Analiza in zasnova programske rešitve vodenja evidenc na uradu Vlade Republike Slovenije za varovanje tajnih podatkov

Miran Skobe, Tomislav Rozman

1 Uvod

Urad Vlade Republike Slovenije za varovanje tajnih podatkov (UVTP) je z Zakonom o tajnih podatkih (ZTP) prevzel vodenje več evidenc s skupnim imenovalcem – dovoljenjem za dostop do tajnih podatkov, tako za fizične osebe (zaposlene v organih in organizacijah) kot tudi za pravne osebe, torej organe in organizacije same. Tako UVTP vodi evidence izdanih dovoljenj fizičnim osebam za dostop do nacionalnih tajnih podatkov, za dostop do tujih tajnih podatkov (zveze NATO in EU), evidenco izdanih varnostnih dovoljenj pravnim osebam za dostop do nacionalnih tajnih podatkov in za dostop do tujih tajnih podatkov ter evidenco začasnih dostopov do tajnih podatkov za fizične osebe. Prav tako je v medresorskem usklajevanju predlog za vodenje še nekaterih drugih evidenc – evidenco akreditiranih komunikacijsko-informacijskih sistemov, evidenco sprejemnih točk tajnih podatkov in evidenco registrov tujih tajnih podatkov. UVTP je v letu 2007 izdelal lastno rešitev enotnega elektronskega vodenja evidenc. Tekom let je rešitev postajala vedno bolj nezadostna, prepočasna in zahteva preveč dodelav. Hkrati pa do podatkov še vedno ne morejo dostopati izdajatelji nacionalnih dovoljenj (Ministrstvo za notranje zadeve, Ministrstvo za obrambo in Slovenska obveščevalna-varnostno agencija). Dostop do evidenc je hkrati tudi ena izmed predlogov tudi v trenutnem usklajevanju sprememb ZTP.

1.1 Sorodno delo

Sorodno literaturo, ki bi povzemalo razvoj programske opreme za evidence tajnih podatkov, je malo in jo je težko najti. To je razumljivo, ker je redkokatera organizacija pripravljena razkriti postopke in tehnologijo, s katero obvladuje tajne podatke.

Sorodno tematiko v ZDA obravnavajo sledeči avtorji.
Avtorji (Rosenbaum, Tenzer, Unger, Alstyne, & Knight, 1983) predstavijo posledice akta (Executive Order 12356) z leta 1982, ki predpisuje sistem za določanje tajnih podatkov na podlagi skrbi za nacionalno varnost. Avtorji opozarjajo na možne posledice, ki lahko nastanejo kot posledica tega akta – državni uradniki lahko kadarkoli označijo raziskave akademikov kot tajni podatek. Posledice so lahko nepredvidljive – ovirajo lahko znanstveni razvoj in s tem tudi nacionalno varnost.
Avtor (Kaiser, 2003) poroča, da je dostop do tajnih podatkov v ZDA za lokalne uradnike in osebje nujen del rešitve za boj proti terorizmu. V Združenih državah je to področje zakonsko urejeno z »Homeland Security Information sharing act of 2002«. Kljub temu prihaja do težav z dostopom do tajnih podatkov, zato avtor predlaga izboljšave sistema.
(Relyea, 2011) predstavi zgodovino ravnanja s tajnimi podatki v ZDA. Predstavi problematiko rasti števila dokumentov (in s tem stroškov), označenih kot tajni. Samo za primer: število novih tajnih dokumentov v letu 2005 je naraslo za 14 milijonov.
Že samo število tajnih dokumentov in povezani stroški kličejo po primerni informatizaciji tega področja.

1.2 UVTP v luči relevantne zakonodaje in informacijskih procesov

UVTP je novejši državni organ, ustanovljen z vladnim sklepom (Sklep o ustanovitvi, nalogah in organizaciji UVTP, Ur. l. RS, št. 6/02) leta 2002. Osnovni namen ustanovitve je bila potreba po zakonski ureditvi področja obravnavanja tajnih podatkov na nacionalni ravni ter zahteve po t.i. »nacionalnem varnostnem organu« (National Security Authority) s strani NATO ter EU, ki bi uredila tudi področje obravnavanja tajnih podatkov navedenih zvez. Dodatno pa status UVTP urejajo še Zakon o tajnih podatkih (Uradni list RS, št. 50/06-uradno prečiščeno besedilo, 9/10 in 60/11, v nadaljnjem besedilu: ZTP), Akt o notranji organizaciji in sistemizaciji delovnih mest v UVTP ter podzakonski akti.

Pojem in pomen tajnih podatkov opredeljuje ZTP kot: »…dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno«. ZTP nadalje loči štiri stopnje tajnosti (INTERNO, ZAUPNO, TAJNO in STROGO TAJNO) glede na možne škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, ki utegnejo nastati, če bi bili razkriti podatki nepoklicani osebi.

