Oznaka poročila: ARRS-RPROJ-ZP-2010-1/64

ZAKLJUČNO POROČILO O REZULTATIH RAZISKOVALNEGA PROJEKTA

A. PODATKI O RAZISKOVALNEM PROJEKTU

1. Osnovni podatki o raziskovalnem projektu

Šifra projekta	L1-9659
Naslov projekta	Anonimizacija podatkovnih baz
Vodja projekta	8724 Aleksandar Jurišić
Tip projekta	L Aplikativni projekt
Obseg raziskovalnih ur	3.150
Cenovni razred	C
Trajanje projekta	01.2007 - 12.2009
Nosilna raziskovalna organizacija	101 Inštitut za matematiko, fiziko in mehaniko
Raziskovalne organizacije - soizvajalke	1539 Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
Družbeno-ekonomski cilj	13. Splošni napredek znanja - RiR financiran iz drugih virov (ne iz splošnih univerzitetnih fondov - SUF)

2. Sofinancerji[1]

1.	Naziv	Ministrstvo za zdravje RS
	Naslov	Štefanova 5, 1000 Ljubljana
2.	Naziv	
	Naslov	
3.	Naziv	
	Naslov	

B. REZULTATI IN DOSEŽKI RAZISKOVALNEGA PROJEKTA

3. Poročilo o realizaciji programa raziskovalnega projekta[2]

Delo je potekalo po programu. Opravljeno je bilo v treh fazah.

I. Analiza obstoječih modelov in algoritmov za anonimizacijo podatkovnih baz. Pri tem smo ugotovili, da obstaja več načinov reševanja problema, glede na potrebe sofinancerja pa je zanj najprimernejša rešitev kombinacija večih modelov.

II. Glede na potrebe naročnika smo izbrali in implementirali naslednja algoritma za implementacijo principa *k*-anonimnosti: Incognito in Mondrian.

III. V zadnji fazi smo opravili načrtovana testiranja na IVZ, in sicer v varni sobi na posebej pripravljenih bazah ob prisotnosti skrbnikov. Posebej smo testirali algoritme na bazi BS (bolniški staleži) ter PERIS (baza rojstev), ker vsebujeta veliko podatkov. Za bazo BS so kvazi identifikatorji že dobro znani, medtem ko jih je potrebno za bazo PERIS še dokončno definirati. Enako je potrebno storiti tudi za ostale baze.

I. in II. faza sta bili opisani že v prejšnjih letnih poročilih.

III. faza. V postopku testiranja smo zagnali algoritem za anonimizacijo ter primerjali rezultate tipičnih poizvedb na anonimiziranih ter originalnih podatkih. Ugotovili smo, da so odstopanja med rezultati poizvedb, izvedenih nad anonimiziranimi podatki, in rezultati poizvedb nad originalnimi podatki v večini primerov zelo majhna. Torej nam da anonimizacija kar dobre rezultate, ki jih je mogoče uporabiti tudi v praksi. Na podlagi rednih pogovorov z IVZ smo ugotovili, da anonimizacijo podatkov potrebujejo pri vsakodnevnem delu, saj morajo za namene raziskav oz. po zakonskih določilih zunanjim uporabnikom posredovati informacije, ki lahko vsebujejo tudi občutljive osebne podatke. Trenutno problematiko varovanja občutljivih osebnih podatkov rešujejo z odstranjevanjem občutljivih atributov. Pri tem velikokrat odstranijo informacije, ki jih ne bi bilo potrebno odstraniti. Včasih določen atribut le prikrijejo, a je ocena o stopnji prikritosti zelo subjektivna. S postopkom anonimizacije atribute na sistematičen način prikrijemo le do mere, da zaščitimo zasebnost posameznikov, katerih osebni podatki so vsebovani v bazi podatkov. Na takšen način lahko zunanjim uporabnikom brez ogrožanja zasebnosti posredujemo večjo količino podatkov, kar pomeni večjo uporabnost podatkov za raziskovalno delo. Ker pa za interne raziskave raziskovalci na IVZ včasih potrebujejo dostop tudi do osebnih podatkov, samo anonimizacija ni dovolj. V ta namen bi potrebovali varnostno politiko dostopa do podatkov ter nadzor dostopa do njih.

