Oznaka poročila: ARRS-RPROG-ZP-2014/39

ZAKLJUČNO POROČILO O REZULTATIH RAZISKOVALNEGA PROGRAMA

A. PODATKI O RAZISKOVALNEM PROGRAMU

1.Osnovni podatki o raziskovalnem programu

Šifra programa	P2-0057
Naslov programa	Informacijski sistemi
Vodja programa	11064 Marjan Heričko
Obseg raziskovalnih ur	19550
Cenovni razred	B
Trajanje programa	01.2009 - 12.2013
Izvajalci raziskovalnega programa (javne raziskovalne organizacije - JRO in/ali RO s koncesijo)	796 Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko
Raziskovalno področje po šifrantu ARRS	2 TEHNIKA 2.07 Računalništvo in informatika
Družbeno-ekonomski cilj	06. Industrijska proizvodnja in tehnologija
Raziskovalno področje po šifrantu FOS	1 Naravoslovne vede 1.02 Računalništvo in informatika

B. REZULTATI IN DOSEŽKI RAZISKOVALNEGA PROGRAMA

2.Povzetek raziskovalnega programa[1]

SLO

Raziskovalni program Informacijski sistemi celovito pokriva razvoj in upravljanje informacijskih sistemov (IS). Raziskovalno naslavljamo področja, ključna za uspešno in učinkovito zagotavljanje kakovostnih IS, in informacijsko-komunikacijske tehnologije (IKT), ki so se izoblikovale na teh področjih. V zadnjem obdobju delovanja raziskovalnega programa smo se tako osredotočili na razvoj novih pristopov, algoritmov in/ali metod na področjih življenjskih ciklov in procesnih modelov razvoja IS, razvoja spletnih storitev in storitvenih arhitektur, inteligentnih sistemov in sistemov na osnovi znanja, upravljanja z znanjem in semantičnih tehnologij, varnosti, zasebnosti in zaupanja, gradnje in načrtovanja vgrajenih sistemov ter zagotavljanja njihove zanesljivosti, e-izobraževanja oz. e-učenja in sprejetosti informacijskih rešitev, prav tako pa smo raziskovali tudi sociološke in kulturne vidike posredovanja informacij, ki jih omogočajo sodobne IKT. Kot tak je raziskovalni program močno v trendu aktualnih raziskav in inovacij na področju IKT ter izdatno naslavlja tehnologije, ki so v vzponu, med drugim računalništvo v oblaku, mobilne naprave in Internet stvari.

V zadnjem obdobju smo v okviru raziskovalnega programa objavili rezultate svojega dela v 97

izvirnih znanstvenih člankih, od tega 61 člankov v revijah JCR in 13 člankov v revijah iz prve četrtine revij JCR glede na faktor vpliva. Poleg tega smo člani raziskovalnega programa objavili še 33 strokovnih člankov, prispevali 29 samostojnih znanstvenih poglavij v monografskih publikacijah ter predstavili 166 znanstvenih člankov na konferencah. Opravili smo 6 vabljenih predavanj na mednarodnih konferencah in 31 predavanj na tujih univerzah, 63 krat smo se pojavili še v uredniški vlogi. Podeljen smo dobili tudi EU patent s področja varnega elektronskega vročanja.

Značilnost raziskovalnega programa Informacijski sistemi so uspešno vzpostavljeni mehanizmi prenosa znanja in močna povezanost z okoljem, tako lokalnim kot mednarodnim, na kar kaže tudi uvrstitev programa v najvišjo kategorijo po razmerju med znanstvenim delom oz. rezultati in sodelovanjem z drugimi uporabniki. Člani raziskovalnega programa smo vključeni v delo mnogih pomembnih mednarodnih odborov in delovnih teles, v zadnjem obdobju pa smo sodelovali pri štirih mednarodnih in devetih bilateralnih raziskovalnih projektih ter uspešno zaključili preko dvajset projektov v sodelovanju z gospodarstvom (eden pomembnejših je interdisciplinarni projekt @Life). Vzpostavili smo tudi več pomembnih mednarodnih povezav, med drugim z EIT ICT Labs, in sodelovali pri ustanovitvi spin-out podjetja Adora-Med. Uspešnost prenosa znanja pa se kaže tudi pri delu s študenti, pri čemer smo bili člani programa v zadnjem obdobju mentorji ali somentorji pri 17 doktoratih, 7 znanstvenih magisterijih, 332 diplomskih delih, 17 magistrskih delih na drugi in 174 diplomskih delih na prvi bolonjski stopnji.

ANG

The research programme Information Systems covers the field of development and the management of information systems (IS). We address research areas crucial for the efficient and successful delivery of quality IS, as well as information and communication technologies (ICT) formed in these areas. In the last period of operation, our research has focused on the development of new approaches, algorithms and/or methods in the areas of life cycles and IS development process models, the development of web services and service architectures, intelligent systems and knowledge-based systems, knowledge management and semantic technologies, security, privacy and trust, the design and implementation of embedded systems and ensuring their security, e-learning, and acceptance of IT solutions. Simultaneously, we have also studied the sociological and cultural aspects of information delivery and distribution, enabled by modern ICT. As such, the research programme is strongly in line with current research and innovation trends in ICT and addresses emerging technologies, including cloud computing, mobile devices and the Internet of Things.

Within the framework of the research programme, in the last operating period we published the results of our work in 97 original scientific articles, including 61 articles in JCR journals (13 articles in the first quarter of JCR journals with regard to the impact factor). In addition, members of the research programme have also published 33 professional articles, 29 scientific chapters in monographs and 166 scientific conference contributions. We have given six invited keynote lectures at international conferences and 31 lectures at foreign universities, and served in an editorial role 63 times. We were also awarded an EU patent in the field of electronic service of certified electronic messages.

An important characteristic of the research programme is that it successfully established knowledge transfer mechanisms and a strong connection with the environment, both local and international, as demonstrated by the classification of the programme in the highest category regarding the relationship between scientific work/results and collaboration with other users. The programme members are included in the work of many important international committees and working groups. In the last period, we coordinated four international and nine bilateral research projects and successfully completed over twenty projects in collaboration with industry (one of the most important being the interdisciplinary project @Life). We have established a number of important international connections, among others with EIT ICT Labs, and participated in the creation of the spin-out company, Adora-Med. The importance of knowledge transfer is also reflected in our work with students – in the last period members of the programme supervised or co-supervised 22 PhD theses, 7 MSc theses, 332 diploma works, 17 master theses on the second – and 174 diploma works on the first -- Bologna level.

3.Poročilo o realizaciji predloženega programa dela na raziskovalnem programu[2]

SLO

Raziskovalni program pokriva področja razvoja in upravljanja informacijskih sistemov (IS) in rešitev ter povezana področja vgrajenih sistemov, vseprisotnih rešitev, elektronskih medijev in informacijske družbe. Raziskovalni cilji so povezani z razvojem novih pristopov, algoritmov in/ali metod glede uporabe inteligentnih sistemov in semantičnega spleta, sistemov na osnovi znanja, razvoja varnih in zaupanja vrednih IS, sodobnih pristopov k razvoju IS in zagotavljanja kakovosti ter gradnje in načrtovanja vgrajenih sistemov.

Na področju življenjskih ciklov in procesnih modelov ter razvoja IS smo na podlagi pregleda obstoječih modelov vpeljave in vrednotenja projektov, razvitih s pristopom programskih tovarn in paradigmo produktnih linij, razvili nov model vrednotenja pridobitev, ki temelji na vrednotenju produktivnosti razvoja ter kakovosti razvitih rešitev. Razvili smo tudi pristop za analizo vpliva strukturnih sprememb izvorne kode in napovedovanje verjetnosti pojavljanja napak med zaporednim razvojem programske opreme z uporabo metrik kompleksnosti. Soavtorstvo prispevkov dokazuje naše sodelovanje na teh področjih z raziskovalci z Blekinge Institute of Technology iz Švedske ter Univerze v Novem Sadu. Proučevali smo tudi vplive lastnosti tehnik razvoja IS in značilnosti razvijalcev IS na sprejetost objektno-orientiranih programskih ogrodij. Na področju kakovosti razvoja IS smo raziskovali tudi uporabnost in sprejetost indeksa kakovosti (QI), ki se uporablja za izračun truda v projektih razvoja IS.

Z IJS in Univerzo v Alabami smo sodelovali pri zasnovi nove metodologije za razvoj programske opreme za sisteme vodenja, ki na izviren način povezuje sodobne pristope programskega inženirstva, in sicer koncepte domensko specifičnih modelirnih jezikov, modelno usmerjenega inženirstva in programskih produktnih linij.

Na področju razvoja spletnih storitev in storitvenih arhitektur smo raziskali model mediacije v storitveno orientiranih arhitekturah z uporabo storitvenih vodil in analizirali uporabo ESB za potrebe povezave in integracije storitev. Predlagali smo več razširitev SOA na področjih WSDL in BPEL.

Raziskave na področju uporabe inteligentnih sistemov in semantičnega spleta ter sistemov na osnovi znanja so bile osredotočene v dopolnjevanje semantičnih informacijskih rešitev z uvedbo sistemov na osnovi pravil. Razvili smo inovativni koncept semantične integracije, kar omogoča učinkovitejšo implementacijo metod inteligentnih sistemov za ekstrakcijo informacij. Model smo uporabili za optimizacijo procesa diagnosticiranja prolapsa mitralne valvule, kar omogoča izvajanje preventivne diagnostike v pediatriji v večjem obsegu in hitrejšim odkritjem sindroma pri mlajših otrocih. Z uporabo genetskih algoritmov za razvoj odločitvenih dreves v medicini smo razvili klasifikacijski model za zgodnje diagnosticiranje Alzheimerjeve bolezni na osnovi značilnosti, pridobljenih iz signalov EEG. Rezultati raziskav bodo uporabljeni za nadaljnje raziskave v smeri podpore zdravemu življenju, aktivnemu staranju in obvladovanju stresa v sklopu interdisciplinarnega industrijskega projekta @life (www.a-life.si).

Razvili smo pristopa in realizirali semantični aplikaciji za samodejno sestavo projektnih skupin ter sklepanje nad ontologijo bolezni v povezavi s specifičnimi geni. Razvili smo pristop za transparentno in performančno učinkovito integracijo distribuiranih heterogenih podatkovnih virov na osnovi semantično označenih storitev.