Pri prenovi programske opreme oziroma procesov je nujna uporaba standardov s tega področja. Zakaj so standardi pomembni? Predvsem zato, ker nam olajšajo komunikacijo med udeleženci prenove programske opreme. Na primer:

• Izvajalci (programerji) se lažje sporazumejo z naročnikom, če so specifikacije zahtev skladne s standardom IEEE 830 (Board, 1998).
• Poslovni analitiki se lažje sporazumevajo med sabo, vodstvom in izvajalci, če uporabljajo standard za modelirane poslovnih procecsov ISO/IEC 19510:2013 (BPMN 2.0.1) (ISO/IEC/JTC1, 2014).
• Nabavno osebje (oz. naročnik programske opreme) in izvajalec lažje izpeljeta nabavo, predajo in testiranje programske opreme, če sledita smernicam CMMI-Acquisition (Carnegie-Mellon-SEI, 2010).
• Varnost programske opreme, podporne infrastrukture in povezanih procesov lažje zagotovimo tako, da sledimo smernicam standarda ISO 27000 (Disterer, 2013).

Obstaja še množica standardov, ki nam je lahko v pomoč pri prenovi programske opreme (npr. UML – Unified Modelling Language, ISO 31000 za obvladovanje tveganj, ISO 9001:2014 za kakovost,...), vendar se bomo v tem prispevku omejili na zgoraj omenjene.

2 Raziskava

Osrednji namen je analizirati obstoječe stanje strojne in programske opreme ter zakonske podlage in predloge sprememb zakonskih podlag v zvezi z evidencami UVTP, pripraviti dokument Specifikacija zahtev za programsko opremo (SZPO), določiti standarde in kriterije za izbor ponudnika programske opreme in sistem nadzora kvalitete izbrane rešitve ter izdelati okvirni časovni načrt celotnega procesa nabave. Cilj študije primera je zagotoviti čimbolj enostavno izvedbo postopka javnega naročanja ter kot rezultat zagotoviti novo programsko rešitev vodenja evidenc UVTP.

V okviru raziskave smo postavili več hipotez:
H1: UVTP dosledno izpolnjuje zakonsko določene naloge v 43. e členu ZTP.
H2: Slovenski trg dobaviteljev programske opreme oziroma storitve programiranja »na

ključ« ponuja večje število ponudnikov tovrstnega blaga in storitev.
H3: Nakup in začetek dela z novo programsko rešitvijo je možen v času enega leta, upoštevajoč dodatna proračunska sredstva, projektno sofinanciranje iz EU ali pa združena namenska proračunska sredstva večih ministrstev in vladnih služb.

Osnovni metodi opazovanja in spoznavanja dejavnosti smo dodali kvalitativno metodo dela - odkrito opazovanje z udeležbo (raziskovalec je opazovalec in udeleženec hkrati) in delno strukturiran intervju (z odgovornimi osebami na UVTP), dodatno smo uporabili kvantitativno metodo sekundarne analize podatkov (predvsem finančnih). Uporabili smo tudi metodo deskripcije, analize in sinteze dejstev ter tudi metodo kompilacije, predvsem dokumenta SZPO, standardov in kriterijev za izbor dobavitelja programske opreme ter nadzora kvalitete izbrane rešitve. Za izbor dobavitelja smo uporabili večkriterijski ponderiran odločitveni model.

Možna omejitev pri raziskavi in predlagani rešitvi je navajanje konkretnih podatkov o obstoječi rešitvi zaradi upoštevanja ZTP v segmentu označevanja le-teh s stopnjami tajnosti. V takih primerih bomo na takšnem mestu navedli opozorilo, izpustili bomo dejanski podatek in ga nadomestili s splošnim opisom, kar po mnenju avtorja ne bo škodovalo realnosti problema. Termin »predlagatelj/i« bomo uporabili splošno za predlagatelje sprememb predpisov na obravnavanem področju.

3 Analiza obstoječega stanja in rezultati

Analizo obstoječega stanja (ugotavljanje sestavnih delov, razčlenjevanje in kritično vrednotenje) vodenja evidenc smo opravili na dveh nivojih: na nivoju strojne opreme in na nivoju programske opreme. Predstavljamo jo z vidika uporabnika programske rešitve, programerja in administratorja lokalnega omrežja.

Programska oprema: trenutno delujoča aplikacija je nastajala v letih 2006 in 2007. UVTP v tem času ni razpolagal s strokovnjaki, ki bi lahko zgradili več-uporabniško in več-nivojsko aplikacijo, zato je izkoristil razpoložljive vire znotraj državne uprave. Kot »front-end « (grafični vmesnik) je uporabljen MS Access, za »back-end « (baza podatkov) se uporablja MySQL. Za povezavo med obema deloma skrbi tehnologija ODBC (Open Database Connectivity).

