženja.

Učinkovitost informacijske varnosti mora biti prioriteta vsake organizacije, ki želi biti uspešna, saj kibernetske grožnje vztrajno naraščajo, gospodarske in druge družbe pa zaradi tega doživljajo vse več napadov na lastne informacijske sisteme (Global information security survey, 2012; Economic Intelligence Unit, 2012; Northcutt, 2012; Wilshusen, 2012; Vršec, 2013; Global state of information security survey, 2013). To dokazujejo tudi različne študije kibernetske kriminalitete. Podjetje Norton navaja, da naj bi bilo zaradi kibernetske kriminalitete na minuto oškodovanih več kot 140 žrtev (Cybercrime report, 2012), med katere uvrščamo tudi organizacije. Ob upoštevanju takšnega podatka lahko sklepamo, da je kibernetska kriminaliteta najbolj pogosta in razširjena grožnja, ki se lahko uresniči v vsakem organizacijskem okolju. Podjetje Symantec je leta 2011 analiziralo informacijskovarnostne incidente v dvesto državah in pri tem zabeležilo skupno 5,5 milijona zlonamernih napadov na informacijske sisteme. Dnevno so tako obravnavali 4.595 primerov, pri čemer je bilo vsak dan zaznanih povprečno 82 primerov napadov na organizacije. Takšni napadi so se zelo pogosto kazali v obliki t. i. »ciljanih napadov« z namenom vohunjenja za zaupnimi podatki (angl. ATP – advanced persistent threat), pri čemer gre za kombinacijo različnih groženj (npr. kombinacija socialnega inženiringa in zlonamerne programske opreme, vstavljene v informacijski sistem organizacije) (Internet security threat report, 2012). Isto podjetje je leta 2012 zaznalo 45-odstotno povečanje varnostnih incidentov, dnevno pa je obravnavalo 165 ciljanih napadov na podjetja (Internet security threat report, 2013). Po poročanju SI-CERT-a so se s takšnimi grožnjami leta 2012 soočala tudi slovenska podjetja, kar pomeni, da je trendu naraščajočih kibernetskih groženj izpostavljeno tudi slovensko poslovno okolje. Zaskrbljujoč je tudi podatek, da je omenjena organizacija v istem letu obravnavala več varnostnih incidentov kot v letih 2010 in 2011 skupaj (Poročilo o omrežni varnosti za leto 2012, 2013). Čeprav ugotovitve takšnih raziskav in viktimizacijskih študij niso popolnoma enotne, lahko iz podatkov upravičeno sklepamo, da so kibernetske grožnje stalno aktivne in pomenijo resno tveganje, ki ga podjetja ne smejo zanemarjati. To dokazuje tudi mednarodna študija, ki ocenjuje, da na tedenski ravni podjetja utrpijo približno dva uspešna kibernetska napada, na letni ravni pa se škoda zaradi teh v večjih korporacijah giba med enim in štirinajstimi milijoni dolarjev (v kar vključujemo tudi kvantitativno oceno posrednih posledic) (Cost of cyber crime study, 2012),[10] so pa posledice odvisne predvsem od vrste uresničene grožnje in velikosti podjetja (Security effectiveness framework study, 2010). Omenjene raziskave navajajo, da finančna škoda, povzročena z uresničenimi kibernetskimi grožnjami, iz leta v leto vztrajno narašča. Pri tem naj bi največje posledice zaradi tovrstne kriminalitete utrpela majhna in srednje velika podjetja, ki imajo v povprečju več kot štirikrat večje izdatke okrevanja kot večje organizacije. Manjša podjetja naj bi bila pogosteje podvržena kriminaliteti, povezani z zlonamerno programsko opremo, krajo informacijsko-komunikacijske tehnologije in zaupnih informacij, večja podjetja pa se najpogosteje srečujejo z bolj organiziranimi oblikami kibernetske kriminalitete, to so grožnje, povezane z notranjimi zlorabami, vdori prek spleta in DOS-napadi (Cost of cyber crime study, 2012; State of the

[10] Mednarodna raziskava o stroških informacijskovarnostnih incidentov, opravljena v 56 organizacijah.

endpoint,[11] 2013). Druga raziskava (Internet security threat report, 2012) ugotavlja, da je 50 odstotkov vseh napadov na podjetja usmerjenih v velike, druga polovica pa v manjše organizacije (pri tem so podjetja v velikosti od 1 do 250 zaposlenih tarča 18 odstotkov vseh zaznanih groženj zoper poslovno okolje).

Na splošno raziskave in viktimizacijske študije navajajo visoko stopnjo pogostosti kibernetske kriminalitete, vendar so takšne analize neenotne, nedosledne in komercialne narave, zato je njihove ugotovitve težko posploševati (Anderson idr., 2012; Sjouwerman, 2011). Kljub temu lahko iz ugotovitev prikazanih raziskav izoblikujemo splošen sklep, da so organizacije relativno neuspešne pri zoperstavljanju kibernetskim grožnjam. Podjetja imajo na trgu sicer na voljo veliko različnih varnostnih rešitev in storitev, s katerimi lahko upravljajo omenjene grožnje, vendar stalen razvoj in napredek na področju informacijsko-komunikacijske tehnologije za veliko organizacij ustvarja nepregleden položaj, v katerem je težko izbrati primerne in racionalne varnostne ukrepe.

4.2 Trendi na področju varnostnih storitev in tehnoloških novosti

Nepravilne odločitve, povezane z informacijsko varnostjo, so v praksi povezane s težnjo organizacij slediti tehnološkim in varnostnim trendom, ki pa niso nujno tudi najbolj učinkovita rešitev. Vprašanje o učinkovitosti se zelo pogosto pojavlja skupaj z vse pogostejšim prenosom odgovornosti za informacijsko varnost k tretjim specializiranim subjektom (zunanje izvajanje ali t. i. outsourcing varnostnih funkcij), prenašanjem podatkov v oblak in eksponentno integracijo mobilne tehnologije in z njimi povezanih aplikacij v delovne procese, česar se organizacije poslužujejo zaradi potrebe po optimizaciji stroškov (Markelj in Bernik, 2011; Järveläinen, 2012).

Zunanje izvajanje se v časih naraščajočih groženj in zahtev po učinkovitosti varnosti kaže kot najpogostejša praksa, ki se jo poslužuje varnostni menedžment v organizacijah, zadolžen za zagotavljanje informacijske varnosti. S tem se sicer določena tveganja prenesejo na zunanje organizacije in se posledično povečujejo druga tveganja in grožnje. Prenos varnostnih funkcij iz organizacijskega v zunanje okolje zelo pogosto vodi tudi v zmanjševanje delovne sile za zagotavljane informacijske varnosti znotraj organizacij, kar še posebno ogroža varnost zaupnega informacijskega kapitala, saj manj zaposlenih pomeni manj znanja in manj nadzora. Posledice tega se kažejo v povečani ranljivosti podjetij in večjih možnostih za napake (Fullbrook, 2009). Iz tega sledi, da se organizacije pri sprejemanju odločitev o vzpostavljanju varnostnega sistema ne smejo držati samo načela zniževanja stroškov in izogibanja odgovornosti, temveč morajo upoštevati prednosti investicij v lastne varnostne zmogljivosti, ki so neotipljive in nefinančne narave (Hriberšek in Ribič, 2013).

Poleg zunanjega izvajanja se organizacije vse pogosteje poslužujejo storitev računalništva v oblaku, pri čemer gre za prenos podatkov v oblak, s tem pa se zmanjšajo stroški informacijsko-komunikacijske tehnologije in vzdrževanja. Poleg pozitivnih strani takšnega ukrepa se vzporedno pojavlja vprašanje informacijske varnosti, saj ni natančno določeno, kdo lahko dostopa do informacij in kje natanko so locirani podatki oz. del oblaka s podatki (Markelj in Bernik, 2011). Takšne storitve zmanjšujejo nadzor nad dostopanjem in upravljanjem informacijskega kapitala. Informacije, shranjene v oblaku, so lahko brez vednosti lastnika dostopne različnim subjektom, zaradi česar je težko zagotoviti njihovo zaupnost in celovitost. Podatki so lahka tarča zlorabe avtoriziranih in neavtoriziranih dostopov, zainteresiranih tujih obveščevalnih in državnih služb, hekerjev oz. posameznih tehnično podkovanih zlonamernih storilcev (Thomson, 2011). Ker je poslovanje neke organizacije odvisno tudi od dobaviteljev, poslovnih partnerjev pogodbenih izvajalcev in navsezadnje tudi od konkurence, so sestavni del poslovnega informacijskega sistema tudi podatki teh zunanjih dejavnikov (Vršec, 2013). Zaradi tega je informacijska varnost v zunanjih, povezanih oz. partnerskih okoljih prav tako izjemno pomembna.

Poleg omenjenih trendov, ki povzročajo dileme na področju učinkovitosti informacijske varnosti, se kot problematično izpostavlja še eno področje. Kot napovedujejo raziskave, bodo v prihodnosti najnevarnejše kibernetske grožnje usmerjene tudi v ranljivost mobilne tehnologije (TMT Global security study, 2011; Internet security threat report, 2012), s katero organizacije skušajo poenostaviti delovne aktivnosti in postajajo vse bolj odvisne od nje. Znano je, da je mobilna informacijsko-komunikacijska tehnologija postala organizacijski trend, v trenutnem kontekstu pa je najmanj zaščitena in najbolj ranljiva.

[11] Raziskava, opravljena med 671 varnostnimi menedžerji velikih organizacij.

Njeni zaščiti zaradi razširjenosti in preproste uporabe, ki zmanjšujeta občutek tveganja, namenjajo izjemno malo pozornosti, tako z vidika politične ureditve kot tehnične zaščite (Global information security survey, 2012). Vse pogosteje je mogoče zaznati tudi t. i. trend BYOD,[12] ki še poglablja takšno stanje neustrezne zaščite. Gre za vnos osebne mobilne naprave, ki jo posameznik uporablja v zasebnem življenju, v organizacijo in delovno okolje za izpolnjevanje službenih obveznosti. To ustvarja položaj, v katerem se združujejo zasebne in poslovne aktivnosti uporabnika, kar povečuje možnosti za zlorabe in ranljivosti v organizacijski strukturi. Trendi razvoja kibernetske kriminalitete v prihodnosti kažejo, da se bodo grožnje razvile v smeri fokusiranih napadov na mobilne naprave zaposlenih, ki imajo dostop do korporativnega omrežja (Sjouwerman, 2012).

Iz opisanega je razvidno, da lahko poizkusi prilagajanja sodobnim varnostnim trendom in tehničnim novostim vodijo v povečane ranljivosti. To se navadno zgodi, kadar organizacije tega ne počno premišljeno in analitično ter novosti uvajajo na podlagi priporočil prodajalcev, ki imajo lahko dvomljive namene. Pri zagotavljanju učinkovitosti informacijske varnosti je zato v primeru načrtovanja in vzpostavljanja varnostnih načrtov treba upoštevati prednosti in slabosti sodobnih informacijskovarnostnih trendov in razumeti tveganja, ki jih povzroča implementacija takšnih ukrepov.

5 SKLEP

Analiza varnostnih trendov in pregled aktualnih raziskav o stanju kibernetske kriminalitete in splošne učinkovitosti informacijske varnosti potrjujejo predpostavko, da je informacijska varnost ena izmed najpomembnejših poslovnih funkcij, ki pa je hkrati najmanj razumljena in urejena. Razlogi neučinkovitega varnostnega stanja se nahajajo v različnih organizacijskih, osebnostnih in okoljskih dejavnikih. Na splošno ugotavljamo, da je učinkovita informacijska varnost pogojena s temi merili:

1. vodstvena podpora informacijski varnosti, ki podpira odprto komunikacijo in ima posluh za varnostne probleme;
2. (informacijsko)varnostna strategija, podprta z varnostno politiko, nad upoštevanjem katere se izvaja ustrezen nadzor;
3. zadostni finančni in kadrovski viri, ki omogočajo implementacijo osnovnih tehničnih rešitev;
4. odgovoren in usposobljen varnostni menedžment z ustrezno stopnjo avtoritete, ki razvija varnostno kulturo in daje pozitiven zgled zaposlenim;
5. ocenjevanje ogroženosti pred kibernetskimi grožnjami, prioritiziranje tveganj in ocenjevanje učinkovitosti izbranih varnostnih ukrepov;
6. skladnost varnostnih ukrepov z organizacijsko strategijo in minimalen vpliv na funkcionalnosti sistemov ter pravice in zasebnost uporabnikov;
7. analiziranje varnostnih trendov in preudarnost pri uvajanju tehnoloških novosti;
8. ozaveščanje zaposlenih o pravilih in postopkih ter motiviranje za pozitivno varnostno vedenje.

V prispevku predstavljene dileme, povezane z vzpostavljanjem informacijske varnosti, dokazujejo, da je izpolnjevanje zahteve po učinkovitosti izjemno zahtevna in problematična naloga varnostnega menedžmenta. Trenutno stanje v zunanjem poslovnem okolju, ki je zaznamovano s finančno nestabilnostjo, vse pogostejšimi varnostnimi tveganji in visoko potrebo po inovativnosti in konkurenčnosti, zahteva od organizacij drugačen pristop pri upravljanju varnosti, kot so ga te poznale v preteklosti. Vodstveni kader se mora pri tem zavedati, da je podpora varnostni funkcija nujna, saj uporaba informacijsko-komunikacijske tehnologije v prihodnosti ne bo upadla (trendi kažejo ravno nasprotno), prav tako pa lahko upravičeno pričakujemo nadaljnji razvoj groženj in tveganj. Prav tako se je treba zavedati, da zaradi heterogenosti in vpliva različnih dejavnikov ni mogoče informacijske varnosti urediti učinkovito na preprost in nenačrtovan način. Pri tem ni zadosti, da organizacije postopke le formalizirajo, temveč je pomembno, da procesi in pravila živijo tudi v praksi. Identificirati moramo tista področja, ki ne funkcionirajo tako, kot si želi menedžment ali vodstvo, in šele potem ustrezno ukrepati. Predvsem pa mora vsaka organizacija poiskati in tako poznati odgovor na dve temeljni vprašanji:

1. kakšno je trenutno varnostno stanje in
2. kakšen je načrt za prihodnost.

Kadar informacijsko varnost načrtujemo strateško in dolgoročno (kar je tudi pogoj njene učinkovitosti) mora odgovorni varnostni menedžment jasno in natančno določiti operativne, taktične in strateške varnostne cilje. Ti morajo biti argumentirani in temeljiti na točnih informacijah o aktualnih varnostnih ukre-

[12] »Bring your own device«.

pih ter njihovih vplivih na upravljanje ogroženosti. Tako lahko identificiramo stopnjo njihove kompatibilnosti s poslovnimi zahtevami in učinkovitosti ter identificiramo vrzeli, ki jih je treba urediti v prihodnosti. Organizacija mora vedeti, kaj si želi in iz kakšnega stanja bo izhajala pri doseganju ciljev. Želene varnostne razmere v prihodnosti pa morajo biti zastavljene racionalno in predvsem izvedljivo, saj lahko pretirana idealizem in optimizem – tako kot ravnodušnost in ignoranca – povečata varnostna tveganja. Poznavanje trenutnega varnostnega stanja, varnostnih potreb in zmogljivosti so torej nujni pogoji učinkovitosti informacijske varnosti. Podprti morajo biti z odprtimi komunikacijskimi kanali, ki preprečujejo pretirane enostranske in avtoritativne odločitve, saj je informacijska varnost multidisciplinarno področje, ki ni samo tehnične, temveč je tudi družboslovne in psihološke narave. Brez razumevanja omenjenih področij so neracionalne odločitve z običajno prekomernimi in nepotrebnimi ukrepi neizogibna posledica.

LITERATURA

[1] Afonso, A., Schuknecht, L. in Tanzi, V. (2006). *Public sector efficiency: Evidence for new EU member states and emerging markets.* Frankfurt: European central bank.

[2] Allen, J. H. in Westby, J. R. (2007). *Governing for enterprise security: Implementation guide US-CERT: Article 1 – Characteristics of effective security governance.* Pittsburg, PA: Carneige Mellon University.

[3] Anderson, A. (2006). Effective management of information security and privacy. *Educause Quartely, 6*(1), 15–20.

[4] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., Moore, T. in Savage, S. (2012). *Measuring the cost of cybercrime.* Pridobljeno na http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

[5] Ashraf, S. (2005). *Organization need and everyone's responsibility: Information security awareness – Global Information Assurance Certification Paper.* Bethesda, MD: SANS Institute. Pridobljeno na http://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113.

[6] Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

[7] BSI Group. (2013). *Moving from ISO/EC 27001:2005 to ISOI/IEC 27001:2013.* Pridobljeno na http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf.

[8] Burton, S. in Stewart, S. (2009). *Security Implications of the global financial crisis.* Austin, TX: Stratfor Global intelligence. Pridobljeno na http://www.stratfor.com/weekly/20090304_security_implications_global_financial_crisis.

[9] Centre for internet security [CIS]. (2010). *The CIS consensus security metrcis*. Pridobljeno na http://benchmarks.cisecurity.org/en-us/?route=downloads.metrics.

[10] *Computer crime and security survey*. (2011). New York, NY: Computer Security Institute. Pridobljeno na http://gocsi.com/survey.

[11] Conklin, W. A., White, G., Williams, D., Davis, R. in Cothren, C. (2011). *CompTIA security*: *Certification guide*. Columbus, GA: McGraw-Hill.

[12] *Cost of cyber crime study: United States*. (2012). Traverse city, MI: Ponemon Instittute. Pridobljeno na http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[13] *Cybercrime report:* 2011. (2012). Mountain View, CA: Symantec. Pridobljeno na http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/.

[14] *Data breach investigation report.* (2012). New York, NY: Verizon. Pridobljeno na http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

[15] Economic Intelligence Unit. (2012). *Cyber theft of corporate intelectual proprety: The nature of the threat.* Pridobljeno na http://www.boozallen.com/media/file/Cyber-Espionage-Brochure.pdf.

[16] Figliuzzi, F. C. (2012). *Statement before the house committee on homeland security, subcommittee on counterterrorism and intelligence.* Federal Bureau of Investigation [FBI]. Pridobljeno na http://www.fbi.gov/news/testimony/economic-espionage-a-foreign-intelligence-threat-to-americans-jobs-and-homeland-security.

[17] Fullbrook, M. (2009). Tips on stamping out data leakage & industrial espionage during recession. *ICT Review: Computer Hardware and Software Review Journal.* Pridobljeno na http://ictreview.blogspot.com/2009/03/tips-on-stamping-out-data-leakage.html.

[18] *Global information security survey: Fighting to close the gap* (2012). London: Ernst&Young. Pridobljeno na http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf.

[19] *Global state of information security survey: Changing the game.* (2013). London: PWC. Pridobljeno na http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf.

[20] *Global state of information security survey: Eye of the storm.* (2012). London: PWC. http://www.pwccn.com/webmedia/doc/634653330562192188_rcs_info_security_2012.pdf.

[21] Hall, J. H., Sarkani, S. in Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155–176.

[22] Herath, T. in Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision support systems, 47*(2), 154–165.

[23] Hriberšek, Z. in Ribič, A. (2013). Korporativna varnost kot konkurenčna prednost podjetja. *Korporativna varnost,* 2(3), 30–33.

[24] Info Security. (2011). *Most enterprises poor at measuring information security effectiveness.* Pridobljeno na http://www.infosecurity-magazine.com/view/16928/most-enterprises-poor-at-measuring-information-security-effectiveness/.

[25] *Internet security threat report*. (2012). Mountain View, CA: Symantec. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17.

[26] *Internet security threat report.* (2013). Mountain View, CA: Symantec. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[27] *ISO/IEC 27000: 2012.* (2012). Joint Technical Committe, JTC1. The International Organization for standardization and International Electotechnical Comission: Geneva.

[28] Ivanc, B. (2013). Varovanje občutljivih podatkov v informacijskih sistemih. V. I. Bernik in B. Markelj (ur.), *Sodobni aspekti informacijske varnosti*, str. 6–11. Ljubljana: Fakulteta za varnostne vede.

[29] Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships*. Information Management & Computer Security, 20*(5), 332–349.

