Sekcija 1.

INFORMACIONI SISTEMI, BEZBEDNOST I ZAŠTITA, TEHNIČKE NAUKE I LOGISTIKA

Tema: “KVALITET-PUT U EVROPU"

JEDNA REALIZACIJA GENERATORA ISTINSKI SLUČAJNIH IMPULSANA BAZI ZVUČNE KARTICE RAČUNARA

Mladen Veinović[1]
Univerzitet Singidunum
e-mail: mveinovic@singidunum.ac.rs

Slaviša Nikolić[2]

[1]Univerzitet Singidunum, Fakultet za informatiku i računarstvo, Beograd, Srbija
[2]Univerzitet Singidunum, Departman za poslediplomske studije, Beograd, Srbija

Sažetak: Zvučne kartice računara se u praksi najčešće koriste za generatore pseudo-slučajnih brojeva (PRNG).Za dobijanje izlazne sekvence neophodna je primena početne vrednosti, a dobijena izlazna sekvenca je periodična.U zahtevnim situacijama, kao što je na primer generisanje kriptografskih ključeva, korišćenje ovakvih softverskih generatora može postati nepouzdano, pre svega zbog njihovihdeterminističkih svojstava. U ovom radu je prikazan postupak dobijanja istinski slučajnih impulsa korišćenjem hardvera zvučne kartice računara, na čiji se audio ulaz preko mikrofona dovodi slučajni analogni signal šuma (buke).Pretpostavka je da analogno-digitalna konverzija slučajnog analognog signala kao rezultat daje slučajne vrednosti digitalnog signala. Problemi koji se javljaju u realizaciji odnose se na visoku učestanost odmeravanja. Zbog toga suu cilju dobijanja što boljih rezultata entropije korišćenetehnike XOR-ovanja i redukovanja broja odmeraka.

Ključne reči: Generator istinski slučajnih impulsa (TRNG), A/Dkonvertor (ADC), zvučna kartica (SC)

Abstract: Computersoundcard, in practicecommonlyusedgenerators for pseudo-randomnumber generator (PRNG). To obtain the outputsequencerequires the application of the initialvalue, and the inducedoutputsequence is periodic. In demandingsituations, such as, for example, generatecryptographickeys, the use of thesesoftwaregeneratorsmaybecomeunreliable, primarilybecause of itsdeterministicproperties. In thispaperwepresent a method of obtaining a trulyrandompulsesusinghardwaresoundcard in yourcomputer, whose audio inputthrough a microphonebringsanalograndomnoise signal. It is assumedthat the analog-to-digitalconversion of analogsignals as randomreturns a randomvalue of the digital signal. The problemsthatarise in the implementationarerelated to the highfrequencymeasurement.Therefore, in order to obtainbetterresultsentropyusedtechniques XOR andreducing the number of samples.

Keywords:Truerandomnumber generator (TRNG), A/D convertor (ADC), soundcard

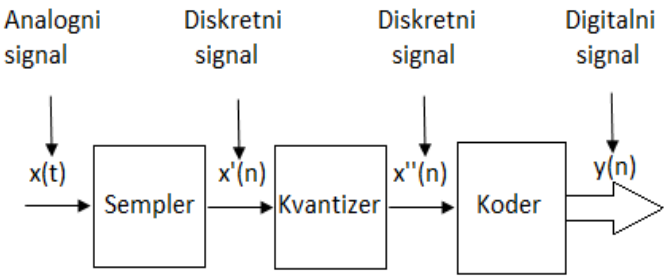
1.Uvod

Najčešće korišćeni generatori slučajnih brojeva su generatori pseudo-slučajnih brojeva (PRNG). PRNG generatori koriste deterministički sistem i inicijalni SID (eng. *seed* - seme) za generisanje izlazne sekvence [1]. Šenonova entropija izlaza zavisi od entropije SID-a i nikada je ne može nadmašiti [2]. Reproduktivnost PRNG-a, tj. mogućnost generisanja iste izlazne sekvence, ima velike prednosti kod simulacija. Pored toga, zavisnost entropije i izbor SID-a jesu veliki izazov za njegovu eksploataciju, paralelizam i skalabilnost. Poznato je da PRNG

