Stipe Čelar, Dubravka Čelar, Mili Turić

MODEL UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U TIJELIMA DRŽAVNE UPRAVE U REPUBLICI HRVATSKOJ

Sažetak

U radu je napravljena kratka analiza povijesnog razvoja i sazrijevanja temeljnih mjera i standarda informacijske sigurnosti ISO/IEC 27001 i ISO/IEC 27002. Ukazano je i na druge bitne pojedinačne sigurnosne mjere i preporuke i njihov odnos s ISO standardima. Pokazano je, nadalje, kako se područje informacijske sigurnosti javne uprave u Republici Hrvatskoj razvijalo tijekom proteklih 20-ak godina i transformiralo iz okrilja ratnog zakona o obrani u područje primjene prava na pristup informacijama, prava na zaštitu osobnih podataka te zaštite intelektualnog vlasništva usporedo s evolucijom međunarodnih mjera i standarda informacijske sigurnosti. U radu je napravljen i konceptualni model informacijske sigurnosti tijela javne uprave u Republici Hrvatskoj koji se temelji na Zakonu o informacijskoj sigurnosti i s njime povezanim zakonima. Model može poslužiti tijelima javne uprave ali i ostalim pravnim subjektima za olakšanje provedbe Zakona o informacijskoj sigurnosti, odnosno za uspostavu sustava za upravljanje informacijskom sigurnošću (ISMS).

Ključne riječi: informacijska sigurnost, ISMS, ISO27001, ISO27002

SECURITY MANAGEMENT MODEL IN GOVERNMENT BODIES IN REPUBLIC OF CROATIA

Abstract

The paper made a brief analysis of historical development and maturation of basic norms and standards for information security (ISO/IEC 27001 and ISO/IEC 27002). Some other important security norms and recommendations and their relationship with the ISO standards are mentioned. It is shown , moreover , that the area of information security of the public administration in the Republic of Croatia has developed over the past 20 years and transformed from the scope of the law of defense to the scope of few laws: the right of access to information, the right to protection of personal data and the intellectual property rights. This transformation was done in parallel with the evolution of the international information security norms and standards. Further on, the conceptual model of information security bodies of the public administration in the Republic of Croatia is done. The model is based on the Law on Information Security and the affiliated laws. The model can serve to the public bodies as well as other legal entities to facilitate the implementation of information security and to establish a information security management system (ISMS).

Key words: information security, ISMS, ISO27001, ISO27002.

UVOD

Podaci danas – iz mnogo izvora, u više oblika i u ogromnim količinama

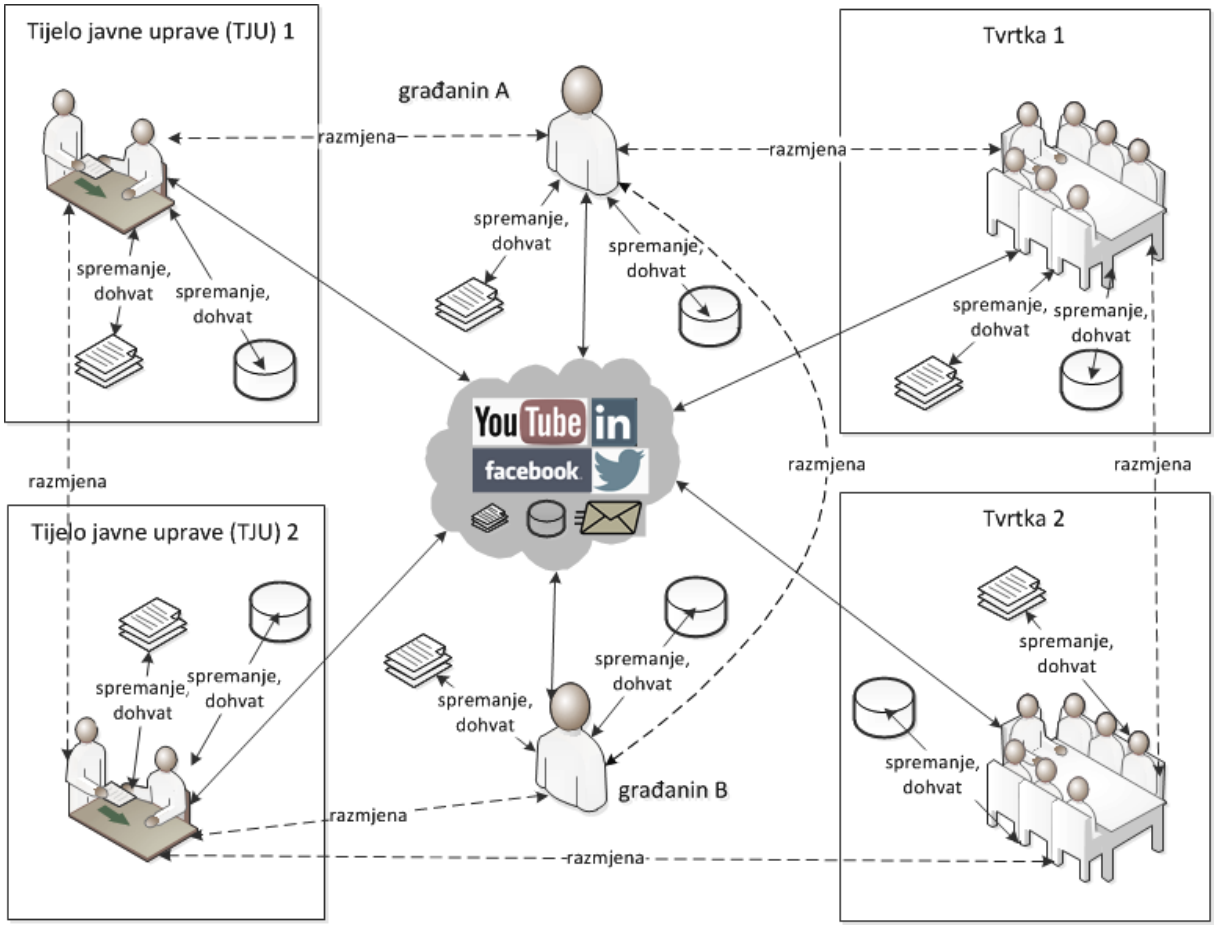
„Vijest je letjela brže od ptice
Brže od vjetra
Brže od munje“