Na področju upravljanja znanja smo predstavili novo metodo klasifikacije podatkov na osnovi evolucijske gradnje odločitvenih pravil. Postopek strojno-podprtega učenja omogoča združitev domenskega ekspertnega znanja s samodejno indukcijo pravil in s tem iskanje novih pravil ter izvirnega znanja. Raziskovali smo tudi učinkovitost delovanja algoritmov nadzorovanega strojnega učenja, kjer smo razvili novo metodo za določanje pogojev, pod katerimi je možno s strojnim učenjem prenehati brez vpliva na končne performance algoritma. Pri tem smo sodelovali tudi s skupino raziskovalcev s Tampere University.

Na področju varnosti smo izvedli primerjavo protokolov za izmenjavo ključev. Na podlagi ugotovitev smo razvili nove algoritme ter njihovo uporabnost, učinkovitost in varnost tudi potrdili. Na interdisciplinarnem področju varnosti v medicinskih okoljih smo analizirali delovanje metode PsychoPass za generiranje gesel, kjer smo ugotovili pomanjkljivosti in predlagali izboljšave. Razvili smo algoritem, ki zaščiti originalne medicinske podatke in jih šifrira na način, da so zunanje podatkovne analize še vedno možne. Rezultate smo predstavili v Journal of Medical Internet Research, reviji najvišjega ranga v kategoriji Medical Informatics.

Na področju gradnje in načrtovanja vgrajenih sistemov ter zagotavljanja njihove zanesljivosti in varnosti smo izvedli raziskave na področju uporabe vgrajenih sistemov za potrebe inovativnih načinov implementacije algoritmov strojnega učenja. Rezultati raziskave so bili objavljeni kot poglavje v znanstveni monografiji. Izdelana in preizkušena je bila strojna implementacija EDF razvrščevalnega algoritma. Sicer pa na področju vgrajenih sistemov nadaljujemo sodelovanje s Fern University (prof. Halang).

Na področju e-izobraževanja oziroma e-učenja in sprejetosti informacijskih rešitev smo proučevali sprejetost sistemov za e-izobraževanje. Poiskali smo konstrukte, ki pomembno vplivajo na uporabnikovo dojemanje o uporabnosti sistemov za e-izobraževanje. Na podlagi empirične analize podatkov smo dopolnili model UTAUT.

Raziskovali smo tudi sociološke in kulturne vidike sodelovanja ter distribucije in posredovanja informacij, ki jih omogočajo sodobne informacijsko-komunikacijske tehnologije.

4. Ocena stopnje realizacije programa dela na raziskovalnem programu in zastavljenih raziskovalnih ciljev[3]

SLO

Na osnovi doseženih rezultatov in njihovih objav ocenjujemo, da smo dosegli cilje, navedene v prijavi raziskovalnega programa.

Raziskave so rezultirale v novih spoznanjih, pristopih, algoritmih in/ali metodah:

- model vrednotenja učinkovitosti uporabe in pridobitev pristopa programskih tovarn (objava v reviji Computer Science and Information Systems);
- pristop za analizo vpliva strukturnih sprememb izvorne kode in napovedovanje verjetnosti pojavljanja napak (rezultate sistematičnega pregleda literature smo objavili v JCR reviji Information&Software Technology, pristop pa v Computer Science and Information Systems);
- identifikacija faktorjev vpliva na sprejetost programskih ogrodij pri razvoju informacijskih rešitev (objave v Computers in Human Behavior; Journal of Systems and Software; Journal of Information Science and Engineering);
- definicija in validacija uporabnosti indeksa kakovosti programskih rešitev (objava v reviji Information Processing Letters);
- nova metodologija razvoja programske opreme za sisteme vodenja (objava v Control Engineering Practice);
- nov pristop k identifikaciji primernih načrtovalskih vzorcev in storitev (objava v reviji Informatica);
- razširitve jezikov za orkestracijo (BPEL) in definicijo storitev (WSDL) (objave v revijah Journal of Systems and Software, Information & Software Technology in Computer Languages, Systems & Structures);
- pristop nadgradnje semantičnih informacijskih rešitev z uvedbo sistemov na osnovi pravil in uporabnost genetskih algoritmov za razvoj odločitvenih dreves v medicini (objave v revijah Data Mining and Knowledge Discovery, Elektronika Ir Elektrotechnika in Lecture Notes in Computer Science);
- pristop za transparentno in performančno učinkovito integracijo distribuiranih heterogenih podatkovnih virov na osnovi semantično označenih storitev (objava v Computer Methods and Programs in Biomedicine);
- metoda za določanje pogojev, pod katerimi je smiselno prenehati s strojnim učenje brez vpliva na končne zmogljivosti algoritma (objava v reviji JCR Informatica);
- postopek za učinkovito zaščito medicinskih podatkov z možnostjo uporabe le-teh v analizi - analiza pomanjkljivosti in izboljšava metode PsychoPass za generiranje gesel (objava v Journal of Medical Internet Research);
- več učinkovitih algoritmov (protokolov) za overjanje in izmenjavo ključev (objave v revijah Computers & Security, Cryptologia, Computer Standards & Interfaces, Journal of Computer and System Sciences, Wireless personal communications);
- metanaliza faktorjev vpliva na sprejetost e-rešitev in e-storitev (objava v Computers in Human Behavior);
- identifikacija in implikacije vpliva sodobnih IKT (objave v revijah Empirical Software Engineering, Journal of information Security and Applications, Informatologia, Lex localis in Anthropological Notebooks).

5. Utemeljitev morebitnih sprememb programa raziskovalnega programa oziroma sprememb, povečanja ali zmanjšanja sestave programske skupine[4]

Programsko skupino je v letu 2011 zapustil dr. Matjaž B. Jurič, ki se je zaposlil na Univerzi v Ljubljani (FRI), kjer se je vključil v drug raziskovalni program.

V skupino pa smo vključili dr. Melito Zajc, dr. Suzano Žilič Fišer (obe 2011) in leta 2012 še dr. Boštjana Šumaka. Vključitev novih članov v raziskovalno delo programske skupine je prispevalo k interdisciplinarnosti opravljenih raziskav oz. je v primeru dr. Šumaka skladu s smernicami ARRS glede vključevanja mlajših raziskovalcev z odličnimi znanstvenimi rezultati.

6. Najpomembnejši znanstveni rezultati programske skupine[5]

	Znanstveni dosežek			
1.	COBISS ID		16928790	Vir: COBISS.SI
	Naslov	SLO	Zunanje izvajanje analiz medicinskih podatkov	
		ANG	Outsourcing medical data analyses	
			Namen prispevka je bil analizirati zasebnostne in zaupnostne zadržke v	

	Opis	*SLO*	povezavi s pravnimi normami, ki se pojavljajo pri obdelavi medicinskih podatkov. Nadalje, v okviru članka smo razvili postopek, s pomočjo katerega je možno zaščititi medicinske podatke na način, da lahko podatkovni analitik izvaja analize na zaščitenih podatkih, pa so analize kljub vsemu smiselne in rezultati primerljivi, če ne enaki, kot če bi analiziral originalne nezaščitene podatke. S pomočjo formalnih metod smo razvili algoritem za zaščito medicinskih podatkov za namene zunanjega izvajanja. Predlagani algoritem zaščiti originalne medicinske podatke in jih kriptira na način, da so zunanje podatkovne analize še vedno možne. Rezultati nakazujejo, da so rezultati analiz v večini primerov identični, ali pa vsaj primerljivi.
		ANG	In the paper we analyze the privacy and confidentiality issues and the associated regulations pertaining the medical data, and to identify technologies to properly address the issues. Secondly, the objective is to develop a procedure to protect medical data in such a way that the outsourced analyst is capable of doing the analyses on protected data, and the results are comparable, if not the same, as if they had been done on the original data. Using formal definitions, we developed an algorithm to protect medical data for outsourced analyses. The proposed algorithm encrypts a file with plaintext medical data into an encrypted file, where the data are protected in such a way that the external data analyses are still possible. The results show that in most cases the results of analyses on original and on protected data are identical or comparably similar.
	Objavljeno v		s. n.; Journal of medical internet research; 2013; Vol. 15, iss. 12; str. 1-18; Impact Factor: 3.768;Srednja vrednost revije / Medium Category Impact Factor: 1.785; A'': 1;A': 1; WoS: HL, PT; Avtorji / Authors: Brumen Boštjan, Heričko Marjan, Sevčnikar Andrej, Završnik Jernej, Hölbl Marko
	Tipologija		1.01 Izvirni znanstveni članek
2.	COBISS ID		16733462 Vir: COBISS.SI
	Naslov	*SLO*	Evolucijska gradnja odločitvenih dreves
		ANG	Evolutionary design of decision trees
	Opis	*SLO*	Najpomembnejši in kritični vidik odločitvenih dreves, ene najbolj priljubljenih simboličnih tehnik strojnega učenja, je proces njihove gradnje. Obstaja več indukcijskih algoritmov, ki uporabljajo načelo rekurzivnega pristopa od zgoraj navzdol za razdelitev učnih primerkov v podskupine, in temeljijo na različnih statističnih merah za doseganje homogenosti podskupin. Čeprav so le-ti robustni in hitri ter na splošno zagotavljajo dobre rezultate, lahko njihova deterministična in hevristična narava privede do neoptimalnih rešitev. Eden izmed najbolj plodnih alternativnih pristopov je uporaba evolucijskih algoritmov, ki lahko ustvarijo boljša odločitvena drevesa, saj iščejo globalno optimalno rešitev, ki zadošča hkrati več kriterijem kakovosti. V članku je uvodoma opisan in razložen celoten evolucijski proces gradnje odločitvenih dreves, ki ga nato podrobno demonstriramo v študiji primera nad izbrano podatkovno množico iz repozitorija UCI.
		ANG	Decision tree (DT) is one of the most popular symbolic machine learning approaches to classification with a wide range of applications. Decision treesare especially attractive in data mining. It has an intuitive representation and is, therefore, easy to understand and interpret, also by nontechnical experts. The most important and critical aspect of DTs is the process of their construction. Several induction algorithms exist that use therecursive top-down principle to divide training objects into subgroups based on different statistical measures in order to achieve homogeneous subgroups. Although being robust and fast, generally providing good results, their deterministic and heuristic nature can lead to suboptimal solutions. Therefore, alternative approaches have developed which try to