[30] Johansson, J. M. (2004). *The fundamental tradeoffs. Microsoft security techcentre*. Pridobljeno na http://technet.microsoft.com/en-us/library/cc512573.aspx.

[31] Knopik, C. in Zhan, J. (2010). *The effects of financial crises on american financial institutions information security.* 5th conference on future information technology, 21.–23. 5. 2010. Madison, WI: Dakota state University.

[32] Lamm Weisel, D. (2005). *Analyzing repeat victimization.* Center for problem oriented policing: Tool guide No. 5. Pridobljeno na http://www.popcenter.org/tools/repeat_victimization/print/.

[33] Markelj, B. in Bernik, I. (2011). Mobilni dostop z vidika informacijske varnosti do podatkov v oblaku. T. P. Mrevlje in I. Areh (ur.), *Zbornik prispevkov 12. slovenski dnevi varstvoslovja*. Ljubljana: Fakulteta za varnostne vede. Pridobljeno na http://www.fvv.uni-mb.si/dv2011/zbornik/informacijska_varnost/Markelj-Bernik-Oblak.pdf.

[34] Melese, F. (2009). *The financial crisis: a similiar effect to a terrorist attack.* NATO. Pridobljeno na http://www.nato.int/docu/review/2009/FinancialCrisis/Financial-terrorist-attack/EN/.

[35] Mimoso, M. S. (2009). *Number-driven risk metrics fundamentally broken.* Pridobljeno na http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350658,00.html#.

[36] Mouzas, S. (2006). Efficiency versus effectiveness in business networks. *Journal of Business Research, 59*(10–11), 1124–1132.

[37] NIST. (2013). *Glossary of key information security terms*. Gaithersburg, MD: NIST, U.S. Departement of Commerce.

[38] Northcutt, S. (2012). *Emerging trends in IT and security 2012 – 2014.* Bethesda, MD: SANS Institute. Pridobljeno na http://www.sans.edu/research/security-laboratory/article/2012-emerging-trends.

[39] OECD. (2009). *OECD Strategic response to the financial and economic crisis.* Pridobljeno na http://www.oecd.org/economy/42061463.pdf.

[40] Peláez, M. H. S. (2010). *Measuring effectiveness in information security controls.* Bethesda, MD: SANS Institute. Pridobljeno na http://www.sans.org/reading_room/whitepapers/basics/measuring-effectiveness-information-security-controls_33398.

[41] *Perception of security awareness study.* (2012). Gothenburg: Cryptzone. Pridobljeno na http://www.cryptzone.com/_download/articles/Cryptzone_Study_Perceptions_Security_Awareness.pdf.

[42] Peters, T. J. in Waterman, R. H. (1982). *In search of excellence: Lessons from America's best-run companies.* London: HarperCollins Publishers.

[43] Pironti, J. P. (2007). Developing metrics for effective information security governance. *ISACA Journal, 7*(2), str. 1–5.

[44] *Poročilo o omrežni varnosti za leto 2012*. (2013). Ljubljana: SI-CERT. Pridobljeno na http://www.cert.si/fileadmin/slike/si-cert/fokus/2013/SI-CERT_porocilo_2012.pdf.

[45] PWC. *(2009).Trial by fire: What global executives expect of information security in the middle of the world's worst economic downturn in thirty years*. London: PWC. Pridobljeno na http://www.ukmediacentre.pwc.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1557.

[46] Rebernik, M., Tominc, P. in Crnogaj, K. (2012). *Usihanje podjetništva v Sloveniji.* GEM Slovenija 2011. Pridobljeno na http://www.gemslovenia.org/gem-porocila/.

[47] Rebernik, M. (1994). *Ekonomika podjetja*. Ljubljana: Gospodarski vestnik**.**

[48] SANS Institute. (2007). *A guide to security metrics.* Pridobljeno na http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55.

[49] Schneier, B. (2008). *The psychology of security*. Pridobljeno na http://www.schneier.com/essay-155.html.

[50] *Security effectiveness framework study.* (2010). Traverse city, MI: Ponemon Institute Pridobljeno na http://h71028.www7.hp.com/enterprise/downloads/software/Security%20Effectiveness%20Framework%20Study.pdf.

[51] Sethuraman, S. in Adaikkappan, A. (2009). Information security program: Establishing it the right way for continued success. *ISACA Journal, 9*(5), str. 1–7.

[52] Sjouwerman, S. (2011). *Cyberheist: The biggest financial threat facing american since the meltdown in 2008*. Clearwater, FL: KNOWB4.

[53] Sjouwerman, S. (2012). 2013 security prediction. *Cyberheist News, 2*(54). Pridobljeno na http://blog.knowbe4.com/cyberheistnews-vol2-53/.

[54] Slagell, A. (2010). Thinking critically about computer security trade-offs. *Skeptical Inquirer.* Pridobljeno na http://www.csicop.org/si/show/thinking_critically_about_computer_security_trade-offs/.

[55] Spears, J. L. in Barkhi, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522.

[56] *State of the endpoint.* (2013). Traverse city, MI: Ponemon Institute. Pridobljeno na http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf.

[57] Stewart, A. (2012). Can spending on information security be justified? *Information Management & Computer Security, 20*(4), 312–326.

[58] Talib, S., Clarke, N. L. in Furnell, S. M. (2010). *An analysis of information security awareness within home and work environments.* 5th International conference on availability, reliability and security: ARES 2010, 15.–18. 2. 2010 (str. 196–203). Cracow: IEEE computer soc. Pridobljeno na http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7348&context=ecuworks.

[59] Thomson, K. L. in Solms, R. (2006). Towards an information security competence maturity model. *Computer fraud&security, 18*(5), 11–15.

[60] Thomson, L. L. (2011). Cybercrime and escalating risks. V L. Thomson (ur.), *Data breach and encrypton handbook*, str. 3–16. Chicago, IL: American Bar Association Section of Science & Technology Law.

[61] *TMT Global security study: Raising the bar.* (2011). New York, NY: Deloitte. Pridobljeno na http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdfTrček, D. (2006). *Managing Infomation Systems Security and Privacy*. Berlin: Springer.

[62] Trček, D. (2006). *Managing Infomation Systems Security and Privacy*. Berlin: Springer.
[63] Vaish, A. in Varma, S. (2010). Parameter Extraction for Measurement of the Effective Information Security Management – Statistical Analysis. *International Journal of Computer and Electrical Engineering, 4*(2), 654–659.
[64] Vila, A. (1994). *Organizacija in organiziranje*. Kranj: Moderna založba.
[65] Vršec, M. (2013). Varovanje poslovnega informacijskega sistema na osnovi politike varovanja informacij. *Korporativna varnost, 2*(3), 9–11.
[66] Whitman, M. E. in Mattord, H. J. (2008). *Management of information security*. Boston, MS: Course Technology Cengage Learning.
[67] Wilshusen, G. C. (2012). *Cyber threats facilitate ability to commit economic espionage.* NorthWest, WA: United states government accountability office, GAO. Pridobljeno na http://www.gao.gov/products/GAO-12-876T.
[68] Wilson, M. in Hash, J. (2003). *Building an information technology security awareness and training Program – NIST Special Publication 800-50.* Gaithersburg, MD: National Institute for standards and technology. Pridobljeno na http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.
[69] Wolter, K. in Reinecke, P. (2010). Performance and security tradeoff. V A. Aldini, M. Bernardo, A. Di Pierro in H. Wiklicky (ur.), *Formal methods for quantitative aspects of programming languages*, 135–167. Berlin: Springer-Verlag.
[70] Xavier, S. R., Kelley, D., Herrington, K. J. in Vorderwulbecke, A. (2013). *2012 Global report.* Global enterpreneurship monitor. Pridobljeno na http://www.gemslovenia.org/news/.

▪

Kaja Prislan, mag. var., doktorska študentka na Fakulteti za varnostne vede, Univerza v Mariboru.

▪

Igor Bernik, docent in predstojnik katedre za informacijsko varnost na Fakulteti za varnostne vede Univerze v Mariboru.

VZGOJA IN IZOBRAŽEVANJE V INFORMACIJSKI DRUŽBI – VIVID 2014

Programski odbor vabi vse, ki želijo s svojimi izkušnjami in pogledi prispevati k reševanju problemov in odgovorom na vprašanja, ki jih prinaša informatizacija vzgojno-izobraževalnega procesa, da pošljejo prispevke v obsegu do 10 strani. Pripravljeni naj bodo v slovenskem, izjemoma v angleškem jeziku.

Pomembni datumi

- 7. julij 2014 – oddaja prispevkov
- 8. september 2014 – obvestilo avtorjem
- 22. september 2014 – oddaja končne, popravljene verzije prispevkov

Dodatne informacije so na voljo na spletni strani *http://vivid.fov.uni-mb.si* in po e-pošti: *mojca.bernik@fov.uni-mb.si*.

Varovanje podatkov v storitvi v oblaku Dropbox

Jernej Flisar, Marko Hölbl
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova ul. 17, 2000 Maribor
{jernej.flisar, marko.holbl}@uni-mb.si

Izvleček

Storitev v oblaku Dropbox je zelo razširjena, uporablja jo več milijonov uporabnikov po vsem svetu. Storitev nam omogoča souporabo datotek in sinhronizacijo podatkov med več računalniki. Podatki so shranjeni v oblaku in so nam vedno dosegljivi. Ker so podatki shranjeni pri ponudniku storitve, se poraja vprašanje glede varnosti in zasebnosti shranjenih podatkov. V prispevku smo obravnavali varnostne mehanizme storitve Dropbox in izpostavili varnostne pomanjkljivosti, ki smo jih odkrili. Za zmanjšanje tveganja pri uporabi storitve Dropbox smo razvili programsko rešitev Secure Share, ki jo je mogoče uporabiti pri uporabi storitve za varovanje shranjenih podatkov. Prednost razvite rešitve pred drugimi orodji je, da podpira funkcionalnosti za souporabo podatkov z drugimi uporabniki in tako omogoča varno uporabo storitve Dropbox z vsemi njenimi funkcionalnostmi.

Ključne besede: Dropbox, varnost, Secure Share, SecretSync, BoxCryptor, TrueCrypt.

Abstract

Protection of Data in the Dropbox File Hosting Service

Dropbox is a very popular file sharing cloud service and has millions of users. It can be used for sharing and synchronizing data on multiple devices. Data is stored in the cloud and can always be accessed. Because the data is stored on the provider's side, issues of data privacy and security arise. In this paper, we address the security mechanisms of Dropbox and discuss potential security weaknesses. Furthermore, we review tools that enable a safer use of Dropbox. However, none of these tools support encryption when using sharing in Dropbox. Therefore we develop a software solution that addresses this issue and enables secure use of the Dropbox with all its functionalities.

Key words: Dropbox, security, Secure Share, SecretSync, BoxCryptor, TrueCrypt.

1 UVOD

Storitev računalništva v oblaku je veliko. Mednje sodijo storitve, ki ponujajo hrambo podatkov v oblaku (Zhang, Cheng & Boutaba, 2010). Ena izmed teh storitev je Dropbox, ki je bila predstavljena leta 2007 in je v prvih dveh letih pridobila dva, do leta 2010 pa že dvajset milijonov uporabnikov (Geron, 2011). Na začetku leta 2012 je imela storitev že preko petdeset milijonov uporabnikov po vsem svetu (Dropbox, 2012). Storitev omogoča shranjevanje, sinhronizacijo in souporabo podatkov z drugimi uporabniki. Podatki so shranjeni v oblaku, zato lahko do njih dostopamo povsod. Pri tem pa se pojavi vprašanje varnosti shranjenih podatkov.

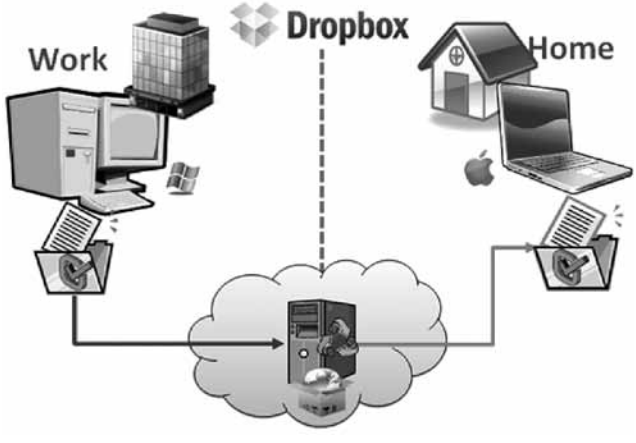
Islovar definira varnost podatkov kot stanje, pri katerem je zagotovljena zaupnost, celovitost in razpoložljivost podatkov. V tem primeru varnost podatkov zagotavlja ponudnik storitve tako, da ta nima dostopa in vpogleda v podatke svojih uporabnikov. Varnost je namreč največja skrb računalništva v oblaku, kar je potrdila tudi raziskava Harvard Business Review, v kateri je nekaj čez 50 odstotkov uporabnikov izrazilo zaskrbljenost, povezano z varnostjo podatkov (Knorr, 2011). Tako tudi Dropbox ni imun na varnostne pomanjkljivosti, kar je razvidno iz številnih virov (Cardwel, 2011; de Icaza, 2011; Kovach, 2011; Mulazzani, Schrittwieser, Leithner, Huber & Weippl, 2011; Newton, 2011). Sodobni standardi aplikacij v oblaku težijo k temu, da je treba varnost nadgraditi (Zhou, Zhang, Xie, Qian & Zhou, 2010) zato tudi Dropbox potrebuje izboljšane mehanizme za varovanje podatkov.

V članku bomo predstavili varnostna tveganja in grožnje zasebnosti storitve Dropbox ter varnostne incidente, povezane z omenjeno storitvijo. Prav tako bomo obravnavali programske rešitve za obravnavanje tveganj in pokazali, da imajo tudi te določene pomanjkljivosti. Predstavili bomo programsko rešitev SecretShare, ki naslavlja pomanjkljivosti obstoječih programskih rešitev za varovanje podatkov v storitvi Dropbox.

V naslednjem razdelku bomo na kratko predstavili storitev v oblaku Dropbox, njeno delovanje in varnostne mehanizme, ki jih vključuje. V tretjem razdelku bomo identificirali varnostne težave in pomanjkljivosti storitve Dropbox. Predzadnji razdelek predstavlja ukrepe, ki jih lahko izvedejo uporabniki, da zavarujejo svoje podatke, shranjene na Dropboxu. Opisali bomo orodja, ki so na voljo, jih primerjali in izpostavili njihove pomanjkljivosti. V zadnjem razdelku bomo opisali aplikacijo, ki naslavlja varnostne pomanjkljivosti in omogoča varno souporabo podatkov, shranjenih na Dropboxu.

2 DROPBOX

Dropbox je brezplačna storitev v oblaku, ki omogoča sinhronizacijo podatkov med več računalniki oz. med več različnimi napravami (slika 1). Storitev je na voljo od leta 2007, upravlja pa jo podjetje Dropbox inc. Začetnika in ustanovitelja Dropboxa sta Drew Houston in Arash Ferdowsi. Dropbox ima danes že več kot 50 milijonov uporabnikov (Dropbox, 2012). Bil je ena izmed prvih storitev za hrambo podatkov v oblaku in je trenutno med najbolj popularnimi (Vaughan-Nichols, 2013). Podobne storitve so SugarSync, iCloud in SkyDrive (Turim-Nygrem, 2012).



Slika 1: **Sinhronizacija podatkov med več računalniki oz. prenosnimi napravami (Dropbox, 2012)**

Dropbox ni samo storitev za hrambo lastnih podatkov v oblaku, omogoča tudi souporabo datotek z drugimi uporabniki. Do podatkov lahko dostopamo z različnih odjemalcev (računalnik, mobilne naprave idr.) ter prek spletnega vmesnika. Prav tako storitev podpira pregled in nadzor nad različicami dokumentov.

2.1 Delovanje

Večji del storitve Dropbox je razvit v programskem jeziku Phyton (Dropbox, 2012). Na odjemalcu uporabnika se vse lokalne datoteke v označeni mapi sinhronizirajo s strežnikom Dropbox in z vsemi drugimi napravami, ki so v lasti uporabnika. Slika 1 prikazuje sinhronizacijo datotek med več različnimi napravami. Uporabnik shrani datoteko na lokalnem računalniku, kopija te datoteke se prenese na storitev in na vse druge naprave, ki so v lasti uporabnika.

Dropbox datoteke razdeli na kose velikosti 4 MB. Kadar uporabnik doda novo datoteko v Dropbox mapo na lokalnem računalniku, aplikacija izračuna prstni odtis datoteke z zgoščevalno funkcijo SHA – 256 (Mulazzani idr., 2011). Izračunano vrednost pošlje na strežnik storitve. Tam preveri, ali že obstaja kakšna datoteka s to izračunano vrednostjo. V primeru, da ne obstaja, prenese na oblak kopijo datoteke uporabnika. Če datoteka že obstaja, pa datoteke ne prenese v oblak, temveč naredi povezavo na to datoteko. S tem Dropbox prihrani prostor in omrežni promet ter pospeši sinhronizacijo podatkov (Cachin & Schunter, 2011).

Za dodatno povečanje učinkovitosti vpeljuje Dropbox tehniko delta kodiranja (angl. delta encoding). Tehnika omogoča, da se na strežnik naložijo samo tisti deli datotek, ki so bili spremenjeni pri predhodni sinhronizaciji s strežnikom (Dropbox, 2012).

2.2 Mehanizmi in tehnike varovanja podatkov

Dropbox zagotavlja več varnostnih mehanizmov za komunikacijo s storitvijo, prenos in shranjevanje podatkov. Za komunikacijo in prenos podatkov uporablja SSL/TLS (angl. Secure Socket Layer/Transport Layer Security), medtem ko za varovanje shranjenih podatkov uporablja šifrirni algoritem AES-256. Za fizično varovanje in varnostne kopije podatkov skrbijo Amazonove storitve (Dropbox, 2012).

Varovana povezava

Za varovanje povezave med odjemalcem in strežnikom uporablja Dropbox protokol SSL (angl. Secure Socket Layer); to je protokol, prek katerega lahko varno pošiljamo podatke. Podatki, ki jih pošiljamo prek SSL so namreč zavarovani s šifriranjem. SSL omogoča, da so podatki, ki jih odjemalec pošilja storitvi v

oblaku Dropbox, zavarovani in nedostopni napadalcem oz. tretjim osebam.

Šifriranje podatkov

Vse datoteke, shranjene na Dropboxu, so šifrirane. Za šifriranje uporabljamo algoritem AES z 256-bitnim ključem. AES (angl. Advanced Encryption Standard) je mednarodni standard za šifriranje in dešifriranje podatkov s simetričnim ključem in velja za varni šifrirni algoritem (NIST, 2001a). Prav tako ni poznan noben učinkovit napad na AES (Ferguson, Schneier & Kohno, 2011). Zaradi 256-bitne dolžine ključa je neučinkovit tudi napad z izčrpnim iskanjem ključa (angl. Exhaustive Key Search).

Uporabljeni šifrirni ključi so neodvisni od uporabnika, saj ta nanje nima vpliva. Ker s šifrirnimi ključi upravlja Dropbox, ni poznano, kako se dodeljujejo ključi in kje se hranijo (Kassner, 2011). Zaradi uporabe šifriranja so shranjeni podatki nedostopni oz. neberljivi drugim uporabnikom.

Amazonove storitve

Za shranjevanje podatkov uporablja Dropbox Amazonovo storitev Simple Storage Service (Dropbox, 2012). Tako je varnost podatkov v veliki meri odvisna od nje.

Podjetje Amazon ponuja številne storitve ter ima veliko izkušenj pri razvoju in načrtovanju velikih in varnih podatkovnih centrov. Glede fizične varnosti infrastrukture imajo pri Amazonu zelo visok vojaški standard (Amazon, 2012). Podatkovni centri so nastanjeni na različnih lokacijah, vgrajene imajo različne kontrole dostopa. Fizični dostop ima samo avtorizirano osebje, ki se mora trikrat overiti z dvema načinoma identifikacije (Two-factor authenticaion[1]) (Rouse, 2005). Prenos podatkov do Amazonovih storitev poteka prek HTTPS. Uporablja različne načine mehanizmov kontrole dostopa:

- IAM (Identity and Access Management),
- ACLs (Access Control Lists) in
- avtentikacijsko povpraševanje (angl. query string authentication).