Grigor Vitez (1911 – 1966)

Da je Pjesnik danas među nama, možda ne bi upotrijebio pojam „informacije“ s ciljem dočaravanja nečega najbržega ali bi se teško mogao oteti dojmu da su vijesti, informacije i podaci ono što nas preplavljuje sa svih strana. Generiraju se u mnogim aktivnostima i to u ogromnim količinama i raznim digitalnim oblicima, od običnih tekstualnih zapisa u elektronskim dokumentima i porukama do sve

češćih fotografija i multimedijalnih sadržaja koje sami korisnici svakodnevno kreiraju. Takvi podaci zapisuju se lokalno na vlastite uređaje (mobilne ili uredske) ili na neka udaljena mjesta, nemajući često vremena za uvođenje reda u takvim sadržajima pa se gomilaju duplicirani ili čak i višestruki zapisi. I što se brže živi, to je sve više informacija potrebno pa se još više novih podataka generira i pohranjuje. I tako iz godine u godinu.
U poslovanju privatnog sektora i tijela javne uprave i njihovoj međusobnoj komunikaciji te u komunikaciji s građanima također je primjetan trend porasta količine i raznovrsnosti podataka koji se svakodnevno generiraju i razmjenjuju (*slika 1*).

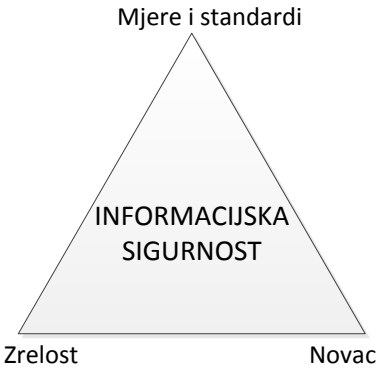
Slika 1. Proces razmjene podataka



Podaci – temelj nove vrijednosti u digitalnom informacijskom dobu
Podaci su danas postali temelj suvremenog informacijsko-komunikacijskog društva jer se na osnovu njih dobivaju informacije i znanja a informacije i znanja su nužne za donošenje zaključaka i poslovnih odluka. Drugim riječima, podaci i informacije su već odavno prepoznati kao imovina koja ima svoju vrijednost. Podaci i informacije su nematerijalne prirode pa se metode utvrđivanja odnosno mjerenja njihove vrijednosti znatno razlikuju od metoda mjerenja vrijednosti varijabli u materijalnom svijetu [10] [11] .
Međutim, objekt koji ima prepoznatu vrijednost ima i moguće izvore ugroze te vrijednosti. Zbog toga se pojavila potreba uspostave svih elemenata planiranja, pripreme, provedbe i nadzora osiguranja te nove imovine pa privatni i javni sektor ulažu napore u razvoj koncepata informacijske sigurnosti. Ti koncepti uključuju suvremene tehnologije i razvijaju se od ideja i teoretskih i iskustvenih modela do raznih praktičnih mjera i međunarodno prihvaćenih sigurnosnih standarda [1] [6] [9] [13] . Podaci, odnosno sigurnost podataka jedno je od temeljnih područja informacijske sigurnosti za koje je nužno definirati mjere i standarde informacijske sigurnosti koji će se primjenjivati kao opće zaštitne mjere u prevenciji, otkrivanju i otklanjanju štete od gubitka ili neovlaštenog otkrivanja informacija.
Doduše, primjena postojećih i razvoj novih sigurnosnih mjera, standarda i tehnologija izravno ovisi o razumijevanju uprava i rukovodećih struktura, odnosno o sposobnosti i zrelosti same organizacije i

cijelog okruženja da provodi željene mjere i standarde. Postizanje željene razine informacijske sigurnosti ovisi također i o novcu koji se uloži u informacijsku sigurnost (*slika 2*).

Slika 2. Trokut informacijske sigurnosti: Novac – Mjere/standardi – Zrelost



Hipoteza: Transparentnost podataka u javnoj upravi RH – od *'tajne'* do *'štićene'* informacije

Dvadesetogodišnja transformacija i sazrijevanje privatnog i javnog sektora u Republici Hrvatskoj ogleda se ne samo u gospodarskim i političkim parametrima nego i u području informacijske sigurnosti. Sustavan pristup problematici informacijske sigurnosti u javnoj upravi u Republici Hrvatskoj (RH) počinje donošenjem Zakona o obrani Zastupničkog doma Sabora RH (NN br. 49/91, NN br. 53/A/91) i Vladine Uredbe o utvrđivanju mjerila za određivanje tajnih podataka obrane te posebnim i općim postupcima za njihovo čuvanje (NN br. 70/91). U to specifično, ratno vrijeme, važnu ulogu u informacijskoj sigurnosti imao je koncept ***vrsta tajne***, odnosno *državne, vojne* i *službene tajne* informacije za što se ne može reći da je u skladu sa zajamčenim ustavnim pravom na pristup informacijama, tj. 'pravom korisnika na traženje i dobivanje informacije kao i obvezom tijela javne vlasti da omogući pristup zatraženoj informaciji' (Zakon o pravu na pristup informacijama, NN br. 25/2013, 77/11, 37/11, 144/10, 172/03).

Za novonastalu državu koja se našla u ratu bilo je i očekivano da neće odmah krenuti s ulaganjem u informacijsko-sigurnosnu infrastrukturu s ciljem omogućavanja pristupa zainteresiranoj javnosti informacijama u vlasništvu tijela javne uprave. Naime, kao što društvo sazrijeva u demokratskom pogledu s jedne strane, tako s druge strane moraju sazriti metode i alati kojima se omogućava primjena koncepta ***štićene*** informacije umjesto koncepta ***tajne*** informacije.

Naime, informacijska sigurnost je kompleksna i podrazumijeva izgradnju informacijske infrastrukture, komunikacijskih mreža i programskih rješenja, pravnog i zakonodavnog okvira te sustava upravljanja sigurnošću [15] [9] .