generatori odgovaraju potrebama mnogih aplikacija. Međutim, u nekim slučajevima generisanim vrednostima nedostaju jake statističke karakteristike. To su zahtevne situacije u kojima se PRNG generatori zamenjuju sa TRNG, kao što su generisanje kriptografskih ključeva, generisanje lista kod igara na sreću ili statističke simulacije. U ovakvim situacijama, korišćenje PRNG može postati nepouzdano zato što njegov izlazniniz postaje predvidljiv zbog geometrijskih svojstava. TRNG generatori se sa druge strane zasnivaju na nedeterminističkim izvorima [3] kao što su radio šumovi, radioaktivno raspadanje, termalni šumovi generisani od strane poluprovodnika, termalni šumovi kod otpornika, itd [2]. TRNG imaju mnoge prednosti u odnosu na PRNG generatore. Prvo, nepredvidivost TRNG-a nudi bolje slučajne vrednosti. Drugo, TRNG nemaju periodičnu zavisnost, što je najvažnija osobina koju treba ispuniti kod strogih uslova za komunikaciju i šifrovanje.
Ovaj rad je organizovan na sledeći način: u sledećem odeljku se objašnjava prva faza rada TRNG-a; Eksperiment i analiza rezultata prikazani su u odeljku 3; Rad se rezimira u odeljku 4.

2. Prva faza rada TRNG-a

U ovom radu se za dobijanje istinski slučajnih impulsa koristi audio ulaz zvučne kartice personalnog računara, na koji se preko mikrofona dovodi slučajni analogni signal šuma (buke).Kretanje, odnosno pomeranje raznih stvari, stvara zvučne talase koji prolazeći kroz vazduh i odbijajuće se od objekata stvaraju u mikrofonu nepredvidive amplitude. Analogni zvuk se u mikrofonu konvertuje u napon a onda nakon ADC-a u podatke u obliku bita. Kako se u ovom slučaju koristi nedeterministički fizički izvor slučajnosti (buka), koji proizvodi analogne slučajne signale koji imaju uniformnu raspodelu amplituda i koji se obrađuju u zvučnoj kartici, očigledno je da se radi o hardverskom generatoru istinski slučajnih impulsa. U drugoj fazi se post-procesomizdvajanja (destilacija)eliminišu slabosti generisanja impulsa (npr. pojava dugih nizova nula ili jedinica).
U prvoj fazi rada TRNG-a neophodno je slučajne analogne veličine (signale) prevesti u digitalan oblik. Proces ili postupak koji omogućuje dobijanje zapisa neke analogne veličine u digitalnom obliku naziva se analogno-digitalna (A/D) konverzija. Uređaj koji omogućuje dobijanje ovog zapisa naziva se analogno-digitalni konvertor - ADC. Tipično, proces A/D konverzije obuhvata odmeravanja analogne veličine u vremenu i po amplitudi. Prema tome, ADC uređaji prevode signale iz domena kontinualno vreme, kontinualna amplituda u domen diskretno vreme, diskretna amplituda (slika 1). Odmeravanje analognog signala *x(t)* vrši se u ritmu taktnog signala i na izlazu se dobija diskretni signal *x'(n)* - odnosno to je diskretizacija analognog signala po vremenu. Analogni kontinualni signal se predstavlja nizom diskretnih odmeraka koji se uzimaju u tačno određenim trenucima vremena. Diskretni signal *x'(n)* je diskretan po vremenu i analogan po amplitudi. Frekvencija odmeravanja treba da zadovolji *Nyquist*-ovu teoremu $f_{odm} \geq 2f_{max}$, da ne bi došlo do preklapanja u spektru. Ako je učestanost odmeravanja manja od teorijske granice, u signalu dolazi do pojave izobličenja – Aliasing.