Dostopnost do podatkov in zanesljivost storitve naj bi bila po trditvah Amazona 99,99-odstotna. Načrtovana je tako, da zagotavlja razpoložljivost podatkov tudi v primeru, če sočasno prenehata delovati dva podatkovna centra (angl. facilities) (Amazon, 2012).

3 VARNOSTNE POMANJKLJIVOSTI STORITVE

Kljub vsem varnostnim mehanizmom smo identificirali določene varnostne pomanjkljivosti, s katerimi je lahko ogrožena varnost shranjenih podatkov. V nadaljevanju bomo obravnavali varnostna tveganja za podatke, shranjene v oblačni storitvi Dropbox.

3.1 Upravljanje s šifrirnimi ključi

Kljub temu da je za šifriranje uporabljen algoritem AES-256, se poraja vprašanje upravljanja s šifrirnimi ključi. Z njimi namreč upravlja Dropbox. Iz tega bi lahko sklepali, da lahko Dropbox dostopa do podatkov, shranjenih na njegovi storitvi v oblaku (De Icaza, 2011). V Dropboxovem pravilniku zasebnosti (angl. private policy) je namreč navedeno, da imajo zaposleni v podjetju Dropbox prepovedan vpogled v datoteke uporabnikov. Največkrat je človek najšibkejši člen verige varovanja, zato se porajajo pomisleki o ustreznosti varovanja podatkov (Cachin & Schunter, 2011). Celo pri »velikanu« Googlu so zaposleni zlorabljali podatke uporabnikov (Popkin, 2010).

Naslednja kočljiva točka v pogojih uporabe storitve Dropbox je dejstvo, da ima Dropbox pravico oz. je zavezan k temu, da podatke uporabnikov posreduje organom pregona. Tudi tako lahko pride do zlorab (Gaddis, 2011).

3.2 Datoteka config.db

Varnostno tveganje pomeni tudi datoteka config.db, ki se namesti na uporabnikov računalnik skupaj z odjemalcem Dropbox. V datoteki config.db so zapisani podatki za overjanje s storitvijo Dropbox. Podatki so shranjeni v formatu SQLite. Zaradi varnostne zasnove, ki jo uporablja Dropbox, je datoteka varnostno kritična. Najzanimivejši podatki v datoteki so:

- e-mail – elektronski naslov uporabnika računa,
- dropbox_path – pot do datoteke, v kateri se nahaja mapa Dropbox,
- host_id – identifikacija sistema, ko je ta nameščen in overjen.

Za overjanje tako uporabljamo samo atribut host_id. Če napadalec pride do vsebine datoteke config.db oz. samo do vrednosti atributa host_id, ima dostop do vseh naših podatkov na Dropboxu (Newton, 2011). Tudi v primeru, da uporabnik spremeni geslo, je host_id še vedno veljaven.

[1] Aventikacija na način »nekaj, kar oseba ima (identifikacijsko kartico), in nekaj, kar oseba zna (geslo)«.

Sicer drži, da ima napadalec verjetno tudi neposreden dostop do vaših datotek Dropbox, če ima dostop do uporabnikove config.db datoteke, vendar se kljub temu porajajo določena varnostna tveganja:

- enostaven virus bi lahko bil implementiran v namen pridobiti vsebino datoteke config.db;
- tudi v primeru odkritja takšnega virusa to napadalcu ne bi preprečilo dostopa do vaših datotek Dropbox, saj bi že imel vsebino datoteke config.db;
- prikrit prenos vsebine datoteke config.db je veliko težje odkriti, kot če bi napadalec želel prenašati celotne datoteke, ki jih ima uporabnik na Dropboxu.

Od Dropboxove verzije 1.2 naprej je bila konfiguracijska datoteka spremenjena. Tako imajo novejše verzije šifrirano datoteko config.dbx, kar preprečuje neavtoriziran dostop do vsebine atributa host_id. (Dropbox, 2012).

Storitev je mogoče uporabljati tudi na mobilnih aplikacijah, vendar določene mobilne naprave ne podpirajo varne povezave HTTPS. V teh primerih lahko napadalec prestreza podatke, ki jih pošiljamo ali pridobivamo iz Dropboxa (Cardwel, 2011; Kovach, 2011).

Kljub ukrepom, ki jih ima Dropbox za zagotavljanje varnosti, se je 20. junija 2011 zgodil incident. Tega dne so bili namreč dostopni vsi uporabniški računi brez overjanja. Napako naj bi povzročila posodobitev programske opreme. Uporabniški računi so bili prosto dostopni štiri ure. Po poročanju Dropboxa je bilo takrat aktivnih manj kot odstotek uporabnikov (Wikipedia, 2012).

4 ORODJA ZA VAROVANJE PODATKOV NA DROPBOXU

Iz do sedaj navedenega lahko sklepamo, da obstajajo določena varnostna tveganja pri uporabi storitve Dropbox. Zavedati se moramo, da podatke s tem, ko jih shranjujemo na Dropboxu, izpostavljamo možnosti nezaželenega vpogleda. Da bi preprečili nepooblaščene vpoglede, moramo podatke ustrezno varovati, kar lahko storimo s programskimi rešitvami. S tem lahko izboljšamo varnost podatkov, shranjenih v storitvah v oblakih. Varovanje podatkov je opredeljeno kot onemogočanje dostopa do podatkov nepooblaščenim osebam, tudi ponudniku storitve v oblaku. Rešitev je udejanjena v obliki šifriranja podatkov, kar pomeni, da podatke iz prvotne oblike pretvorimo v neberljivo obliko. Le z ustreznim geslom in ključem je nato mogoče dobiti prvotne, torej berljive podatke.

Vsi progami za šifriranje podatkov na Dropboxu delujejo podobno. Najprej šifrirajo podatke, nato jih predajo programu za shranjevanje v oblaku, ki jih sinhronizira v oblak. Ker sta šifriranje in sinhronizacija podatkov med seboj neodvisna, program za šifriranje ne pozna uporabniškega imena in gesla za Dropbox, Dropbox pa ne gesla za šifriranje oziroma dešifriranje podatkov.

Tudi Dropbox svetuje uporabo orodij za šifriranje, kot je recimo TrueCrypt (Dropbox, 2012). V ta namen smo obravnavali programska orodja, s katerimi lahko šifriramo podatke, ki jih shranjujemo na Dropbox. Programi uporabljajo različne postopke šifriranja, pri vseh pa so uporabljeni postopki varni, saj uporabljajo standardizirane šifrirne algoritme (Ferguson idr., 2011).

V tabeli 1 je predstavljena primerjava programov in njihovih glavnih značilnosti. Orodja smo primerjali glede na kriptografske lastnosti, s katerimi določamo raven varovanja podatkov. Zaščita je odvisna od uporabljenega algoritma in velikosti ključa – večji kot je uporabljeni ključ, višja je raven varnosti šifriranih podatkov (Ferguson idr., 2011).

Orodji TrueCrypt in AxCrypt sta splošno namenski, medtem ko sta SecretSync in BoxCryptor namenjena izključno šifriranju podatkov na Dropboxu. S tega vidika sta seveda tudi bolj primerna za takšno vrsto uporabe, njuna uporaba pa je preprostejša.

Tabela 1: **Primerjava orodij za varovanje podatkov**

Naziv orodja	**TrueCrypt**	**SecretSync**	**BoxCryptor Classic**	**AxCrypt**
Verzija	7.1a	1.3	1.6	1.7
Spletna stran izdelka	www.truecrypt.org	getsecretsync.com, http://www.viivo.com/	www.boxcryptor.com	www.axantum.com/axcrypt/
Podprte platforme	Windows, Linux, Mac OS	Windows, Linux, Mac OS, Android	Windows, Mac Os, Android, iOS	Windows
Cena	Odprtokoden	Do 2GB zastonj	Do 2GB zastonj	Odprtokoden
		Kriptografija		
Šifrirni algoritem[2]	AES, Blowfish, Twofish	AES	AES	AES
Velikost ključa (v bitih)	256	256	128–256	128
		Dropbox		
Upravljanje s ključi	Pri uporabniku	Na spletni storitvi	Pri uporabniku	Pri uporabniku
Način šifriranja podatkov	V celoti	Po datoteki	Po datoteki	Po datoteki
Šifriranje nazivov datotek	Podprto	Ni podprto	Podprto	Ni podprto
Souporaba podatkov	Ni podprto	Ni podprto	Ni podprto	Ni podprto

Vsi primerjani programi so brezplačni, vsaj v osnovni različici. Najučinkovitejše varovanje podatkov zagotavlja TrueCrypt, saj lahko izbiramo in kombiniramo med več različnimi šifrirnimi algoritmi (TrueCrypt, 2012). Nadloga pri uporabi je vnaprejšnje določanje velikosti šifrirnega navideznega pogona oz. datoteke. Težko je namreč predvidevati, koliko prostora bomo potrebovali. Prav tako je treba datoteko (navidezni pogon) najprej zapreti, da se lahko sinhronizira z oblakom, to pa lahko marsikomu povzroča nevšečnosti. S podobnimi težavami se srečujemo tudi pri uporabi AxCrpyta, saj ne omogoča samodejnega šifriranja datotek. Datoteke je namreč treba šifrirati in dešifrirati ročno. Tukaj sta v prednosti SecretSync in BoxCryptor, ki podatke šifrirata samodejno. Za razliko od TrueCrypta uporabljata šifriranje po posameznih datotekah. Največja razlika med njima je pri upravljanju s šifrirnimi ključi. Pri SecretSync z njimi upravlja storitev, pri BoxCryptorju pa uporabnik. Zaradi tega se zdi BoxCryptor primernejša izbira, saj zagotavlja večjo neodvisnost od ponudnika.

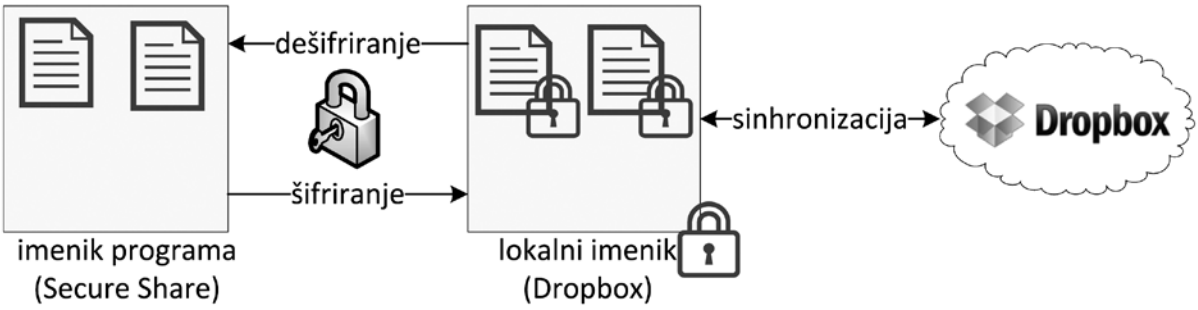
Težava nastane, ko želimo šifrirati podatke in omogočiti dostop do njih tudi drugim (izbranim) uporabnikom. Dropbox sicer omogoča deljenje datotek, vendar tega ne moremo več uporabljati, če uporabljamo katero izmed navedenih rešitev. Zaradi tega se poraja potreba po programski rešitvi, ki bi to omogočala.

5 SECURE SHARE

Kot smo ugotovili v prejšnjih razdelkih, je za zagotavljanje večje varnosti podatkov, shranjenih na Dropboxu, te treba dodatno zavarovati s šifriranjem. Obravnavali smo tudi prednosti in slabosti uporabe obstoječih orodij, s katerimi lahko šifriramo podatke. Ugotovili smo, da imajo vsi programi določene pomanjkljivosti, vendar je najbolj izstopajoče dejstvo, da souporaba datotek med uporabniki ni mogoča, če uporabljamo katero izmed obravnavanih programskih orodij.

Za zagotavljanje omenjene funkcionalnosti smo razvili novo programsko rešitev – Secure Share. Secure Share deluje podobno kot SecretSync, saj zagotavlja dodaten sloj nad podatki Dropbox. Slika 2 prikazuje njegovo delovanje. Šifrirni ključi so shranjeni pri uporabniku kot pri programskem orodju Box Cryptor. Prednost takšne rešitve je neodvisnost od delovanja in dosegljivosti ponudnika oz. storitve.

[1] (Ferguson, Schneier & Kohno, 2011)



Slika 2: **Delovanje šifriranja in sinhronizacije podatkov na Dropbox**

5.1 Predstavitev rešitve

Da bi dosegli čim večjo uporabnost orodja na vseh operacijskih sistemih, smo se odločili implementirati orodje v programskem jeziku Java. Uporabili smo najnovejšo različico Jave SE 7. Dodatnih knjižnic nismo vključevali, saj ima Java že v osnovi vključene implementacije potrebnih in preizkušenih šifrirnih algoritmov (Oracle, 2012).

Za šifriranje podatkov rešitev uporablja simetrične in asimetrične kriptografske algoritme. Pri simetričnih algoritmih imamo samo en zasebni ključ, s katerim šifriramo in dešifriramo podatke. Ti algoritmi so hitri in varni, težko pa je varno izmenjati ključ. Asimetrični algoritmi pa uporabljajo par ključev – zasebnega in javnega. Uporabnik si ustvari dva med seboj povezana ključa in enega objavi. Vsi, ki mu hočejo poslati sporočilo, bodo uporabili njegov javni ključ za šifriranje sporočila. Dešifriral pa ga bo lahko le uporabnik s svojim zasebnim ključem, ki je poznan samo njemu. Asimetrični šifrirni algoritmi so računsko bolj zahtevni kot simetrični in zato počasnejši (Ferguson idr., 2011).

Za šifriranje podatkov smo uporabili šifrirni algoritem AES z velikostjo ključa 256 bitov. Šifrirni algoritem je varen, vsestransko uporaben in hiter. Največjo velikost ključa, ki jo predvideva standard, smo uporabili z namenom zagotavljanja visoke ravni varovanja podatkov. Ker je AES bločna šifra, smo za način šifriranja uporabili veriženje šifriranih blokov (angl. Cipher Block Chaining – CBC) (NIST, 2001b). Za generiranje 256-bitnega ključa, ki je dejansko psevdonaključno število, smo uporabili javanski razred javax.crypto.KeyGenerator.

Da bi zagotovili varno izmenjavo ključev pri implementaciji funkcionalnosti za souporabo podatkov med več udeleženci, je bilo treba izbrati tudi asimetričen šifrirni algoritem (angl. Asymmetric Encryption Algorithm). Ker je v praksi najbolj splošno uporaben, smo uporabili algoritem RSA (Ferguson idr., 2011). Za dolžino parov ključev smo izbrali 2048 bitov, kar je tudi največja možna dolžina pri trenutni implementaciji v Javi (Oracle, 2012). Za generiranje parov ključev poskrbi razred java.security.KeyPairGenerator.

Za shranjevanje nastavitvenih lastnosti in šifrirnih ključev uporabljamo tri datoteke:

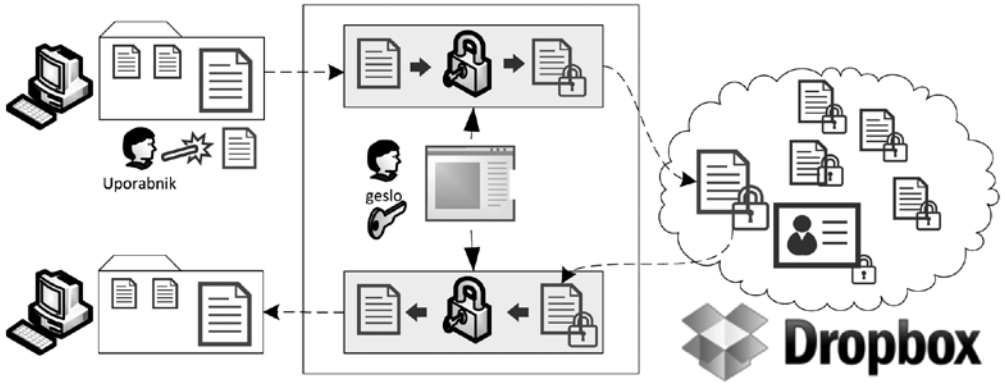
- Host.xyz: shranjeni so podatki o e-naslovu uporabnika ter lokacija mape Secure Share in lokalne mape Dropbox;
- Config.xyz: shranjuje podatke o uporabniku; datoteka se shranjuje v imeniku Settings, v katerem je nameščena aplikacija; podatki, ki jih hranimo, so e-naslov, geslo, šifrirni ključ, javni in zasebni ključ ter vrednost soli (angl. salt);
- Keys.xyz: vsebuje podatke o ustvarjalcu imenika, ki je bil dodan za souporabo, ter seznam javnih ključev oz. uporabnikov, ki imajo dostop do skupnega imenika.

Datoteke so šifrirane z uporabniškim geslom, kar onemogoča napadalcem pridobivanje nastavitvenih podatkov uporabnika.

Prikaz osnovnega delovanja šifriranja je viden na sliki 3. Uporabnik shrani datoteko v lokalnem imeniku programa Secure Share. Ko programska rešitev prepozna spremembo v imeniku, začne s postopkom šifriranja:

1. prebere šifrirani uporabniški ključ za simetrično šifriranje;
2. z uporabniškim geslom dešifrira simetrični ključ;
3. prebere vsebino nove ali spremenjene datoteke;
4. s simetričnim ključem šifrira novo ali spremenjeno datoteko in jo nato prekopira na Dropbox.

Dešifriranje poteka podobno:
1. program zazna spremembo v imeniku Dropbox;
2. prekopira vsebino datoteke;
3. pridobi uporabniški ključ za dešifriranje;
4. prekopira dešifrirano datoteko v lokalni imenik uporabnika.

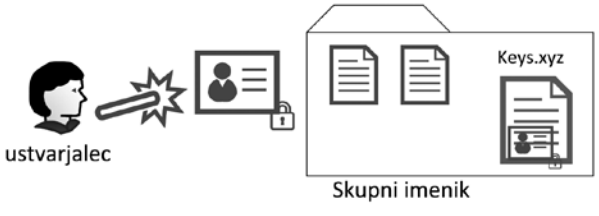


Slika 3: **Prikaz osnovnega poteka šifriranja**

Program tako vodi dvojno evidenco datotek. Lokalne izvorne in šifrirane na Dropboxu. Simetrični ključ, ki se uporablja za šifriranje, je shranjen v Dropboxovem imeniku in je zato vedno dosegljiv uporabniku. Zaradi varnosti je ključ šifriran z uporabniškim geslom.

Za implementacijo šifriranja podatkov za souporabo le-teh med več uporabniki smo uporabili asimetrično šifriranje za varno izmenjavo simetričnega ključa. Pri izvedbi je bilo treba poznati delovanje funkcionalnosti souporabe datotek v Dropboxu, ki jo bomo na kratko opisali v nadaljevanju.

Ko uporabnik doda določen imenik v souporabo, se zanj ustvari sejni ključ. Ključ ustvari aplikacija Dropbox tistega uporabnika, ki je prvi dodal imenik v skupno uporabo, in ta uporabnik je nato zadolžen za nadaljnjo distribucijo ključa. Ključ nato uporabljamo za šifriranje in dešifriranje datotek v imeniku, ki je v skupni rabi. V datoteko *keys.xyz* se zapiše, da je sejni ključ ustvarjen in kateri uporabnik ga je ustvaril (slika 4).