U radu se istražuje model prelaska javne uprave u RH s koncepta *tajne informacije* na koncept *štićene informacije* uz poštivanje Ustavom zajamčenih prava na pristup informacijama, zaštitu osobnih podataka i intelektualnog vlasništva. U radu se razrađuje konceptualni model informacijske sigurnosti koji može poslužiti kao konceptualni model za upravljanje informacijskom sigurnošću odnosno za izradu sustava upravljanja informacijskom sigurnošću (*engl. Information Security Management System – ISMS*)

METODE

Analiza izvora literature

U radu je korištena analitičko-sintetička metoda. Za analizu postojećeg stanja informacijske sigurnosti i primjene mjera i standarda u javnoj upravi korišteni su objavljeni zakonski propisi u elektronskom izdanju Službenog lista Republike Hrvatske Narodne novine (www.nn.hr) kao i druga dostupna stručna literatura u elektronskom obliku navedena u popisu literature (standardi) kao i recenzirane knjige u tiskanom obliku. Nadalje, vrijedan izvor informacija predstavljale su digitalne bibliografske baze znanstvenih radova:

- SCOPUS (www.scopus.com),
- IEEE *Xplore* Digital Library (www.ieee.org) i
- ACM Digital Library (www.acm.org).

S obzirom na izabrano tematsko područje i postavljenu hipotezu ('javna uprava u RH' i 'informacijska sigurnost') pronađena je odgovarajuća literatura.

Analiza informacijske sigurnosti u RH i sinteza (modeliranje)
Na temelju selektirane literature dan je kratki pregled najvažnijih međunarodnih standarda i preporuka informacijske sigurnosti koji su temelj za mjere i standarde informacijske sigurnosti u javnoj upravi. Zatim su analizirani koncepti informacijske sigurnosti korišteni u javnoj upravi RH od prve godine njene opstojnosti, preko poratnih godina i vremena priprema za ulazak u Europsku Uniju do danas. Na temelju toga prikazana je evolucija koncepata informacijske sigurnosti te je napravljen konceptualni model sustava upravljanja informacijskom sigurnošću.

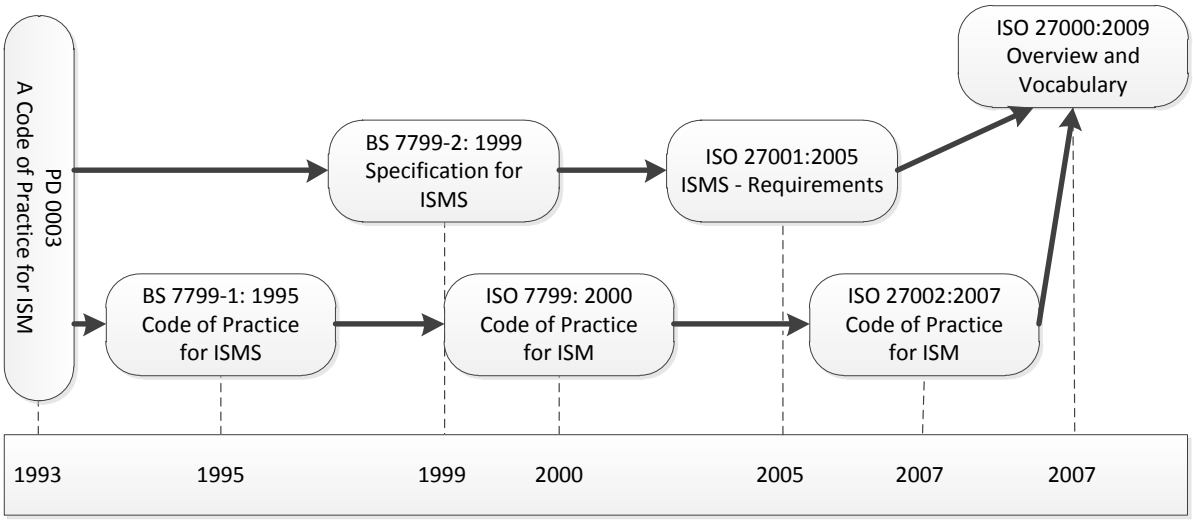
UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

Sustav upravljanja informacijskom sigurnošću
Fokusiranje na tehničku provedbu mjera i standarda informacijske sigurnosti nije dovoljno za postizanje željenih ciljeva informacijske sigurnosti [7] . Upravljanje informacijskom sigurnošću nije operativni ili tehnički zadatak nego mora biti povezano sa strateškim ciljevima organizacije u cjelini, tj. poželjno je postojanje sustava upravljanja informacijskom sigurnošću (ISMS). ISMS se može jednostavno opisati kao skup sigurnosnih mjera i standarda kojima se smanjuju mogućnosti napadača koji ugrožava štićeni objekt, odnosno kao sredstvo pomoću kojeg više poslovodstvo organizacije prati i nadzire sigurnost cijele organizacije, umanjujući poslovni rizik i osiguravajući da sigurnosni zahtjevi poslovanja ispunjavaju korporacijske i pravne obveze (ISO 27001:2005, [14]). Uvođenje adekvatnog ISMS-a u organizaciju (tijelo javne uprave ili u tvrtku u privatnom sektoru) traje od par mjeseci do nekoliko godina, i jako ovisi o zrelosti upravljanja sigurnošću unutar organizacije [1] [8] [12] [14] .