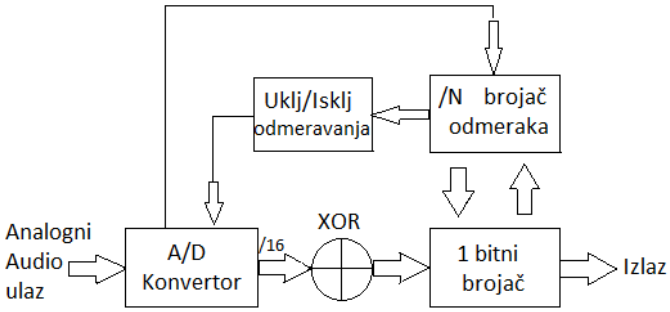
Slika 1. Analogno-digitalna konverzija: odmeravanje,kvantovanje i kodovanje

Kvantizacija je zaokruživanje amplitude odmeraka na najbližu dozvoljenu vrednost iz ukupnog opsega vrednosti, odnosno to je postupak određivanja amplitude pojedinih uzoraka. Kvantizacija smanjuje broj dozvoljenih (unapred definisanih) amplitudskih vrednosti. Korak kvantovanja je nivo signala podeljen sa brojem kvantizacijskih nivoa. Broj nivoa kvantizacije je ograničen i određen ukupnim brojem bita po odmerku. Kvalitet digitalnog signala određen je brojem kvantizacijskih nivoa koji zavisi od broja bita. Što je veći broj kvantizacijskih nivoa, to je šum kvantizacije manji, a dinamika signala veća.

U koderu se vrši kodovanje, prema definisanom kodu i generisanje digitalnog signala *y(n)*, koji je pogodan za obradu i prenos u digitalnim sistemima. To je postupak dodeljivanja binarnog koda svakom kvantizacijskom nivou, odnosno to je dodeljivanje svakom odmerku određene kombinacije 0 i 1. Manji broj kvantizacijskih nivoa određen je manjim brojem bita potrebnih da se svaki odmerak predstavi i obrnuto.

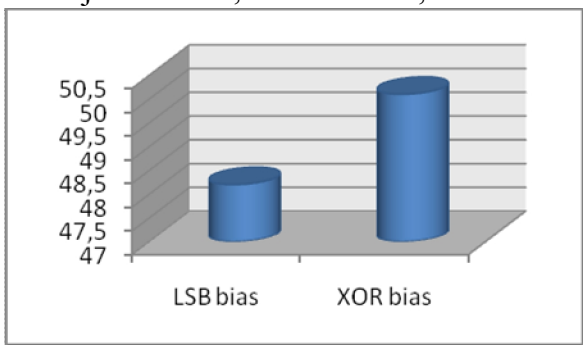
3. Eksperiment i analiza rezultata

Podaci koji se dobijaju posle odmeravanja velikom brzinom imaju nedozvoljeno visoka korelaciona svojstva. Ovo je očekivano jer se odmerava kontinualan i ponekad sporo promenljiv analogni signal. Nivo šuma (stepen promene ulaznog signala) u mikrofonu i brzina odmeravanja na različite načine utiču i određuju finalni bit strim. Povećavanje frekvencije odmeravanja ima kao direktnu posledicu pojavljivanje većeg broja korelisanih bita. Nivo šuma zavisi od: tišine okoline (što rezultuje sa ne više od 2 LSB bita u bilo koje vreme); šuma radio muzike u pozadini; upadljivo bučne okoline (koja uzrokuje značajan broj bita na izlazu ADC); 10 KHz-ne interferencije koja se projektuje direktno u mikrofonu; 11,025 KHz-ne interferencije tona koja se generiše pri sinhronizovanom semplovanju ulaznog zvuka; okruženju unutar prostorije (koja u vremenu može na više od pola A/D bita uticati više od 10% što zavisi od same osetljivosti mikrofona). Međutim, postoje metode destilacije odnosno popravljanja entropije izlaznih bitskih vrednosti. U ovom radu korišćen je metod prikazan na slici 2. Odmerci (16-to bitni) se sabiraju u sumatoru a odmerava se velikom periodom. Na ovaj način se entropija svakog odmerka predaje izlaznim bitima. Ustupak je to što se povećanjem periode odmeravanja smanjuje broj bita na izlazu. Takođe treba primetiti da je entropija LSB-ova najveća i da se smanjuje kako bitovi postaju manje precizni na putu do MSB-a.