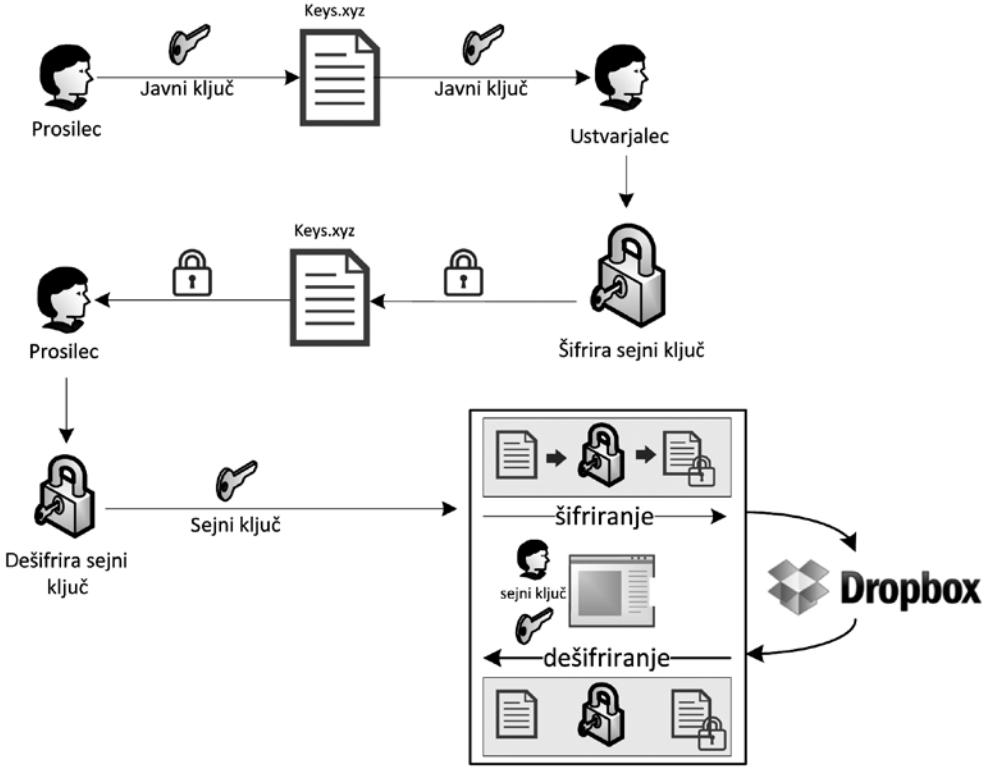


Slika 4: **Začetek postopka za šifriranje datotek v souporabi**

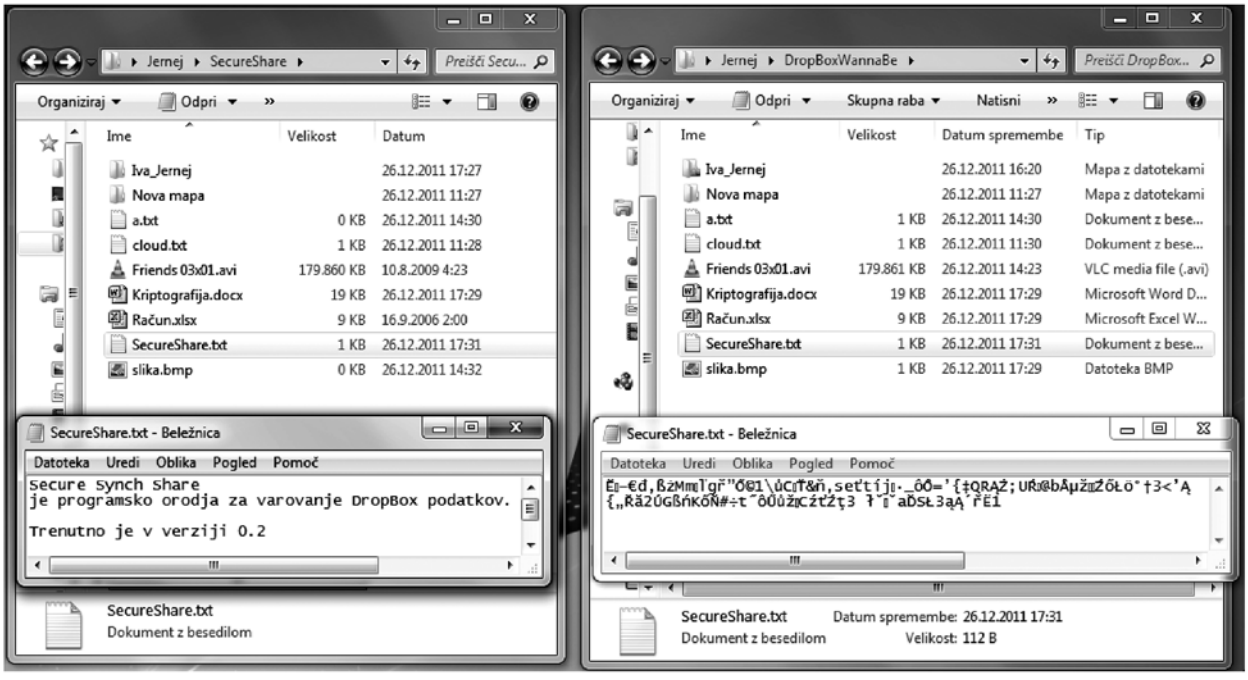
Da bi drugi uporabnik oz. uporabniki (v nadaljevanju prosilec) lahko začeli dešifrirati ali šifrirati datoteke v skupnem imeniku, mora najprej pridobiti ustrezen sejni ključ. Proces izmenjave sejnega ključa poteka takole (slika 5):
1. prosilec spremeni vsebino datoteke *keys.xyz* s tem, da ji doda vrednost svojega javnega ključa;
2. ustvarjalec skupnega imenika prepozna spremembo datoteke, prebere javni ključ prosilca ter šifrira z njim sejni ključ mape; spremembe shrani nazaj v datoteko keys.xyz;
3. prosilec zazna ponovno spremembo datoteke keys.xyz, prebere šifrirano vrednost sejnega ključa in ga dešifrira z zasebnim ključem; s tem pridobi vrednost sejnega ključa;
4. vsi uporabniki nato uporabljajo ta sejni ključ za šifriranje datotek za skupni imenik.

Ko so izmenjani ključi, poteka šifriranje datotek simetrično. Postopek se ponovi posebej za vsak skupni imenik ter za vsakega uporabnika.

Predstavljena rešitev je preprosta za uporabo in deluje popolnoma samodejno. Izvorne podatke shranjuje lokalno na računalniku uporabnika v posebnem imeniku, ki ga določi uporabnik. Ti podatki se nato šifrirajo in sinhronizirajo z mapo Dropbox. Na sliki 6 vidimo, kako so prikazani izvorni in šifrirani podatki na Dropboxu.



Slika 5: **Postopek izmenjave sejnega ključa**



Slika 6: **Prikaz izvornih in kriptiranih datotek, ki so med seboj sinhronizirane**

Pri dodajanju uporabnikov v skupni imenik se – vsaj z vidika uporabnika – nič ne spremeni. Ko doda uporabnik določen imenik v souporabo drugim uporabnikom, se datoteke samodejno začnejo šifrirati s skrivnim ključem, ki je poznan samo uporabnikom tega imenika.

Trenutna različica programske rešitve Secure Share ima tudi možnosti nadgradnje in izboljšave. Izpostavili bi optimizacijo branja datotek in njihovega šifriranja glede na njihovo velikost, s čimer bi lahko izboljšali odzivni čas. Izboljšati je mogoče tudi implementacijo izmenjave sejnega ključa oz. njegovo distribucijo. Trenutno lahko ključ distribuira le uporabnik, ki ustvari skupen imenik. Nadgradnja bi lahko omogočala, da bi sejni ključ distribuirali vsi uporabniki, ki ga posedujejo (za določen imenik v skupni rabi).

6 SKLEP

V prispevku smo predstavili programsko rešitev za varovanje podatkov na Dropboxu, imenovano Secure Share. Implementirana je v programskem jeziku Java, kar omogoča uporabo na več platformah. Rešitev omogoča lokalno šifriranje podatkov, preden te prenesemo v Dropboxov oblak. Dodatne mehanizme varovanja s pomočjo šifriranja je smiselno vpeljati, ko imamo opravka s korporativnimi uporabniki in občutljivimi (tudi zaupnimi) podatki. Pri analizi varnostnega vidika storitve Dropbox smo namreč ugotovili, da storitev ni popolnoma varna, kljub temu da uporablja varno povezavo in šifriranje podatkov (AES),. Varnostno tveganje pomeni upravljanje s ključi za šifriranje. Kljub temu da je šifriranje po standardu AES-256 zelo varno, je ključ pod nadzorom ponudnika shrambe v oblaku. Prav tako incident, ki se je pripetil, nakazuje, da ima storitev Dropbox določena tveganja in da je treba vpeljati dodatne varnostne mehanizme. Primerjali smo tudi orodja za varovanje podatkov in ugotovili, da sta orodji za šifriranje podatkov, kot sta TrueCrypt in SecretSync, primerni za dodatno varovanje podatkov. Podatke šifrirata lokalno, pri uporabniku. Do podatkov ima tako dostop le overjeni uporabnik, saj se šele šifrirani podatki prenesejo na Dropbox. Ob njuni uporabi pa nastopijo težave, saj se uporabnost Dropboxa lahko zmanjša. Težava je predvsem v omejeni zmožnosti souporabe podatkov (z drugimi uporabniki), saj je ne omogočajo omenjeni programi za varovanje. Predstavljena programska rešitev Secure Share rešuje omenjeni problem, kar je njena poglavitna prednost pred obstoječimi orodji oz. programskimi rešitvami. Funkcionalnost je realizirana z uporabo asimetričnega šifriranja, kar zagotavlja varno izmenjavo ključa za šifriranje podatkov, ki so v skupni rabi.

VIRI IN LITERATURA

[1] Amazon. (2012). Amazon Simple Storage Service (Amazon S3). Dostopno na http://aws.amazon.com/s3/ [oktober 2012].

[2] Cachin, C. & M. Schunter (2011). A cloud you can trust. IEEE Spectrum 48 (12) (December): 28–51. doi:10.1109/MSPEC.2011.6085778.

[3] Cardwel, M. (2011). Dropbox Mobile: Less Secure Than Dropbox Desktop. Dostopno na https://grepular.com/Dropbox_Mobile_Less_Secure_Than_Dropbox_Desktop [oktober 2012].

[4] De Icaza, M. Dropbox Lack of Security (2011). Dostopno na http://tirania.org/blog/archive/2011/Apr-19.html [oktober 2012].

[5] Dropbox. (2012). Dropbox. Dostopno na https://www.dropbox.com [oktober 2012].

[6] Geron, T. (2011, November 4). Dropbox Hits 25M Users, Expanding Internationally - Forbes. Forbes. Dostopno na http://www.forbes.com/sites/tomiogeron/2011/04/18/dropbox-ramping-up-towards-mainstream/ [januar 2013].

[7] Jeremy L. Gaddis. (2011). Why I Use Jungle Disk and Tarnsnap. Evilrouters. Dostopno na http://evilrouters.net/2011/04/20/why-i-use-jungle-disk-and-tarsnap/ [oktober 2012].

[8] Ferguson, N., Schneier, B. & Kohno, T. (2011). Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons.

[9] Kassner, M. (2011). Dropbox: Convenient? Absolutely, but is it secure? Dostopno na http://www.techrepublic.com/blog/security/dropbox-convenient-absolutely-but-is-it-secure/5618.

[10] Knorr, E. (2011). Cloud computing by the numbers. InfoWorld. Retrieved May 29, 2012, from http://www.infoworld.com/t/cloud-computing/cloud-computing-the-numbers-983.

[11] Kovach, S. (2011). Don't Use Dropbox's Mobile Apps To Store Sensitive Files. Dostopno na http://articles.businessinsider.com/2011-03-14/tech/30018925_1_mobile-apps-private-files-sensitive-files [oktober 2012].

[12] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, & Aoying Zhou. (2010). Security and Privacy in Cloud Computing: A Survey. In 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG) (str. 105–112). Presented at the 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), IEEE. doi:10.1109/SKG.2010.19

[13] Mulazzani, M., S. Schrittwieser, M. Leithner, M. Huber & E. Weippl (2011). Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space. In USENIX Security, 8:5–5. http://www.usenix.org/event/sec11/tech/full_papers/Mulazzani6-24-11.pdf.

[14] Newton, D. (2011). Dropbox Authentication: Insecure by Design. Dostopno na http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/ [oktober 2012].

[15] NIST. (2001a). Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197 (FIPS PUBS). Dostopno na http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[16] NIST. (2001b). Recommendation for Block Cipher Modes of Operation: Methods and Techniques (NIST Special Publication 800-38A 2001 Edition). Washington, DC: U. S. Government Printing Office. Dostopno na http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.
[17] Oracle. (2012). Java Cryptography Architecture. Dostopno na http://docs.oracle.com/javase/7/docs/technotes/guides/security/StandardNames.html [oktober 2012].
[18] Popkin A. S., H. (2010). Google Had at Least Two Creepy Stalker Engineers. Technolog. Dostopno na http://www.technolog.msnbc.msn.com/technology/technolog/google-had-least-two-creepy-stalker-engineers-127006 [oktober 2012].
[19] Rouse, M. (2005). What Is Two-factor Authentication? WhatIs.com. Dostopno na http://searchsecurity.techtarget.com/definition/two-factor-authentication [oktober 2012].
[20] TrueCrypt. (2012). TrueCrypt - Free Open-Source Disk Encryption - Documentation - Version History. Dostopno na http://www.truecrypt.org/docs/?s=version-history [oktober 2012].
[21] Turim-Nygren, M.(2012). Best of the cloud: 7 top cloud storage services compared. Dostopno na http://www.digitaltrends.com/computing/the-7-best-cloud-storage-services-compared [december 2012].
[22] Vaughan-Nichols, S. J. (2013). The top 10 personal cloud-storage services. ZDNet. Dostopno na http://www.zdnet.com/the-top-10-personal-cloud-storage-services-7000011729/ [februar 2013].
[23] Wikipedia. (2012). Dropbox (service). Wikipedia, the Free Encyclopedia. Wikimedia Foundation, Dostopno na http://en.wikipedia.org/w/index.php?title=Dropbox_(service) [oktober 2012].
[24] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7–18.

▪

Jernej Flisar je tehniški sodelavec na Fakulteti za informatiko, računalništvo in informatiko Univerze v Mariboru. Diplomiral je leta 2010 in magistriral leta 2012. Njegova raziskovalna področja zajemajo semantični splet, varovanje podatkov in računalništvo v oblaku.

▪

Marko Hölbl je diplomiral leta 2004 in doktoriral leta 2009 na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Trenutno je na tej fakulteti zaposlen kot docent. Raziskovalno se ukvarja z informacijsko in računalniško varnostjo, s kriptografijo in z varnostjo e-poslovanja..

Doseganje strateških ciljev policije z boljšim upravljanjem investicij v informatiko

Borut Jereb
Univerza v Mariboru, Fakulteta za logistiko, Mariborska c. 7, 3000 Celje
borut.jereb@fl.uni-mb.si

Izvleček

Obstoječi model upravljanja informatike policije temelji na obravnavi tehničnih in tehnoloških izzivov. Pri tem je prezrt novejši, poslovno orientiran vidik upravljanja, ki temelji na učinkovitem upravljanju investicij v informacijska sredstva in s temi investicijami povezanimi tveganji. V informacijska sredstva in v njihov zaščito ni mogoče ustrezno investirati brez vedenja o njihovi vrednosti, ki jih imajo pri doseganju poslovnih ciljev policije. V prispevku dokazujemo, da je potrebno in mogoče z učinkovitim upravljanjem investicij v informacijska sredstva zagotavljati doseganje poslovnih ciljev policije. To dosežemo prek predlagane razširitve informacijskega varnostnega modela, ki ga predstavlja obstoječa informacijska varnostna politika. Tudi sama implementacija dopolnjenega modela zahteva investicijo – tokrat v dopolnitev organizacije upravljavske piramide in v spremembo obstoječega poslovanja policije. Pri tem gre predvsem za investicijo v človeški kapital in za vzpostavitev okolja, ki omogoča uspešno realizacijo sprememb. S predlaganim modelom, pri katerem v ospredje upravljanja informatike postavimo njihove poslovne vrednosti, ki jih imajo pri doseganju strateških ciljev, so v ZDA na primeru, ki ga povzemamo v prispevku, dokazali izboljšanje ključnih kazalnikov delovanja njihovega oddelka policije.
Ključne besede: upravljanje informatike, investicije v informacijska sredstva, informacijska varnost, informacijska varnostna politika, upravljanje vrednosti, upravljanje tveganj.

Abstract

Achieving the Strategic Goals of Police Service by Improved Management of Investments in Information Technology

The existing model of Police Information Technology (IT) management is based on overcoming technical and technological challenges. At the same time the modern, business-oriented aspect of IT management that is based on effective investments and risk management in IT is largely ignored. Not understanding the value of individual information resources in achieving the business objectives and goals of the Police directly results in an inability to properly invest in them. The paper aims to show that it is necessary and feasible to assure the business objectives of the Police with effective investments management in IT. This can be achieved by proposing an extension of the security model, represented by the existing Information Security Policy. The implementation of the revised model calls for investments, particularly in supplementing the organization of management pyramid and in a modification of the existing performance of the business. The investment in human resources and the establishment of an environment which ensures an effective realization of modifications is of utmost importance. In the USA, the proposed model which is summarized in this paper has been implemented and has shown that by exposing the values that help accomplish strategic goals the key indicators that influence the efficiency of a particular police department can be improved.
Key words: IT management, IT investments, information security, information security policy, value management, risk management.

1 OPREDELITEV PROBLEMA

V vsaki organizaciji je osnovna vloga informatike podpora, vzdrževanje in razvoj poslovnih strategij in ciljev organizacije. Pri tem se pri posameznih poslovnih procesih, ciljih, tveganjih, investicijah in poslovnih varnostnih ciljih srečujemo z informacijskimi procesi, cilji, tveganji, investicijami in informacijskimi varnostnimi cilji. Pri tem praviloma poslovni varnostni cilji definirajo informacijske varnostne cilje. Za informacijska tveganja velja, da jih upravljamo v okviru poslovnih tveganj na taktični in predvsem na strateški ravni. Investicije v informacijska sredstva so podvržena upravljanju v okviru portfelja vseh poslovnih investicij. To je pristop pri upravljanju informatike, ki vključuje potrebe odjemalcev že v osnovi in zagotavlja upoštevanje poslovnih zahtev in pričakovanj zunanjih in notranjih deležnikov organizacije [9].

Vse, kar imamo na razpolago za izvajanje informatike in informacijskih procesov, so informacijska

sredstva. To so informacije, aplikacije, informacijska infrastruktura in ljudje, ki so vključeni v informacijske procese. Ta sredstva so tisto, s čimer imamo opravka v informatiki. Upravljamo jih, investiramo vanje in jih tudi prek investicij varujemo, da bi zagotovili zahtevano razpoložljivost, celovitost in zaupnost informacij. Omenjena sredstva in tri zahteve so osnovni parametri informacijske varnosti. So temelj sodobnega upravljanja informatike, kar običajno izrazimo prek dokumenta informacijske varnostne politike, ki narekuje cilje in načine za doseganje teh ciljev na področju informatike. [10]

Investicije omogočajo vzdrževanje obstoječega poslovanja, njegovo povečanje ali spremembo [8]. V večini primerov je skupni imenovalec investicij to, da pomeni velik ali celo pretežni del poslovne investicije investicija v informacijska sredstva in spremljajočo informacijsko varnost, saj se v večini primerov informatika izrazi kot poslovno kritična komponenta. Zato je pomen konkretnih poslovnih koristi podjetja ob tovrstnih investicijah tako velik. Še več: pomembno je upravljanje investicije v njenem celotnem življenjskem ciklu v okviru upravljanja poslovnih investicij – tako investicije v informatiko naj ne bi obravnavali kot samostojno celoto, temveč le kot investicijo, vpeto v mrežo drugih poslovnih investicij. Vsaka investicija v informatiko in informacijsko varnost mora imeti jasno poslovno korist, mora prispevati k poslovnim ciljem podjetja in mora biti ocenjena skozi prizmo doprinosa k poslovnim ciljem. Imeti mora svojo upravičenost in pričakovano razmerje med vložkom in koristnostjo. Povedano drugače: podjetja dosegajo svojo želeno in pričakovano poslovno korist predvsem z izbiro pravih investicij ter z učinkovitim upravljanjem izbranih investicij – tudi v informacijska sredstva. [11] [13]

Poslovno vrednost je pri storitvah, še posebno v javnem sektorju, težje predstaviti, ker je ocenjevanje uspešnosti investicij v informatiki v javnem sektorju težje, saj gre pri javnih organizacijah za poudarjeno večplastnost ocenjevanja, kar prispeva k povečani kompleksnosti ocenjevanja. Vendar je mogoče in potrebno te vrednosti definirati za uspešno upravljanje investicij v informatiko – tudi pri policiji. Na podlagi siceršnjih znanih nalog policije, njenih strateških ciljev in siceršnjih poslovnih vrednosti in/ali vrednot, ki so v policiji splošno sprejete in znane na vseh ravneh upravljanja, je mogoče izračunati poslovne vrednosti njenih informacijskih sredstev.