Standardi informacijske sigurnosti
Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti. Poslovanje u skladu s normom (standardom) omogućava sigurno i kvalitetno upravljanje informacijskom sigurnošću sustava i stvara povjerenje u poslovanju s međunarodnim organizacijama.
Kako bi se olakšala implementacija sustava upravljanja informacijskom sigurnošću, koriste se brojni standardi koji su danas dostupni na tržištu. Dva najpoznatija međunarodna standarda zasigurno su ISO/IEC 17799 (27002) i ISO/IEC 27001. ISO (*engl. the International Organization for Standardization*) i IEC (*engl. the International Electrotechnical Commission*) dva su tijela koja zajedno čine sustav za međunarodnu standardizaciju. Mnoge međunarodne organizacije surađuju s ISO i IEC organizacijama za standardizaciju.
Ova dva standarda se međusobno ne isključuju [1] [4] [9] [12] , a preporuka je da se za uspostavu kvalitetnog sustava upravljanja informacijskom sigurnošću koriste oba standarda. Ova dva standarda proizašla su iz standarda Britanskog instituta (*engl. British Standards Institute*) BS 7799, odnosno njihovog skupa mjera za upravljanje informacijskom sigurnošću iz 1993. godine (*PD 0003 A Code of Practice for Information Security Management*) – *slika 3*.
ISO je u rujnu 2013. godine objavila revidirane verzije standarda 27001 i 27002.

ISO/IEC 27002:2013 „Code of practice for information security controls“
Standard ISO/IEC 17799 (27002) nastao je kao prvi službeni dokument vezan uz informacijsku sigurnost kojeg je prihvatilo britansko ministarstvo za razmjenu i industriju, sa ciljem da problematiku informacijske sigurnosti predstavi neinformatičkom svijetu, prvenstveno rukovoditeljima. Od kada je donesen, predstavlja najraširenij pokušaj uvođenja međunarodno priznatih normi (mjera) na području upravljanja informacijskom sigurnošću. Standard ISO/IEC 17799 usvojio je prvi dio standarda BS 7799 (BS 7799-1), a sadrži popis sigurnosnih kontrola i predstavlja općenit i opsežan kodeks postupaka za upravljanje informacijskom sigurnošću. Standard je izričito posvećen *informacijskoj sigurnosti* i uključuje sve oblike *informacija* a ne samo informacije dobivene iz podataka u računalnom obliku nego i obliku dokumenata, znanja i intelektualnog vlasništva.
Prva verzija ISO/IEC 17799 standarda nazvana je 17799:2000, a 2005. godine izdana je nova verzija nazvana ISO/IEC 17799:2005. Standard ISO/IEC 17799 je 2007. godine preimenovan u ISO/IEC 27002 zbog kompatibilnosti s ostalim standardima ISO/IEC 27000 serije.

Slika 3. Razvoj standarda informacijske sigurnosti ISO 27000, ISO 27001 i ISO 27002



Izvor slike: [3]

Broj kontrolnih mjera mijenja se od verzije do verzije standarda (u najnovijoj verziji 2013 smanjen je broj sa 133 na 114 mjera) a razvijaju se i specijalizirane verzije za pojedina područja (npr. zdravstvo, proizvodnju, telekomunikacije i sl.).

ISO/IEC 27001:2013 „Information technology – Security techniques – Information security management systems – Requirements“

Standard ISO/IEC 27001 usvojio je drugi dio standarda britanskog standarda BS 7799 (BS 7799-2), a opisuje proces uvođenja sustava upravljanja informacijskom sigurnošću (ISMS). Takav proces pruža sustavan pristup upravljanju osjetljivim informacijama s ciljem očuvanja njihove sigurnosti. Cilj procesa je postići sigurnost informacija s tri glavna aspekta:

- povjerljivosti,
- integriteta i
- dostupnosti,

uključivši pritom relevantne organizacijske resurse, politike, procedure i informacijske sustave.
Standard je općenit, namijenjen organizacijama u javnoj upravi i onima u privatnom sektoru a mogu ga primijeniti male, srednje i najveće organizacije [5] Nova verzija standarda (2013) stavlja više naglasak na mjerenje i procjenu učinaka koje organizaciji donosi provedba sustava upravljanja informacijskom sigurnošću (ISMS). Za razliku od ISO 27001:2005, ISO 27001:2013 ne naglašava PDCA model (odnosno „*Plan-Do-Check-Act“* ciklus) nego više pažnje posvećuje informacijskoj sigurnosti i organizacijskom kontekstu a i više je usklađen s drugim upravljačkim standardima (ISO 9000 i ISO 20000).

Ostali sigurnosni standardi i sigurnosne mjere i preporuke

Pored široko primjenjivih i prihvaćenih internacionalnih ISO 27000 serije standarda postoje mjere i standardi još nekoliko organizacija koje promiču specifične sigurnosne mjere i standarde, npr. američki institut NIST (*engl. National Institute of Standards and Technology*), COBIT (*engl. Control Objectives for Information and related Technology*), FISCAM (*engl. Federal Information System Controls Audit Manual*) i CISA (*engl. Certified Information Systems Auditors*) [1] [5] [13] [14] .
Nadalje postoje i brojne preporuke s kojima se organizacije ponekad moraju usklađivati, tj. moraju zadovoljavati takve strukovne preporuke iako same ne djeluju u pojedinom sektoru. Takav je slučaj npr. s HIPAA preporukama (*engl. Health Insurance Portability and Accountability Act*) savezne agencije u USA iz 1996. godine i ne-zdravstvenim organizacijama koje imaju zdravstvene podatke o pojedinačnim djelatnicima. HIPAA propisuje mjere zaštite osobnih podataka za organizacije koje u svom poslovanju imaju pravo pristupa takvim informacijama [5] [6] [14] . Sličan je slučaj i s preporukama Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB), PCI-DSS (*engl. Payment Card Industry Data Security Standard*) [1] [5] [6] [9] [14] . Neke preporuke informacijske sigurnosti nisu obvezujuće ali su ipak široko prihvaćene, poput preporuke NIST instituta koje se odnose na proces upravljanja rizicima [5] .

REZULTATI I RASPRAVA

Zakonski akti RH o informacijskoj sigurnosti

Zakonom o informacijskoj sigurnosti (NN br. 79/2007) definirana je informacijska sigurnost kao stanje povjerljivosti, cjelovitosti i raspoloživosti podatka a postiže se primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. Zakon o tajnosti podataka (NN br. 79/2007) definira podatak kao „*dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika*". Informacije koje po svojoj prirodi nisu dostupne javnosti mogu biti osobne, znanstvene, industrijske, poslovne ili poslovne prirode (EU IPR Helpdesk).