Strojna oprema: UVTP interno omrežje je zaprto lokalno omrežje Fast Ethernet (fizično ločeno od ostalih omrežij) in nima povezave v Prostrano omrežje HKOM in od tam v svetovni splet. V LAN je povezanih skupno 11 delovnih postaj, dva strežnika in dva mrežna tiskalnika. Vlogo strežnika opravljata dva starejša Fujitsu-Siemens Primergy RX300 brez zunanjih diskovnih modulov za shranjevanje podatkov (le 2 notranja »hot-swap« diska). Prvi strežnik je operativni, drugi služi le za t.i. »mirroring«. Delovne postaje (11) so znamke DELL Optiplex z operacijskim sistemom Microsoft Windows 7 in nameščenimi petimi aplikacijami za dostop do podatkovnih baz. Delovne postaje so v primerjavi s strežnikoma novejše (deloma iz leta 2008, deloma iz leta 2010), kar trenutno še ne predstavlja ozkega grla. Tiskalnika sta HP4520C, ki zadovoljujeta vse potrebe po tiskanju.

Rezultati analize pokažejo šibko točko predvsem pri programski opremi:

• s stališča uporabnosti in razumljivosti aplikacij ocenjujemo, da bi se lahko nekateri deli aplikacij poenostavili (preveč odprtih oken naenkrat), čeprav gre pri aplikacijah, ki

omogočajo izdajo NATO in EU dovoljenja, za isto poizvedbo, sta grafična vmesnika vizualno čisto drugačna (drugačni menuji), vendar vodita do istih operativnosti. Pri priklicu podatkov na ekran je odzivni čas zelo dolg, tudi do 10 sekund, nekaterim izpisom manjka dodaten filter;
• s stališča poznavanja programiranja, avtor ocenjuje, da bi morala biti rešitev primerna le za nujno zakonsko izpolnitev obveze o vzpostavitvi evidenc, torej za neko kratko prehodno obdobje (do dveh let); aplikacijo, ki bi bila hkrati sodobna, hitra, odzivna in stabilna ter enostavna, bi morali zgraditi programerji, ki so na neprimerno višjem nivoju znanja, s poprejšnjo analizo stanja in več predlogi rešitev;
• pri pregledu porabe sistemskih virov smo opazili preveliko zasedenost le-teh ob izvrševanju nekaterih poizvedb aplikacij; shranjevanje podatkov je urejeno na nivoju MySQL in samega sistema, kar je v tem trenutku primerno in ustrezno.

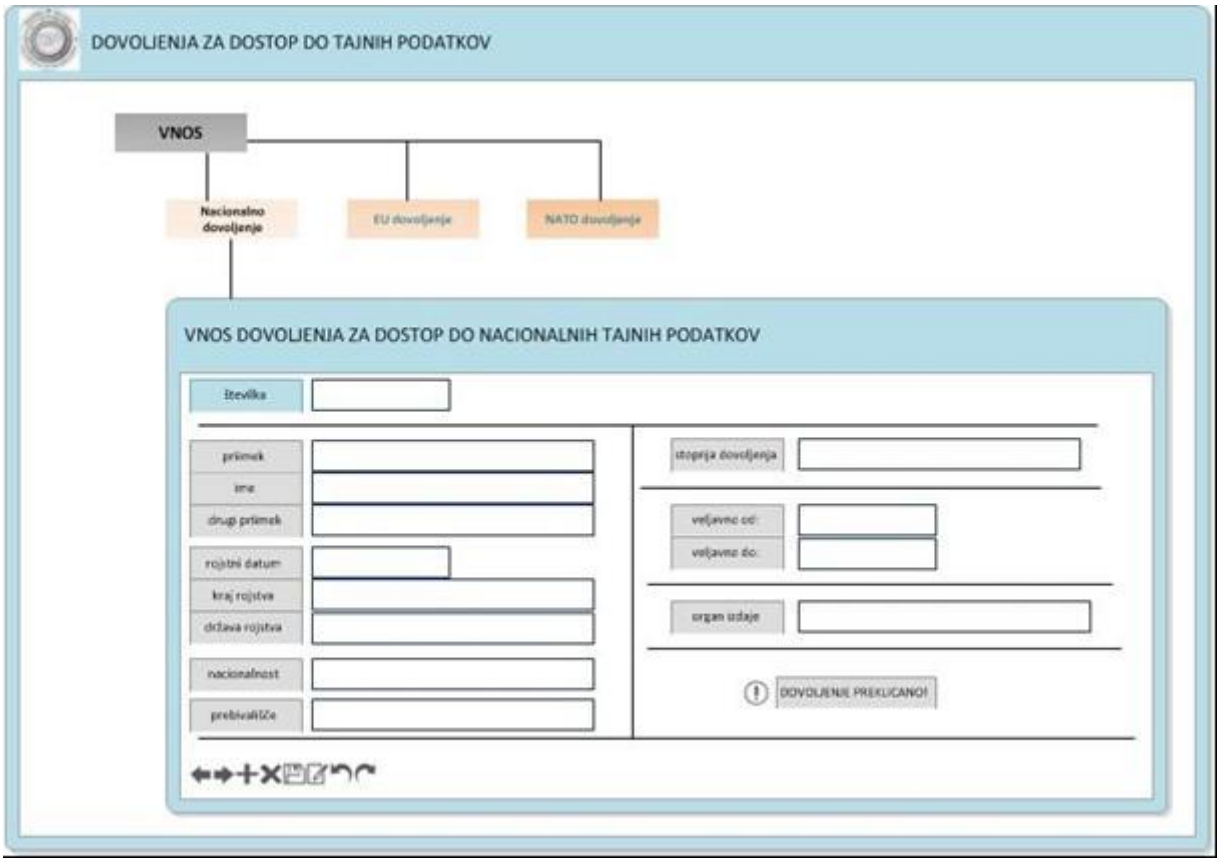
Splošno velja, da MS Access ni več primeren kot »front-end« del aplikacije. Za izgradnjo novega uporabniškega grafičnega vmesnika bi lahko uporabili bolj profesionalne rešitve, kot so Visual Studio, Java, C++, ali celo spletni vmesnik.