Pri tem trčimo na izziv kompleksnosti upravljanja informacijske varnosti, ki je tesno povezana z uspešnostjo upravljanja investicij v varovanje informacijskih sredstev [14]. Vrednosti informacijskih sredstev ne morejo določiti tehnični strokovnjaki sami, saj so vrednosti, ne glede na to, kako so te vrednosti izražene in s čim, domena strokovnjakov, ki so odgovorni za poslovanje policije. Pri tem je ključno spoznanje, da je informacijska varnost ne samo tehnično-tehnološki izziv, temveč tudi in predvsem poslovni [20] [12]. Brez tega spoznanja informacijska podpora delu policije ne more biti učinkovita in uspešna pri doseganju njenih strateških ciljev, kar bomo skušali dokazati v nadaljevanju.

V informacijsko varnostno politiko moramo vnesti dimenzijo poslovnosti, da prek ključnih parametrov informacijske varnosti – razpoložljivosti, celovitosti in zaupnosti – izražamo in postavljamo poslovne zahteve, ki jih mora izpolnjevati informatika [10]. To zahteva poznavanje poslovne vrednosti informacijskih sredstev. Te vrednosti so podlaga za odločanje o tem, koliko investirati vanje in kako ter koliko investirati v njihovo zaščito [7].

V prispevku s pomočjo indukcije in dedukcije, analize in sinteze ter na primeru realnega dogodka dokazujemo, da je policija trenutno vsaj formalno soočena samo s tehničnim vidikom varovanja informacij. Tega bo treba znati nadgraditi tako, da bodo z na novo osmišljeno informacijsko varnostjo dosegli poslovne cilje, ki so zapisani v dokumentih, kot so Temeljne usmeritve za pripravo srednjeročnega načrta razvoja in dela policije v obdobju 2008–2012 [17], Usmeritve in obvezna navodila za pripravo letnega načrta policije v letu 2012 [19] in Srednjeročni načrt razvoja in dela policije za obdobje 2008–2012 [16].

2 ANALIZA OBSTOJEČEGA STANJA UPRAVLJANJA INFORMACIJSKE VARNOSTI PRI POLICIJI

Pri analizi obstoječega stanja v policiji smo se osredinili samo na javno dostopne dokumente, na podlagi katerih smo sintetizirali obstoječe stanje. Pri tem ne vemo, ali so v pripravi morebitni novi, še neobjavljeni dokumenti, ki bi lahko ovrgli naše predpostavke o trenutnem stanju v policiji. Pri analizi stanja bomo uporabili tudi primer izginotja zaseženih elektronskih nosilcev podatkov. Pri deduktivnem pristopu bomo med drugim uporabili primer uspešnega upravljanja investicij v informacijska sredstva, s ka-

terim so na policijski postaji v ZDA dosegli zastavljene poslovne cilje [5].

Po vseh dostopnih formalnih virih sodeč, je pri policiji njena informacijska varnost v »pasivnem načinu upravljanja«. To pomeni, da so informacijski varnostni inženirji praviloma predvsem tehniki in tehnologi, ki se dnevno srečujejo z nevarnostmi, informacijskimi tveganji in kršitvami, novimi tehnologijami in z njimi povezanimi varnostnimi luknjami ter z drugimi težavami. So v nezavidljivem položaju in kot predstavniki relativno mladega področja so soočeni s pomanjkanjem temeljnih raziskav in orodij, s katerimi bi si pomagali pri izboljševanju informacijske varnosti, tako da bi upoštevali tudi njen poslovni vidik. Zagotavljati morajo skladnost z razdrobljenimi zahtevami, ki jih pred njih postavljajo standardi, okviri za delo in zakonodaja. Pri vsem tem jim verjetno ostane prav malo časa, da bi se pri svojem delu ukvarjali z ugotavljanjem vrednosti, ki jih informacijska tehnologija prinaša v poslovnem pomenu, ter z drugimi inovacijami pri upravljanju informacijskih sredstev.

Kot posledica problema nezadostnih kompetenc, ki jih imajo tehniki in tehnologi za samostojno upravljanje investicij v informacijska sredstva, se kaže zahteva po spremembi upravljavskih praks v informatiki. Prakse, ki so bile še do včeraj aktualne, postajajo premalo kompleksne in nezadostne. Še včeraj namreč nismo investicijam v informatiko namenjali tolikšne pozornosti, kot jo zahteva današnji čas. Videti je, kot da postaja proučevanje uspešnosti investicij v informacijska sredstva osrednja tema, s katero se ukvarjajo ali se bodo ukvarjali vodje informatike v organizacijah. [8]

2.1 Poslovni cilji policije

Pri policiji ne gre iskati poslovnega cilja v razmerju med vloženim denarjem in zaslužkom, ki ga prinese vloženi denar, temveč v temeljnih usmeritvah za delo policije, ki se s časom bistveno ne spreminjajo. Na prvem mestu med najpomembnejšimi strateškimi cilji so preprečevanje, odkrivanje in preiskovanje kriminalitete [17]. V usmeritvah [19] so med pomembnejšimi cilji eksplicitno navedeni zmanjšanje gospodarske in kibernetske kriminalitete, informacijsko povezovanje, analize stanj itn. [19]. Vse to so poslovni cilji policije.

Poleg tega je v temeljnih usmeritvah podana še splošna zahteva, ki pravi [17]: »Izdelajte celovito strategijo ITK (informatika in telekomunikacije) za zagotavljanje optimalne organizacije in vsebine dela.« Gre za zelo splošno zahtevo, brez nakazanih ciljev na ravni informatike ali nakazanih načinov za dosego teh ciljev. Iz teh dokumentov tako ni razbrati neposrednih zahtev za informacijsko varovanje. Ni razbrati, s katerimi informacijskimi sredstvi bomo podprli poslovne zahteve in kako. Ni nakazane povezave med poslovnimi cilji in cilji informatike, ki bi izhajali iz informacijske varnostne politike.

Dokument, ki prehaja iz strateške na operativno raven, je Srednjeročni načrt razvoja in dela policije za obdobje 2008–2012 [16]. V njem je med mnogimi strateškimi cilji in zahtevami mogoče zaznati dovolj natančno določene programe s področja informacijske tehnologije. Med takšnimi so:

1. posodobitev forenzično-informacijske tehnologije,
2. spremembe in dopolnitve informacijskega sistema s področja kriminalitete,
3. prehod na schengenski informacijski sistem druge generacije (SIS II),
4. informacijsko-telekomunikacijska podpora policijskemu delu (mobilni in stacionarni sistem avtomatske prepoznave registrskih tablic – ANPR, sistem avtomatskega lociranja vozil – GPS/AVL, mobilni dostop do podatkov, digitalni radijski sistem za prikrito kriminalistično delovanje, uvedba digitalnega sprejemnika LEO, termovizija idr.),
5. sprejetje strategije informacijsko-telekomunikacijskega sistema policije,
6. izdelava metodologije prikaza podatkov o varnostnih dogodkih v okviru geografskega informacijskega sistema na intranetu policije in izdelava programa za časovno in prostorsko razporejanje policijskih patrulj na podlagi teh podatkov.

Iz tega (nepopolnega) seznama je razbrati, da je – poleg informacijskih rešitev – v igri tudi izdelava strategij in metodologij. Vendar nikjer ni mogoče zaznati, da bi bila eksplicitno navedena zahteva po izdelavi ali pripravi rešitve, strategije ali metodologije tako, da bo v zvezi z informatiko upoštevan tudi poslovni vidik policije.

2.2 Umeščenost urada za informatiko in telekomunikacije v organiziranost policije in njegove ključne naloge

V katalogu informacij javnega značaja policije [20] je mogoče razbrati, da je v sestavi policije tudi Urad za informatiko in telekomunikacije. To je eden od

sedmih organizacijskih enot na ravni generalne policijske uprave. Takšna organiziranost daje področju informatike pričakovano vplivnost.

Pri pregledu nalog, ki jih izvaja urad, sta dve izmed štirih točk [20]:

1. upravlja z informacijskim in telekomunikacijskim sistemom policije;
2. pripravlja, izdeluje in nadzira izvajanje srednjeročnih in letnih načrtov razvoja ter nabave programske in strojne opreme informacijskega in telekomunikacijskega sistema policije ter elektronske opreme in sistemov tehničnega varovanja.

Iz teh nalog je razvidno, da je urad odgovoren za nabavo (to je investicije) in delovanje informacijskih sredstev policije.

Pri podrobnejšem pregledu nalog, ki jih izvaja urad, največkrat zasledimo besedne zveze in pojme, kot jih prikazuje tabela 1. Ob analizi besedila z opisom nalog lahko ugotovimo, da se beseda nabava, ki jo lahko v našem primeru jemljemo kot sopomenko besede investicija, pojavi samo enkrat. Analizirano besedilo je sicer vsebovalo 393 besed, med katerimi jih je 220 različnih. Za ta prispevek so se nam zdele še posebno zanimive besedne zveze:

1. načrtovanje, razvoj, uvajanje in vzdrževanje,
2. standardizacija,
3. strokovna pomoč,
4. zagotavljanje neprekinjenega delovanja,
5. okrevanja po izpadih,
6. zaščita in varovanje,
7. testiranje,
8. upravljanje z varnostnimi dogodki in incidenti.

Besede iz tabele 1 ter zgornjih osem pojmov in besednih zvez nakazujejo predvsem tehnično ali tehnološko usmerjenost pri določanju (in predpostavljamo tudi izvajanju) nalog. Torej imamo pri investicijah opraviti predvsem s tem, da se v policiji trudijo doseči tehnične zahteve in standarde (zagotovo v okviru obstoječega proračuna), pri čemer poslovne vrednosti niso omenjene. Iz nalog je torej razvidno, da se v policiji sprašujejo:

1. Delamo pravilno? Gre za vprašanje arhitekture informacijske tehnologije.
2. Izvajamo informacijske procese dovolj dobro? Pri tem se sprašujemo o kakovosti servisov.

Smiselno bi bilo, da se sprašujejo še o dveh vprašanjih, in sicer:

1. Delamo prave stvari? So investicije pravilne? Pri tem gre za strateška vprašanja.
2. Kolikšne in kakšne so dejanske koristi od investicije? Kolikšne in kakšne so glede na pričakovanja? Gre za vprašanje poslovne koristi.

Tabela 1: **Najpogosteje uporabljene besede pri opisu izvajanja nalog urada za informatiko in telekomunikacije policije, ki jih je zaslediti v informacijah javnega značaja (statistika je izdelana s spletno aplikacijo Textalyzer [22])**

Beseda	Pojavitev	Frekvenca	Rang
sistemov	17	4,3 %	1
upravljanja	15	3,8 %	2
podatkov	14	3,6 %	3
opreme	13	3,3 %	4
načrtovanja	11	2,8 %	5
uvajanja	10	2,5 %	6
policije	10	2,5 %	6
storitev	8	2 %	7
razvoja	8	2 %	7
vzdrževanja	6	1,5 %	8
varovanja	6	1,5 %	8
drugih	5	1,3 %	9
elektronske	4	1 %	10
zaščite	4	1 %	10
informacijskih	4	1 %	10
sodelovanja	3	0,8 %	11
vseh	3	0,8 %	11
tehničnega	3	0,8 %	11
izvajanja	3	0,8 %	11
standardizacije	3	08 %	11

Iz ciljev in nalog urada (ki je odgovoren za izvajanje informacijske politike v policiji) ni razbrati, da bi se njihovo delo pri investicijah v informacijska sredstva vrtelo okrog poslovnih vrednosti – ni zaznati povezave med poslovnimi cilji in investicijami v informatiki. Ta ugotovitev je podobna, kot je bila opisana pri analizi poslovnih ciljev policije, vendar tokrat z diametralno nasprotnega gledišča.

2.3 Informacijska varnostna politika policije

Informacijska varnostna politika policije [18] je najpomembnejši in glavni dokument, na podlagi katerega policija upravlja z informacijskimi sredstvi in tveganji. Z njo vodstvo policije prevzema pooblastila in odgovornosti za upravljanje tveganj (v bistvu varnosti) njenih informacijskih virov. Eksplicitno se pri definiciji njenega namena v drugem členu sklicuje na standardno zagotavljanje razpoložljivosti, celovitosti

in zaupnosti informacij. Pri ciljih v tretjem členu navaja, da je treba:

1. ugotoviti vrednost informacijskih sredstev (ki pa niso predhodno definirana in lahko le sklepamo, da so avtorji dokumenta imeli v mislih aplikacije, infrastrukturo, informacije in ljudi kot tista informacijska sredstva, s katerimi »izvajamo« informatiko) prek analize informacijskih tveganj;
2. ugotoviti in razumeti ranljivosti teh sredstev ter določiti njihovo izpostavljenost tveganjem;
3. v tretji točki tretjega člena dokument preskoči na splošno upravljanje tveganj (kar že samo po sebi vključuje zgornja dva cilja kot potrebne aktivnosti pri upravljanju tveganj – npr. ISO 31000:2009 [3], ISO 31010:2009 [2], ISO/IEC 27005:2011 [4]).

Kot zadnji, četrti, večji cilj eksplicitno navede deset ciljev, med katerimi so (ponovno) navedeni zagotavljanje razpoložljivosti, celovitosti in zaupnosti informacij in še sedem drugih.

Na koncu se dokument sklicuje na osem področnih informacijskih varnostnih politik, ki niso predmet tega prispevka, vendar se iz njihovega imena in namena da sklepati, da se ne nanašajo na kakršne koli poslovne cilje policije.

Informacijska varnostna politika se tako v nobenem delu ne sklicuje na poslovne cilje policije. Poslovni cilji pri upravljanju informatike niso vključeni. Obravnavan je le tehnološki vidik upravljanja. Še manj so poslovni cilji predstavljeni kot temelj, na katerem bi slonelo upravljanje in s katerimi bi bilo prežeto temeljno poslanstvo in upravljanje informatike v policiji.

Pri upravljanju sistema vedno upoštevamo neko temeljno poslanstvo in takšen pristop se bolj ali manj prenaša tudi na upravljanje njegovih podsistemov. Zato verjamemo, da so poslovni cilji pri upravljanju informatike nekako v ozadju, verjetno v različnih primerih sicer upoštevani različno, vendar niso sistemsko vgrajeni v upravljanje informatike. Ali je takšno stanje zadovoljivo? Po stari, vendar še zdaleč ne zastareli metodologiji ugotavljanja zrelosti takšno stanje spada na prvo raven zrelosti [1], na kateri je aktivnost poznana le *de facto* in ne *de jure*. Z drugimi besedami to pomeni, da v policiji ni aktivnosti, ki bi se ukvarjala z investicijami v informacijska sredstva na podlagi poslovne vrednosti, ki jo prinaša informatika. Vsaj uradno ni (raz)poznane nikakršne dejavnosti v zvezi s tem. Tako tudi ne (pre)poznamo tveganj, ki bi jih bilo treba upravljati v povezavi s to dejavnostjo, in ni notranjega nadzora nad njo – seveda govorimo v kontekstu poslovnega vidika upravljanja informatike v policiji.

2.4 Primer: analiza vrednosti odtujenega zaseženega nosilca elektronskih podatkov

Zasežene elektronske naprave so lahko ključne pri doseganju poslovnih ciljev policije. Ob izgubi ali odtujitvi zaseženih nosilcev elektronskih podatkov (npr. diskov iz računalnika) so načeti temeljni poslovni cilji policije, kot sta »preprečevanje, odkrivanje in preiskovanje kriminalitete« ali »povečevanje ugleda policije«. Pri analizi realnega primera [21] so za tematiko tega prispevka zanimiva predvsem dejstva.

1. Zaradi neustreznih prostorov, kjer so shranjene zasežene elektronske naprave in elektronski nosilci podatkov na oddelku za računalniško preiskovanje sektorja kriminalistične policije Policijske uprave Ljubljana, bi bilo treba urediti skladiščni prostor z ustrezno tehnologijo, ki bi služila večji sledljivosti in mobilnosti [15]. Avtorja v nadaljevanju pravilno ugotavljata, da ne gre samo za neustrezne prostore, temveč gre za neustrezne pristope v procesu skladiščenja zaseženih predmetov.
2. Seveda se postavlja vprašanje, ali so zasežene elektronske naprave to, kar spada v okvire informacijske varnostne politike (torej veljajo principi upravljanja, ki veljajo za informacijska sredstva). Odgovor je pritrdilen. Pri zaseženih diskih gre za informacije, ki pomenijo enega od štirih informacijskih sredstev, s katerimi izvajamo informacijske procese [6]. Ta sredstva varujemo in investiramo vanje. Torej mora biti skladiščenje elektronskih naprav in nosilcev elektronskih podatkov urejeno v skladu z informacijsko varnostno politiko policije.
3. Zaradi povečanja količine zaseženih elektronskih naprav in elektronskih nosilcev podatkov sektorja kriminalistične policije PU Ljubljana bo v prihodnje prišlo do logističnih zapletov pri njihovem hranjenju in skladiščenju. Na oddelku se zavedajo, da bo treba nekaj storiti z opravili, povezanimi z njihovim upravljanjem. Takšna opravila so evidentiranje, označevanje, hranjenje, sprejem in vračanje zaseženih elektronskih nosilcev podatkov, povezovanje zaseženih elektronskih nosilcev podatkov s spisi, sledljivost zaseženih elektronskih naprav in elektronskih nosilcev podatkov

od zasega do vrnitve itd. Z drugimi besedami: na oddelku se zavedajo, da bo treba investirati v spremembo poslovanja.

Vprašajmo se, ali se je mogoče tovrstnim problemom izogniti z dopolnitvijo obstoječe informacijske varnostne politike in iz nje izhajajočih področnih navodil ali usmeritev. Odgovor je pritrdilen, če je ta zastavljena tako, da bi se v konkretnem primeru vprašali, kolikšna bi bila poslovna škoda v primeru odtujitve ali izgube elektronskega nosilca podatkov. S strogo tehnično-tehnološkega vidika nas poslovna škoda sploh ne zanima in nimamo pripravljenega, dogovorjenega, splošno sprejetega in predpisanega ogrodja za njeno oceno. Zato je ne moremo »izračunati«. Seveda jo posamezniki slutijo, vendar ta slutnja temelji na subjektivnem odnosu posameznika do nje. Samo slutnja pa je premalo, če želimo vrednosti in tveganja, povezana z vrednostmi, upravljati učinkovito. Podobno kot s tehnološkega je treba upravljati tveganja informacijskih sredstev tudi s poslovnega vidika. Seveda v tem primeru delamo z vrednostmi iz poslovnega sveta in ne tehnološkega.