Osnovni zakonski akti u Republici Hrvatskoj koji danas reguliraju područje informacijske sigurnosti su:

- Zakon o informacijskoj sigurnosti (ZOIS), NN br. 79/2007.
- Zakon o tajnosti podataka (ZOTP), NN br. 86/2012. i 79/2007.
- Zakon o zaštiti osobnih podataka (ZOZOP), NN br. 106/2012, 130/2011, 41/2008, 118/2006. i 103/2003.
- Zakon o pravu na pristup informacijama (ZOPPI), NN br. 25/20013, 77/2011, 144/2010. i 172/2003. i
- skupina zakona o intelektualnom vlasništvu.

Pored navedenih zakona Vlada RH i tijela javne uprave donosila su tijekom godina brojne podzakonske akte (uredbe i pravilnike) za provedbu tih zakonskih propisa.

Transformacija 'tajne' informacije u '(za)štićenu' informaciju

Odnos i evolutivna transformacija ključnih koncepata u zakonskim propisima o tajnosti i zaštiti podataka prikazani su na slici 4. Temeljenje područja informacijske sigurnosti u RH na Zakonu o obrani dogodilo se prije nego je BSI predložio mjerena za upravljanje informacijskom sigurnošću (PD 0003, 1993. godine). Do tada je sigurnost i u drugim državama bila skoro isključivo 'rezervirana' za vojne i policijske domene te se ovoj problematici izvan tih domena nije sustavno pristupalo. Čak su i u drugim stručnim područjima mjere i standardi ministarstava obrane bili često upotrebljavani (npr. mjere i standardi američkog Ministarstva obrane – Department of Defense). Usporedo s razvojem mjera i standarda informacijske sigurnosti evoluirala je i zakonska regulativa u RH (*usp. sliku 3 i sliku 4*). Tako se može primijetiti da je koncept *VRSTA TAJNE*, u ratno vrijeme vrlo bitan, u postratnom vremenu uključivao još i *POSLOVNU TAJNU* i *PROFESIONALNU TAJNU*. Formuliranjem Zakona o tajnosti podataka (ZOTP), koji je 2007. godine stupio na snagu i zamijenio dotadašnji Zakon o zaštiti tajnosti podataka (ZOZTP) iz 1996. godine, koncept *VRSTA TAJNE* nestao je iz upotrebe a u njemu definirani stupnjevi tajnosti klasificiranih dokumenata prevedeni su u pojednostavljenu shemu štićenja podataka *STUPNJEVIMA TAJNOSTI*:

- vrlo tajno,
- tajno,
- povjerljivo i
- ograničeno.

Vrste tajne *DRŽAVNA, VOJNA I SLUŽBENA TAJNA* nestale su u potpunosti iz upotrebe stupanjem na snagu ZOTP-a dok su druge dvije, *POSLOVNA* i *PROFESIONALNA* evoluirale i postale sastavnim dijelovima poslovnih i profesionalnih područja u okviru kojih se informacije na odgovarajući način štite. Usporedbom slika 3 i 4 s podacima u tablici 1 vidljivo je da se sazrijevanje mjera i standarda informacijske sigurnosti vremenski preklapa s porastom interesa znanstvene i istraživačke zajednice za područje intelektualnog vlasništva. Rezultati tih istraživanja omogućili su štićenje poslovnih informacija konceptima intelektualnog vlasništva (patentom, industrijskim dizajnom,…) i posebnim, novim zakonskim propisima umjesto dotadašnjim načinom putem *poslovne tajne* (EU IPR Helpdesk, pravilnici o intelektualnom vlasništvu). Dok je *poslovna tajna* evoluirala u skoro sva znanstvena i poslovna područja, *profesionalna tajna* je ostala skoro 'rezervirana' za medicine, odvjetništva, poreza, psihologije i dušebrižništva (*v. tablicu 2*).

Tablica 1. Broj objavljenih znanstvenih radova o intelektualnom vlasništvu u bazi SCOPUS (*po godinama*)

9	**12**	**24**	**34**	**41**	**57**	**91**	**152**	**357**	**570**	**719**	**933**	**1.478**	**1.795**	**1.811**	**2.091**	**1.969**
1964 - 81	1982 - 83	1984 - 85	1986 - 87	1988 - 89	1990 - 91	1992 - 93	1994 - 95	1996 - 97	1998 - 99	2000 - 01	2002 - 03	2004 - 05	2006 - 07	2008 - 09	2010 - 11	2012 - 13

Ukupno	**12.143**
Radovi u časopisima	8.131
Radovi u zbornicima	4.012

Izvor: www.scopus.com, upit: "intellectual property right" OR "intellectual property" OR "intellectual right" (14. travnja 2014.)

Tablica 2. Broj objavljenih znanstvenih radova u bazi SCOPUS 1951-2014 o profesionalnoj tajni (*po znanstveom području*)

Područje	**Broj radova**
Medicina i medicinska njega	84
Psihologija	7
Socijalne znanosti	7
Umjetnost i humanističke znanosti	1
Stomatologija	1
Ekonomija i financije	1
Neuroznanost	1
Farmakologija, toksikologija i farmaceutika	1
Neklasificirano	1
Ukupno	**93**
Radovi u časopisima	89
Radovi u zbornicima	4

Izvor: www.scopus.com, upit: "professional secret" (09. travnja 2014.)

Konceptualni model informacijske sigurnosti

Zakon o informacijskoj sigurnosti (ZOIS) donesen je u Hrvatskom saboru 2007. godine, zajedno sa ZOTP-om i time je zaokružen novi, unaprijeđeni zakonski okvir informacijske sigurnosti. Osim manjih izmjena ranije donesenih zakona (ZOZOP, ZOPPI) i izmjena ZOTP-a koje su uslijedile tijekom predpristupnih pregovora RH i EU, može se reći da je zakonski okvir informacijske sigurnosti već 2007. godine bio formiran u svim bitnim odrednicama.