Slika 2. Proces dobijanja slučajnih bita

Funkcija XOR ima karakteristiku povećanja entropije nekorelisanih bitova, a odmerci iz ADC-a su korelisani od odmerka do odmerka. Međutim, odmerci nisu korelisani između bita najveće težine (MSB) i bita najmanje težine (LSB). Ako se slučajni analogni signal odmerava duž celog ulaznog opsega ADC-a onda dobijeni biti ne bi trebalo da budu međusobno korelisani. Takođe ako signal nije ravnomerno distribuiran duž ulaznog opsega, uticaj MSB bitova (zbog svojih korelacionih vrednosti) će težiti nuli i neće naškoditi entropiji koja će sada zavisiti pre svega od LSB-a. Za bolje razumevanje ovog koncepta može se uzeti primer korišćenja decimalnih brojeva. Ako se slučajni broj poveća za nula, on će zadržati svoje slučajnosti. XOR-ovanjem se dobija da je *bias* razmeštaja jedinica u semplu (između MSB i LSB) paran ili neparan. Povećanje dobiti XOR-ovanjem bitova semplovanog signala znači da je *bias* redukovan. Kod testa, izvršenog na velikom broju odmeraka, u prvom slučaju *bias* je bio 48,2% jedinica. Kod XOR-ovanja*bias* je bio virtuelno eliminisan – slika 3. Konačni izlaz podataka određen je kombinovanjem velike periode semplovanja i XOR-ovanja. Svaki put se bitovi, dobijeni iz ADC odmeraka audio signala, XOR-uju unakrsno, MSB sa LSB, a onda se dodaju brojaču.



Slika 3. Bias

Pošto brojač ima prostora za samo jedan bit, dodaju mu se dobijene vrednosti XOR-ovanja. Kada brojač izbroji N perioda odmeraka, gde je N fiksni broj odmeraka ADC, podatak se kao član slučajnog niza bitova stavlja u bafer i startuje se novi odmerak. Testirane frekvencije odmeravanja ADC bile su 11.025 KHz i 44.100 KHz, a vrednost N bila je podešavana na 1, 10 i 100 odmeraka. Mada slučajnosti ne mogu nikada biti dokazive, bilo je moguće primeniti nekoliko testova koji se koriste za testiranje korelacije i *bias*-a. Posle najmanje 1 Mbita podataka, koji su bili sakupljeni pri svakom uzimanju uzoraka, uzorci su prošli testove koji su definisani prema NIST standardu FIPS 140-1.

Nepravilnosti su se javljale uvek kada je *N* bilo podešeno na 1 i 10, kada je okolina bila suviše tiha ili bučna. Ovo je razumljivo jer je frekvencija odmeravanja bila visoka a ulazni signali su imali intenciju gubljenja entropije. Mikrofon i ADC nisu bili u stanju da skupe dovoljno

entropije iz signala a zbog kratkih perioda vremena i susedni odmerci su bili u korelaciji. Za sva ostala podešavanja izlazni biti su prošli sve statističke testove slučajnosti.Čak i kada su testovi imali tendenciju sabotaže, forsiranjem prostom fiksnom frekvencijom u mikrofonu, nisu povećane korelacije ili *bias* kada je N bilo veće od 10. Na ovaj način se proizvodi bitska brzina od 4,41 Kbit/s pri frekvenciji odmeravanja 44,1 KHz, što može biti dovoljno za mnoge kriptografske aplikacije.

4. Zaključak

U ovom radu je prikazan način dobijanja istinski slučajnih impulsa korišćenjem audio ulaza zvučne kartice, koja je sastavni deo hardvera svakog kućnog računara, na koji se preko mikrofona dovodi slučajni analogni signal buke. Kretanje, odnosno pomeranje raznih stvari, stvara zvučne talase koji prolazeći kroz vazduh i odbijajuće se od objekata stvaraju u mikrofonu nepredvidive amplitude. Analogni zvuk se u mikrofonu konvertuje u napon a onda nakon ADC-a u podatke u obliku bita. Konačni izlaz podataka, predstavljenog generatora, određen je kombinovanjem velike periode semplovanja i XOR-ovanja LSB i MSB odmeraka. Koristeći ovaj metod, korisnici kućnih računara mogu generisati kriptografski sigurne slučajne bite bez potrebe za ugradnjom ili korišćenjem nekog specijalnog hardvera. Prikazani generator istinski slučajnih impulsa obezbeđuje visok kvalitet slučajnih bita, što znači da ima veliku brzinu generisanja, da je nepredvidiv i da nema periodičnu zavisnost.