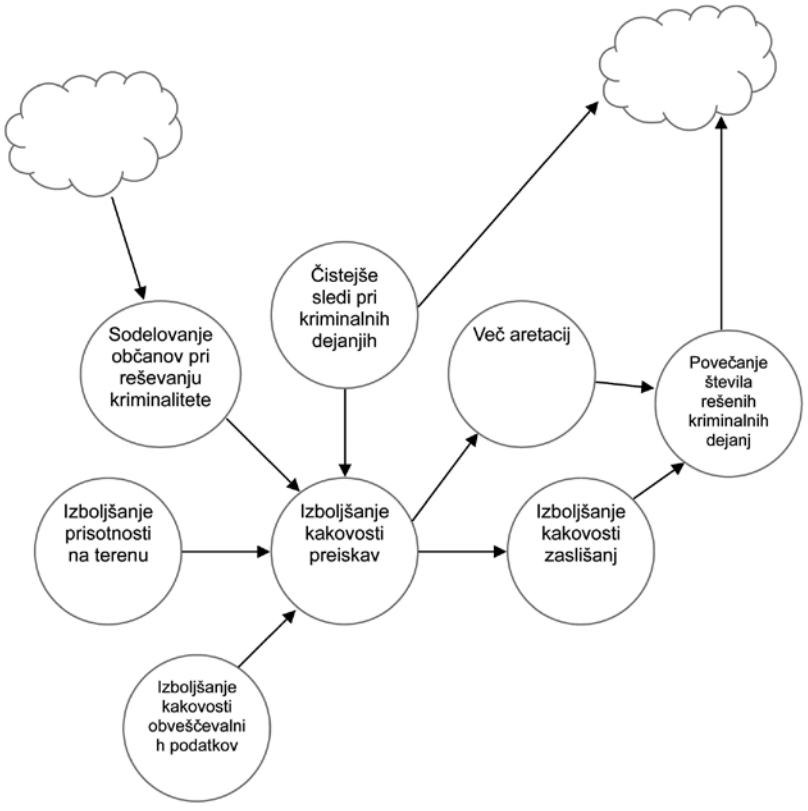
Torej bi morali informacijska varnostna politika in množica dokumentov, ki izhajajo iz nje (področne politike, organizacijska navodila itd.) vsebovati tudi poslovne cilje policije. Če bi bilo tako, bi bilo mnogo manj možnosti, da bi se primeri omenjene odtujitve »izmuznile« sistemskemu pristopu in nas presenetile. Posamezna informacijska sredstva bi imela svojo poslovno vrednost in glede na to vrednost tudi predpisano zaščito. Sedaj, ko se vrednosti vsesplošno ne zavedamo, oziroma ta ni v prvem planu, obstaja večja verjetnost, da sredstva ne bodo ustrezno zaščitena. Ena bodo preveč, druga premalo. Ljudje, ki se ukvarjajo s tehniko, ne morejo vedeti, koliko je treba kaj varovati, če ne upoštevajo poslovnega vidika vrednosti posameznih sredstev.

3 INVESTICIJE V INFORMATIKO NA PODLAGI PRIMERA SREDNJE VELIKE POLICIJSKE POSTAJE V ZDA

Okvir Val IT, ki podaja pristope za uspešno upravljanje investicij v informacijska sredstva [8], je poznan že dolgo. Prve različice tega dokumenta so bile objavljene že leta 2006. Ni pa bilo objavljenih veliko kritičnih analiz o upravljanju tovrstnih investicij. Posebno malo je objavljenih tovrstnih analiz v javnem sektorju. Ena od objavljenih študij investicij v informatiko v javnem sektorju je Val IT Case Study: Value Governance – Police Case Study [5]. V njej je opisano, kako so z osredinjenjem na poslovne cilje v srednje veliki ameriški policijski postaji dosegli zelo dobre rezultate po spremembah njihovega poslovanja. S pomočjo Val IT so upravljali investicije v informacijska sredstva skozi njihov celoten cikel.

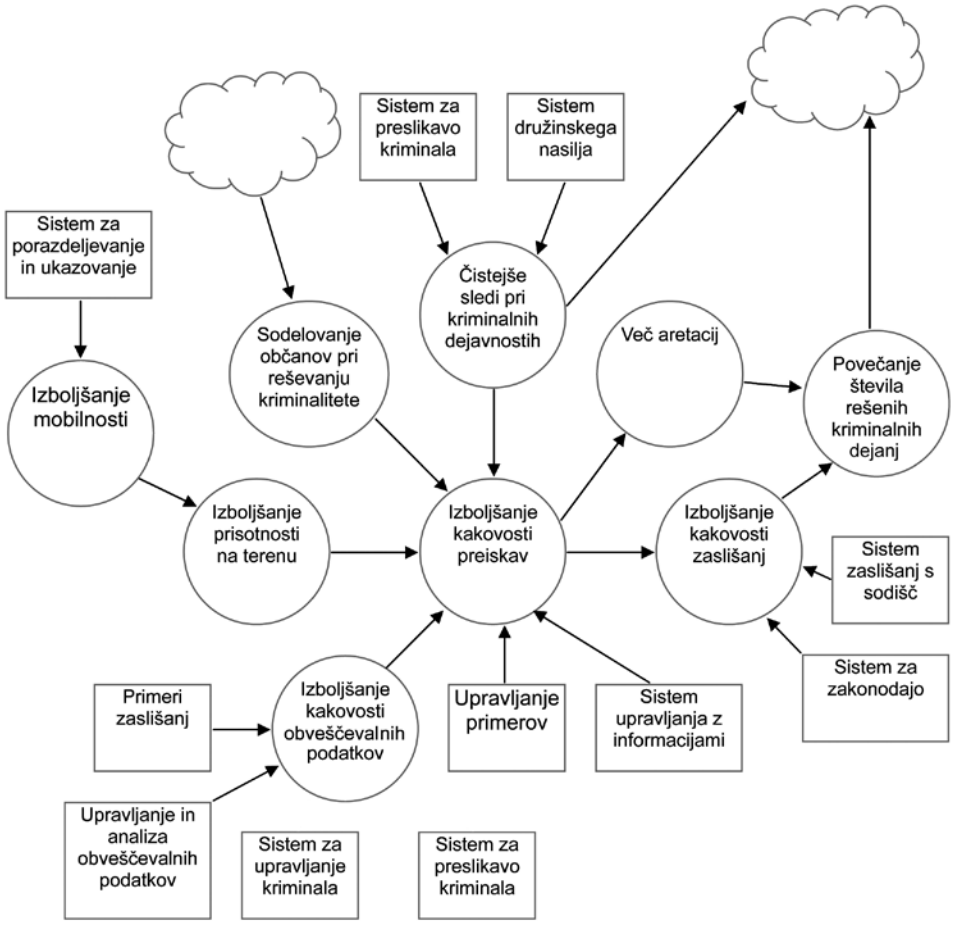
Upoštevali in razpoznali so veliko komplementarnih aktivnosti in dejstev, ki pripomorejo k doseganju strateških ciljev. Med temi so tudi zmanjšanje kriminalitete, povečanje rešenih primerov, zmanjšanje administrativnega dela, zanesljivo delovanje informacijskih sredstev v kritičnih situacijah in podobno. V življenjskem ciklu investicije so vseskozi zagotavljali čisto sliko pri postavljanju odgovornosti in pri meritvah doseženih rezultatov. Študija temelji na petletnih izkušnjah, katerih začetek sega v leto 1999. Šlo je za pomembno investicijo, ki jo je podprla politika in je zahtevala velike časovne in druge nematerialne vložke njihove policije. Izbrati so morali prave investicije v zaostrenih investicijskih pogojih in poročati o poslovni uspešnosti teh investicij političnim predstavnikom, ki so vsako leto posebej odločali o nadaljevanju financiranja.

Poslovno vrednost, ki jo prinaša investicija v informacijska sredstva, so merili z doseganjem poslovnih ciljev in ne z denarnim tokom ali vračilom naložbe. Določali so, kolikšen je tisti del vrednosti, ki ga prinaša informatika pri doseganju posameznega cilja iz njihovega poslovnega načrta. Tako je najprej nastal načrt ciljev, ki so medsebojno povezani. Del tega načrta prikazuje slika 1. V krogih so cilji, usmerjene puščice pa kažejo na njihovo medsebojno povezanost. Smer puščice prikazuje, kateri cilji podpirajo druge pri njihovem uresničevanju. Seveda je treba za dosego vsakega posameznega cilja (to so v bistvu izboljšave obstoječega poslovanja) izvajati neke iniciative.



Slika 1: **Nekatere aktivnosti v procesu kriminaliteta in njihove medsebojne odvisnosti (povzeto po [5])**

Za doseganje cilja *izboljšanje obveščevalnih podatkov* je bilo treba vpeljati *sistem za upravljanje kriminalitete* (ki je informacijski sistem), medtem ko je bilo treba pri doseganju cilja *več aretacij* reorganizirati obstoječe poslovanje in uvesti nov oddelek v policijsko postajo. Že ob tem želimo poudariti pristop, pri katerem se po definiranju poslovnih zahtev lahko začnejo jasneje kazati druge iniciative (to je cel nabor potreb), med katerimi so tudi iniciative za informacijske zahteve. Torej iz poslovnih zahtev prehajamo na iniciative, povezane z informacijskimi sredstvi – informacijskih iniciativ pa ni brez jasnih poslovnih potreb. Slika 2 prikazuje informacijske iniciative za doseganje ciljev s slike 1. V tem prispevku se osredinjamo na informatiko in zato pišemo le o informacijskih iniciativah in ne o drugih, ki tudi obstajajo in se jih moramo zavedati.



Slika 2: **Nekatere aktivnosti v procesu kriminaliteta, njihove medsebojne odvisnosti in podpora z informacijskimi sistemi (povzeto po [5])**

Na podlagi slike 2 (ki v tem prispevku prikazuje le del ciljev in informacijskih iniciativ za doseganje le-teh) je mogoče opredeliti portfelj posameznih informacijskih projektov, ki jih je treba preslikati v delež zadovoljevanja posameznih poslovnih ciljev. Upoštevamo tudi, da lahko z enim informacijskim projektom podpremo več posameznih poslovnih ciljev, kar dodatno uteži takšen projekt. V primeru policijske postaje, ki jo opisujemo, so za vsak posamezni projekt ocenjevali:

1. njegov neposredni prispevek k doseganju posameznih poslovnih ciljev; ta prispevek so razvrstili glede na pomembnost v več razredov;
2. pomembnost, ki ga ima posamezen poslovni cilj (ki ga sicer podpira opazovani projekt) za poslovanje policije v celoti;
3. poleg prispevka, ki ga ima posamezni projekt za doseganje poslovnih ciljev, so projekt ocenili še s klasičnimi ocenami, ki so:
   a) prihranek časa, ki ga bo omogočila izvedba projekta pri delu na policijski postaji v enem letu;
   b) prihranek vloženega dela (ljudi), ki ga bo omogočila izvedba projekta pri delu na policijski postaji v enem letu;
   c) prihranek denarja.

S pomočjo točkovanja so nato odločili o pomembnosti projektov (kar pomeni pomembnost razpoložljivosti, celovitosti in razpoložljivosti informacij) in s tem posledično o pomembnosti investicij (ki omogočajo spremembo, razširitev ali le vzdrževanje obstoječega stanja) v informacijska sredstva (informacije, aplikacije, infrastruktura in ljudje).

Z osredinjanjem na poslovne cilje pri vodenju investicij (projektov) v informacijska sredstva in s sistematičnim pristopom pri njihovem upravljanju so dosegli zastavljene kratkoročne cilje, medtem ko za doseganje nekaterih dolgoročnih ciljev v omenjeni

analizi primera ni opisa, ker je za analizo njihovega doseganja potrebna časovna distanca. V študiji je povzet način upravljanja projektov in za investicije pomembnejših projektnih mejnikov. Na kratko so opisani postopki za razvrščanje projektov po prioritetah in za merjenje učinkovitosti. Pri tem so sledili navodilom, ki izhajajo iz procesov, ki jih definira Val IT. Med temi so pomembnejša navodila za določanje odgovornosti in pooblastil – tabela RACI (glej Val IT [5] in COBIT 5 [9]).

Verjetno so strateški cilji na področju kriminalitete vseh policijskih postaj v razvitem svetu podobni. Te cilje predpisujejo na državni ravni, same policijske postaje pa ravnajo skladno z njimi. Upoštevaje dejstvo, da se strateški cilji policije in cilji v opisanem primeru v veliki meri prekrivajo, lahko sklepamo, da opisani primer daje dovolj trdno podlago za upoštevanje smiselnosti upravljanja investicije v informacijska sredstva na podlagi smernic, ki nam jih ponuja Val IT tudi pri policiji. Izzivi in cilji so tako v opisanem primeru kot pri slovenski policiji v bistvu identični. Investicije na podlagi resnične vrednosti posameznih informacijskih sredstev bi, kot kaže primer, lahko tudi pri slovenski policiji pripomogle k temu, da bi bilo njeno poslovanje uspešnejše ob sočasnem zmanjšanju dela, ki ni tisto, kar pričakujemo od policistov. Tako torej na podlagi raziskave in primerjave predlagamo, da tudi slovenska policija pristopi k upravljanju investicij v informacijska sredstva na podlagi priporočil Val IT.

4 SKLEP

Model poslovnega upravljanja informacijske varnosti je nedvomno bistveno kompleksnejši in pomembnejši, kot smo ga bili vajeni videti in sprejemati pri modelu tehnično-tehnološkega upravljanja. Po eni strani gre za evolucijo, prek katere spoznavamo in priznavamo nove elemente vpliva, ki jih ima informatika na poslovanje, po drugi strani pa gre za dejstvo, da postaja informatika vse večji in pomembnejši del poslovanja, s tem pa se močno veča tudi njen vpliv na poslovanje.

Posledično se ta proces evolucije kaže tudi v zahtevi po spremembi upravljavskih praks. Prakse, ki so bile še do včeraj aktualne, postajajo premalo kompleksne in nezadostne. Še včeraj namreč nismo poslovnemu vidiku informacijske varnosti namenjali tolikšne pozornosti, kot jo zahtevajo današnje razmere. Videti je, kot da postaja proučevanje uspešnosti investicij v informacijska sredstva osrednja tema, s katero se ukvarjajo ali se bodo ukvarjali tako vodje informatike v podjetjih, kako tudi sam vrh upravljavske piramide. Pri tem gre tako za zasebni kot za javni sektor, kamor spada tudi policija. Med obema sektorjema je razlika samo v tem, da je ocenjevanje poslovne uspešnosti investicij v informacijska sredstva v javnem sektorju težje, saj gre pri javnih organizacijah za poudarjeno večplastnost ocenjevanja, kar prispeva k dodatni kompleksnosti ocenjevanja.

Pogoj za določanje poslovne koristi investicije v informacijska sredstva je, da najprej pri odgovornih za poslovne investicije (to je poslovodstvo) dosežemo, da ti razumejo, kako informatika prispeva k doseganju zastavljenih nalog na področju preprečevanja kriminalitete. Nato je treba doseči to razumevanje na vseh ravneh upravljanja policije. Na vseh ravneh upravljanja mora biti jasno, kako in koliko lahko neka investicija v informacijska sredstva omogoči realizacijo posamezne naloge policije. To je običajno izvedeno z dobrim načrtovanjem komuniciranja z internimi javnostmi in presega okvire tega prispevka.

V prispevku smo opozorili, da se običajno najprej sprašujemo ali počnemo stvari pravilno, vendar kmalu presežemo to stanje in se začnemo spraševati o koristih, ki jih prinaša naše delo. Pri informacijski varnosti to pomeni, da začenja poslovni del upravljati z informatiko in ne govorimo več o upravljanju informatike s strani informatikov tehnikov. Tako zagotovimo neposredno povezavo med tem, kar se dogaja na področju informatike, in med tem, kar se dogaja na poslovnem področju. S tem presežemo predsodek, da informacijski projekti stanejo, poslovni projekti pa prinašajo. Takšen pogled sploh ni nov, že velikokrat je preizkušen v praksi, a na področju informacijske varnosti je tokrat uporabljen na novo. Tudi pri policiji smo ali pa bomo kmalu na točki, ko se bo treba odločiti, kdaj dvigniti kakovost njenega poslovanja z dopolnitvijo obstoječega modela upravljanja njenih informacijskih sredstev in kako.

Učinkovitosti v tem prispevku predlaganega modela ni mogoče dokazati, dokler ta ni pravilno implementiran v konkretnem primeru z vsemi potrebnimi predpostavkami za njegovo implementacijo. Tudi sama implementacija modela zahteva investicijo z vsemi tveganji, ki spremljajo vsako investicijo. Vendar brez investicij ni mogoče nadaljevati v nedogled. Investicija v dopolnjen model informacije varnosti

bi, glede na izkušnje od drugod, povečala kompetence in ugled policije.

LITERATURA

[1] Humphrey, W. (1988). Characterizing the software process: a maturity framework. IEEE Software 5 (2), 73–79.

[2] International Organization for Standardization. (2009). IEC/ISO 31010: Risk management – Risk assessment techniques; Edition 1.0.

[3] International Organization for Standardization. (2009). ISO 31000: Risk management - Principles and guidelines; First edition.

[4] International Organization for Standardization. (2011). ISO/IEC 27005:2011; Information technology - Security techniques - Information security risk management, Second edition.

[5] IT Governance Institute. (2006). Enterprise Value: Governance of IT Investments, The ING Case Study, Rolling Meadows: IT Governance Institute.

[6] IT Governance Institute. (2007). COBIT 4.1, Rolling Meadows: IT Governance Institute

[7] IT Governance Institute. (2008). Enterprise Value: Governance of IT Investments, Getting Started With Value Management, Rolling Meadows: IT Governance Institute.

[8] IT Governance Institute. (2008). Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, Rolling Meadows: IT Governance Institute

[9] IT Governance Institute. (2011). COBIT 5, Rolling Meadows: IT Governance Institute

[10] Jereb, B. (2007). Informatika in računalništvo. Celje: ABakus in Jereb.

[11] Jereb, B. (2008). Val IT - Upravljanje IT investicij. Zbornik referatov. Ljubljana: Slovenski inštitut za revizijo.

[12] Jereb, B., & Brumen B. (2010). Upravljanje IT tveganj s pomočjo Risk IT. Dnevi slovenske informatike. Uravnotežite naložbe, tveganja in razvoj za uspeh. Ljubljana: Slovensko društvo Informatika.

[13] Jereb, B., Cvahte, T., & Rosi, B. (2012) Managing logistics investments by using experience from IT. XII. znanstveni skup s međunarodnim sudjelovanjem Poslovna logistika u suvremenom menadžmentu, Osijek: Ekonomski fakultet.

[14] Jereb, B., Cvahte, T., & Rosi, B. (2012). Val IT v logistiki. Dnevi slovenske informatike. Ustvarimo nove rešitve! Ljubljana: Slovensko društvo Informatika.

[15] Matjašič, K., & Jereb, B. (2012). Študija primera upravljanja zaseženih nosilcev elektronskih podatkov. 13. slovenski dnevi varstvoslovja, Zbornik povzetkov (str. 24). Ljubljana: Fakulteta za varnostne vede.

[16] Republika Slovenija, Ministrstvo za notranje zadeve. (2007). Srednjeročni načrt razvoja in dela policije za obdobje 2008-2012. Pridobljeno na http://www.policija.si/images/stories/O_Policiji/NacrtiPorocila/nacrtDela2008-2012.pdf.

[17] Republika Slovenija, Ministrstvo za notranje zadeve. (2007). Temeljne usmeritve za pripravo srednjeročnega načrta razvoja in dela policije v obdobju 2008Ð2012. (2007). Pridobljeno na http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/SOJ/word/2011/temeljne_usmeritve_2008-2012.doc.

[18] Republika Slovenija, Ministrstvo za notranje zadeve. (2010). Informacijska varnostna politika Policije – krovna politika, Različica 1.1. Pridobljeno na http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/JAVNA_NAROCILA/PRILOGA_7-Varnostna_politika.pdf.

[19] Republika Slovenija, Ministrstvo za notranje zadeve. (2011). Usmeritve in obvezna navodila za pripravo letnega načrta dela policije v letu 2012. Pridobljeno na http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/DPDVN/Nadzor/Usmeritve_za_leto_2012.pdf.

[20] Republika Slovenija, Ministrstvo za notranje zadeve. (2012). Katalog informacij javnega značaja, Policija. Pridobljeno na http://www.policija.si/index.php/informacije-javnega-znaaja/katalog-ijz/974-urad-za-informatiko-in-telekomunikacije.

[21] Slovenska tiskovna agencija. (2011). Izginili ključni dokazi v primeru Magajna, Pridobljeno na http://www.iusinfo.si/DnevneVsebine/Novice.aspx?id=71649.

[22] Textalyser. (2012). Pridobljeno na http://textalyser.net/index.php?lang=en#analysis.

▪

Borut Jereb je predavatelj na Fakulteti za logistiko. Leta 1991 je uspešno zagovarjal doktorat s področja računalniških znanosti na Univerzi v Ljubljani. Od leta 1991 do leta 1992 je kot vabljeni profesor raziskoval in poučeval na Oregon State University. Po vrnitvi v Slovenijo si je skoraj dve desetletji kot svetovalec in kot vodja v podjetjih in v javnem sektorju pridobil veliko praktičnih izkušenj na področju optimizacije poslovanja. V zadnjem času se ukvarja predvsem z upravljanjem tveganj, IT-varnostjo, standardizacijo in zakonodajo.