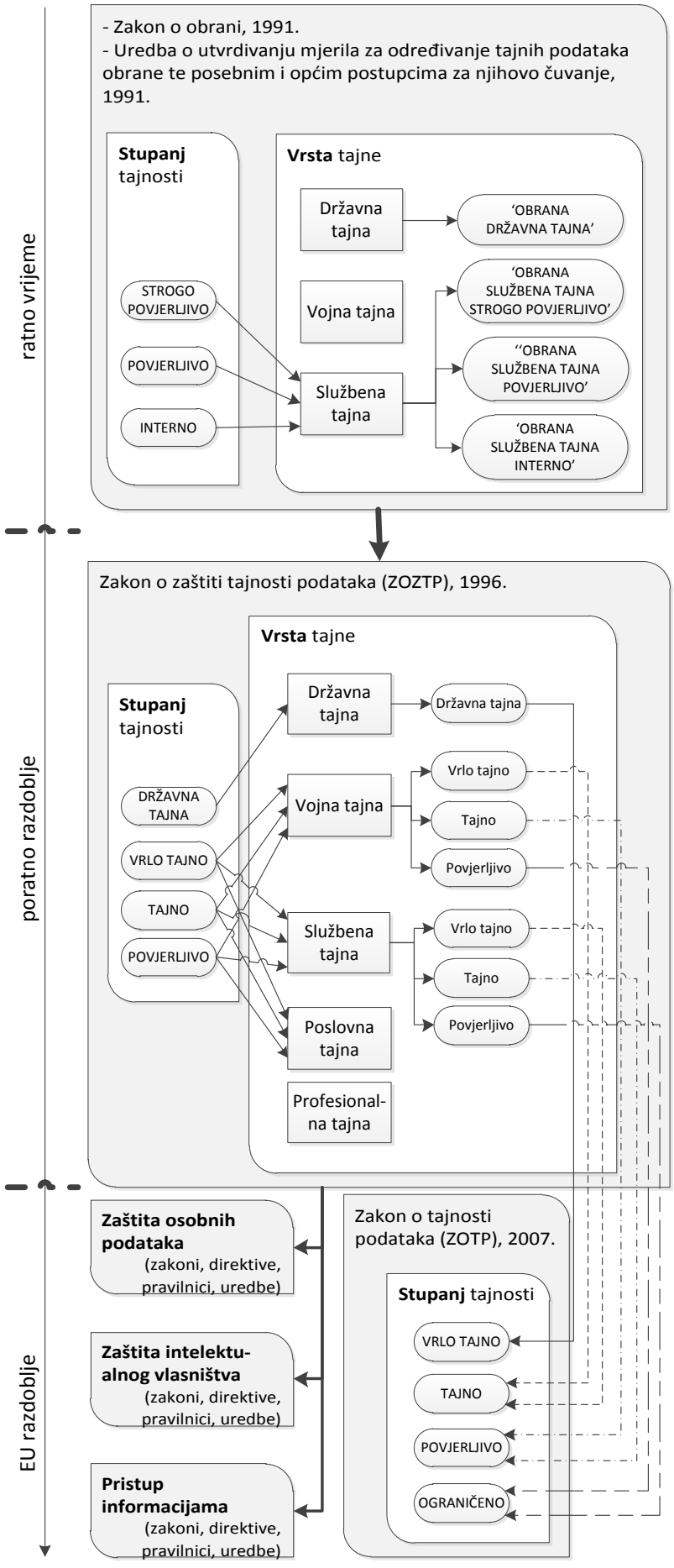
Zakon o informacijskoj sigurnosti propisuje ***mjere*** i ***standarde*** informacijske sigurnosti kojima se utvrđuju minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka za obveznike primjene ZOIS-a (*slika 5*). A obveznici njegove primjene su tijela javne uprave i pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke. ***Obveznici primjene*** ZOIS-a su također i ostale pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima. Nadalje, ZOIS pobliže definira pet ***područja primjene*** informacijske sigurnosti:

- sigurnosnu provjera,
- fizičku sigurnost,
- sigurnost podatka,
- sigurnost informacijskog sustava i
- sigurnost poslovne suradnje.

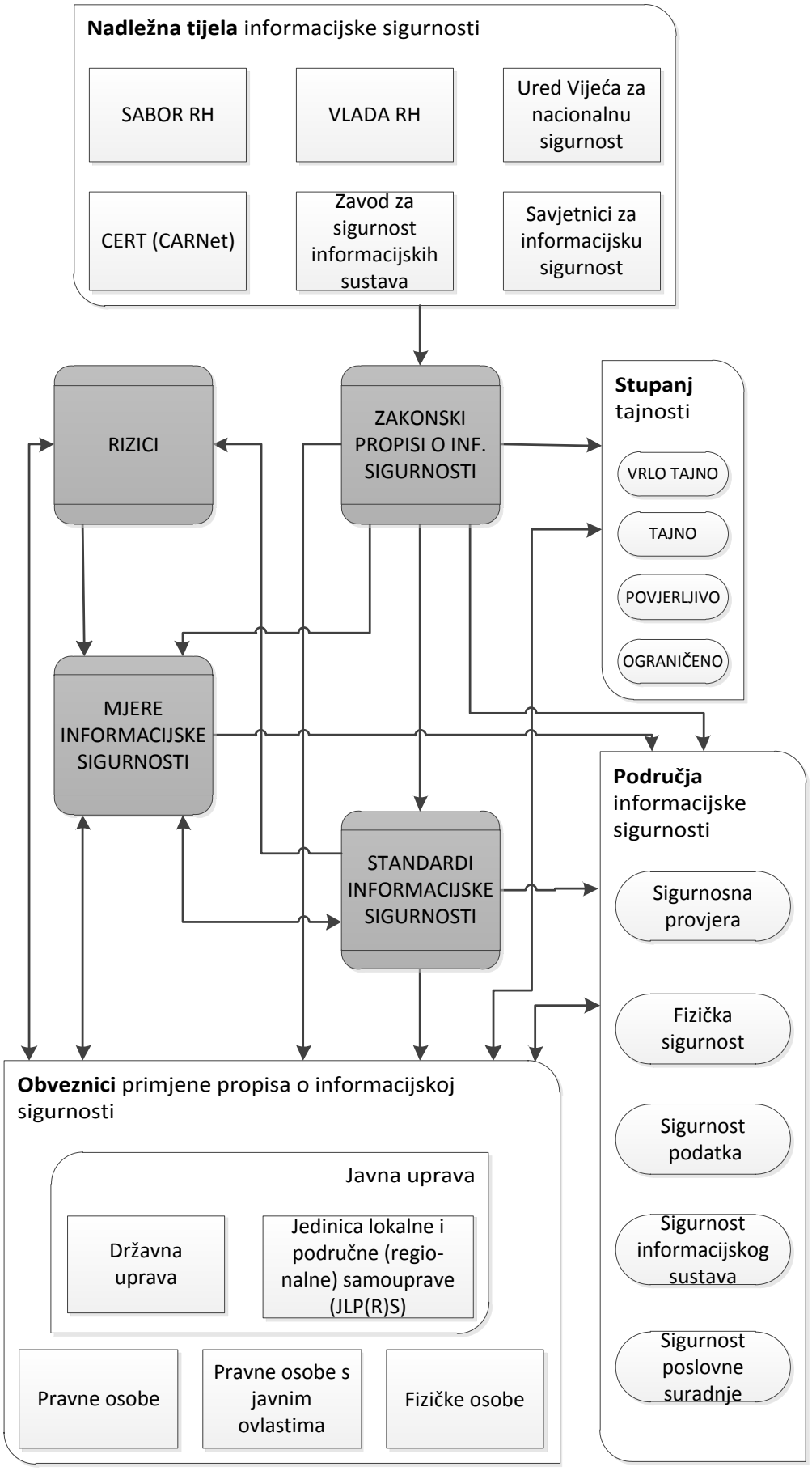
Nadležna tijela koja koordiniraju i usklađuju donošenje i primjenu mjera i standarda od strane obveznika primjene, te obavljaju poslove sigurnosne akreditacije informacijskih sustava i poslove prevencije i zaštite javnih informacijskih sustava također su opisana u ZOIS-u.