Naš projekt popolnoma sovpada s smernicami projekta "PRODOR" (informatizacija IVZ, 2006-2010), rezultati pa so pomembni za razvoj področja. Na podlagi testiranj in predhodne študije se pripravlja predlog anonimizacije baz kot rezultat triletnega projekta. V ta namen zaključujemo priročnik z natančnejšim opisom predloga rešitve. Priročnik vsebuje naslednje vsebine (s kratkim opisom poglavij):

1. **Uvod.** Podane so različne definicije zasebnosti, pregled zakonodaje glede doseganja zasebnosti in zahteve za učinkovitost algoritmov. Predstavimo problem vzdrževanja ravnovesja med uporabnostjo in zasebnostjo podatkov. Izhajamo iz dejstva, da imajo ljudje pravico do zasebnosti svojega zdravstvenega stanja, saj so zdravstveni podatki zasebni in kot taki zelo občutljivi.
2. **Opredelitev problema v zdravstvu**. Inštitut za varovanje zdravja Republike Slovenije (IVZ) je skrbnik velike količine podatkov, ki vsebujejo tudi osebne informacije o pacientih. Ti podatki se uporabljajo za razne raziskave in statistične obdelave. Zakon o varstvu osebnih podatkov narekuje, da jih morajo pred uporabo anonimizirati in zagotoviti uporabnost le-teh. Varnost pa je potrebno zagotoviti tudi že pri zbiranju, nato pri hrambi, kasneje pri obdelavi in končno pri objavi podatkov. V nadaljevanju je podan opis podatkovnih zbirk na IVZ-ju po različnih lastnostih.
3. **Podatkovne baze in varnost rudarjenja podatkov**. V poglavju pregledamo in opišemo celovitost podatkovnih baz (celovitost zapisa, pravilnost zapisa, celovitost obnavljanja), varnost podatkovnih baz (kontrola dostopa, sklepanje, združevanje) in varnost pri aplikacijah za rudarjenje podatkov.
4. **Kriptografski gradniki**. Predstavljeni so osnovni kriptografski algoritmi za simetrično kriptografijo in kriptografijo z javnimi ključi, digitalni podpis, zgoščevalne funkcije in protokoli, ki nam zagotavljajo varno komunikacijo. Le-ta nam zagotavlja zasebnost, overjanje, celovitost in preprečevanje možnosti zanikanja. Poleg osnovnih kripto-algoritmov smo vključili tudi pregled kripto-algoritmov, ki so povezani z anonimnostjo na splošno. S tem smo pripravili dobro izhodišče za sestavljanje povsem novih kriptografskih shem, ki jih potrebujemo za rešitev problema IVZ.
5. **Uporaba kriptografije za doseganje anonimnosti.** Navedeni so primeri uporabe kriptografije za doseganje anonimnosti. Posebej smo raziskovali anonimnost v zdravstvu. Za reševanje tega občutljivega problema, ki zahteva iskanje pravega ravnovesja med prikrivanjem in razkrivanjem podatkov, je bilo predlaganih več različnih pristopov.
6. **Anonimnost v zbirkah podatkov.** Predstavljen je koncept *k*-anonimnosti, ki sta ga predlagali Samarati in Sweeney ter princip ℓ-raznolikosti, ki so ga formulirali Machanavajjhala et al.
7. **Algoritmi.** Opisana je praktična implementacija anonimizacijskih principov, opisanih v

prejšnjem poglavju. Pokazali smo, da je že samo iskanje optimalne *k*-anonimizacije težek problem. Zato se v praksi uporabljajo aproksimacijski algoritmi, saj so eksaktni prepočasni. Implementirali smo dva aproksimacijska algoritma, ki zagotavljata zadovoljivo natančne rezultate. Na IVZ smo algoritme zagnali na podatkovnih bazah s podatki o bolniških staležih (BS), porodih in rojstvih (perinatalni informacijski sistem RS, PERIS) in bolnišničnih obravnavah (BOLOB). V tem poglavju je podana tudi analiza testiranj.

8. **Zaključek.** V zaključku so podani predlogi za doseganje računalniške varnosti in anonimizacije za potrebe IVZ.

4. Ocena stopnje realizacije zastavljenih raziskovalnih ciljev[3]

Delo na aplikativnem raziskovalnem projektu Anonimizacija podatkovnih baz (L1-9659) je potekalo po načrtu in je v celoti realizirano. Načrti projekta so izpolnjeni. Po podrobni analizi obstoječih modelov in algoritmov za anonimizacijo podatkovnih baz smo implementirali nekaj algoritmov, preverili njihovo delovanje na realnih podatkih ter podali predloge za njihovo uporabo na IVZ. V ta namen smo izdelali priročnik Anonimizacija baz podatkov.

5. Utemeljitev morebitnih sprememb programa raziskovalnega projekta[4]

Sprememb ni bilo.