			overcome the drawbacks of classical induction. One of the most viable approaches seems to be the use of evolutionary algorithms, which can produce better DTs as they are searching for globally optimal solutions, evaluating potential solutions with regard to different criteria. We review the process of evolutionary design of DTs, providing the description of the most common approaches as wellas referring to recognized specializations. The overall process is first explained and later demonstrated in a step-by-step case study using a dataset from the University of California, Irvine (UCI) machine learning repository.
	Objavljeno v		John Wiley & Sons; Wiley interdisciplinary reviews, Data mining and knowledge discovery; 2013; Vol. 3, iss. 2; str. 63-82; Impact Factor: 1.422;Srednja vrednost revije / Medium Category Impact Factor: 1.024; A': 1; WoS: EP, EX; Avtorji / Authors: Podgorelec Vili, Šprogar Matej, Pohorec Sandi
	Tipologija		1.01 Izvirni znanstveni članek
3.	COBISS ID		14779926 Vir: COBISS.SI
	Naslov	*SLO*	Izboljšan protokol za izmenjavo ključev na podlagi identitet z uporabo operacij parjenja za dvostranska okolja
		ANG	An improved two-party identity-based authenticated key agreement protocol using pairings
	Opis	*SLO*	Protokoli za izmenjavo ključev za dvostranska okolja z uporabo operacij parjenja so aktualni na področju raziskav v kriptografiji. Predstavljenih je bilo že nekaj protokolov omenjenega tipa, ki so se izkazali kot ranljivi in posledični niso izpolnjevali zahtevanih varnostnih kriterijev. V prispevku predstavljamo učinkovit in varen protokol za izmenjavo ključev na podlagi identitet z uporabo operacij parjenja za dvostranska okolja, ki uporablja specifičen algoritem za elektronsko podpisovanje. V okviru članka smo prav tako izvedli primerjavo med predstavljenim protokolom in konkurenčnimi z vidika varnostni in učinkovitosti. Prispevek je rezultat raziskovalnega dela, v okviru katerega so bili razviti in publicirani tudi drugi overjeni protokoli za izmenjavo ključev in sicer v revijah s faktorjem vpliva, ki se uvrščajo v zgornjo polovico revij.
		ANG	Two-party authenticated key agreement protocols using pairings have gained much attention in the cryptographic community. Several protocols of this type where proposed in the past of which many were found to be flawed. This resulted in attacks or the inability to conform to security attributes. In this paper, we propose an efficient identity-based authenticated key agreementprotocol employing pairings which employs a variant of a signature scheme and conforms to security attributes. Additionally, existing competitiveand the proposed protocol are compared regarding efficiency and security. The criteria for efficiency are defined in this paper, whereas the criteria for security are defined by the fulfilment of security attributes from literature.
	Objavljeno v		Academic Press; Journal of computer and system sciences; 2012; Vol. 78, iss. 1; str. 142-150; Impact Factor: 1.000;Srednja vrednost revije / Medium Category Impact Factor: 1.024; WoS: ES, EX; Avtorji / Authors: Hölbl Marko, Welzer-Družovec Tatjana, Brumen Boštjan
	Tipologija		1.01 Izvirni znanstveni članek
4.	COBISS ID		17252886 Vir: COBISS.SI
	Naslov	*SLO*	Primerjava produktivnosti individualnega in skupinskega dela z uporabo namiznih orodij za modeliranje in orodij za modeliranje v oblaku
		ANG	An experimental investigation comparing individual and collaborative work productivity when using desktop and cloud modeling tools
			Kakovostna orodja za modeliranje morajo uspešno podpirati individualno in

	Opis	*SLO*	skupinsko delo (sodelovanje) v enotnem ter virtualnem okolju. Doseganje slednjega je bilo v preteklosti težavno, saj orodja za modeliranje običajno prihajajo v obliki namiznih aplikacij in so posledično primerna zgolj za posamično modeliranje oz. modeliranje v skupini v istem prostoru. Z vzponom spletnih arhitektur in oblačnih paradigem so namizna orodja za modeliranje dobila tekmece v spletnih različicah, ki so še posebej primerna za spletno oziroma e-sodelovanje. Cilj naše raziskave je bil odgovoriti na vprašanje »katera vrsta orodij za modeliranje (namizno ali v oblaku) je bolj učinkovita v primeru individualnega dela in e-sodelovanja«. Prav tako smo želeli identificirati prednosti in slabosti glede obeh vrst orodij za modeliranje. V ta namen smo izvedli nadzorovan eksperiment, ki je naslavljal dve vrsti modeliranih orodij – namizna in v oblaku, v zvezi z individualnim delom in e-sodelovanjem. Opazovali smo produktivnost 129 dodiplomskih študentov informacijskih tehnologij, ki so izvedli različne vrste modeliranih dejavnosti. V sklopu samoocenjevanja strokovnega znanja z izbranimi modeliranimi orodji med udeleženci ni bilo statistično signifikantnih razlik. Kljub temu so individualne aktivnosti končali hitreje z uporabo modelirnega orodja v oblaku. V primeru aktivnosti e-sodelovanja so bile razlike med namiznim orodjem in orodjem v oblaku signifikantne v prid slednjega. Rezultati raziskave nakazujejo, da so v primeru individualnega modeliranja orodja v oblaku primerljiva z namiznimi različicami, medtem ko so v primeru e-sodelovanja signifikantno boljša. Naše ugotovitve so skladne z obstoječimi raziskavami, ki navajajo, da lahko z uporabo sodobnih spletnih tehnologij orodja v oblaku dosegajo uporabniško izkušnjo namiznih aplikacij.
		ANG	Successful modeling tools need to effectively support individual as well as team-based work (collaboration) within colocated and virtual environments. In the past, achieving this has been challenging, since traditional modeling tools are desktop-based and thus suitable for individual and colocated work only. However, with the rise of web-based architectures and the cloud paradigm, desktop modeling tools now have rivals in their web-based counterparts that are especially suited for online collaboration (e-collaboration). The objective of our research was to probe the question as to 'which type of modeling tools (desktop or cloud-based) performs better in cases of individual work and e-collaboration', and to obtain insights into thesources of the strengths and weaknesses regarding both types of modeling tools. A controlled experiment was performed in which we addressed two types of modeling tools-desktop and cloud-based, in respect to two types of work-individual and e-collaboration. Within these treatments, we observed the productivity of 129 undergraduate IT students, who performed different types of modeling activities. The experimental participants reported no statistical significant differences between self-reported expertise with the investigated tools as well as their overall characteristics. However, they did finish individual and e-collaborative activities faster when using cloud modeling tool, where significant differences in favor of the cloud modeling tool were detected during e-collaboration. If we aggregate the results, we can argue that cloud modeling tools are comparable with desktop modeling tools during individual activities and outperform them during e-collaboration. Our findings also correlate with the related research, stating that with the use of state-of-the-art Web technologies, cloud-based applications can achieve the user experience of desktop applications.
	Objavljeno v		Kluwer; Empirical software engineering; 2013; str. 1-34; Impact Factor: 1.180;Srednja vrednost revije / Medium Category Impact Factor: 1.068; WoS: EW; Avtorji / Authors: Polančič Gregor, Jošt Gregor, Heričko Marjan
	Tipologija		1.01 Izvirni znanstveni članek
5.	COBISS ID		15270166 Vir: COBISS.SI
	Naslov	*SLO*	Meta-analiza sprejetosti tehnologij za e-učenje

		ANG	A meta-analysis of e-learning technology acceptance
	Opis	SLO	V obstoječi literaturi na področju sprejetosti tehnologij za e-učenje najdemo veliko neodvisnih študij, ki se ukvarjajo z raziskovanjem vzročnih povezav, definiranih na osnovi teorij sprejetosti tehnologij, kot je na primer teorija TAM. V študiji smo izvedli sistematični pregled literature 42 neodvisnih člankov, ki so bili objavljeni v glavnem v revijah s faktorjem vpliva in izvedli meta-analizo velikost vzročnih vplivov med TAM konstrukti. Rezultati študije so pokazali, da je (1) TAM najbolj sprejeta in uporabljena teorija v raziskavah, ki se ukvarjajo s sprejetostjo tehnologij za e-učenje, in (2) velikost vzročnih vplivov med posameznimi TAM konstrukti odvisna od tipa uporabnika in vrste tehnologije za e-učenje. Meta-analiza je za več kavzalnih povezav pokazala, da tako tip uporabnika kot vrsta tehnologije za e-učenje vplivata na velikost vpliva. Prav tako smo v študiji dokazali, da je velikost faktorjev dojete enostavnosti uporabe in uporabnosti na odnos do uporabe sistema neodvisna od vrste uporabnika in tehnologije za e-učenje.
		ANG	Existing literature in the field of e-learning technology acceptance reflects a significant number of independent studies that primarily investigate the causal relationships proposed by technology acceptance theory, such as the technology acceptance model (TAM). To synthesize the existing knowledge in the field of e-learning technology acceptance, we have conducted a systematic literature review of 42 independent papers, mostly published in major journals. Furthermore, in order to view the research context by combining and analyzing the quantitative results of the reviewed research studies, a meta-analysis of the causal effect sizes between common TAM-related relationships was conducted. The main findings of this study, which is the first of its kind, are: (1) TAM is the most-used acceptance theory in e-learning acceptance research, and (2) the size of the causal effects between individual TAM-related factors depends on the type of user and the type of e-learning technology. The results of the meta-analysis demonstrated a moderating effect for user-related factors and technology-related factors for several evaluated causal paths. We have gathered proof that the perceived ease of use and the perceived usefulness tend to be the factors that can influence the attitudes of users toward using an e-learning technology in equal measure for different user types and types of e-learning technology settings.
	Objavljeno v		Elsevier Science; Computers in human behavior; 2011; Vol. 27, iss. 6; str. 2067-2077; Impact Factor: 2.293;Srednja vrednost revije / Medium Category Impact Factor: 1.569; A'': 1;A': 1; WoS: VJ, VX; Avtorji / Authors: Šumak Boštjan, Heričko Marjan, Pušnik Maja
	Tipologija		1.02 Pregledni znanstveni članek

7.Najpomembnejši družbeno-ekonomski rezultati programske skupine[6]