Metamorfoza tehnološko-uporabniške fascinacije v dejansko informacijsko družbo

József Györkös
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova ul. 17, 2000 Maribor
Jozsef.Gyorkos@uni-mb.si

Izvleček

Kljub temu da je têrmin informacijska družba v široki uporabi že od devetdesetih let 20. stoletja, je zares zaživel šele s široko uporabo informacijskih tehnologij v povezavi z mobilnim dostopom. V sorodnih primerih družbeno vplivnih tehnologij se praviloma zgodi, da visokotehnološko pogojene uporabniške prakse povzročijo prehod nove/inovativne tehnologije v samoumevno infrastrukturo. Ocenjujem, da samoumevna vseprisotnost informacijsko-komunikacijskih tehnologij v raziskovanju in inoviranju postavlja še višje zahteve ter da njihova infrastrukturna danost ne povzroča zasičenja, temveč prav obratno, v multidisciplinarnih implikacijah širi obzorja mogočeganega. Pojem konvergence še ni izčrpal vseh svojih potencialov in se je doslej javno in vidno odražal predvsem na medijskem področju. Konvergenca pridobiva nove razsežnosti v obliki združevanja tehnoloških, naravoslovnih ter humanistično-družboslovnih ved. V prispevku bo identificiran izbor propulzivnih raziskovalnih področij, ki jih ocenjujem kot uporabniško atraktivna in tržno zanimiva in ki v diverzificiranih uporabniških praksah s pridom izkoriščajo infrastrukturno zrelost informacijsko-komunikacijskega tehnološkega cikla.

Ključne besede: informacijska družba, uporabniške prakse, konvergenca, odprti podatki, multidisciplinarnost.

Abstract

Metamorphosys of Technology-Based User Fascination into Authentic Information Society

The term information society has been in wide use since the mid-nineties, however it was only through mobile access that information and communication technologies (ICT) reached a broad community of users and we were truly able to talk about an information society. Historically, technologies with high societal influence usually evlove into an inevitable long-term infrastructure. The omnipresence of information and communication technologies sets higher requirements for research and innovation. In reality the ICT infrastructure does not lead to a saturation of research and innovative efforts, on the contrary, it opens up new possibilities through multidisciplinarity. Convergence as a term has not exhausted all of its potentials yet, it is gaining ground in new dimensions of joint cooperation between technological, natural, humanistic and social sciences. In this paper an identification of propulsive research areas is made based on observations of mature ICT-based infrastructures. Such cases are marked by their continuous and diversified user scenarios and show appropriate market viability.

Key words: information society, user experience, convergence, open data, multidisciplinarity.

1 UVOD

Konceptualizacija informacijske družbe izpred dobrega desetletja resnično lahko deluje zastarelo, vendar je danes že znameniti Webstrov članek [23], v katerem se avtor sprašuje o obstoju in bistvu informacijske družbe kot tehnološko-sociološkem fenomenu, pridobil nov pomen. Medtem ko se Webster pridružuje Castellsovemu razmišljanju o »ukinitvi« pojma informacijska družba ([3], str. 21–25), po tehtni analizi z vidika sprememb uporabe tehnologije, sprememb na področju dela, prostora in kulture, tudi s pomočjo Giddensovega argumenta o refleksivnosti postmoderne družbe ([23], str. 30–31) ponuja pojem *družba znanja* kot najbolj primeren za opis družbenih pojavov, do katerih je privedla dnevna uporaba informacijsko-komunikacijskih tehnologij.

Ne glede na pomisleke vodilnih akademskih avtoritet se je pojem informacijska družba prijel v okviru političnega *establišmenta* tako na ravni Evropske unije,[1] kakor tudi Združenih narodov,[2] res pa je na ravni Evropske unije v zadnjem obdobju zaznati or-

[1] Evropska unija je besedno zvezo informacijska družba inicirala z znamenitim Bangemannovim poročilom [5] in jo kasneje utrdila s tako poimenovanim generalnim direktoratom v svoji organizacijski strukturi ter sorodno imenovanimi ključnimi strategijami za podporo krovni lizbonski strategiji. Serija strategij eEvropa (eEurope) iz preteklega desetletja je dobila nov koncept v okviru Digitalne agende leta 2010 [7].

[2] Prizadevanja Združenih narodov so se začela leta 2002 (ICT Taskforce) in se nadaljevala v okviru globalnih konferenc Svetovni vrh informacijske družbe (World Summit on Information Society) leta 2003 v Ženevi in 2005 v Tuniziji. Danes aktivnosti Združenih narodov potekajo v okviru WSIS Knowledge Community (http://www.wsis-community.org).

ganizacijsko terminološke spremembe, kot je preimenovanje generalnega direktorata z imenom Informacijska družba sredi leta 2012 v Generalni direktorat *Connect*, kar je angleška okrajšava za komunikacijska omrežja, vsebine in tehnologijo[3] (*communication networks, content and technology*).

Tehnološko-uporabniška fascinacija z informacijsko-komunikacijsko tehnologijo je zadnjih dvajset let učinkovito in eksponentno vključevala uporabnike, jih povezovala na vseh ravneh in s svojo samoumevnostjo vse bolj poganjala do skrajnosti globalizirane trge. Selitev na nova, pretežno mobilna uporabniška okolja je navedenemu dala pospešek. Vseprisotnost že krepko presega le urbana okolja in ekonomsko razvite države. V prispevku je obdelanih nekaj razsežnosti, ki pritrjujejo Webstrovemu skepticizmu glede obstoja informacijske družbe na prelomu tisočletja in pritrjujejo ideji, da postopni prehod oz. metamorfoza iz tehnološko-uporabniške fascinacije dobiva zgostitveno obliko, v kateri izstopajo izzivi, kot so potreba po drugačnem pojmovanju intelektualne lastnine, odprt dostop do podatkov javnega sektorja ter preseganje razmejitve med storitvijo in uporabnikom. Z zavestnim poudarjanjem teh izzivov družba postaja ireverzibilno informacijska, pri čemer ireverzibilnost pomeni, da morebitni korak nazaj ne pomeni vrnitve v neko prejšnje varno stanje, temveč prehod v nepredvidljivo obdobje tehnološkega in družbenega razvoja.

2 ZNANILCI SPREMEMB

Med temeljne značilnosti tehnoloških transformacij spadajo tudi spremembe znotraj posameznih poklicev in prestrukturiranje delovnih skupin. Razvoj informacijske družbe po eni strani nedvomno omogoča udejanitev korporativnega skupinskega dela in konsenzualnega odločanja, kar Castells imenuje »toyotizem« ([3], str. 169–72), po drugi strani pa sili v entropičnost specifičnih, v stroko usmerjenih, predvsem inženirskih poklicev oz. njihovo ohranjanje prek tržno množičnih, vendar zaradi nišne naravnanosti tudi geografsko omejenih produkcijskih kompleksov. Informacijsko-komunikacijska tehnologija je dosegla široko uporabo in je generator novih potreb, kar je bistvena razlika v primerjavi s starejšimi vrstami tehnološko pogojenih družbenih ciklov, pri katerih je večinoma šlo za nadomeščanje zamudnih ročnih del (npr. parni batni stroji) ali premagovanje logističnih izzivov (npr. evropsko obdobje gradnje rečnih kanalov okrog leta 1800). Pri informacijsko-komunikacijski tehnologiji je po Flichyju bistvenega pomena prodor v prosti čas in zasebnost ([9], str. 143–149) ter njena ponovna, vendar tokrat sočasna transformacija v produktivno, poslovno donosno sfero. Shirky ([21], str. 20–27) opozarja na kognitivni presežek, ki ga je treba izkoristiti. »asovno rezervo iz obdobja uporabe starih medijev in njihovih vsebin, ki jo imenuje ekonomija potrošnje (ponazarja jo s primerom *sitcomov* in siceršnjega časovno sinhronega spremljanja medijev), želi preliti v ekonomijo ustvarjanja in medsebojne delitve. Vse navedeno je mogoče opredeliti kot ključne parametre »šumpeterjanskih« tehnoloških razvojnih ciklov, ki jih je v obdobje elektronskih komunikacij implementirala Carlotta Perez [15]. Nazorna je njena modifikacija izhodiščnega modela tehnološkega razvojnega cikla z enim, konvencionalnim prelomom oz. zlomom, ki ga je ista avtorica zagovarjala na začetku prvega desetletja enaindvajsetega stoletja, v cikel z dvema prelomnima točkama. Prva prelomna točka je opredeljena predvidljivo: zaradi tehnoloških inovacij, ki jih je povzročil razvoj informacijsko-komunikacijske tehnologije, so borzna pričakovanja glede vrednosti podjetij, povezanih s to dejavnostjo, postala tako nerealna, da je 10. marca 2000 njihova vrednost nenadoma znatno padla, kar označujemo s pokom t. i. *borznega mehurja dot-com*, ki so ga dogodki po 11. septembru 2011 še dodatno okrepili [23]. Drugo prelomno točko po Carlotti Perez opredeljuje finančna kriza, ki se je začela v letih 2007 in 2008, posebno zanimivo pa je, da jo opredeljujejo finančne inovacije, ki jih je omogočila sama informacijsko-komunikacijska tehnologija. Inovacije so v tem primeru le evfemizem za špekulacije,[4] ki jih je, paradoksalno, z omogočeno omreženostjo, posledično hitro komunikacijo in občutkom transparentnosti omogočilo prav elektronsko poslovanje. Rešitev (ibid.) je v strukturnih spremembah, pri katerih igra informacijsko-komunikacijska tehnologija pomembno, tako rekoč infrastrukturno vlogo, vendar brez politične inovacije na ravni institucij, pojmovanja blaginje in enakopravnejšega razumevanja globalizacije bo uspeh izostal.

[3] Poslanstvo in prioritete Generalnega direktorata EU za komunikacijska omrežja, vsebine in tehnologijo pokriva Digitalno agendo v najširšem smislu s poudarkom tudi na raiskovalnih programih prihajajoče finančne perspektive (http://ec.europa.eu/dgs/connect/mission/index_en.htm).

[4] S primerom stranskih učinkov dobro obveščenih informacijskih delavcev in zaupanja višjih (informacijsko manj veščih) vodstvenih struktur je Phillips [15] razložil problem polarizacije med dejanskim upravljanjem z informacijami in njihovo uporabo za strateško odločanje. Sklepamo lahko, da je pomanjkanje novega razreda (odgovornih) informacijskih profesionalcev (ibid.) odločno vplivala na poglobitev finančno-gospodarske krize v naslednjih letih.

3 ZAPOZNELE REAKCIJE NORMATIVNEGA SISTEMA

Normativni in paranormativni sistem sta zapoznela spremljevalca vsake tehnološke revolucije. Odgovor na vprašanje, kdaj je regulacija rezultatov inovativnosti prezgodnja, kdaj prepozna in kdaj sploh ni potrebna, lahko spremljamo v realnem času, npr. v okviru dilem pri sprejemanju trgovskega sporazuma za boj proti ponarejanju ACTA [10]. Vsaka nova tehnologija ima (pogojno rečeno) anarhično komponento, ki jo Ferdinand Braudel opisuje kot konflikt med zgodovinsko »zavoro« in »pospeševalniki« tehnološkega razvoja ([25], str. 11 in 342). Winston (ibid.) je postavil model, v katerem daje izrazito vlogo družbenemu okolju oz. zakasneli družbeni potrebi, ki prototip pretvori v iznajdbo ter jo z difuzijo tehnologije umesti v širše okolje. Omenjena zakasnitev je ključnega pomena za zorenje, uporabniško prilagoditev ter poslovno umestitev aktualne tehnologije.

V vmesnem poročilu prejšnje strategije informacijske družbe i2010 [6], ki jo je sprejela Evropska unija leta 2005 in je bila predhodnica Digitalne agende, je povzeta zgovorna ilustracija, ki jo je za potrebe vmesnega poročila pripravila svetovalna agencija DLA Piper (povzemamo posredno po zgornjem viru), na kateri je označen izbor tehnološko-uporabniških prelomnih točk razvoja informacijske družbe na eni krivulji, na drugi pa sledijo normativni instrumenti, ki regulirajo omenjene tehnologije. Vidne zakasnitve regulacije zaradi ohranjanja pionirsko-inovativnega potenciala delujejo pozitivno; če bi bile (ali v nekaterih primerih tudi so) predolge, bi povzročile motnje, kot so npr. ustvarjanje monopolov ali težja dosegljivost storitev.

4 ZGODILA SE JE METAMORFOZA

V svetovnem merilu že od začetka devetdesetih let po Winsecku v gospodinjstvih beležimo znaten porast sredstev, ki jih namenijo za množične medije in kulturo ([24], str. 102–103), medtem ko se stroški za ta namen v gospodarstvu in v javnem sektorju komaj kaj povečujejo. Winseck navaja podatke za Kanado in izpostavlja poziv svetovalne hiše Proctor & Gamble iz leta 1998 po razvoju digitalnih medijev kot novih množičnih medijev (ibid.). V obdobju nastajajoče konvergence so bile dodane nove ključne besede glede na stare medije: interaktivnost, personalizacija in dostopnost.

Ker je za adaptacijo nove tehnologije, v tem primeru internetnih storitev kot novega medija, potrebna določena fascinacija javnosti in poslovnega sveta, bom razpravo začasno usmeril v McLuhanovo opredelitev vročih in hladnih medijev (v knjigi Razumevanje medijev [12]) ter ovrednotil njegovo teorijo v luči nujne metamorfoze, ki nas pripelje do informacijske družbe. McLuhanova dela iz zgodnjih šestdesetih let, kot so npr. *Gutenbergova galaksija* in *Razumeti medije*, kakor tudi njegovi številni intervjuji in predavanja, so se s prodorom interneta na prelomu tisočletja obudila in postala predmet mnogih kritičnih interpretativnih analiz, mnoge obravnave ga celo povzdigujejo do zvezdniških dimenzij [18]. V akademskih krogih so avtorji (npr. Rosenberg v [20]) že v devetdesetih letih poskušali umestiti internet v vročo ali hladno kategorijo medijev, vendar je odgovor vsakič nekje vmes, kar je treba razumeti kot manifestacijo konvergenčne sposobnosti novega medija. Spomnimo, da je bilo to obdobje (na začetku in sredi devetdesetih let) intenzivnega uvajanja svetovnega spleta in standardiziranega spletnega hipertekstovnega metajezikovnega zapisa (HTML). Če nekoliko poenostavim, kakovostno spletno komuniciranje glede na trenutne potrebe uporabnika nastopi kot (a) vroč medij z visoko vizualno definiranostjo, številnimi podatki, pri čemer je lahko uporabnik pasiven, saj medij sam poskrbi za informacijo, ali (b) hladen medij z manjšo koncentracijo informacij, ki zahteva večjo vključenost uporabnika, v kar štejem njegovo verbalno, vizualno ali tudi imaginativno participacijo. Iz te predpostavke lahko izpeljem utemeljitev o nastopu metamorfoze, ki jo pojmujem kot prehod znanega in predvidljivega komunikološkega okolja v novo (tehnološko) obliko in s tem vsebinsko preobrazbo, ki nima samo predvidljivih in že videnih družbenih in ekonomskih učinkov.

5 RAZISKOVALNI PODROČJI, ZAZNAMOVANI S KONVERGENCO

Raziskovalna področja so v evropskem prostoru formalno začrtana z okvirnimi raziskovalnimi programi. Njihova zgodovina sega v leto 1984, aktualni sedmi okvirni program pa se izteče z letom 2013. Splošno podani cilji okvirnih programov so okrepiti znanstveno odličnost in tehnološko osnovo industrije znotraj Evropske skupnosti, zagotavljati visoko konkurenčnost gospodarstva na mednarodni ravni ustvariti sinergije v evropskem raziskovalnem prostoru [8]. Načrtovanje osmega okvirnega programa je mnogo bolj prilagojeno gospodarsko-finančni realnosti in pravkar poteka razprava med Evropskim parlamentom in Evropsko komisijo o programu Obzorje 2020, ki naj bi bil vreden 80 milijard evrov. V svojem kratkem video sporočilu na promocijski stra-

ni programa Obzorje 2020 tako na primer nobelovec Peter Doherty z Univerze v Melbournu [4] slikovito ponazori ključna izziva raziskav v prihajajočem obdobju – trajnostni razvoj in zagotavljanje kakovosti življenja –, kategoriji, ki se ob današnjem pojmovanju kakovosti življenja ne samo v zahodnih civilizacijah temveč tudi v državah s trenutno največjim gospodarskim zagonom prepogosto povsem izključujeta.

Temeljne usmeritve in ključne prednostne naloge so v okviru Obzorja 2020 usmerjene v tri področja; to so (1) odlična znanost, (2) vodilni položaj v industriji in (3) družbeni izzivi. Informacijsko-komunikacijske tehnologije so tako iz osrednje vloge prešle v pomembno infrastrukturo in jih še vedno lahko zaznamo med industrijami, ki v evropskem prostoru lahko zasedajo vodilni položaj, kakor tudi kot infrastrukturo,[5] ki omogoča soočanje z družbenimi izzivi, in jih sporočilo komisiji taksativno našteje: zdravje, demografske spremembe in blaginja; zagotavljanje hrane, trajnostno kmetijstvo, raziskave morja in pomorske raziskave ter biogospodarstvo; varna, čista in učinkovita energija; pameten, okolju prijazen in integriran promet; podnebni ukrepi, učinkovitost virov in surovine; vključujoče, inovativne in varne družbe.

V perspektivi nastajanja novega evropskega okvira raziskav, z opazovanjem okolja v Republiki Sloveniji, kadrovskih in poslovnih migracij, sta spodaj navedeni precej različni raziskovalni področji, za kateri je videti, da imata potencial tržne uspešnosti, hkrati pa za njuno podlago potrebujemo raziskave, ki so lahko in morajo biti konkurenčne v svetovnem evropskem merilu. Pojmovanje informatike je treba odmakniti od konvencionalnega obzorja, priznati, da nekatere dejavnosti spadajo v temeljno infrastrukturo, ter tako z nišnimi usmeritvami doseči ponovno prodornost, znano izpred desetletij. Omejitev na spodnji dve področji je plod avtorske odločitve, ki metodološko sloni na aktivni udeležbi pri oblikovanju raziskovalnih politik, preučevanju literature in vrednotenju implementacijske realnosti informatike v slovenskem prostoru. Področji sta zamejeni tudi z orientacijo h konvergenčnim okoljem, ki v večini aspektov presegajo konvencionalno medijsko konvergenco. Tudi zaradi poslovnih priložnosti, ki jih ponujajo, sta opredeljeni področji: (1) odprti podatki in (2) konvergenca *NBIC (nano-bio-info-cogno)*.

5.1 Odprti podatki kot realizacija paradigme dostopa do informacij javnega značaja

Pojem informacije javnega značaja je na koncu prejšnjega tisočletja opredeljeval željo in potrebo po odprtem dostopu do podatkov, ki jih ima na voljo javni sektor. Želja je bila povezana z demokratizacijskimi težnjami v smislu transparentnega dela vlad in drugih državnih organov, potrebo pa je narekoval tudi zasebni sektor, ki je želel javnim podatkom dodati vrednost in jih tržiti. Združitev teh dveh komplementarnih konceptov je na evropski ravni rezultirala v uredbi o ponovni uporabi informacij javnega značaja, kar nekaj mesecev pred njenim sprejetjem pa je bil na predlog takratnega ministrstva za informacijsko družbo ter vlade RS v državnem zboru sprejet zakon o dostopu do informacij javnega značaja (ZDIJZ). Ob sprejetju ZDIJZ so bile razprave usmerjene predvsem k samemu dostopu do prej težje dostopnih ali nedostopnih informacij, kar je pri medijih in posameznikih spodbudilo dodatno poizvedovanje po informacijah. Na žalost lahko danes ugotovimo, da je bila posledica ZDIJZ predvsem poizvedba po posameznih podatkih in mnogo manj po podatkovnih bazah ali segmentih teh baz, ki bi jih neka propulzivna gospodarska družba nadgradila in tržno izkoriščala.