6. Najpomembnejši znanstveni rezultati projektne skupine[5]

	Znanstveni rezultat		
1.	Naslov	*SLO*	Napredne metode varovanja podatkov in kriptografija
		ANG	Advanced methods of data protection and cryptography
	Opis	*SLO*	V elektronsko povezani družbi so informacije, transakcije, upravni in tehnološki postopki vezani izključno na uporabo digitalnih tehnologij. Zato je uporaba kriptografije ključen, če že ne nujen pogoj za varovanje in posredovanje občutljivih podatkov in s tem za varno delovanje družbe v celoti. V članku je prikazan spremenjen model varnosti podatkov ter obravnavana vloga, ki jo pri tem igra kriptografija. V novem modelu poudarek ni več na varovanju določenega teritorija (perimetra), ampak na varovanju posameznih podatkovnih struktur in aplikacij.
		ANG	Information, transactions, management and technological procedures in the e-connected society are exclusively based on digital technologies. Therefore, the use of cryptography is a key element for data security and secure transmission of sensitive data. As such, it is a key element for secure society as a whole. The article introduces a modified security model and discusses the role of cryptography within this model. In the new model, the emphasis is no longer on protection of a given territory (perimeter), instead the goal is to protect and secure individual data structures and applications.
	Objavljeno v		M. GOLOB in A. JURIŠIĆ, Bilt.-ekon. organ. inform. zdrav., jun. 2007, letn. 23, št. 2, str. 46-52.
	Tipologija		1.08 Objavljeni znanstveni prispevek na konferenci
	COBISS.SI-ID		1799397
2.	Naslov	*SLO*	Anonimizacija podatkovnih baz
		ANG	Database anonymization
	Opis	*SLO*	Obseg zbirk osebnih podatkov v današnjem času hitro narašča. Kadar se uporabljajo v raziskovalne namene, so zaželeni čim bolj natančni podatki. Hkrati pa je nujno zagotoviti zasebnost osebnih podatkov. Če podatke na račun varovanja zasebnosti preveč posplošimo, je oteženo delo raziskovalcev, ki v teh podatkih iščejo korelacije. V nasprotnem primeru so lahko razkriti občutljivi osebni podatki. Potrebno je poiskati pravo razmerje med uporabnostjo in zaupnostjo podatkov. V ta namen je bilo predlagano, da se uporabljajo anonimizirani podatki, ki zagotavljajo tako uporabnost kot tudi anonimnost.

		ANG	The amount of collected personal data is constantly increasing. These data are often used for research, where the most specific information is desired. At the same time it is necessary to assure privacy of personal data. If data are too general, the researchers have more difficulties when searching for correlations. If data are too specific, some sensitive personal information could be revealed. That is why the balance between the usefulness and the privacy of data has to be found. For this purpose the use of the anonymized data, which ensure usability and anonymity, was suggested.
	Objavljeno v		M. STANEK, A. JURIŠIĆ, M. BABIĆ, Bilt.-ekon. organ. inform. zdrav., 2009, letn. 25, št. 2, str. 53-59.
	Tipologija		1.02 Pregledni znanstveni članek
	COBISS.SI-ID		1024081748
3.	Naslov	*SLO*	Karakterizacija Pattersonovega grafa
		ANG	Characterization of the Patterson graph
	Opis	*SLO*	Karakterizacija nekaterih največjih diskretnih struktur, ki ne pripadajo nobeni neskončni družini (kot npr. Johnsonove ali Hammingove sheme), s pomočjo njihovih zaporedij presečnih števil. Največji med njimi je objekt, ki je povezan s sporadično enostavno končno grupo Suzukija. S tem smo dobili tudi karakterizacijo te izjemne grupe s samo sedmimi parametri. Gre za sporadičen primitiven objekt na 22.880 vozliščih in valenco 280 - pred tem je bil rekord za primitivne objekte 819 vozlišč, v splošnem pa 4096 vozlišč.
		ANG	Characterization of some of the biggest discrete structures, which do not belong to any of the infinite families (like Johnson and Hamming schemes), by using their intersection array. The biggest among them is an object related to the sporadic simple finite Suzuki group. In this way we characterized this remarkable group using only seven parameters. This is a sporadic primitive object with 22,880 vertices and valency 280 - before that the record mark was a primitive object on 819 vertices, and in general on 4096 vertices.
	Objavljeno v		A. E. Brouwer, A. Jurišić in J. H. Koolen, Journal of Algebra 320 (2008), 1186-1199.
	Tipologija		1.01 Izvirni znanstveni članek
	COBISS.SI-ID		14632537
4.	Naslov	*SLO*	Psevdo 1-homogeni razdaljno-regularni grafi
		ANG	Pseudo 1-homogeneous distance-regular graphs
	Opis	*SLO*	Cilj tega članka je bil posplošiti 1-homogene grafe, pri tem pa zadržati večino njihovih algebraičnih lastnosti.
		ANG	The aim of this paper was to relax the notion of 1-homogeneous graphs, while trying to maintain most of their algebraic properties.
	Objavljeno v		A. JURIŠIĆ in P. TERWILLIGER, J. Algebr. Comb., 2008, issue 4, vol. 28, str. 509-529.
	Tipologija		1.01 Izvirni znanstveni članek
	COBISS.SI-ID		14632793
5.	Naslov	*SLO*	Uporaba enakosti pri Kreinovih pogojih za dokaz neobstoja nekaterih razdaljno-regularnih grafov
		ANG	Using equality in the Krein conditions to prove nonexistence of certain distance-regular graphs
	Opis	*SLO*	Dokažemo, da razdaljno-regularni grafi s presečnim zaporedjem {74,54,15;1,9,60} in {4r^3+8r^2+6r+1, 2r(r+1)(2r+1), 2r^2+2r+1; 1,2r (r+1), (2r+1)(2r^2+2r+1)}, kjer je r poljubno naravno število, ne obstajajo. Oba primera služita kot ilustracija za tehniko, ki nam pomaga določiti strukturne lastnosti razdaljno-regularnih grafov in asociativnih shem z dovolj velikim številom ničelnih Kreinovih parametrov.
		ANG	The nonexistence of a distance-regular graphs with intersection array {74,54,15;1,9,60} and {4r^3+8r^2+6r+1, 2r(r+1)(2r+1), 2r^2+2r+1;1,2r (r+1), (2r+1)(2r^2+2r+1)}, with r a positive integer was proven. Both cases serve to illustrate a technique, which can help determine the structural properties for distance-regular graphs and association schemes with a sufficient number of vanishing Krein parameters.
	Objavljeno v		K. COOLSAET in A. JURIŠIĆ, J. Comb. Theory. Ser. A, 2008, vol. 115, iss. 6,