	Družbeno-ekonomski dosežek			
1.	COBISS ID		17615382	Vir: COBISS.SI
	Naslov	SLO	Metoda in naprava za elektronsko vročanje elektronskih sporočil	
		ANG	Method and device for electronic service of certified electronic messages	
	Opis	SLO	Metoda in naprava za elektronsko vročanje elektronskih sporočil rešuje problem splošno uporabnega, varnega elektronskega vročanja. Metoda in naprava rešuje tehnični problem kako zagotoviti pošiljatelju sporočila, da bo po pošiljanju sporočila lahko prejel potrdilo o poslanem sporočilu in hkrati zagotoviti zaščito, ki bo prejemniku onemogočala vpogled v sporočilo, če ne bo potrdil elektronske vročilnice in to s čim manj ali brez posegov v obstoječo infrastrukturo za izmenjavo sporočil pri	

			pošiljatelju in prejemniku.
		ANG	Method and device for electronic service solves a technical problem of a generally useful, secure electronic service. Method and device for electronic service of certified electronic messages solves technical problem of assuring sender of the message that it can obtain the message sent receipt and provides protection that will prohibit receiving party reading of the message content without confirming electronic message received receipt at the same time with as minimum change in existing infrastructure of the sending and receiving party as possible.
	Šifra		F.32 Mednarodni patent
	Objavljeno v		Europäisches Patentamt = European Patent Office = Office européen des brevets; 2013; [3] str.; A'': 1;A': 1; Avtorji / Authors: Kežmah Boštjan, Kežmah Urška, Heričko Marjan
	Tipologija		2.24 Patent
2.	COBISS ID		13875478 Vir: COBISS.SI
	Naslov	*SLO*	Organizacija mednarodnih in domačih znanstvenih konferenc
		ANG	Organization of international and national scientific conferences
	Opis	*SLO*	Raziskovalni program je v okviru svojega financiranja deloval povezovalno v smislu organizacije številnih mednarodnih in nacionalnih znanstvenih ter strokovnih srečanj. Med najbolj odmevne mednarodne konference, ki smo jih organizirali v Mariboru, sodijo ECOOP 2010 - The 24th European Conference on Object-Oriented Programming (ecoop2010.uni-mb.si), EJC 2009 - European-Japanese Conference in EAEEIE 2011- The 22nd EAEEIE Annual Conference. Prva (ECOOP) je ena vodilnih konferencna področju objektno-usmerjenega razvoja in sorodnih tem, druga na področju upravljanja in modeliranja znanja, tretja pa je tradicionalna mednarodna konferenca združenja za izobražvanje v elektrotehniki in informacijskem inženirstvu. Med odmevne nacionalne konference sodi konferenca OTS Sodobne tehnologije in storitve. OTS je že od leta 1996 ena vodilnih neodvisnih IT konferenc v Sloveniji, ki povezuje in omogoča izmenjavo informacij o sodobnih informacijskih tehnologijah med strokovnjaki iz prakse in raziskovalci iz akademske sfere. Namenjena je IT/IS strokovnjakom in raziskovalcem kot tudi razvijalcem. Člani raziskovalnega programa pa so tudi uredniki, recenzenti ali programski vodje številnih konferenc. Med pomembnejše sodijo mednarodne konference KMO - Knowledge Management in Organizations in CESCIT - IFAC Conference on Embedded Systems, Computational Intelligence and Telematics in Control, IS - International Multiconference Information Society.
		ANG	The research programe has been acting in a linkable sense through the organization of several international and national scentific conferences. The most important international conferences include ECOOP 2010 - The 24th European Conference on Object-Oriented Programming, EJC 2009 - European-Japanese Conference, EAEEIE 2011- The 22nd EAEEIE Annual Conference. The first is the leading conference in the field of object-oriented development and related topics, the second one in the filed of knowledge management and modeling, the third one is the traditional international conference of the European Association For Education In Electrical And Information Engineering. The most important national conference organized by the members of the research program is the OTS conference (2009-2013) - Advanced technologies and services. It is one of the leading independent IT conferences in Slovenia connecting companies and academia enabling

			transfer of knowledge on advanced IS/IT approaches, tools, services and technologies. The conference is aimed at IS/IT professionals, researchers and developers. Additionally, the members of the research programe are also editors, reviewers and program chairs of several conferences. The most important include KMO - Knowledge Management in Organizations, CESCIT - IFAC Conference on Embedded Systems, Computational Intelligence and Telematics in Control, and IS - International Multiconference Information Society.
	Šifra		B.01 Organizator znanstvenega srečanja
	Objavljeno v		IOS Press; 2010; XI, 441 str.; A'': 1;A': 1; Avtorji / Authors: Welzer-Družovec Tatjana, Jaakkola Hannu, Kiyoki Yasushi, Tokuda Takehiro, Yoshida Naofumi
	Tipologija		2.01 Znanstvena monografija
3.	COBISS ID		13436182 Vir: COBISS.SI
	Naslov	*SLO*	Prenova in re-akreditacija študijskih programov Informatika in tehnologije komuniciranja
		ANG	Renewal and re-accreditation of curriculum Informatics and technologies of communication
	Opis	*SLO*	V skladu s smernicami bolonjskega procesa smo člani raziskovalnega programa v preteklem obdobju na osnovi analize izvajanja študijskih programov v preteklih letih izvedli celovito prenovo univerzitetnega, visokošolskega strokovnega in magistrskega študijskega programa Informatika in tehnologije komuniciranja. Tako je skupina optimizirala skladnost programa z zahtevami gospodarskega okolja in smernicami informacijske stroke ter sprožila postopke re-akreditacije. Magistrski študij IKT med drugim vključuje izrazito interdisciplinirani modul, imenovan storitvena znanost. Študijski program Informatika in tehnologije komuniciranja se izvaja na prvi in drugi bolonjski stopnji na Univerzi v Mariboru kot redni in izredni študij; število vseh študentov je okrog 500. Delovanje na tem področju neposredno ključno vpliva na G.01 razvoj visoko-šolskega izobraževanja, poleg tega pa še vsaj na G.2.6 večjo konkurenčno sposobnost in G.2.10 dvig izobrazbene strukture zaposlenih.
		ANG	In accordance with the guidelines of the Bologna process in the years 2012 our group carried out a complete renewal of the university, higher professional and master's degree program of curriculum Informatics and technologies of communication, based on the analysis of the implementation of the programs within the past 6 years. In this way we optimized the compliance of the program with the requirements and guidelines from the economic environment and IT profession and initiated the re-accreditation procedure. The curriculum Informatics and technologies of communication is implemented at the first and second Bologna level at the University of Maribor. The number of all students enrolled in these programs is currently approximately 500. Actions in this area have directly affected G.01 Development of higher education, as well as at least G.2.6 Boosting the competitive ability, and G.2.10 Rise of the educational level of employees.
	Šifra		D.10 Pedagoško delo
	Objavljeno v		Fakulteta za elektrotehniko, računalništvo in informatiko; 2009; IV, 70 str.; Avtorji / Authors: Grčar Bojan, Muškinja Nenad, Šafarič Riko, Dogša Tomaž, Hamler Anton, Kapus Tatjana, Družovec Marjan, Petek Tatjana, Cafuta Peter, Brest Janez, Podgorelec Vili, Brezočnik Zmago, Kačič Zdravko, Horvat Bogomir
	Tipologija		2.13 Elaborat, predštudija, študija

4.	COBISS ID		16957974	Vir: COBISS.SI
	Naslov	*SLO*	I3E: Pospeševanje inovacij na področjih industrijske informatike in vgrajenih sistemov z medsebojnim povezovanjem	
		ANG	I3E: Promoting Innovation in the Industrial Informatics and Embedded Systems Sectors through Networking	
	Opis	*SLO*	EU projekt iz programa SEE, financiran od 2009 do 2012. Cilji: (1) Vzpostavitev široke mednarodne mreže, ki bo vključevala nosilce tehnologij in promotorje inovacij iz akademske sfere, industrije in javnih ustanov; (2) Izdelava dokumenta za skupne strateške raziskovalne usmeritve (SRA-Strategic Research Agenda) za področji industrijske informatike in vgrajenih sistemov v Jugovzhodni Evropi (3); Izdelava metodoloških navodil za učinkovit prenos raziskav v inovacije (MGI-Methodology Guidelines for Innovation); (4) Promocija skupnih strateških raziskovalnih usmeritev in metodoloških navodil (SRA in MGI) na različnih nacionalnih in mednarodnih delavnicah in konferencah v območju Jugovzhodne Evrope; (5) Strateško povezovanje s sorodnimi iniciativami in interesnimi povezavami v Evropi ter z ustreznimi finančnimi mehanizmi v javnem in privatnem sektorju.	
		ANG	EU SEE programme project , financed from 2009 to 2012. Main goals: (1) Establishment of a broad international network, including technology leaders and promoters of innovations from the academy, industry and public institutions; (2) elaboration of the SRA-Strategic Research Agenda for the areas of industrial informatics and embedded systems in South - Eastern Europe; (3) establishing MGI-Methodology Guidelines for Innovation for the effective transfer of research results into innovations; (4) Promotion of common strategic research directions and methodological guidelines (SRA in MGI) at various national and international workshops and conferences in South-Eastern Europe; (5) Strategic collaboration of related initiatives as well as with appropriate financial mechanisms in public and private sector.	
	Šifra		D.01 Vodenje/koordiniranje (mednarodnih in domačih) projektov	
	Objavljeno v		s. n.; 2012; 88 str.; Avtorji / Authors: Kalogeras Athanasios P., Colnarič Matjaž, Jovan Vladimir	
	Tipologija		2.13 Elaborat, predštudija, študija	
5.	COBISS ID		16978710	Vir: COBISS.SI
	Naslov	*SLO*	Razvoj večplatformske rešitve @Life	
		ANG	Development of multi-platform solution @Life	
	Opis	*SLO*	V okviru interdisciplinarne projektne skupine @Life, ki jo sestavljajo strokovnjaki z več področij (kineziologije, psihologije, medicine, informatike) tako iz akademskih kot gospodarskih krogov, člani programske skupine aktivno sodelujemo pri zasnovi, vrednotenju in pilotnem razvoju informacijskih rešitev na osnovi najsodobnejših pristopov in tehnologij. Projekt @Life je namenjen razvoju inovativnih konceptov za nadzor in upravljanje s stresom ter doseganje boljšega počutja in zdravja z uporabo najsodobnejše IT podporo tako pri ovrednotenju trenutnega stanja posameznika kot pri usmerjanju in spremljanju doseganja zastavljenih osebnih ciljev. Rešitev združuje rešitve za pametne telefone z zalednim spletnim strežnikom in storitvami v oblaku. Uporabnik spremlja svoj napredek med izvajanjem fizičnih in psihičnih vaj, dokler ne doseže želenega stanja. Raziskovalni vidiki pri tem vključujejo predvsem uporabo naprednih pristopov k projektnemu vodenju v heterogenih okoljih, učinkovito predstavitev in vizualizacijo zdravstvenih kazalcev na spletu in mobilnih napravah, prilagajanje razvojnih pristopov mobilnim rešitvam in storitvam. Prve pilotne rešitve so že v produkciji – glej www.a-life.si.	