4 Zasnova nove programske rešitve

Namen izdelave nove programske opreme za vodenje evidenc UVTP ima več osnovnih poudarkov:
• izdelati sodoben, hiter, odziven in stabilen grafični vmesnik,
• enostavno upravljanje s pravicami in uporabniki,
• dostop do podatkovnih baz preko omrežja HKOM,
• priprava in dnevno polnjenje podatkov o izdanih dovoljenjih s strani izdajateljev in
• neprekinjeno poslovanje – dostopnost podatkov (Skobe, 2012).

Idejna zasnova nove rešitve

Slika 1: Predlog novega grafičnega vmesnika (prototip):

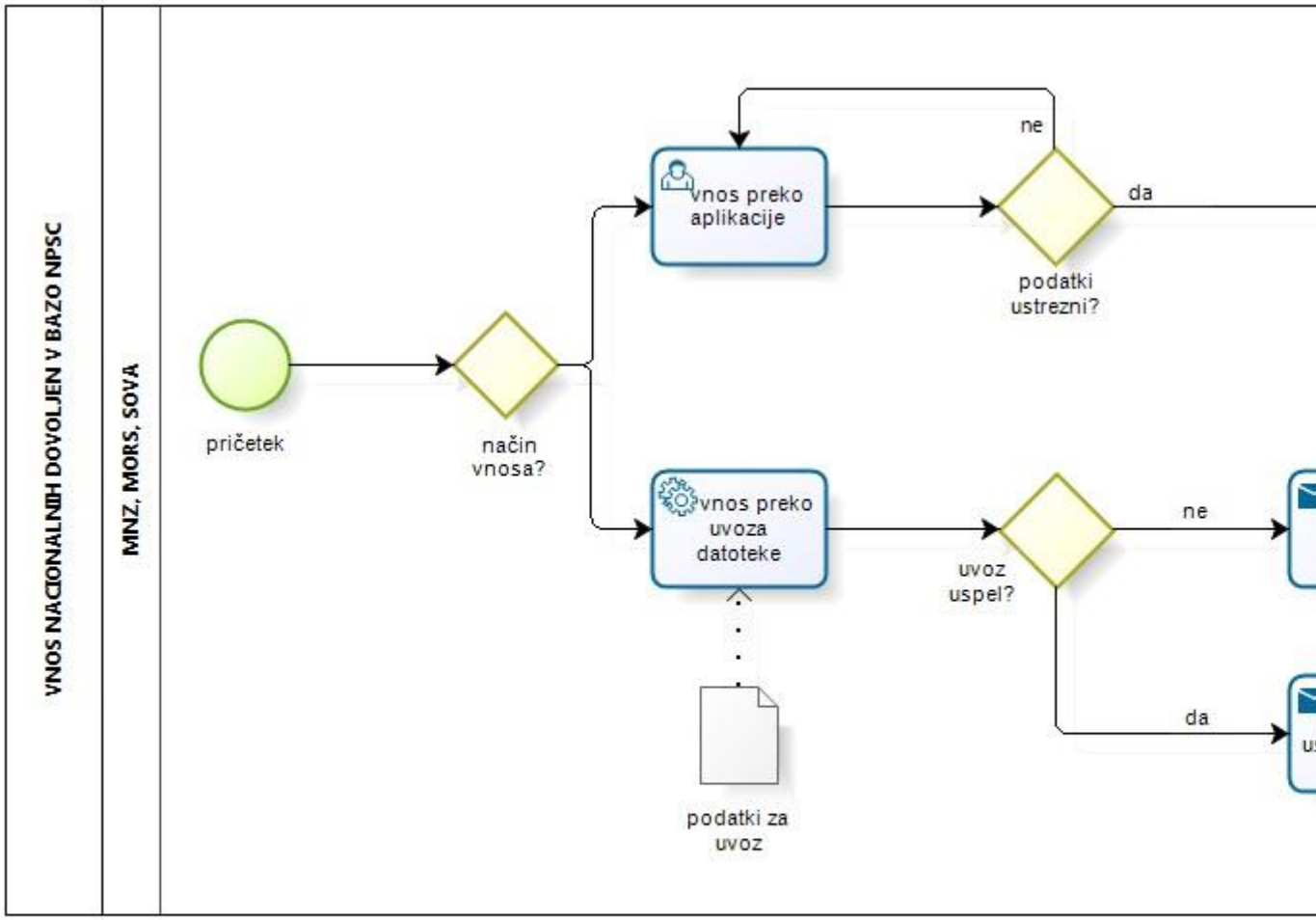


Vir: Skobe (2013)

Prototip rešuje več trenutnih problemov pri vnosu, pregledu in izpisu različnih dovoljenj (sedaj vse v enem vmesniku, logični meniji, jasno definirane pravice uporabnikov, ipd.)