		str. 1086-1095.
	Tipologija	1.01 Izvirni znanstveni članek
	COBISS.SI-ID	15264601

7. Najpomembnejši družbeno-ekonomsko relevantni rezultati projektne skupine[6]

	Družbeno-ekonomsko relevantni rezultat		
1.	Naslov	*SLO*	Napredne metode varovanja podatkov in kriptografija
		ANG	Advanced methods of data protection and cryptography
	Opis	*SLO*	V elektronsko povezani družbi so informacije, transakcije, upravni in tehnološki postopki vezani izključno na uporabo digitalnih tehnologij. Zato je uporaba kriptografije ključen, če že ne nujen pogoj za varovanje in posredovanje občutljivih podatkov in s tem za varno delovanje družbe v celoti. V članku je prikazan spremenjen model varnosti podatkov ter obravnavana vloga, ki jo pri tem igra kriptografija. V novem modelu poudarek ni več na varovanju določenega teritorija (perimetra), ampak na varovanju posameznih podatkovnih struktur in aplikacij.
		ANG	Information, transactions, management and technological procedures in the e-connected society are exclusively based on digital technologies. Therefore, the use of cryptography is a key element for data security and secure transmission of sensitive data. As such, it is a key element for secure society as a whole. The article introduces a modified security model and discusses the role of cryptography within this model. In the new model, the emphasis is no longer on protection of a given territory (perimeter), instead the goal is to protect and secure individual data structures and applications.
	Šifra		B.06 Drugo
	Objavljeno v		A. JURIŠIĆ, M. GOLOB, Bilt.-ekon. organ. inform. zdrav., jun. 2007, letn. 23, št. 2, str. 46-52.
	Tipologija		1.08 Objavljeni znanstveni prispevek na konferenci
	COBISS.SI-ID		1799397
2.	Naslov	*SLO*	
		ANG	
	Opis	*SLO*	
		ANG	
	Šifra		
	Objavljeno v		
	Tipologija		
	COBISS.SI-ID		
3.	Naslov	*SLO*	
		ANG	
	Opis	*SLO*	
		ANG	
	Šifra		
	Objavljeno v		
	Tipologija		
	COBISS.SI-ID		
4.	Naslov	*SLO*	
		ANG	
	Opis	*SLO*	
		ANG	
	Šifra		
	Objavljeno v		

	Tipologija		
	COBISS.SI-ID		
5.	Naslov	*SLO*	
		ANG	
	Opis	*SLO*	
		ANG	
	Šifra		
	Objavljeno v		
	Tipologija		
	COBISS.SI-ID		

8. Drugi pomembni rezultati projetne skupine[7]

Delovno poročilo za IVZ, namenjeno za interno uporabo: anonimizacija podatkovnih baz (Anonymization of databases).

Opis: Študija izboljšave varovanja osebnih občutljivih podatkov v podatkovnih zbirkah IVZ. Z njo omogočimo uporabo podatkov v zbirkah v raziskovalne in druge namene, kljub temu da mora biti dostop do teh podatkov strogo nadzorovan in omogočen le pooblaščenim osebam.