Literatura

[1] J. Gentle: RandomNumberGenerationandMonte CarloMethods. *StatisticsandComputing*. Springer (2004).

[2] B. Jun, P. Kocher. The Intel RandomNumber Generator. WhitePaperPrepared For Intel CorporationbyCryptographyResearchInc. http://www.cryptography.com/public/pdf/IntelRNG.pdf

[3] P. Grabher, J. Grosschadland D. Page. 2009. Non-deterministicprocessors: FPGA-basedanalysis of area, performanceandsecurity. In *Proceedings of the 4th Workshop on EmbeddedSystemsSecurity*. Grenoble, France. 2009.

[4] W. Schindler, W. Killmann. AIS 31: Functionalityclassesandevaluationmethodology for true (physical) randomnumbergenerators, version 3.1, BundesamtfurSicherheit in derInformationstechnik (BSI), Bonn, 2001.

[5] M. Bucciand R. Luzzi. Design of TestableRandom Bit Generators. *In Workshop of CryptographicHardwareandEmbeddedSystems (CHES '05)*,131-146, Springer-Verlag. Edinburgh, UK. August 2005.

[6] NIST: SecurityRequirements for CryptographicModules. FIPS PUB 140-1 (11.04.1994). http://www.itl.nist.gov/fipspubs/fip140-1.htm

[7] M. Bucci, V. Bagini. A Design of ReliableTrueRandomNumber Generator for CryptographicApplications. *In Workshop on CryptographicHardwareandEmbeddedSystems (CHES 1999)*. pages 204–218, Berlin, Germany. Springer-Verlag. August 1999.

DOPRINOS SISTEMU KVALITETA DIGITALNIH FORENZIČKIH SERVISA U CLOUD COMPUTING OKRUŽENJU

CONTRIBUTION OF DIGITAL FORENSIC QUALITY ASSURANCE IN CLOUD COMPUTING EVIRONMENTS

Gojko Grubor
Fakultet za informatiku i računarstvo, Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: ggrubor@singidunum.ac.rs
Angelina Njeguš
Fakultet za informatiku i računarstvo, Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: anjegus@singidunum.ac.rs
Nenad Ristić
Univerzitet Sinergija
Raje Baničića bb, Bijeljina, BIH
E-mail: nristic@sinergija.edu.ba

Sažetak
Osiguranje kvaliteta forenzičkih servisa danas predstavlja glavni izazov za servis provajdere i njihove korisnike. U ovom radu će se razmatrati problematika integracije forenzičkih veb servisa i SOA arhitekture u Cloud Computing (CC) okruženje, a potom analizirati doprinos forenzičkih servisa sistemu kvaliteta CC servisa.
Ključne reči*: digitalna forenzika, osiguranje kvaliteta, Cloud Computing, veb servisi, SOA*

Abstract
Quality assurance of forensic services today is a major challenge for service providers and for their users. In this paper we will consider the issue of forensic web services and SOA integration in cloud computing environment, and then analyze a contribution of the digital forensic services to the cloud computing serviceses quality assurance.
Key words: *Digital Fornesics, Quality Assurance, Cloud Computing, Web Services, SOA*