Pri novi programski rešitvi je velik poudarek tudi na poslovnem procesu in delovnih tokovih. Za opis procesa vnosa dovoljenj za dostop do nacionalnih tajnih podatkov je bil uporabljen Business Process Model and Notation (BPMN), ki zaradi svoje preprostosti in izrazne moči popolnoma ustreza namenu.

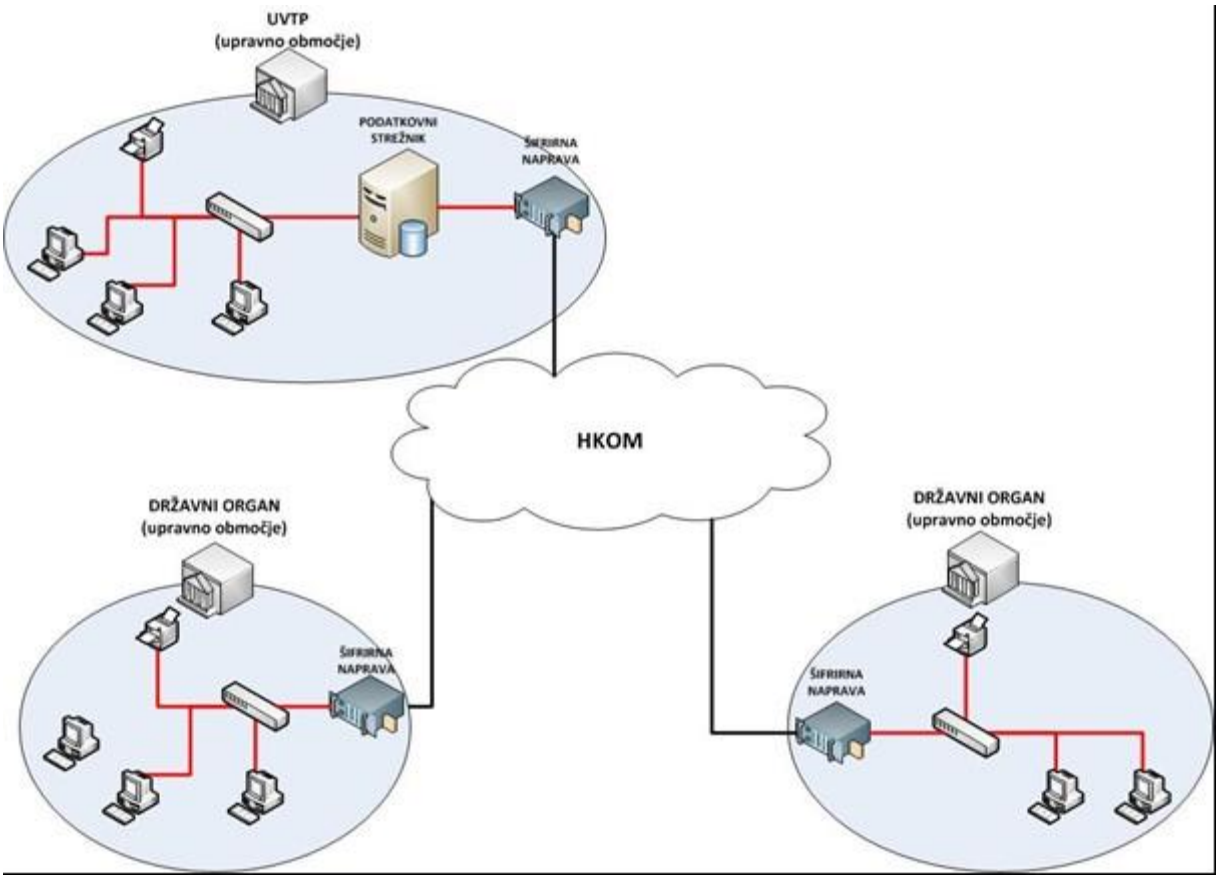
Slika 2: Model procesa vnosa dovoljenj za dostop do nacionalnih tajnih podatkov



Vir: Skobe (2013)

Varovanje tajnih podatkov in osebnih podatkov v komunikacijsko-informacijskih sistemih je zagotovljeno z uporabo šifrirnih rešitev, ki poleg klasičnih varnostnih mehanizmov dostopa (avtentikacije in avtorizacije) zagotavlja zakonsko ustrezen nivo varnosti.