9. Pomen raziskovalnih rezultatov projektne skupine[8]

9.1. Pomen za razvoj znanosti[9]

SLO

Varnost podatkovnih baz se je na področju kriptografije in računalniške varnosti kot raziskovalni problem pojavila že okoli leta 1980. Čeprav večine problemov do današnjega dne niso rešili, pa se je povečalo zanimanje zanje prav zaradi zahtevane zasebnosti zdravstvenih podatkov (npr. kartotek). Izvirnost naših rezultatov predstavlja znanstvena definicija problema anonimizacije podatkovnih baz IVZ, ki pa smo ga postavili v širši okvir - od zbiranja podatkov pa vse do njihove uporabe za medicinske in statistične študije. Predlagali smo praktični model, ki z učinkovitimi kriptografskimi in probabilističnimi metodami izboljša obstoječe stanje. Uporabili smo koncepta k-anonimnosti ter ℓ-raznolikosti. Pri tem smo študirali nove kriptografske sheme ter konkretne optimizacijske metode za povečano učinkovitost algoritmov. Preučevali smo učinkovite metode za anonimizacijo podatkovnih baz in jih preizkusili na dejanskih podatkih, ki smo jih prejeli od IVZ. Naš cilj je bil priti do praktične uporabe sodobnih tehnik za anonimizacijo. Algoritmi so se izkazali za učinkovite pri bolj statičnih podatkovnih bazah. Študijo je potrebno nadaljevati tudi na dinamičnih podatkovnih bazah (saj se v številnih primerih novi podatki neprestano dodajajo). Za te vrste baz bo potrebno razviti povsem nove algoritme za anonimizacijo, kar pa presega okvire tega projekta.

ANG

Database security became an active research area in the field of cryptography and computer security in the 1980s. Although the problems have not been solved the new medical privacy regulations are bringing about a resurgence. The novelty of our approach is the scientific formulation of the problem of database anonymization at IVZ that was considered within a broader framework - from data collection to its use for medical and statistical research. We proposed a practial model which uses efficient cryptographic and probabilistic methods to improve the current situation. The concepts of k-anonymity and ℓ-diversity were employed. We studied new cryptographic shemes and specific optimization methods for increased efficiency of the algorithms. We investigated new methods for database anonymization and tested them on the actual data that we received from IVZ. Our aim was to provide a practical application of known anonymization techniques. The algorithms proved to be effective in the case of more static databases. Our investigation needs to be continued also for dynamic databases (since in many cases new data are being constantly added). For these kind of databases completely new algorithms need to be designed, however this is out of the scope for this project.

9.2. Pomen za razvoj Slovenije[10]

SLO

Relevantnost in potencialni vpliv rezultatov sta neposredna, saj rešujemo konkreten pereč problem (torej ne gre samo za temeljne raziskave, pač pa za popolnoma problemsko orientirano raziskavo in pilotski projekt kot konkreten odgovor na zastavljeni problem).

Etični problem uporabe osebnih zdravstvenih podatkov je izjemen, s tem pa tudi obveznost, da se zagotovi anonimnost posameznika, kar je tudi opredeljeno v evropski in slovenski zakonodaji. V primeru IVZ je glede na obseg atributov individualnih zapisov, ki so vsebovani v posameznih zbirkah, število zbirk in možnosti njihovega povezovanja, zagotavljanje anonimnosti osebnih podatkov zahtevna naloga.

Do sedaj je IVZ problem zakrivanja osebnih podatkov reševal predvsem z večjo restriktivnostjo dostopa do uporabe podatkovnih zbirk in odstranjevanja občutljivih atributov. Večja restriktivnost pa je vplivala na manjši obseg in intenzivnost uporabe teh zbirk, zaradi česar ni bil izkoriščen poln potencial, ki bi ga uporaba takšne zbirke podatkov omogočala.

ANG

The proposed project is solving a concrete and urgent problem and its relevance and the potential impact of the results are immediate (the project is not only of theoretical value, it includes completely problem-oriented research and a pilot solution as a concrete answer to the posed questions).

The ethical problem of using personal medical data is enormous and so is the responsibility to guarantee the anonymity of individuals, as mandated by the European and Slovene legislature. In case of the National Health Institute of Slovenia (IVZ) the number of attributes for individual entries contained in the databases, and the sheer number of the databases and the possible links among them make the problem of ensuring the anonymity a daunting task.

So far the only methods of protecting personal data used at IVZ were to highly restrict the access to the databases and their use. The higher restrictiveness led to a smaller scope of use of these databases, defying their main purpose.