ZOIS je u skladu s temeljnim odredbama standarda ISO/IEC 27001 i ISO/IEC27002 [3] [6] [14] . Međutim, za efikasno upravljanje rizicima i uspostavu sustava upravljanja informacijskom sigurnošću preporučljivo je primijeniti neki kompletan interni [2] ili međunarodno prepoznati kvantitativni i kvalitativni model upravljanja rizicima, npr. NIST-ov model upravljanja rizicima [5] [7] [13] [14] .

Slika 4. Evolucija koncepata informacijske sigurnosti u tijelima državne uprave RH



Slika 5. Konceptualni model informacijske sigurnosti u RH



ZAKLJUČAK

U radu je napravljena kratka analiza temeljnih mjera i standarda informacijske sigurnosti ISO/IEC 27001 i ISO/IEC 27002 te je dan prikaz njihovog povijesnog razvoja i sazrijevanja u proteklih 20 godina. Ukazano je i na druge bitne pojedinačne sigurnosne mjere i preporuke i njihov odnos s ISO standardima kao osnovom izgradnje informacijske sigurnosti i sustava upravljanja informacijskom sigurnošću.

Prikazano je, nadalje, kako se područje informacijske sigurnosti javne uprave u Republici Hrvatskoj razvijalo tijekom proteklih 20-ak godina i kako je evoluiralo iz okrilja ratnog zakona o obrani u područje primjene prava na pristup informacijama, prava na zaštitu osobnih podataka te zaštite intelektualnog vlasništva. U radu je pojašnjeno kako je koncept VRSTA TAJNE (*državna – vojna – službena*), inicijalno temeljni koncept ***tajnosti podataka***, kroz ovih 15-20 godina 'umirovljen' i transformiran u suvremeni koncept VRSTA TAJNOSTI (*vrlo tajno – tajno – povjerljivo – ograničeno*), odnosno koncept ***informacijske sigurnosti***.

Usporedbom evolucije ovih koncepata u aktualnim zakonskim propisima RH s prikazom sazrijevanja temeljnih međunarodnih mjera i standarda informacijske sigurnosti, koji i jesu osnova zakonskih propisa RH, potvrđena je početna hipoteza o evolutivnom putu od 'tajnog' podatka ka 'štićenoj' informaciji.

U radu je napravljen i konceptualni model informacijske sigurnosti tijela javne uprave u RH koji se temelji na Zakonu o informacijskoj sigurnosti i s njime povezanim zakonima. Model može poslužiti tijelima javne uprave ali i ostalim pravnim subjektima za olakšanje provedbe Zakona o informacijskoj sigurnosti, odnosno za uspostavu sustava za upravljanje informacijskom sigurnošću (ISMS). Za informacijsku sigurnost je, naime, osim zakonskih propisa i novaca, potrebna i određena razina zrelosti. A zrelost se postiže ustrajnom primjenom propisa i unaprijeđenjem prakse.

LITERATURA

[1] Berghel, H.: **Better-Than-Nothing Security Practices**, Communications of the ACM, 50, 2007(8), 15-18, DOI: 10.1145/1278201.1278222

[2] Čelar, S.: **Project Management in IT-Projects - A Framework for the Risk Management Approach in SW Maintenance,** 16th International DAAAM Symposium, 19-22. listopada 2005, Vienna (Austria), 2005, 61-62

[3] Disterer, G.: **ISO/IEC 27000, 27001 and 27002 for Information Security Management**, Journal of Information Security, 4, 2013(2), 92-100

[4] Elof, J., Eloff, M.: **Information Security Management – A New Paradigm**, Proceedings of SAICSIT 2003, Rujan 2003, ACM, 2003, 130 –136

[5] Gantz, S.D., Philpott, D.R.: **FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security**, Syngress (Elsevier), ISBN: 978-1-59749-641-4, USA, 2013.