Slika 3: Shema varovanja tajnih podatkov stopnje tajnosti INTERNO in prenos le-teh



Vir: Skobe (2013)

4.1 Analiza in rezultati

Osnova vsem aktivnostim so sodobni dokumenti, standardi in navodila. Izbrali smo: ISO/IEC družine 27000 (za področje informacijske varnosti), Specifikacija zahtev za programsko opremo (SZPO) – STANDARD IEEE 830-1998 (za področje razvoja ali nakupa programske rešitve), CMMI For Acquisition (za namen vodenja in upravljanja razvojnih projektov s poudarkom na nabavni strategiji), testiranje programske opreme se je odvijalo po metodah »white box« in »black box« (glede na to »kaj preverjamo, kako preverjamo in kakšen je cilj preverjanja). Dodatno smo uporabili še diagram BPMN. Business Process Model and Notation je grafični zapis, ki prikazuje korake v poslovnem procesu in delovnih tokovih. Za zadostitev varovanju tajnih podatkov in osebnih podatkov smo vključili mehanizme strojnega šifriranja.

Opravili smo raziskavo trga ponudnikov, kjer smo z določitvijo kriterijev za izbor dobavitelja opredelili področja (kriterije), zaloge vrednosti ter dejanske vrednosti, ki so prispevali k končnemu izboru. Da bi lažje določili oz. ocenili vrednost projekta, smo opravili izračun srednje vrednosti urne postavke po ceniku Gospodarske zbornice Slovenije za različne strokovnjake s področja programiranja. Nadalje smo opredelili možne vire financiranja projekta, ki so vključevali različne kombinacije lastnih (proračunskih) in tujih (predvsem EU) sredstev.

Zavedamo se, da je lahko izbira lastnega odločitvenega modela tvegana, saj gre za nabor in težo posameznih kriterijev na podlagi odločitve posameznikov, torej subjektivno odločitev. Le-ta pa je kompromis znanja in izkušenj tistih strokovnjakov s področja IT, ki bodo tak

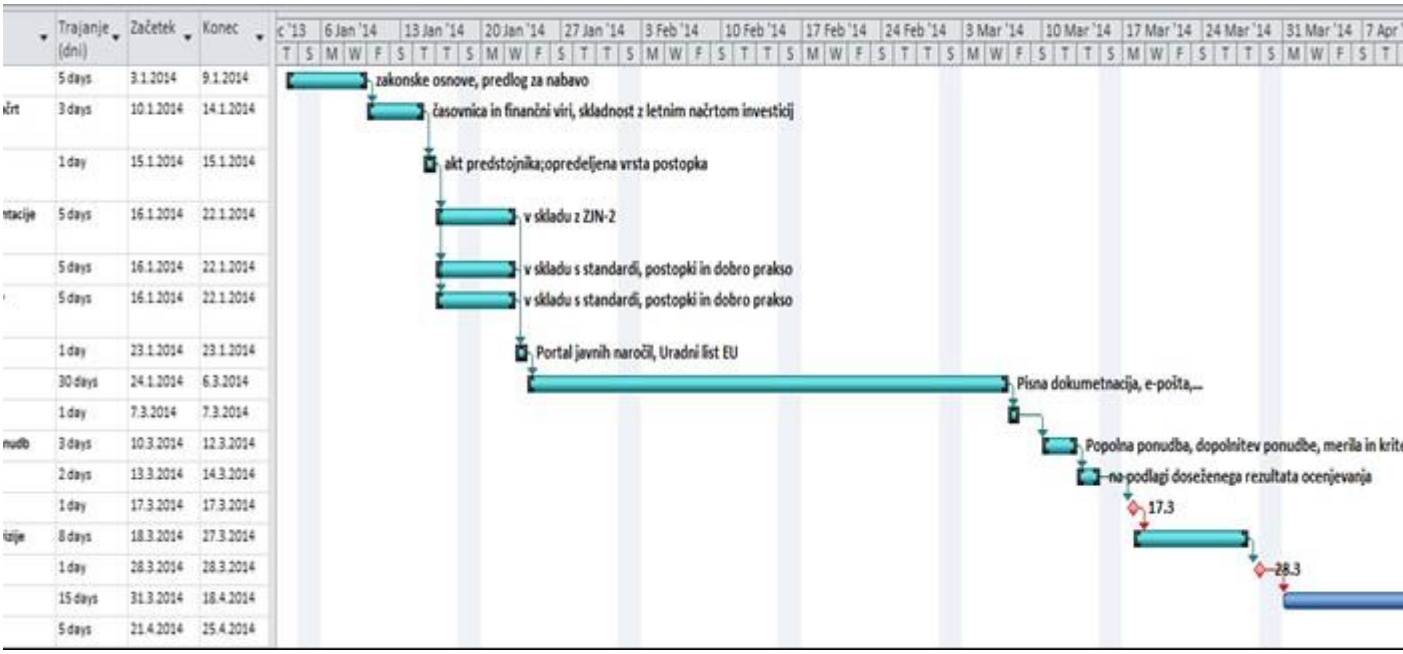
nabor pripravili in tudi ocenili. Vendar menimo, da je takšna odločitev prej prednost kot slabost, saj bodo v projekt povabljeni strokovnjaki z več deset-letnimi izkušnjami. Kriteriji za izbor so zajeti v preglednici 1:

SPLOŠNI KRITERIJ/PODROBNI KRITERIJ	ZALOGA VREDNOSTI	OPIS KRITERIJA GLEDE NA ZALOGO VREDNOSTI	VREDNOSTI	
1. sklop				
UPORABNOST in ZANESLJIVOST				
1.1.delovanje brez programskih napak	0, 5, 10	ocenjuje se posamezna fukcionalnost; v primeru kritične napake je vrednost 0	0 ->5 napak	3 do 5 napak - 5
1.2.dokumentacija, priročniki, "help desk" *	0 do 2	ustreznost z vmesnikom; dejanska pomoč; F1	0 - slabo	1 - pogojno
1.3.enostavnost, jedrnatost in celovitost *	0 do 3	ustreznost glede na povprečnega uporabnika	0 - slabo	1 - 2: pogojno
1.4.konsistentnost podatkovnih baz	0, 5	ustreznost le, če se upošteva vse integritetne omejitve baze	0 - ne upošteva	
1.5.natančnost prikaza podatkov	0, 5	vrne le iskano vrednost	0 -vrne več	
1.6.ponovljivost operacij	0, 5	ob določenih pogojih se vzpostavi prejšnje stanje in zahteva ponovitev	0 -ne omogoča	
1.7.povezljivost z ostalimi bazami podatkov (CRP, MFERAC) *	0, 1, 2	za možnost kasnejšega povezovanja podatkovnih baz	0 - ni povezljivosti	1 - poveznje eno
1.8.razumljivost, preglednost in strukturiranost	0 do 3	ustreznost glede na povprečnega uporabnika	0 - slabo	1 - 2: pogojno
1.9.skladnost s standardi in zakonodajo	0, 5	ustreznost glede na veljavno zakonodajo iz večih področij	0 - ni skladno	
1.10.uporabniku prijazna rešitev ("user-friendly")	0, 2	ustreznost glede na povprečnega uporabnika	0 - slabo	1 - pogojno
2. sklop				
VARNOST in UČINKOVITOST				
2.1.delovanje pod več operacijskimi sistemi (MS Windows)	0, 1, 2	MS Windows XP, Vista, 7	0 - samo eden OS	1 - do dva OS
2.2.izvajanje nadzora nad uporabniki in vlogami	0, 2	administracija uporabniških vlog	0 - ne omogoča	
2.3.splošna stabilnost podatkovne baze in programske rešitve	0 do 10	v času testiranja do 10 uporabnikov izvaja različne operacije	0 do 5 - nestabilnost	6 do 8 - pogojna stabilnost
2.4.varnostno shranjevanje ("backup")	0, 1	avtomatiziran proces varnostnega shranjevanja	0 - ne omogoča	
2.5.zaščita pred vdori ("intrusion detection")	0, 3	dodaten mehanizem beleženja in sporočanja	0 - ne omogoča	
3. sklop				
EKONOMIČNOST in VZDRŽEVANJE				
3.1.dobavni rok	0, 1, 2	poudarek na hitri dobavi produkta ni velik; prednost je v kvaliteti	0 - nad 3 mesece	1 - od dva meseca do tri mesece
3.2.enostavne namestitve "client" rešitve	0 do 2	administrator sam namešča produkt na delovne postaje	0 - zahteven proces	1 - polprogramira proces
3.3.FAQ (pogosto zastavljena vprašanja)	0, 1	administrator pošilja vprašanja izvajalcu, odgovore zapiše v FAQ rubriko	0 - ni možnosti izvedbe	
3.4.odnos do strojne opreme ("utilisation")	0 do 5	izmerljivi učinek programske opreme nad strojno opremo	0 - utilizacija >50% CPU	1 do 4 za vsakih
3.5.odzivni čas (dobavitelja) za napake	0 do 5	izmerljiv čas v urah od sporočila o napaki do prihoda dobavitelja	0 - nad 2 dni	1 do 4 za vsakih 1 ur hitrejši odziv
3.6.usposabljanje	0, 1	usposabljanje v ceni	0 - ne nudi	
3.7.zasedba diskovnega prostora *	0 do 2	izmerljiv v GB (podatkovna baza) in MB (uporabniški vmesnik)	0 - nad 10 GB/MB	1 - med 5 GB/MB in 10 GB/MB

* vrednost za vsako področje

Vir: Skobe (2013)

Rezultati vseh dejavnikov analize so pokazali, da je ob popolni pripravi in nedvoumnem upoštevanju vseh naštetih orodij, standardov, dokumentov, navodil,…sorazmerno hitro (celo v roku štirih mesecev od začetka projekta) in za sprejemljivo ceno (v okviru proračuna UVTP) lahko pridemo do programske rešitve. Nova informacijska rešitev bi ne samo nadomestila neprimerno obstoječo, ampak jo tudi ustrezno nadgradila, še posebej v segmentu interoperabilnosti in varnosti. Časovnico predstavlja slika 4.



Vir: Skobe (2013)

5 Povzetek rezultatov raziskave in diskusija

Raziskava sama je potrdila prvotno postavljene hipoteze, še več, skozi njen cikel je bilo ugotovljenih tudi več pozitivnih dejstev, kot so obstoji razpoložljivih virov, tako finančnih (pri združevanju sredstev več državnih organov), kot tudi človeških (državna uprava zaposluje nezanemarljivo število strokovnjakov-programerjev). Hkrati pa je dodatno potrdila potrebo po novi programski opremi kot osnovi za zakonsko delovanje UVTP.