10. Samo za aplikativne projekte!
Označite, katerega od navedenih ciljev ste si zastavili pri aplikativnem projektu, katere konkretne rezultate ste dosegli in v kakšni meri so doseženi rezultati uporabljeni

Cilj		
F.01	**Pridobitev novih praktičnih znanj, informacij in veščin**	
	Zastavljen cilj	(•) DA ( ) NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.02	**Pridobitev novih znanstvenih spoznanj**	
	Zastavljen cilj	(•) DA ( ) NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.03	**Večja usposobljenost raziskovalno-razvojnega osebja**	
	Zastavljen cilj	(•) DA ( ) NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.04	**Dvig tehnološke ravni**	
	Zastavljen cilj	(•) DA ( ) NE
	Rezultat	Dosežen
	Uporaba rezultatov	Delno

F.05	**Sposobnost za začetek novega tehnološkega razvoja**	
	Zastavljen cilj	(•) DA ( ) NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.06	**Razvoj novega izdelka**	
	Zastavljen cilj	( ) DA (•) NE
	Rezultat	
	Uporaba rezultatov	
F.07	**Izboljšanje obstoječega izdelka**	
	Zastavljen cilj	( ) DA (•) NE
	Rezultat	
	Uporaba rezultatov	
F.08	**Razvoj in izdelava prototipa**	
	Zastavljen cilj	( ) DA (•) NE
	Rezultat	
	Uporaba rezultatov	
F.09	**Razvoj novega tehnološkega procesa oz. tehnologije**	
	Zastavljen cilj	(•) DA ( ) NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.10	**Izboljšanje obstoječega tehnološkega procesa oz. tehnologije**	
	Zastavljen cilj	(•) DA ( ) NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.11	**Razvoj nove storitve**	
	Zastavljen cilj	( ) DA (•) NE
	Rezultat	
	Uporaba rezultatov	
F.12	**Izboljšanje obstoječe storitve**	
	Zastavljen cilj	( ) DA (•) NE
	Rezultat	
	Uporaba rezultatov	
F.13	**Razvoj novih proizvodnih metod in instrumentov oz. proizvodnih procesov**	
	Zastavljen cilj	( ) DA (•) NE
	Rezultat	
	Uporaba rezultatov	
F.14	**Izboljšanje obstoječih proizvodnih metod in instrumentov oz. proizvodnih procesov**	
	Zastavljen cilj	( ) DA (•) NE

	Rezultat	
	Uporaba rezultatov	
F.15	**Razvoj novega informacijskega sistema/podatkovnih baz**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.16	**Izboljšanje obstoječega informacijskega sistema/podatkovnih baz**	
	Zastavljen cilj	◉ DA ○ NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.17	**Prenos obstoječih tehnologij, znanj, metod in postopkov v prakso**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.18	**Posredovanje novih znanj neposrednim uporabnikom (seminarji, forumi, konference)**	
	Zastavljen cilj	◉ DA ○ NE
	Rezultat	Dosežen
	Uporaba rezultatov	V celoti
F.19	**Znanje, ki vodi k ustanovitvi novega podjetja ("spin off")**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.20	**Ustanovitev novega podjetja ("spin off")**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.21	**Razvoj novih zdravstvenih/diagnostičnih metod/postopkov**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.22	**Izboljšanje obstoječih zdravstvenih/diagnostičnih metod/postopkov**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.23	**Razvoj novih sistemskih, normativnih, programskih in metodoloških rešitev**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	

	Uporaba rezultatov	
F.24	**Izboljšanje obstoječih sistemskih, normativnih, programskih in metodoloških rešitev**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.25	**Razvoj novih organizacijskih in upravljavskih rešitev**	
	Zastavljen cilj	◉ DA ○ NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.26	**Izboljšanje obstoječih organizacijskih in upravljavskih rešitev**	
	Zastavljen cilj	◉ DA ○ NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.27	**Prispevek k ohranjanju/varovanje naravne in kulturne dediščine**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.28	**Priprava/organizacija razstave**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.29	**Prispevek k razvoju nacionalne kulturne identitete**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.30	**Strokovna ocena stanja**	
	Zastavljen cilj	◉ DA ○ NE
	Rezultat	Dosežen
	Uporaba rezultatov	Uporabljen bo v naslednjih 3 letih
F.31	**Razvoj standardov**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.32	**Mednarodni patent**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.33	**Patent v Sloveniji**	

	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	
F.34	**Svetovalna dejavnost**	
	Zastavljen cilj	◉ DA ○ NE
	Rezultat	Dosežen
	Uporaba rezultatov	V celoti
F.35	**Drugo**	
	Zastavljen cilj	○ DA ◉ NE
	Rezultat	
	Uporaba rezultatov	