Konec prejšnjega desetletja je prišlo do znatnejših premikov tudi v evropskem merilu, saj je aktualna komisarka in podpredsednica Evropske komisije Neelie Kroes spodbudila dostop do podatkov s področja kulture, komisarka Quinn pa je začela posvetovanja glede odprtega dostopa do znanstvenih podatkov. Obe področji, tako kultura kot znanost, se v luči odprtosti podatkov soočata s svojstvenimi izzivi. Pri pojmovanju odprtih podatkov s področja kulture prihaja do dveh dihotomnih ovir: prva je povezana z neprilagojeno zakonodajo varovanja intelektualne lastnine glede na principe digitalne kulture ([11] in [10]), druga pa izhaja iz mnogokrat lastniškega odnosa javne sfere glede samega pojma javnosti. Primer, ki ga navajamo kot ilustracijo, je pripomba tipa »saj smo vendar mi financirali te podatkovne baze« (npr. umetniških zbirk, muzejev ipd.), ki je napačna v svojem bistvu, saj je dejstvo, da je podatkovna zbirka nastala z javnim denarjem in mora zato tudi služiti javnosti.[6]

[5] V tem kontekstu izraz infrastruktura na področju informacijsko-komunikacijskih tehnologij interpretiramo kot kompleksen splet komunikacijske, strojne in vmesniške opreme, sistemskega programja in storitvenih aplikacij. Za infrastrukturo je značilno, da omogoča napredne rešitve na področjih, ki v svojem razvojnem bistvu (kot dejavnost) ne izvirajo iz informacijsko-komunikacijske tehnologije, vendar so skozi čas postale odvisne od nje.

[6] Problemsko področje v Republiki Sloveniji podrobneje razloži video zapis javnega posveta z naslovom Predstavitev okvirnega stališča RS k predlogu sprememb direktive z vidika kulturnega sektorja [17].

5.2 Konvergenca NBIC

NBIC je okrajšava za multidisciplinarno in s tem konvergenčno obravnavo tehnologij, kot so informacijske tehnologije, nanotehnologija, biotehnologija in energetska tehnologija. Njihov (skupni) pomen je bil prvič izpostavljen že leta 2000 na prvi konferenci Nacionalne fundacije za znanost iz ZDA[7] o družbenih vidikih nanotehnologije kot nove tehnologije. Avtorja Roco in Bainbridge [19] sta na podlagi tega oblikovala koncept konvergenčnih tehnologij NBIC. Opredeljujeta jih kot sinergistično kombinacijo štirih glavnih vej znanosti in tehnologije NBIC (nano, bio, info, kogno), ki trenutno napredujejo z veliko hitrostjo: (1) nanotehnologije in nanoznanosti, (2) biotehnologije in biomedicine, (3) informacijske tehnologije, vključno z naprednim računalništvom in elektronskimi komunikacijami, (4) kognitivne znanosti, vključno s kognitivno nevroznanostjo (ibid.). Beckert [1] s soavtorji meni, da Roco in Bainbridge ne odgovarjata na vprašanje, ali je konvergenca nekaj, kar se že dogaja in se združuje pod novo oznako konvergence, ali pa je konvergenca proces, ki bo v prihodnosti potreben za doseganje novih znanstvenih prebojev. Navaja, da je treba konvergenco razumeti kot dinamičen in trajen proces, ki ga spremlja neprekinjena reorganizacija disciplinarnih podpodročij. Po Schummerju je pri procesu konvergence treba upoštevati tudi transformativna orodja in ne samo discipline [22]. Ameriška poročila o konvergentnih tehnologijah so spodbudila primerljive analitične projekte tudi v drugih državah, predvsem v Evropi, Južni Koreji in na Japonskem. Na stari celini je pristop upošteval svojevrsten evropski kontekst in se usmeril na področja, na katerih bi lahko konvergentne tehnologije delovale kot spodbujevalec znanstvenih prebojev in inovacij. Projekt Konvergentne tehnologije za Evropsko družbo znanja[8] je tako usmerjen v štiri področja, in sicer v zdravje, izobraževanje, informacijsko-komunikacijsko infrastrukturo in energijo [13].

V Sloveniji vidimo možnost konvergentne obravnave tehnologij tudi kot nadaljevanje raziskovalnih prizadevanj v okviru centrov odličnosti in kompetenčnih centrov skladno z resolucijo o raziskovalni in inovacijski strategiji Republike Slovenije v obdobju od 2011–2020 (Uradni list RS, št. 43/2011). Raziskave in razvoj so namreč ključni pogoj za doseganje evolucije konvergentnih tehnologij in njihovih konkurenčnih prednosti. Posebno v panogah s hitrimi spremembami tehnoloških in tržnih razmer je ustrezno vrednotenje tovrstnih projektov nujnost. Zato na Inštitutu za informatiko v okviru podiplomskega študija na UM FERI posamezne študente usmerjamo tudi v področje konvergentnih tehnologij (npr. [16]).

6 SKLEP

Prehod iz pionirskih tehnološko pogojenih ter občasno prestižnih uporabniških skupin v množično uporabo informacijsko-komunikacijske tehnologije se je v zadnjih desetih do petnajstih letih zgodil tako mehko in hkrati tako intenzivno, da lahko govorimo o metamorfozi začetnih uporabniških fascinacij v dejansko informacijsko družbo. Morda je paradoksalno, da ta pojav vodi tako rekoč k samoukinitvi pojma informacijska družba, čeprav ta še vedno odlično zaokrožuje posledice uporabe komunikacijskih omrežij, vsebin in tehnologij. V obdobju intenzivnega prodora spletnega poslovanja in s spletom povezane kreativnosti so na raziskovalna področja začele močno vplivati ideje in tudi pritiski iz poslovnega sveta. Nova podjetja so vse bolj podkrepljena z naprednimi študenti ter visoko izobraženimi posamezniki multidisciplinarnih veščin, ki svojih raziskav ne omejujejo na konvencionalno akademsko okolje, temveč prej obratno, usmerjeni so povsem v aplikativno vrednost storitev in v njihov komercialni uspeh. Ker tovrstne komercialne rešitve zahtevajo visokotehnološko ozadje, je prostora za koeksistenco še vedno dovolj, kljub temu da »vsiljeni« parametri zunanjega sveta, kot so tržna uspešnost, lastniške migracije in podobno, vnašajo precejšnja tveganja.

Znana in preverjena je trditev, da je inovativnost eden ključnih dejavnikov konkurenčnosti sodobnega gospodarstva, centri odličnosti ter kompetenčni centri kot nov model znanstvenoraziskovalne dejavnosti pa pomenijo oblikovanje inovativnega sistema v povezavi z univerzami in izobraževalnim okoljem [2]. Neproduktivni polemiki o omejevanju akademskega duha skozi pričakovanja, da morajo univerze postati bolj inovativne, podjetniške in slediti potrebam družbe in ekonomije oziroma trga, se lahko izognemo le, če pojmujemo inovativnost skozi hkratno avtonomijo posameznih ved in nujo njihove multidisciplinarne povezanosti.

Slovenija ima dva relativno sveža strateška dokumenta tako na področju visokega šolstva kot na področjih znanosti in inovacij, ki sta bila sprejeta leta 2011 v obliki resolucij državnega zbora: Resolucija o stra-

[7] NSF (National Science Foundation), http://www.nsf.gov.
[8] V angl. Converging Technologies for the European Knowledge Society–CTEKS.

tegiji visokega šolstva 2012–2020 in Resolucija o strategiji raziskovanja in inovacij 2012–2020. Dokumenta sta združena pod imenom Drzna Slovenija in ker ob strateških smernicah podajata tudi analizo dosedanjega dela ter ponujata instrumentarij sledenja razvoju na tem področjih, ju je smiselno uporabljati pri načrtovanju strateških premikov. Tudi tistih, ki jih ponujajo in omogočajo informacijsko-komunikacijske tehnologije.

VIRI IN LITERATURA

[1] Becker, B. idr. (2008). *The technology base for convergence, v Converging Technologies and their impact on the Social Sciences and Humanities (CONTECS)*. Fraunhofer Institute for Systems and Innovation Research. Dostopno na http://www.contecs.fraunhofer.de.

[2] Beerkens, E. (2009). Centres of Exellence and Relevance: The Contextualisation of Global Models. *Science, Technology & Society* 14:1 (2009): 153–175.

[3] Castells, M. (1996/2000). *The Rise of the Network Society*. Blackwell Publishing.

[4] Doherty, P., *What are your main concerns for the future?*, video sporočilo na spletni strani http://ec.europa.eu/research/horizon2020.

[5] Evropean Commission (1994). *Europe and the Global Information Society*. Brussels: European Council, arhivska spletna stran http://www.echo.lu/eudocs/en/bangemann.html).

[6] European Commission (2008). Preparing Europe's Digital Future. *i2010 Mid-Term Review, COM(2008) 199 SEC(2008) 470* Volumes 1, 2, 3 April 2008.

[7] Evropska komisija (2010). *Evropska digitalna agenda – Sporočilo Komisije Evropskemu parlamentu, Evropskemu ekonomsko-socialnemu odboru in Odboru Regij*. COM(2010) 245 konč./2, 2010.

[8] Evropska komisija (2011). *Obzorje 2020 – Okvirni program za raziskave in inovacije*. Bruselj, 30. 11. 2011 COM(2011) 808 konč., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0808:FIN:sl:PDF.

[9] Flichy, P., (2001). New Media History, v *Hanbook of New Media,* SAGE Publications, 136–150.

[10] Györkös, J., Bogataj Jančič, M., Ćosić, V. (ur.) (2011). *K javni obravnavi Sporazuma ACTA v Državnem zboru Republike Slovenije, Zbrani prispevki*. Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko.

[11] Lessig, L., (2005). *Svobodna kulture, narava in prihodnost ustvarjalnosti*. Knjižna zbirka Krt. Izvirnik: Free Culture. The Nature and Future of Creativity, Tribune Media Services, 2004.

[12] McLuhan, M., (2001). *Understanding Media, The Extensions of Man*. pon. Routhledge, izvirnik Routledge and Kegan Paul, 1964.

[13] Nordmann, A. (rapporteur) (2004). *High Level Expert Group, Converging Tehnologies – Shaping the Future of European Societies*. Luxembourg: Office for Official Publications of the European Communities. Dostopno na http://www.ntnu.no/2020/final_report_en.pdf.

[14] Perez, C., (2010). *Major Bubble Collapses and the Changing Roles of Markets and Governments*, Schumpeter Conference 2010, Aalborg University; http://www.schumpeter2010.dk/index.php/schumpeter/schumpeter2010/paper/viewFile/493/212 (8. 3. 2012).

[15] Phillips, S., (2005). Realigning a business information service for future success, Opportunities for well-informed information professionals. *Business Information Review Copyright*, SAGE Publications.

[16] Pižmoht, F., (2012). *Evolucija NBIC tehnologij: nano, bio, informacijske in kognitivne tehnologije*, Individualno raziskovalno delo 3 v okviru doktorskega študija. Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko.

[17] Prešeren, M. idr. (2012). *Javni posvet o predlogu sprememb Direktive o ponovni uporabi informacij javnega sektorja 2012*. Ministrstvo za izobraževanje, znanost, kulturo in šport, Ljubljana; video zapis; http://videolectures.net/uporabainformacij_kultura2012_ljubljana/.

[18] Robinson, W., McLuhan, M. (2005). Reconsidered: review of reprintd editions, previously unpublished work, and two tributes. *New Media & Society*, Sage Publications, Vol 7(2): 271–279.

[19] Roco, M. C., Bainbridge, W..S. (2003). *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science* (e-knjiga), Dordrecht: Springer.

[20] Rosenberg, S., (1995). *Taking the Internet's Temperature, What Would Marshall McLuhan Have Said: Hot or Cold? Digital Culture*, http://www.wordyard.com/dmz/digicult/mcluhan-5-3-95.html.

[21] Shirky, C. (2010). *Cognitive Surplus, Creativity and Generosity in Connected Age*. Penguin Books.

[22] Schummer, J. (2008). From Nano-Convergence to NIBC--Convergence: The best way to predict the future is to create it, v Maasen, S., Kaiser, M., Kurath, M. in Rehmann-Sutter C. (ur.) *Governing Future Technologies: Identity, Ethics, and the Governance of Nanotechnology*. Springer. Dostopno na http://www.joachimschummer.net/papers/2008_Nano-NBIC--Convergence_Maasen-et-al.pdf.

[23] Webster, F. (2002). The Information Society Revisited, v Lievrouw, L. A., Livingstone, S. (ur.) *Handbook of New Media*. London: Sage. 255–266 (preštevilčeno).

[24] Winseck, D. (2002). Illusions of perfect information and fantasies of control in the information society. *New Media & Society*, Sage Publications, Vol 4 (1); 93–122.

[25] Winston, B., (1998). *Media Technology and Society, A History: From the Telegraph to the Internet*. Routhledge.

▪

József Györkös je redni profesor na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, kjer predava na študijskih programih Informatika in tehnologije komuniciranja ter Medijske komunikacije. Leta 1992 je doktoriral s področja prediktivne analize razvoja informacijskih sistemov, v postdoktorskih študijih in raziskovanju pa se je usmeril tudi na področja zagotavljanja kakovosti, sistemov za podporo odločanju in medijske konvergence. Dva mandata je opravljal funkcijo državnega sekretarja na Ministrstvu za informacijsko družbo (2001–2004) ter na Ministrstvu za visoko šolstvo, znanost in tehnologijo (2008–2011). Sodeloval je pri pripravi strategij in zakonodaje s področja informacijske družbe, visokega šolstva ter raziskav in inovacij. Januarja 2013 je bil na podlagi razpisa Evropske komisije imenovan za člana in nato izvoljen za predsednika Svetovalnega foruma CONNECT za raziskave in inovacije na področju informacijsko-komunikacijskih tehnologij (CAF: Advisory Forum for ICT Research and Innovation). Glavna naloga foruma je svetovanje Generalnemu direktoratu za komunikacije, omrežja, vsebine in tehnologije (DG CONNECT) pri Evropski komisiji pri pripravi in izvedbi raziskovalnega programa Obzorja 2020.

Iz Islovarja

Tokrat predstavljamo zbirko »igre«. Računalniške igre so se že pred časom uveljavile med mladino, otroki in odraslimi. Ob tem nastaja cela vrsta novih, tudi žargonskih izrazov. Nekaj teh smo uredili tudi v Islovarju. Pri izboru izrazov smo si pomagali z zbirko, ki jo je kot seminarsko nalogo prispeval študent Filozofske fakultete, Oddelka za prevajalstvo. Vabimo vas, da v Islovar www.islovar.org prispevate svoje pripombe ali predloge novih izrazov.

arkádna ígra -e -e ž (*angl. arcade game)*
videoigra z več stopnjami, sobami, ki se po težavnosti stopnjujejo, in jo lahko igralec igra, dokler njegov avatar ne izgubi vseh življenj

avatár -e m (*angl. avatar*)
lutka ali ikona, ki predstavlja igralca in njegov položaj v virtualnem svetu

borílna ígra -e -e ž (*angl. fighting game*)
videoigra, pri kateri merijo moči igralci ali njihovi avatarji

didáktična ígra -e -e ž (*angl. didactic game*)
igra, ki ima učni, vzgojni ali drug poučen namen; prim. izobraževalna igra

dirkálna ígra -e -e ž (*angl. racing game*)
videoigra, pri kateri je pomembna hitrost premikajočih se predmetov ali oseb; prim. hitrostna igra

ênouporábniška ígra -e -e ž (*angl. single user game*)
videoigra, namenjena enemu igralcu; prim. večuporabniška igra, večigralska igra

hitróstna ígra -e -e ž (*angl. speed game*)
videoigra, pri kateri je pomembno igralčevo hitro odzivanje; prim. dirkalna igra

ígra -e ž (*angl. game*)
1. s pravili opredeljena dejavnost, namenjena zabavi in razvedrilu, npr. človek ne jezi se, videoigra
2. za to dejavnost prirejena programska, strojna oprema

ígra RPG -- [erpegé] ž (*angl. role-playing game*, krat. RPG)
videoigra, v kateri igralec prevzame eno od vlog v domišljijskem okolju; sin. igra igranja vlog

ígra za úrjenje -e -- -- ž (*angl. drill game*)
didaktična igra, s katero učenci ponavljajo, utrjujejo znanje na privlačen način, npr. urjenje poštevanke

igrálna konzóla -e -e ž (*angl. game console*)
za videoigre prilagojen računalniški sistem, ki ustvarja videosignal za prikaz na zaslonu, npr. na televizorju, računalniškem monitorju

igrálna plôščica -e -e ž (*angl. game pad*)
igralni pripomoček v obliki ploščice z gumbi za krmiljenje; prim. igralna palica, igralni volan

igrálni pripomóček -ega -čka m (*angl. game controller*)
vhodno-izhodna enota, namenjena igranju videoiger na igralnih konzolah, računalnikih

igrálnik -a m (*angl. 1. game portal, 2. gaming device*)
1. portal, na katerem so zbrane videoigre
2. naprava, ki je prirejena za igranje

ígrica -e ž (*angl. computer game*)
preprosta računalniška igra za igranje na računalniku, mobilnem telefonu, igralni konzoli

ígričar -rja m (*angl. gamer*)
1. kdor ima računalniške igre za konjiček
2. kdor programira računalniške igre, videoigre

izobraževálna ígra -e -e ž (*angl. instructional game*)
igra, katere namen je pridobivanje novih znanj ali veščin; prim. didaktična igra

míselna ígra -e -e ž (*angl. mind game*)
igra, ki razvija miselne procese

nasílna ígra -e -e ž (*angl. violent game*)
igra, katere glavni namen je izvajanje nasilnih dejanj, npr. streljanja, mučenja, pretepanja

neodvísna ígra -e -e ž (*angl. indie game, indie video game, independent game, independent video game*)
videoigra, ki jo razvijejo neodvisni razvijalci brez založnikov; prim. neodvisna programska oprema

Izbor pripravlja in ureja Katarina Puc
s sodelavci Islovarja

21. konferenca

Dnevi slovenske informatike 2014

Informatika – neizkoriščeni dejavnik razvoja

Kongresni center Grand hotel Bernardin, Portorož – 14. do 16. aprila 2014

Rdeča nit konference DSI 2014 Informatika – neizkoriščeni dejavnik razvoja postavlja informatiko v vlogo, v kakršni jo je predvidela Evropska komisija že v devetdesetih letih prejšnjega stoletja. Bangemannovo poročilo je identificiralo informatiko kot gonilo razvoja pri prehodu v informacijsko družbo, danes pa vidimo, da je njen potencial celo še večji. Recesija, ki je Evropa in tudi Slovenija še nista povsem preboleli, sicer nobene dejavnosti ni pustila nedotaknjene, analitiki pa ocenjujejo, da je gospodarske družbe s področja informatike informatika prizadela manj kot večino drugih dejavnosti.

Potencial informatike bi radi predstavili in izkoristili tudi na DSI 2014. Za ta namen smo dosedanji koncept dogodka nadgradili v smer večje poslovne aktualnosti in zanimivosti. Vse ustaljene oblike – častni govornik, podelitev priznanj in nagrad, vabljena predavanja, sekcije, okrogle mize, delavnice – ostajajo tudi še naprej, razširili pa smo vsebine, ki povečujejo poslovno aktualnost in seznanjanje udeležencev z aktualno ponudbo proizvodov in storitev. Izostal tudi ne bo tradicionalni obkonferenčni družabni dogodek, ki je za izmenjavo mnenj in pridobivanje informacij pomemben vsaj toliko kot uradni program konference.

Novost konference je poslovna predkonferenca, na katero bomo povabili eminentne ponudnike in uporabnike informacijske tehnologije in storitev. To bo tudi priložnost, da dogodek preseže državne meje, saj na njem pričakujemo tudi udeležence iz držav zahodnega Balkana.

Slovensko društvo INFORMATIKA

Znanstveni prispevki

Pregledni znanstveni prispevki

Strokovni prispevki

Razprave

Informacije

ISSN 1318-1882
9 771318 188001