			Projekt @-life je aprila 2013 prejel priznanje Slovenskega društva Informatika na razpisu za najboljši projekt s področja informatike v letu 2013. V plenarnem delu konference DSI 2013 je nagrajeni projekt predstavil dr. Heričko.
		ANG	As a part of the inter-disciplinary @Life project group with experts from different domains (kinesiology, psychology, medicine, informatics), the members of the research program are actively involved in the conceptual and architectural design, evaluation and prototype development of the IT solution using the latest technological advances in IT and informatics. The @Life project is aimed at developing innovative concepts for stress management, well-being and healthy way of living, including state-of-the art IT support for assessment of the current state of the individual, as well as guidance towards specific personal goals. The solution combines smart phone solutions with a web enabled back-end system as well as cloud. The end user monitors progress while practicing different physical and psychical exercises until the desired state is reached. Research challenges include the use of innovative project management approaches in heterogeneous environments as well as on multidisciplinary research and development projects, efficient presentation and visualization of medical information in mobile and web-based solutions, adaptation of development approaches to the mobile development needs and services. First pilot solutions are already available online (www.a-life.si). The @life project received an award for the best IT project in 2013 from Slovenian Informatics Association. In the opening ceremony of the DSI 2013 conference, Dr. Heričko presented the awarded @life project.
	Šifra		F.11 Razvoj nove storitve
	Objavljeno v		[Fakulteta za elektrotehniko, računalništvo in informatiko]; 2013; Avtorji / Authors: Heričko Marjan, Pavlič Luka, Ovčjak Boris, Taneski Viktor, Gradišnik Mitja, Kuhar Saša, Živkovič Aleš, Košič Kristjan, Schweighofer Tina, Kocbek Mateja, Plavčak Gregor, Huber Jernej
	Tipologija		2.21 Programska oprema

8.Drugi pomembni rezultati programske skupine[7]

Člani raziskovalnega programa smo leta 2010 prejeli nagrado, ki je bila v sklopu SPRERS podeljena za objavo (s področja programskih storitev) raziskovalne skupine iz ene novih članic EU v reviji z velikim vplivom na raziskovalno skupnost.

9.Pomen raziskovalnih rezultatov programske skupine[8]

9.1.Pomen za razvoj znanosti[9]

SLO

Rezultati raziskav, ki smo jih izvajali v okviru raziskovalnega programa, vplivajo na razvoj znanosti področja informacijskih sistemov in povezanih področij.

Na področju inteligentnih sistemov smo razvili nove modele, metode in algoritme za inteligentno analizo podatkov iz kompleksnih podatkovnih zbirk ter za učinkovito vzpostavitev ekspertnih sistemov in baz znanja.

Raziskave na področju vseprisotnih sistemov ter na informacijskih tehnologijah temelječih storitev vplivajo na pristope za zagotavljanje učinkovitosti (tudi mobilnih) rešitev in e-storitev ter vrednotenje njihove sprejetost v družbenih in poslovnih okoljih.

Na področju varnosti in zaupanja smo prispevali nove in izboljšane modele, pristope, postopke za zagotavljanje varne izmenjave podatkov, njihove dokazne vrednosti, preprečevanja

zanikanja dejanj in varnosti ter zaupanja.

Na znanstvenem področju informacijskih sistemov je naš prispevek predvsem na področjih razvojnih modelov, napovedovanja napak ter načinov vrednotenja pridobitev mehanizmov ponovne uporabe kot so npr. ogrodja in programske tovarne. Izvirni so tudi predlagani pristopi za zagotavljanje kakovosti rešitev na osnovi uporabe metrik, s čemer prispevamo k razvoju empiričnega programskega inženirstva.

ANG

Our research activities and objectives have impacted the development of science in the field of information systems and in related research areas as well.

Research in the field of intelligent systems has resulted in new models, methods and algorithms for the intelligent data analysis of complex, big data from heterogeneous data sources, as well as for the efficient implementation of expert systems and knowledge bases.

The research of pervasive systems and acceptance of e-services impacts the efficiency of pervasive solutions and their acceptance in business and social environments.
Research in the field of security and trust has resulted in new and improved models, approaches and procedures to ensure secure information exchange, its probative value, assure non-repudiation and security and trust.

In the field of information systems our contribution is manifested in new and improved development models, fault prediction models, as well as the reuse evaluation of frameworks and software factories. Original approaches for software quality assurance contribute to the field of empirical software engineering.

9.2.Pomen za razvoj Slovenije[10]

SLO

Rezultati raziskovalnega programa so vidni skozi vpliv na razvoj, zagotavljanje in vrednotenje kakovosti in upravljanje informacijskih sistemov, rešitev in storitev. Omogočajo učinkovitejše poslovne procese in izboljšanje inovativnosti z visoko vključenostjo gospodarstva in javnega sektorja.

Dokaz, da je rezultate programske skupine mogoče posredno ali neposredno uporabiti v praksi, so mnoga uspešna sodelovanja s podjetji in organizacijami.

Pri obravnavi družbeno-ekonomskih vplivov posebej poudarjamo pomen že danes uspešnih aplikativnih rešitev raziskovalne skupine (npr. @life, ADORA). Pridobljene uporabniške izkušnje ter tehnološke aktualizacije spodbujajo raziskave ter možnost njihove neposredne uporabe v poslovnih okoljih (npr. uporaba inovativnih uporabniških vmesnikov v poslovnih in družbenih rešitvah). Znanstveno odličnost skupine obravnavamo kot predpogoj za uspešen družbeno-ekonomski vpliv znanstvenih rezultatov (npr. analiziranje sprejetosti novih rešitev preden se le te vpeljejo v realno okolje).

Primeri družbeno-ekonomskega pomena raziskovalnega programa, povezani s širšimi nacionalnimi, pa tudi evropskimi cilji so:
(1) prenos znanj s ciljem krepitve inovacijskega potenciala v sektorju informacijsko komunikacijskih tehnologij (npr. implikacije rezultatov sklopa inovacijski ekosistemi), skladno z Resolucijo o raziskovalni in inovacijski strategiji RS,
(2) izboljšanje kakovosti storitev gospodarskih družb, ki primarno ne delujejo na področju IKT (npr. povečanje uspešnosti in učinkovitosti upravljanja poslovnih procesov), vendar je le-ta ključna za njihov položaj na trgu,
(3) izboljšanje uporabniške participacije in transparentnosti delovanja javne uprave (npr. z uporabo razumljivih modelov procesov in z integracijo konceptov družbenega programja in upravljanja poslovnih procesov) ter
(4) povečana uporaba informacij javnega značaja kot veznega člena med javno upravo in novimi, inovacijsko usmerjenimi gospodarskimi družbami (npr. z uporabo vseprisotnih rešitev in sodobnih načinov komuniciranja).

ANG

The socio-economic dimensions of the research program are visible through its impact on development, quality assurance, and information system management. The results increase the efficiency of business processes and innovative improvements with the notable participation of industry representatives and the public sector. Considering the socio-economic impact of the research program, it is worth highlighting the importance of successful applied solutions (e.g. @life, ADORA). Research outcomes also resulted in the use of innovative user interfaces in business and social software. The scientific excellence of the research program is the key-enabling factor for socio-economic impacts (e.g. with an investigation of user acceptance of new IT solutions prior to real-world deployment). The list of socio-economic dimensions/impacts related to broader national (and also European) goals is as follows: (1) Knowledge transfer aimed at the reinforcement of innovative potential in ICT sectors (e.g. implications of the research of innovation ecosystems) in line with the goals of the Resolution on Research and Innovation Strategy of Slovenia. (2) Quality of service enhancement for ICT-dependent non-ICT companies, related to the first pillar of the Digital Agenda for Europe (DAE): Single Digital Market (e.g. with the improvement of effectiveness and efficiency of business process management). (3) Improved and increased user participation and of public administration operations transparency (e.g. with the use of understandable process models and with the integration of social software concepts and business process management). (4) Increased use and reuse of public sector information (e.g. with the use of pervasive computing and new ways of communicating) as a binding element of public administration and new/innovative SMEs.

10. Zaključena mentorstva članov programske skupine pri vzgoji kadrov v obdobju 1.1.2009-31.12.2013[11]

10.1. Diplome[12]

vrsta usposabljanja	število diplom
bolonjski program - I. stopnja	174
bolonjski program - II. stopnja	17
univerzitetni (stari) program	214

10.2. Magisterij znanosti in doktorat znanosti[13]

Šifra raziskovalca	Ime in priimek	Mag.	Dr.	MR	
25033	Marko Tekavc	◉	○	☐	
30943	Črt Gerlec	○	◉	☑	
30128	Aleš Frece	○	◉	☑	
29532	Tomaž Lukman	○	◉	☑	
23392	Boštjan Šumak	○	◉	☐	
29575	Boštjan Grašič	○	◉	☑	
27854	Andrej Krajnc	○	◉	☑	
24912	Aida Kamišalić Latifić	○	◉	☐	
29072	Andrej Sevčnikar	◉	○	☐	
4944	Giovanni Godena	◉	○	☐	
30942	Marcel Križevnik	○	◉	☑	

0	Jernej Bravc	◉	○	☐	
0	Tomaž Hunjadi	◉	○	☐	
0	Blanka Šauperl	◉	○	☐	
0	Dejan Paler	◉	○	☐	
23613	Katja Harej Pulko	○	◉	☑	
31768	Danijel Radjenović	○	◉	☐	
30948	Damjan Obal	○	◉	☑	
32011	Rok Žontar	○	◉	☑	
32733	Miro Puhek	○	◉	☐	
0	Andreja Špernjak	○	◉	☐	
25426	Marko Holbl	○	◉	☑	
27561	Luka Pavlič	○	◉	☑	
20034	Andrej Bregar	○	◉	☐	

Legenda:

Mag. - Znanstveni magisterij
Dr. - Doktorat znanosti
MR - mladi raziskovalec

11. Pretok mladih raziskovalcev – zaposlitev po zaključenem usposabljanju[14]

Šifra raziskovalca	Ime in priimek	Mag.	Dr.	Zaposlitev	
30943	Črt Gerlec	○	◉	E - Tujina	
27854	Andrej Krajnc	○	◉	D - Javni zavod	
30128	Aleš Frece	○	◉	A - raziskovalni zavodi	
27561	Luka Pavlič	○	◉	A - raziskovalni zavodi	
23613	Katja Harej Pulko	○	◉	A - raziskovalni zavodi	
25426	Marko Holbl	○	◉	A - raziskovalni zavodi	
29575	Boštjan Grašič	○	◉	E - Tujina	
29532	Tomaž Lukman	○	◉	E - Tujina	
30942	Marcel Križevnik	○	◉	C - Gospodarstvo	
30948	Damjan Obal	○	◉	C - Gospodarstvo	
32011	Rok Žontar	○	◉	E - Tujina	

Legenda zaposlitev:

A - visokošolski in javni raziskovalni zavodi
B - gospodarstvo
C - javna uprava
D - družbene dejavnosti
E - tujina
F - drugo

12. Vključenost raziskovalcev iz podjetij in gostovanje raziskovalcev, podoktorandov ter študentov iz tujine, daljše od enega meseca, v obdobju 1.1.2009-31.12.2013