Komentar

11. Samo za aplikativne projekte!
Označite potencialne vplive oziroma učinke vaših rezultatov na navedena področja

	Vpliv	**Ni vpliva**	**Majhen vpliv**	**Srednji vpliv**	**Velik vpliv**	
G.01	**Razvoj visoko-šolskega izobraževanja**					
G.01.01.	Razvoj dodiplomskega izobraževanja	○	○	◉	○	
G.01.02.	Razvoj podiplomskega izobraževanja	○	◉	○	○	
G.01.03.	Drugo:	○	○	○	○	
G.02	**Gospodarski razvoj**					
G.02.01	Razširitev ponudbe novih izdelkov/storitev na trgu	◉	○	○	○	
G.02.02.	Širitev obstoječih trgov	◉	○	○	○	
G.02.03.	Znižanje stroškov proizvodnje	◉	○	○	○	
G.02.04.	Zmanjšanje porabe materialov in energije	◉	○	○	○	
G.02.05.	Razširitev področja dejavnosti	◉	○	○	○	
G.02.06.	Večja konkurenčna sposobnost	◉	○	○	○	
G.02.07.	Večji delež izvoza	◉	○	○	○	
G.02.08.	Povečanje dobička	◉	○	○	○	
G.02.09.	Nova delovna mesta	◉	○	○	○	
G.02.10.	Dvig izobrazbene strukture zaposlenih	◉	○	○	○	
G.02.11.	Nov investicijski zagon	◉	○	○	○	
G.02.12.	Drugo:	○	○	○	○	
G.03	**Tehnološki razvoj**					
G.03.01.	Tehnološka razširitev/posodobitev dejavnosti	◉	○	○	○	

G.03.02.	Tehnološko prestrukturiranje dejavnosti	◉	○	○	○	
G.03.03.	Uvajanje novih tehnologij	○	○	◉	○	
G.03.04.	Drugo:	○	○	○	○	
G.04	**Družbeni razvoj**					
G.04.01	Dvig kvalitete življenja	○	○	○	◉	
G.04.02.	Izboljšanje vodenja in upravljanja	○	○	◉	○	
G.04.03.	Izboljšanje delovanja administracije in javne uprave	○	○	○	◉	
G.04.04.	Razvoj socialnih dejavnosti	○	○	◉	○	
G.04.05.	Razvoj civilne družbe	○	○	◉	○	
G.04.06.	Drugo:	○	○	○	○	
G.05.	**Ohranjanje in razvoj nacionalne naravne in kulturne dediščine in identitete**	◉	○	○	○	
G.06.	**Varovanje okolja in trajnostni razvoj**	◉	○	○	○	
G.07	**Razvoj družbene infrastrukture**					
G.07.01.	Informacijsko-komunikacijska infrastruktura	○	○	○	◉	
G.07.02.	Prometna infrastruktura	◉	○	○	○	
G.07.03.	Energetska infrastruktura	◉	○	○	○	
G.07.04.	Drugo:	○	○	○	○	
G.08.	**Varovanje zdravja in razvoj zdravstvenega varstva**	○	○	○	◉	
G.09.	**Drugo:**	○	○	○	○	

Komentar

12. Pomen raziskovanja za sofinancerje, navedene v 2. točki[11]

1.	**Sofinancer**	Ministrstvo za zdravje RS		
	Vrednost sofinanciranja za celotno obdobje trajanja projekta je znašala:		33.384,00	**EUR**
	Odstotek od utemeljenih stroškov projekta:		25,00	**%**
	Najpomembnejši rezultati raziskovanja za sofinancerja			**Šifra**
	1.	Anonimizacija podatkovnih baz.		A.02
	2.	Praktična uporaba postopkov k-anonimizacije in ℓ-raznolikosti pri anonimizaciji podatkovnih baz.		F.01
	3.	XXV. delavnica iz kriptografije in anonimizacije, Lj, IVZ: 18.,20.2.09): glej http://lkrv.fri.uni-lj.si/~ajurisic/seminar/stari_seminarji.html#09		F.03
	4.	Strokovna ocena stanja je podana v priročniku Anonimizacija baz podatkov.		F.30
		Svetovanje o uporabi kriptografskih metod za doseganje		

		5.	anonimizacije je podano v priročniku Anonimizacija baz podatkov.	F.34
	Komentar			
	Ocena		V celoti izpolnjen načrt.	
2.	**Sofinancer**			
	Vrednost sofinanciranja za celotno obdobje trajanja projekta je znašala:			**EUR**
	Odstotek od utemeljenih stroškov projekta:			**%**
	Najpomembnejši rezultati raziskovanja za sofinancerja			**Šifra**
		1.		
		2.		
		3.		
		4.		
		5.		
	Komentar			
	Ocena			
3.	**Sofinancer**			
	Vrednost sofinanciranja za celotno obdobje trajanja projekta je znašala:			**EUR**
	Odstotek od utemeljenih stroškov projekta:			**%**
	Najpomembnejši rezultati raziskovanja za sofinancerja			**Šifra**
		1.		
		2.		
		3.		
		4.		
		5.		
	Komentar			
	Ocena			