[6] Gikas, C.: **A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards**, Information Security Journal: A Global Perspective, DOI: 10.1080/19393551003657019, 19, 2010(3), 132-141

[7] Hardy, C.A., Williams, S.P.: **Managing Information Risks and Protecting Information Assets in a Web 2.0 era**, 23rd Bled eConference, eTrust: Implications for the Individual, Enterprises and Society, June 20 - 23, 2010; Bled, Slovenia, 2010. 234-247

[8] Humphreys, E.: **Information Security Management System Standards**, Datenschutz und Datensicherheit, 35, 2011(1), 7-11, DOI:10.1007/s11623-011-0004-3

[9] Julisch, K., Hall, M.: **Security and Control in the Cloud**, Information Security Journal: A Global Perspective, Taylor & Francis Group, ISSN: 1939-3555 print / 1939-3547 online, DOI: 10.1080/19393555.2010.514654, 19, 2010(6), 299–309

[10] Liautaud, B.: **e-Business Intelligence: Turning Information into Knowledge into Profit**, McGraw-Hill, Ney York, 2001.

[11] Panian, Ž., Klepac, G.: **Poslovna inteligencija**, Masmedia, Zagreb, 2003.

[12] Pelnekar, C.: **Planning for and Implementing ISO 27001**, ISACA Journal, 4, 2011(4), 1-8

[13] Radovanovic, D., Radojevic, T., Lucic, D., Sarac, M.: **Analysis of methodology for IT governance and information systems audit**, 6th International Scientific Conference, May 13–14, 2010, Vilnius, Lithuania, Business and Management 2010, Selected papers. Vilnius, 2010, 943-949

[14] Winkler, V.: **Securing the Cloud. Cloud Computer Security Techniques and Tactics**, Syngress (Elsevier), ISBN: 978-1-59749-592-9, Waltham, 2011.
[15] Zhu, L., Mao, H., Hu, Z.: **A New Construction Scheme for Information Security Lab**, Creative Education, 3, 2012(4), 406-412

Propisi

- Zakon o informacijskoj sigurnosti, Narodne novine, br. 79/2007,
- Uredba o utvrđivanju mjerila za određivanje tajnih podataka obrane te posebnim i općim postupcima za njihovo čuvanje, Narodne novine br. 70/1991.
- Zakon o pravu na pristup informacijama, Narodne novine br. 172/2003, 144/2010, 37/2011, 77/2011, 25/2013
- Direktiva 95/46/EZ Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom prijenosu takvih podataka (CELEX 31995L0046), 24. listopada 1995.
- Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima, Narodne novine br. 102/2007.
- Zakon o zaštiti osobnih podataka, Narodne novine br. 103/2003, 118/2006, 41/2008, 130/2011.

Internet

- International Organization for Standardization, ISO/IEC 27001:2013: "Information technology – Security techniques – Information security management systems – Requirements“, http://www.iso.org (10.4.2014.)
- European Intellectual Property Rights Helpdesk, https://www.iprhelpdesk.eu/ (10.4.2014.)
- Department of Defense, http://www.dtic.mil/whs/directives/ (10.4.2014.)

Interni dokumenti

- Pravilnik o upravljanju intelektualnim vlasništvom, Sveučilište u Splitu, Split, 2011.
- Pravilnik o poslovnoj i profesionalnoj tajni, Tehnički fakultet Sveučilišta u Rijeci, Rijeka, 2009. (http://www.riteh.uniri.hr/o_faxu/stat_prav/Pravilnik_o_poslovnoj_profesionalnoj_tajni.pdf)
- Pravilnik o poslovnoj i profesionalnoj tajni, Institut za fiziku, Zagreb, 2010. (http://www.ifs.hr/PublicDocuments/Pravilnik_o_poslo._i_profes._tajni.pdf)

BIOGRAFIJA PRVOG AUTORA

doc. dr. sc. Stipe Čelar
Sveučilište u Splitu, Fakultet elektrotehnike, strojarstva i brodogradnje
Split, Hrvatska
stipe.celar@fesb.hr

Doc. dr. sc. Stipe Čelar diplomirao je elektrotehniku na FESB-u 1992. godine a doktorirao tehničke znanosti na Technische Universitaet Wien (Beč, Austrija) 1997. godine. Po povratku u Hrvatsku 10 godina je radio na brojnim stručnim projektima softverskog inženjerstva u SME sektoru. Od 2008. godine je docent na Fakultetu elektrotehnike, strojarstva i brodogradnje (FESB) u Splitu. Sudjelovao je na nekoliko međunarodnih znanstveno-istraživačkih projekata koje su financirala ministarstva znanosti europskih država. Autor je tridesetak znanstvenih i stručnih radova u međunarodnim časopisima i zbornicima međunarodnih konferencija. Član je organizacijskog i znanstvenog odbora nekoliko desetaka međunarodnih znanstvenih konferencija. Član je više znanstvenih i stručnih

međunarodnih udruženja (IEEE, ACM, PMI, DAAAM). Područje njegovog znanstvenog i stručnog interesa uključuje softverske arhitekture, organizacijske arhitekture, strojno učenje, softverske metrike.

BIOGRAPHY OF THE FIRST AUTHOR

Stipe Celar Ph.D. completed his BSc in electrical engineering at the University of Split, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture (FESB, 1992) and PhD studies at the Vienna University of Technology (Vienna, Austria – 1997). After 10 years of experience in software engineering in the SME sector in Croatia and status of university honorary lecturer he moved to the University. Since 2008. he is Assistant Professor at FESB. He published about 30 scientific and professional articles and conference papers. He participated in few internationaly scientific research projects fund by science ministries of european countries. As a member of orgnanizing and scientific boards of international committees he participated in few dozens of international conferences. He is a member of IEEE, ACM, PMI, DAAAM. His fields of research and professional interests include information system and enterprise architectures, machine learning and software metrics.

PODACI O SUATORIMA (DATA ON CO-AUTHORS)

2)
dipl. iur. Dubravka Čelar
Ministarstvo unutarnjih poslova RH
Policijska uprava Splitsko-dalmatinska
Split, Hrvatska
dcelar@mup.hr

3)
mag.ing. comp. Mili Turić
Venio Indicium d.o.o.
Split, Hrvatska
mili.turic@venio.hr