Ob začetku vodenja skupnih elektronskih evidenc v letu 2007 je prevladovalo večinsko mnenje, da bo začasna rešitev zadostovala za veliko let zanesljivega delovanja ob minimalnih spremembah zakonodaje, torej ob minimalnih posegih v aplikacije. S potekom časa je postajalo vse bolj jasno, da tudi najboljši nameni in rešitve v določenem času ne bodo zagotovilo za delovanje na dolgi rok, da pa so po drugi strani lahko dober prototip za trajnejšo in celovitejšo IT rešitev. Dejansko je prva rešitev poskrbela za začasno ureditev evidenc in tako zadostila zakonodaji, ob pripravi nove zakonodaje ter predvidenem vodenju novih evidenc pa služila kot dobra osnova za modeliranje novega sistema. Glede na hiter razvoj tako strojne in programske opreme ter komunikacij pa menimo, da je že ob začetku projekta novega sistema potrebno razmišljati naprej – torej na naslednji sistem. Dejstvo, da bo potrebno izdelati novo programsko rešitev, je več kot očitno. Sicer se njen nakup iz obdobje v obdobje prelaga, vendar bo to ob spremembi zakonodaje enostavno potrebno storiti. Predvidena nova programska rešitev ter možnost njenega nadgrajevanja bo zadostila vsem trenutnim potrebam ter tudi prihajajočim novostim, ki jih bo terjala sprememba zakonodaje. Vendar zakonodaja s področja obravnavanja in varovanja tajnih podatkov še zdaleč ni edina zakonodaja, po kateri se bodo evidence in njihova programska rešitev morale ozirati.

Literatura

• Board, I.-S. S. (1998). IEEE 830: Recomended Practice for Software Requirements Specification. Practice.
• Board, I.-S. S. (1998). IEEE 830: Recomended Practice for Software Requirements

Specification. Practice.
• Business Process Model and Notation. 2012. BPMN.info. Dostopno na: http://www.bpmn.info/ (25. 11 2012).
• Carnegie-Mellon-SEI. (2010). CMMI® for Acquisition, Version 1.3 CMMI-ACQ. Engineering (p. 438). Dostopno na: http://www.sei.cmu.edu (16. 2. 2013).
• Carnegie-Mellon-SEI. (2010). CMMI® for Acquisition, Version 1.3 CMMI-ACQ. Engineering.
• CMMI for Acquisition, Version 1.2. 2007. Software Ingeniring Institute. Dostopno na: http://www.sei.cmu.edu/reports/07tr017.pdf, (20. 10. 2012).
• Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4, 92–100.
• Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4, 92–100. Dostopno na: http://doi.org/10.4236/jis.2013.42011 (29. 10. 29015).
• ISO/IEC 27000. 2012. International organisation of standardization. Dostopno na: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm, (24. 11. 2012).
• ISO/IEC/JTC1. (2014). ISO/IEC 19510:2013 - Information technology - Object Management Group Business Process Model and Notation. Dostopno na: http://www.iso.org/iso/catalogue_detail.htm?csnumber=62652 (6. 1. 2015)
• ISO/IEC/JTC1. (2014). ISO/IEC 19510:2013 - Information technology -- Object Management Group Business Process Model and Notation.
• Kaiser, F. M. (2003). Access to classified information: seeking security clearances for state and local officials and personnel. Government Information Quarterly, 20(3), 213–232. Dostopno na: http://doi.org/10.1016/S0740-624X(03)00040-6 (29. 10. 29015).
• Myers, G. J. 2004 The art of software testing 2nd edition. New Jersey: John Wiley & Sons, Inc.
• Relyea, H. C. (2011). Security classified and controlled information: History, status, and emerging management issues. In Classified Information: Protections and Issues (pp. 1–42).
• Rosenbaum, R. A., Tenzer, M. J., Unger, S. H., Alstyne, W. Van, & Knight, J. (1983). Academic Freedom and the Classified Information System. Science, 219(4582), 257–259.
• Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov. 2002. Uradni list RS, št. 6/02. Dostopno na: http://www.uradni-list.si/1/content?id=21439 (16. 2. 2013).
• Skobe, M. (2013). Programska rešitev vodenja evidenc po Zakonu o tajnih podatkih na Uradu Vlade Republike Slovenije za varovanje tajnih podatkov. Maribor. Fakulteta DOBA.
• Software testing fundamentals. 2012. Software Testing Fundamentals. Dostopno na: http://softwaretestingfundamentals.com/ (2. 9. 2012).
• STANDARD IEEE 830-1998. 1998. Institute of Electrical and Electronics Engineers. Dostopno na: http://standards.ieee.org/findstds/standard/830-1998.html (15. 12. 2012).
• Zakon o tajnih podatkih. 2001. Uradni list RS, št. 87/2001. Dostopno na: http://www.uradni-list.si/1/objava.jsp?urlid=200187&stevilka=4450 (16. 2. 2013).