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, za objavo 6., 7. in 8. točke na spletni strani http://sicris.izum.si/ ter obdelavo teh podatkov za evidence ARRS
- so vsi podatki v obrazcu v elektronski obliki identični podatkom v obrazcu v pisni obliki
- so z vsebino zaključnega poročila seznanjeni in se strinjajo vsi soizvajalci projekta

Podpisi:

Aleksandar Jurišić	in	
podpis vodje raziskovalnega projekta		zastopnik oz. pooblaščena oseba RO

Kraj in datum:	Ljubljana	19.4.2010

Oznaka poročila: ARRS-RPROJ-ZP-2010-1/64

---

[1] Samo za aplikativne projekte. Nazaj

[2] Napišite kratko vsebinsko poročilo, kjer boste predstavili raziskovalno hipotezo in opis raziskovanja. Navedite ključne ugotovitve, znanstvena spoznanja ter rezultate in učinke raziskovalnega projekta. Največ 18.000 znakov vključno s presledki (približno tri strani, velikosti pisave 11). Nazaj

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

[4] Samo v primeru bistvenih odstopanj in sprememb od predvidenega programa raziskovalnega projekta, kot je bil zapisan v predlogu raziskovalnega projekta. Največ 3.000 znakov vključno s presledki (približno pol strani, velikosti pisave 11). Nazaj

[5] Navedite največ pet najpomembnejših znanstvenih rezultatov projektne skupine, ki so nastali v času trajanja projekta v okviru raziskovalnega projekta, ki je predmet poročanja. Za vsak rezultat navedite naslov v slovenskem in angleškem jeziku (največ 150 znakov vključno s presledki), rezultat opišite (največ 600 znakov vključno s presledki) v slovenskem in angleškem jeziku, navedite, kje je objavljen (največ 500 znakov vključno s presledki), izberite ustrezno šifro tipa objave po Tipologiji dokumentov/del za vodenje bibliografij v sistemu COBISS ter napišite ustrezno COBISS.SI-ID številko bibliografske enote.
Navedeni rezultati bodo objavljeni na spletni strani http://sicris.izum.si/.

PRIMER (v slovenskem jeziku):
Naslov: Regulacija delovanja beta-2 integrinskih receptorjev s katepsinom X;
Opis: Cisteinske proteaze imajo pomembno vlogo pri nastanku in napredovanju raka. Zadnje študije kažejo njihovo povezanost s procesi celičnega signaliziranja in imunskega odziva. V tem znanstvenem članku smo prvi dokazali… (največ 600 znakov vključno s presledki)
Objavljeno v: OBERMAJER, N., PREMZL, A., ZAVAŠNIK-BERGANT, T., TURK, B., KOS, J.. Carboxypeptidase cathepsin X mediates ß2 - integrin dependent adhesion of differentiated U-937 cells. Exp. Cell Res., 2006, 312, 2515-2527, JCR IF (2005): 4.148
Tipopologija: 1.01 - Izvirni znanstveni članek
COBISS.SI-ID: 1920113 Nazaj

[6] Navedite največ pet najpomembnejših družbeno-ekonomsko relevantnih rezultatov projektne skupine, ki so nastali v času trajanja projekta v okviru raziskovalnega projekta, ki je predmet poročanja. Za vsak rezultat navedite naslov (največ 150 znakov vključno s presledki), rezultat opišite (največ 600 znakov vključno s presledki), izberite ustrezen rezultat, ki je v Šifrantu raziskovalnih rezultatov in učinkov (Glej: http://www.arrs.gov.si/sl/gradivo/sifranti/sif-razisk-rezult.asp), navedite, kje je rezultat objavljen (največ 500 znakov vključno s presledki), izberite ustrezno šifro tipa objave po Tipologiji dokumentov/del za vodenje bibliografij v sistemu COBISS ter napišite ustrezno COBISS.SI-ID številko bibliografske enote.
Navedeni rezultati bodo objavljeni na spletni strani http://sicris.izum.si/. Nazaj

[7] Navedite rezultate raziskovalnega projekta 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. Nazaj

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

[9] Največ 4.000 znakov vključno s presledki Nazaj

[10] Največ 4.000 znakov vključno s presledki Nazaj

[11] Rubrike izpolnite/prepišite skladno z obrazcem "Izjava sofinancerja" (http://www.arrs.gov.si/sl/progproj/rproj/gradivo/), ki ga mora izpolniti sofinancer. Podpisan obrazec "Izjava sofinancerja" pridobi in hrani nosilna raziskovalna organizacija – izvajalka projekta. Nazaj

Obrazec: ARRS-RPROJ-ZP/2010 v1.00a
F1-22-6A-51-A4-7F-C9-A2-D4-E4-97-AD-8B-BA-4B-F9-E1-F2-E2-10