Šifra raziskovalca	Ime in priimek	Sodelovanje v programski skupini	Število mesecev	

Legenda sodelovanja v programski skupini:
A - raziskovalec/strokovnjak iz podjetja
B - uveljavljeni raziskovalec iz tujine
C - študent – doktorand iz tujine
D - podoktorand iz tujine

13. Vključevanje v raziskovalne programe Evropske unije in v druge mednarodne raziskovalne in razvojne programe ter drugo mednarodno sodelovanje v obdobju 1.1.2009-31.12.2013 z vsebinsko obrazložitvijo porabe dodeljenih sredstev iz naslova dodatnega letnega sofinanciranja mednarodnega sodelovanja na podlagi pozivov za EU vpetost.[15]

SLO

Člani raziskovalnega programa Informacijski sistemi so vključeni v delo mnogih pomembnih mednarodnih odborov in delovnih teles, npr.:

- J. Györkös - član EU CONNECT Advisory Forum (CAF).
- M. Colnarič - predsednik IFAC CC3 (Computers, Cognition and Communication) & član IFAC Technical Board.
- T. Welzer Družovec - članica IFIP TC11 - Security and Privacy Protection in Information Processing Systems.
- M. Heričko - kot strokovni koordinator in predstavnik NESSI Slovenija aktivno sodeloval pri delu skupine za koordinacijo nacionalnih iniciativ evropske tehnološke platforme za programsko opremo in storitve (NESSI NIs).
- M. Hölbl – član NIS WG 3 (Network and Information Security – Working Group 3 on secure ICT research and innovation) in tajnik CEPIS LSI (Council of European Professional Informatics Societies – Legal and Security Issues Special Interest Network).

Mednarodni projekti:

- I3E - Pospeševanje inovacij na področjih industrijske informatike in vgrajenih sistemov z medsebojnim povezovanjem (Promoting Innovation in the Industrial Informatics and Embedded Systems Sectors through Networking); M. Colnarič, 12 partnerjev.
- PRAXIS project: Project/internship Excellence Center, Project Reference No. 518811-LLP-1-2011-1-PT-ERASMUS-ENW; T. Welzer Družovec.
- SALEIE project: Strategic Alignment of Electrical and Information Engineering in European Higher Education Institutions, Project Reference No. 527877-LLP-1-2012-1-UK-ERASMUS-ENW; T. Welzer Družovec.
- Mednarodno sodelovanje v mreži International Cooperation in Computer Science (CII-HU-0019-05), M. Heričko.

Bilaterani projekti:

- BI-CN/11-13-019: Ontology Based Advisement Approach for SOA Design Patterns, vodji: M. Heričko in L. Liu.
- BI-AT/09-10-004: Service invovation in small and medium enterprises, vodji: M. Heričko in R. Bernstein.
- BI-FI/09-09-007: Cultural awareness in information society, vodji: T. Welzer Družovec in H. Jaakkola.
- BI-FI/11-12-014: Improving the Acceptance of Business Process Models by Introducing Aspects, vodji: M. Heričko in J. Soini.
- BI-IT/11-13: Evaluation of the Quality Index using the Software Metrics Repository PROM, vodja: M. Heričko in G. Succi.
- BI-HU/11-12-011: Analysis of e-services acceptance factors in the future internet, vodji: M. Heričko in B. László.
- BI-RS/10-11-027: Towards a More Useful Software Metrics Tools, vodji: M. Heričko in Z. Budimac.
- BI-TR/11-13-008: New social movements, media and new communication technologies, vodji: T. Welzer Družovec in B. Yarar Doguyildizi.
- BI-ZDA/11-12-028: Efficient Data Utilization for Large-Scale Medical Processes, vodji T.

Welzer Družovec.in Vladimir I. Zadorozhny.

Kot gostujoči uredniki smo sodelovali pri izdaji posebnih številk pri naslednjih revijah:
- Information and Software Technology,Advances in functional size measurement and effort estimation, Vol 53, No. 8, 2011; A. Živkovič.
- International Journal of Web Engineering and Technology, Service Science Management and Engineering (SSME) or Service Science, Vol. 5, No. 3, 2009; M. Heričko.

14. Vključenost v projekte za uporabnike, ki v so obdobju trajanja raziskovalnega programa (1. 1. 2009 – 31. 12. 2013), potekali izven financiranja ARRS[16]

SLO

Člani raziskovalnega programa Informacijski sistemi so vključeni v številne projekte za uporabnike:
- Sodelovanje pri projektih KC CLASS (koordinatorji)
  - na področju PaaS in semantike (M. Heričko)
  - na področju IaaS in varnosti (T. Welzer Družovec, M. Hölbl)
  - na področju PaaS in mobilnih aplikacij (D. Verber)
- Sodelovanje s podjetji člani RC IKT Savinja, M. Heričko
  - interdisciplinarni projekt @life – obvladovanje stresa in spodbujanje zdravega načina življenja
  - vzpostavitev učinkovitih procesov razvoja sodobnih informacijskih rešitev in storitev
- Storitvena platforma za zdravstvo (iHUB) - varnostni vidiki, SRC d.o.o. in MVZT, M. Heričko
- Storitve v sklopu izvajanja postopkov akreditacije storitev v skladu z ZVDAGA, Arhiv RS, A. Živkovič
- Revizija projekta in informacijske rešitve, DARS, vodja: A. Živkovič
- Sodelovanje pri analizi in implementaciji upravljanja dostopovnega vozlišča telefonskih central preko enega IP naslova ter analiza, načrtovanje in implementacija podatkovne zbirke za shranjevanje podatkov centralnega upravljanja telefonskih central, Iskratel d.o.o., M. Colnarič
- Uvajalni projekt Vgrajena programska oprema družine pomorskih transponderjev BlueTraker, EMA, Celje, M. Colnarič
- Prenos izkušenj o sodobnih informacijskih tehnologijah in pristopih, Razvojni center IRC d.o.o., M. Heričko
- Sistem za razpisovanje in spremljanje projektov (SRSP), MO, projektni partnerji: Gaudeamus, izobraževanje, svetovanje, poslovne in informacijske storitve Simon Vrečar, s. p., eCTRL, INFORMACIJSKE TEHNOLOGIJE, d. o. o., A. Živkovič
- Sodelovanje na področjih obvladovanja, razvoja in prenove informacijskih sistemov po konceptih SOA, Informatika d.d. (do 2009), MB Jurič
- Svetovanje in sodelovanje pri organizaciji in procesih uvajanja in udejanjanja storitvene arhitekture v skupini Telekom Slovenija, do 2009, MB Jurič
- Svetovanje pri implementaciji razvitega podatkovnega modela podatkovnega skladišča in sistema OLAP za PIS ELES, I. Golob
- Študija izvedljivosti razvoja ter načrt implementacije baze znanja v okviru projekta Kontaktni center ZRSZ, M: Heričko
- Študija možnosti integracije modelov ebIX in BPMN (ebIX+BPMN), JARSE, M. Heričko
- Študija primernosti in upravičenosti uporabe odprtokodnih rešitev v portfoliju aplikacij ZRSZ, A. Živkovič
- Testiranje uporabnosti programske opreme COBISS/OPAC V6.0, IZUM, A. Živkovič
- Usposabljanje za načrtovanje realno-časovnih aplikacij z FPGA vezji, Apolon – Darko Obretan s.p., Maribor, M. Colnarič
- Vzpostavitev sistema za upravljanje znanja in izobraževanje (VSUZIZ), Razvojni center IRC Celje, d. o. o., I. Rozman
- CORE@UM Center za Odprte Inovacije in RaziskavE Univerze v Mariboru, MIZKŠ, koordinatorI: V. Podgorelec
- eCall4All -Usklajeni eCall: napredna e-storitev za pomoč voznikom v težavah, MIZKŠ, nosilec: Iskratel d.o.o., koordinator na II: B. Kežmah

Glede na predstavitev dr. Demšarja v Mariboru, 8.3.2013, ima raziskovalni program "Informacijski sistemi" ustrezno razmerje med znanstvenim delom/rezultati in sodelovanjem z drugi uporabniki - program je namreč po tem kriteriju uvrščen v kategorijo 1A.

15. Ocena tehnološke zrelosti rezultatov programa in možnosti za njihovo implementacijo v praksi (točka ni namenjena raziskovalnim programom s področij humanističnih ved)[17]

SLO

Dokaz, da je rezultate programske skupine mogoče posredno ali neposredno uporabiti v praksi,

so mnoga uspešna sodelovanja s podjetji in organizacijami kot tudi sodelovanje pri ustanovitvi spin-out podjetja Adora-Med.

Na področju varnosti informacijski sistemov je mogoče s pomočjo spoznanj pri snovanju varnih protokolov za izmenjavo ključev izboljšati obstoječe tehnike in postopke v smislu učinkovitosti in ob enaki stopnji varnosti. Omenjeni rezultati se tako lahko uporabljajo pri izboljšanju trenutnih programskih rešitev, predvsem tistih, ki so vezane na splet in računalništvo v oblaku in za učinkovito zaščito podatkov v medicini in tudi drugih domenah.

Rezultate na področju inteligentnih sistemov je mogoče uporabiti za bolj natančno vrednotenje uspešnosti strojnega učenja. Tako lahko ocenimo, kdaj prekiniti s strojnim učenjem ter tako optimizirati učenje in narediti strojno učenje kot orodje bolj učinkovito. Rezultati na področju strojnega učenja v medicinski diagnostiki zagotavljajo pomoč in usmerjanje zdravstvenega osebja s pomočjo informacijske tehnologije in bolj učinkovito in uspešno diagnostiko. Nadalje rezultati na področju učinkovite implementacije tehnik strojnega učenja omogočajo pohitritev omenjenih tehnik.

Razvit koncept semantične integracije podatkov iz heterogenih virov, ki je doslej preizkušen le v eni domeni, je v prihodnje treba preizkusiti z vidika prenosljivosti na druga področja in z vidika interoperabilnosti, skalabilnosti in performans. Pri vpeljavi v praksi je potrebno upoštevati še nivo tehnološke usposobljenosti okolij, kjer bi koncept želeli uporabiti.

Programabilna vezja skupaj z modelom kontrolne celice, ki neodvisno zaznava napake v delovanju vgrajenih sistemov, in strojno implementacijo EDF algoritma so osnova za načrtovanje robustnejših vgrajenih sistemov. To omogoča prodor adekvatnih teoretičnih rešitev v praktično uporabo. Zaradi dodatnih stroškov, ki jih zahteva vpeljava takšne tehnologije, so rešitve zaenkrat uporabne v kompleksnejših varnostno kritičnih sistemih, kjer je ta del stroškov dovolj majhen, da ne ogrozi celotnega projekta.

Določeni predlogi na področju storitvenih tehnologij in jezikov za modeliranje so primerni za vključitev v nove različice standardov WSDL in BPEL.

Neposredna uporaba dosežkov na področju razvoja sodobnih informacijskih rešitev se kaže tudi skozi sodelovanje na interdisciplinarnem projektu @life oz. celoviti rešitvi za obvladovanje stresa. Omenjena rešitev vključuje tako mobilne aplikacije kot spletni portal ter združuje znanja s področij kineziologije, psihologije, medicine in informatike. V sklopu projekta je pomembno ustrezno zagotavljanje varnosti in zaupnosti, zagotavljanje ustrezne zmogljivosti rešitev, prilagodljivost in visok nivo ponovne uporabe za zagotovitev produktivnosti kot tudi učinkovita in vizualizacija velikih količin podatkov. Celovita rešitev @life je tako tipičen primer prenosa rezultatov raziskav programske skupine v prakso.

16. Ocenite, ali bi doseženi rezultati v okviru programa lahko vodili do ustanovitve spin-off podjetja, kolikšen finančni vložek bi zahteval ta korak ter kakšno infrastrukturo in opremo bi potrebovali

možnost ustanovitve spin-off podjetja	(•) DA ( ) NE
potrebni finančni vložek	200.000
ocena potrebne infrastrukture in opreme[18]	Spin-out podjetje ADORA-MED d.o.o. je bilo ustanovljeno leta 2014 v sklopu univerzitenega inkubatorja. Zgoraj navedeni finančni vložek za komercializacijo rešitve za interaktivno podporo kirurškim posegom vključuje potreben trud za zaključne razvojne aktivnosti, certikacije in klinična testiranja ter potrebno opremo (namenska certificirana računaniška zasloni, naprave za HCI).

17. Izjemni dosežek v 2013[19]

17.1. Izjemni znanstveni dosežek

Izboljšava metode Psychopass

Na področju tekstovnih gesel se na raziskovalnem področju ni zgodil bistven preboj v zadnjih 35 letih. Tekstovna gesla so nizi alfanumeričnih znakov, ki si jih uporabnik mora zapomniti. PsychoPass metoda generiranja varnih tekstovnih gesel temelji na ideji, da si uporabnik ne zapomni niza znakov, pač pa grafično predstavitev znakov na določeni podlagi, konkretno na tipkovnici. Takšna predstavitev je mentalno manj zahtevna in je lažje zapomnljiva. V prispevku je predstavljena varnostna analiza metode PsychoPass za generiranje varnih gesel in njena varnostna izboljšava. Z izboljšano metodo PsychoPass je možno generirati lahko zapomnljiva gesla, ki so po dolžini primerljiva naključno izbranim geslom, hkrati pa distinkcija med naključno izbranimi gesli in PsychoPass gesli ni preprosta, kar precej otežuje napad z izdelavo posebno-namenskega slovarja.

17.2. Izjemni družbeno-ekonomski dosežek

Patent: Metoda in naprava za elektronsko vročanje certificiranih elektronskih sporočil

Ta izum rešuje problem splošno uporabnega, varnega elektronskega vročanja z značilnostmi:
- združljivost z obstoječimi protokoli in odjemalci za izmenjavo elektronskih sporočil (tudi spletnimi odjemalci kot npr. GMail),
- možnost avtomatizacije postopkov elektronskega vročanja brez spremembe obstoječega postopka prenosa dokumentov in brez posegov v obstoječo infrastrukturo,
- optimalno število izmenjanih sporočil med uporabniki sistema,
- možnost zagotavljanja zaupnosti sporočil tako, da ponudnik storitve nima vpogleda v njihovo vsebino,
- ne zahteva shranjevanja sporočil pri ponudniku storitve elektronskega vročanja,
- omogoča ločevanje ponudnika storitev vročanja, ponudnika zaračunavanja storitev in ponudnika prenosa in shranjevanja dokumentov ter
- delovanje sistema je neodvisno od vsebine in oblike poslanega sporočila.

C. IZJAVE

Podpisani izjavljam/o, da:
- so vsi podatki, ki jih navajamo v poročilu, resnični in točni
- se strinjamo z obdelavo podatkov v skladu z zakonodajo o varstvu osebnih podatkov za potrebe ocenjevanja in obdelavo teh podatkov za evidence ARRS
- so vsi podatki v obrazcu v elektronski obliki identični podatkom v obrazcu v papirnati obliki
- so z vsebino poročila seznanjeni in se strinjajo vsi izvajalci raziskovalnega programa

Podpisi:

zastopnik oz. pooblaščena oseba JRO in/ali RO s koncesijo:	in	*vodja raziskovalnega programa:*
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko		Marjan Heričko
_____		_____

ŽIG

Kraj in datum:	Maribor	11.4.2014

Oznaka prijave: ARRS-RPROG-ZP-2014/39

[1] Napišite povzetek raziskovalnega programa v slovenskem jeziku (največ 3.000 znakov vključno s presledki – približno pol strani, velikost pisave 11) in angleškem jeziku (največ 3.000 znakov vključno s presledki – približno pol strani, velikost pisave 11). Nazaj

[2] Napišite kratko vsebinsko poročilo, v katerem predstavite raziskovalno hipotezo in opis raziskovanja. Navedite

ključne ugotovitve, znanstvena spoznanja, rezultate in učinke raziskovalnega programa in njihovo uporabo ter sodelovanje s tujimi partnerji. Največ 12.000 znakov vključno s presledki (približno dve strani, velikosti pisave 11). Nazaj

[3] Realizacija raziskovalne hipoteze. Največ 3.000 znakov vključno s presledki (približno pol strani, velikosti pisave 11). Nazaj

[4] V primeru bistvenih odstopanj in sprememb od predvidenega programa dela raziskovalnega programa, kot je bil zapisan v predlogu raziskovalnega programa oziroma v primeru sprememb, povečanja ali zmanjšanja sestave programske skupine v zadnjem letu izvajanja raziskovalnega programa, napišite obrazložitev. V primeru, da sprememb ni bilo, to navedite. Največ 6.000 znakov vključno s presledki (približno ena stran, velikosti pisave 11). Nazaj

[5] Navedite znanstvene dosežke (največ pet), ki so nastali v okviru tega programa. Raziskovalni dosežek iz obdobja izvajanja programa (do oddaje zaključnega poročila) vpišete tako, da izpolnite COBISS kodo dosežka – sistem nato sam izpolni naslov objave, naziv, IF in srednjo vrednost revije, naziv FOS področja ter podatek, ali je dosežek uvrščen v A'' ali A'. Nazaj

[6] Navedite družbeno-ekonomske dosežke (največ pet), ki so nastali v okviru tega programa. Družbeno-ekonomski dosežek iz obdobja izvajanja programa (do oddaje zaključnega poročila) vpišete tako, da izpolnite COBISS kodo dosežka – sistem nato sam izpolni naslov objave, naziv, IF in srednjo vrednost revije, naziv FOS področja ter podatek, ali je dosežek uvrščen v A'' ali A'.

Družbeno-ekonomski dosežek je po svoji strukturi drugačen kot znanstveni dosežek. Povzetek znanstvenega dosežka je praviloma povzetek bibliografske enote (članka, knjige), v kateri je dosežek objavljen.

Povzetek družbeno-ekonomskega dosežka praviloma ni povzetek bibliografske enote, ki ta dosežek dokumentira, ker je dosežek sklop več rezultatov raziskovanja, ki je lahko dokumentiran v različnih bibliografskih enotah. COBISS ID zato ni enoznačen, izjemoma pa ga lahko tudi ni (npr. prehod mlajših sodelavcev v gospodarstvo na pomembnih raziskovalnih nalogah, ali ustanovitev podjetja kot rezultat programa … - v obeh primerih ni COBISS ID). Nazaj

[7] Navedite rezultate raziskovalnega programa iz obdobja izvajanja programa (do oddaje zaključnega poročila) v primeru, da katerega od rezultatov ni mogoče navesti v točkah 6 in 7 (npr. ker se ga v sistemu COBISS ne vodi). Največ 2.000 znakov vključno s presledki (približno 1/3 strani, velikost pisave 11). Nazaj

[8] Pomen raziskovalnih rezultatov za razvoj znanosti in za razvoj Slovenije bo objavljen na spletni strani: http://sicris.izum.si/ za posamezen program, ki je predmet poročanja. Nazaj

[9] Največ 4.000 znakov vključno s presledki. Nazaj

[10] Največ 4.000 znakov vključno s presledki. Nazaj

[11] Upoštevajo se le tiste diplome, magisteriji znanosti in doktorati znanosti (zaključene/i v obdobju 1. 1. 2009 – 31. 12. 2013), pri katerih so kot mentorji sodelovali člani programske skupine. Nazaj

[12] Vpišite število opravljenih diplom v času trajanja raziskovalnega programa glede na vrsto usposabljanja. Nazaj

[13] Vpišite šifro raziskovalca in/ali ime in priimek osebe, ki je v času trajanja raziskovalnega programa pridobila naziv magister znanosti in/ali doktor znanosti ter označite doseženo izobrazbo. V primeru, da se je oseba usposabljala po programu Mladi raziskovalci, označite MR. Nazaj

[14] Za mlade raziskovalce, ki ste jih navedli v tabeli 11.2. točke (usposabljanje so uspešno zaključili v obdobju od 1. 1. 2009 do 31. 12. 2013), ustrezno označite, kje so se zaposlili po zaključenem usposabljanju. Nazaj

[15] Navedite naslove projektov in ime člana programske skupine, ki je bil vodja/koordinator navedenega projekta. Točko izpolnijo tudi izvajalci raziskovalnega programa, prejemniki sredstev iz naslova dodatnega letnega sofinanciranja raziskovalnega programa zaradi mednarodnega sodelovanja (sodelovanja v projektih okvirnih programov Evropske unije). Izvajalec, ki je na podlagi pogodbe prejel sredstva iz navedenega naslova, vsebinsko opiše porabo prejetih sredstev za financiranje stroškov blaga in storitev ter amortizacije, nastalih pri izvajanju tega raziskovalnega programa. V primeru, da so bili v okviru raziskovalnega programa prejemniki sredstev različni izvajalci, vsak pripravi vsebinsko poročilo za svoj delež pogodbenih sredstev. Vodja raziskovalnega programa poskrbi, da je vsebinsko poročilo, ločeno za vsakega izvajalca, vključeno v navedeno točko poročila.
Največ 6.000 znakov vključno s presledki (približno ena stran, velikosti pisave 11). Nazaj

[16] Navedite naslove projektov, ki ne sodijo v okvir financiranja ARRS (npr: industrijski projekti, projekti za druge naročnike, državno upravo, občine idr.) in ime člana programske skupine, ki je bil vodja/koordinator navedenega projekta. Največ 3.000 znakov vključno s presledki (približno pol strani, velikosti pisave 11). Nazaj

[17] Opišite možnosti za uporabo rezultatov v praksi. Opišite izdelke oziroma tehnologijo in potencialne trge oziroma tržne niše, v katere sodijo. Ocenite dodano vrednost izdelkov, katerih osnova je znanje, razvito v okviru programa oziroma dodano vrednost na zaposlenega, če jo je mogoče oceniti (npr. v primerih, ko je rezultat izboljšava obstoječih tehnologij oziroma izdelkov). Največ 3.000 znakov vključno s presledki (približno pol strani, velikosti pisave 11). Nazaj

[18] Največ 1.000 znakov vključno s presledki (približno 1/6 strani, velikost pisave 11) Nazaj

[19] Navedite en izjemni znanstveni dosežek in/ali en izjemni družbeno-ekonomski dosežek raziskovalnega programa v letu 2013 (največ 1000 znakov, vključno s presledki, velikost pisave 11). Za dosežek pripravite diapozitiv, ki vsebuje sliko ali drugo slikovno gradivo v zvezi z izjemnim dosežkom (velikost pisave najmanj 16, približno pol strani) in opis izjemnega dosežka (velikost pisave 12, približno pol strani). Diapozitiv/-a priložite kot priponko/-i k temu poročilu. Vzorec diapozitiva je objavljen na spletni strani ARRS http://www.arrs.gov.si/sl/gradivo/, predstavitve dosežkov za pretekla leta pa so objavljena na spletni strani http://www.arrs.gov.si/sl/analize/dosez/. Nazaj

Obrazec: ARRS-RPROG-ZP/2014 v1.00a
A3-37-66-96-47-8E-67-8E-37-EB-02-09-44-F8-AF-81-9B-FC-FC-90

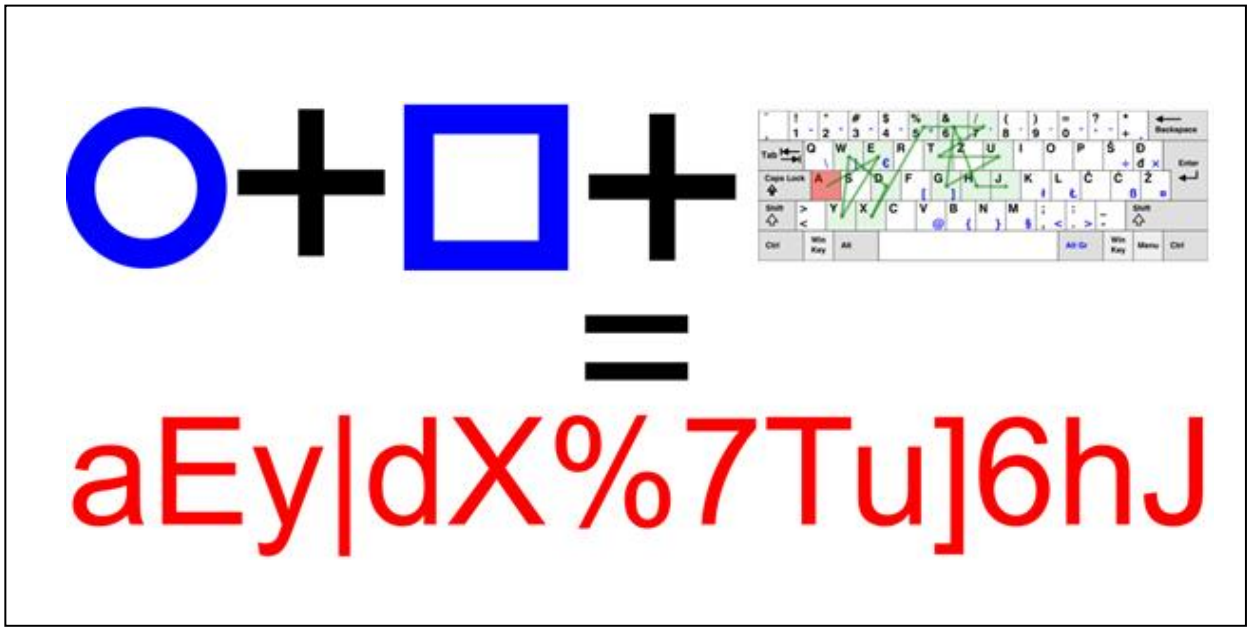
Priloga 1

TEHNIKA

Področje: 2.07 – Računalništvo in informatika

Dosežek: **Varnostna analiza in izboljšava metode PsychoPass za generiranje varnih gesel**

Vir: Brumen B, Heričko M, Rozman I, Hölbl M. Security Analysis and Improvements to the PsychoPass Method. J Med Internet Res 2013;15(8):e161. URL: http://www.jmir.org/2013/8/e161/, doi: 10.2196/jmir.2366 (prva revija s področja medicinske informatike glede na JCR IF)



Tekstovna gesla so Ahilova peta današnjih informacijskih sistemov, saj so povsem v domeni uporabnikov, ki se ne zavedajo pomena varnih gesel, pri čemer se glavnina avtentikacije še vedno odvija na nivoju preverjanja ujemanja dodeljenega uporabniškega imena z vnesenim geslom uporabnika. Na področju tekstovnih gesel se na raziskovalnem področju ni zgodil prav noben preboj v zadnjih 35 letih, vse odkar sta Morris in Thompson ugotovila pomanjkljivosti varovanja z gesli in članek objavila v poznih sedemdesetih letih prejšnjega stoletja. Tekstovna gesla so nizi alfanumeričnih znakov, ki si jih uporabnik mora zapomniti. PsychoPass metoda generiranja varnih tekstovnih gesel temelji na ideji, da si uporabnik ne zapomni niza znakov, pač pa grafično predstavitev znakov na določeni podlagi, konkretno na tipkovnici. Takšna predstavitev je mentalno manj zahtevna in je lažje zapomnljiva. V prispevku je predstavljena varnostna analiza PsychoPass metode za generiranje varnih gesel in njena varnostna izboljšava. Z izboljšano PsychoPass metodo je možno generirati lahko zapomnljiva gesla, ki so po dolžini primerljiva naključno izbranim geslom, hkrati pa distinkcija med naključno izbranimi gesli in PsychoPass gesli ni preprosta, kar precej otežuje napad z izdelavo posebno-namenskega slovarja.

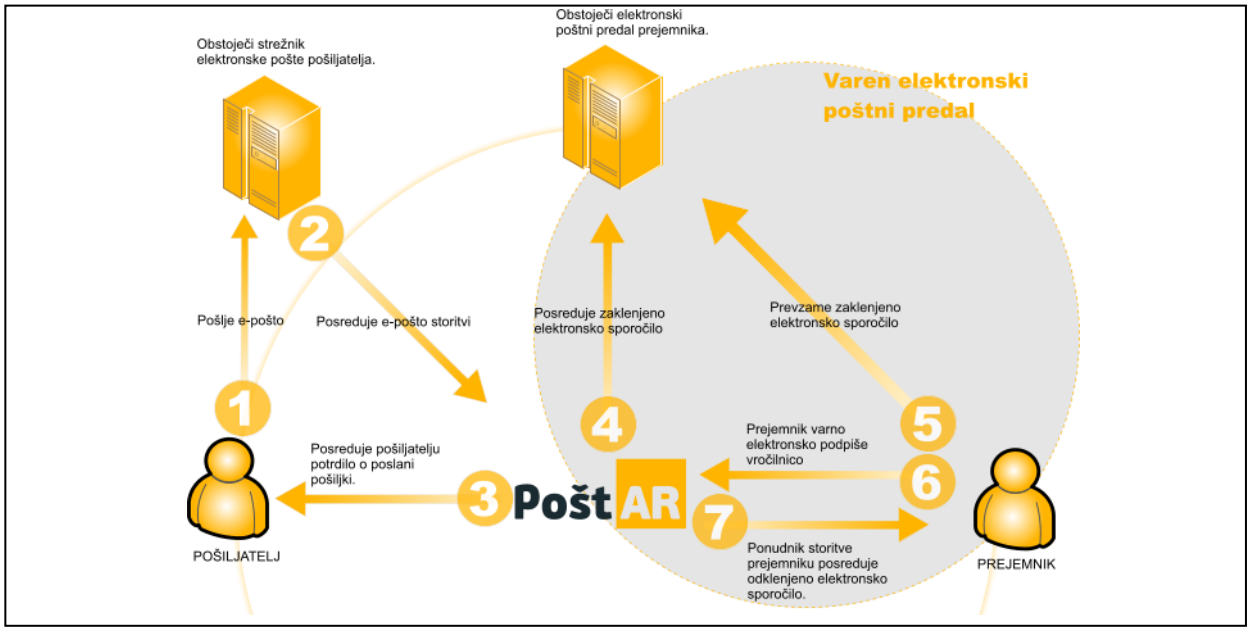
Priloga 2

TEHNIKA

Področje: 2.07 – Računalništvo in informatika

Dosežek: **Metoda in naprava za elektronsko vročanje certificiranih elektronskih sporočil**

Vir: KEŽMAH, Boštjan, KEŽMAH, Urška, HERIČKO, Marjan. Method and device for electronic service of certified electronic messages : EP 2365669 (B1), 2013-07-31. Munich: Europäisches Patentamt: = European Patent Office: = Office européen des brevets, 2013. [3] str. https://register.epo.org/application?number=EP10002543&tab=main.



Predmet tega patenta je naprava, metoda in sistem za elektronsko vročanje sporočil. Izum rešuje problem splošno uporabnega, varnega elektronskega vročanja z značilnostmi:

•Združljivost z obstoječimi protokoli in odjemalci za izmenjavo elektronskih sporočil (tudi spletnimi odjemalci kot npr. GMail).

•Možnost avtomatizacije postopkov elektronskega vročanja brez spremembe obstoječega postopka prenosa dokumentov in brez posegov v obstoječo infrastrukturo.

•Optimalno število izmenjanih sporočil med uporabniki sistema.

•Možnost zagotavljanja zaupnosti sporočil tako, da ponudnik storitve nima vpogleda v njihovo vsebino.

•Ne zahteva shranjevanja sporočil pri ponudniku storitve elektronskega vročanja.

•Omogoča ločevanje ponudnika storitev vročanja, ponudnika zaračunavanja storitev in ponudnika prenosa in shranjevanja dokumentov.

•Delovanje sistema je neodvisno od vsebine in oblike poslanega sporočila.