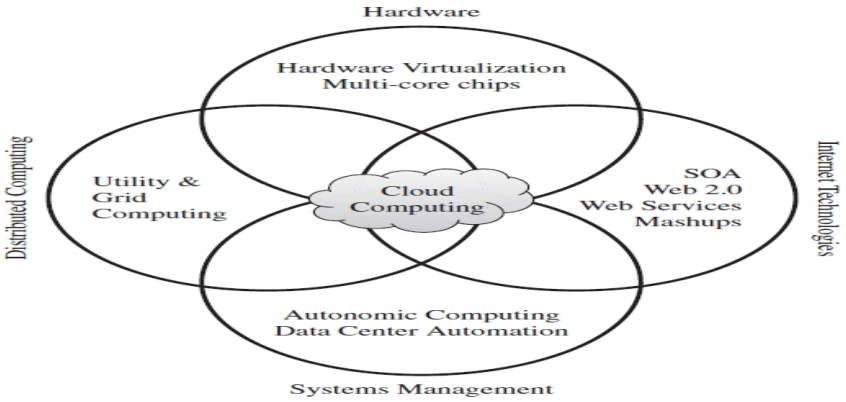
1. UVOD

U eri digitalizacije, računari registruju svaki ljudski rad u formi digitalnog (binarnog) zapisa. Potreba za digitalnom forenzičkom (DF) istragom digitalnih podataka je svakodnevna, bilo da se koristi za dokazivanje kompjuterskog kriminala, krađe intelektualne imovine ili povrede politike zaštite organizacije. Samo veštine, tehnike i alati digitalne forenzika, koji otkrivaju i analiziraju uskladištene ili računarskim sistemom generisane digitalne podatke, mogu trajno otkloniti uzrok kompjuterskog incidenta i sprečiti njegovo ponavljanje [14]. Pojavom *Cloud Computing* servisa (CCS) i rada u tipično virtuelnom, visoko distribuiranom okruženju, postavljaju se novi izazovi u zaštiti [22] i DF istrazi, uključujući sumnju u mogućnost DF istrage u CC sistemu uopšte [11]. U trendu konvergencije DF istrage i zaštite informacija [14], procesi istrage, otkrivanja, pripreme,

analize i obrade elektronskih podataka, postaju dnevna potreba i neophodni servisi u menadžment sistemu bezbednosti informacija - ISMS (*Information Security Management System*) [19]. Uspostavljanjem sistema proaktivne DF za skupljanje forenzički relevantnih podataka, obezbeđuju se realni uslovi za, SLA ugovorm definisan [7], određeni nivo DF istrage u slučaju kompjuterskog kriminala u CC sistemu. Servis DF istrage sprečava korišćenje istog tipa ranjivosti CC sistema za ponavljanje napada i daju značajan doprinos održavanju stabilnih procesa zaštite i sistema kvalitet CCS-a

2. PREGLED LITERATURE

U postojećoj literaturi postoji više definicija pojma CCS, koje su suštinski identične, ali polaze od različitih premisa. Dakle, CC je pružanje IT resursa i servisa korisnicima najčešće preko Interneta i korišćenjem virtualizacije [18]. Prema [32] CCS je model obezbeđivanja pristupačnog i "po zahtevu korisnika" mrežnog pristupa zajedničkom skupu podesivih računarskih resursa koji mogu biti brzo dostupni i aktivirani uz minimalni menadžment i interakciju sa CC provajderom usluga (CSP). Kompletna CC filozofija se, između ostalih, zasniva na servisno-orijentisanoj arhitekturi - SOA (*Service-Oriented Arhitecture*) [26,29], koja podrazumeva arhitekturu sistema zasnivanu na servisima (slika 1).



Slika 1. Konvergencija rezultata razvoja različitih IT oblasti u cloud computing

Glavni gradivni blokovi za razvoj SOA sistema su [29]:

- Upravljanje poslovnim procesima i realizacija poslovanja
- Agilnost poslovanja
- Veb servisi – platforma za opsluživanje poslovanja
- XML – osnovna tehnologija

2.1. Servisno-orijentisana arhitektura i veb servisi

Servisno-orijentisana arhitektura, kao rezultat evolucije softverske arhitekture, zasniva se na primeni labavo povezanih servisa u cilju dostizanja maksimalne poslovne fleksibilnosti na interoperabilan i tehnološki nezavisan način. Veb servis predstavlja bilo koji servis (softversku aplikaciju), dostupan u distribuiranom Internet okruženju, a koji koristi standardizovani XML sistem za razmenu poruka, te koji nije isključivo vezan za bilo koji operativni sistem ili

programskijezik. Organizacije koriste veb servise da bi rešile problem nekompatibilnosti između različitih formata podataka i računarskih sistema, koji otežavaju i uvećavaju troškove slanja podataka od tačke A do tačke B. Veb servisi prevazilaze nekompatibilnosti skupom softverskih standarda kao što su: XML, SOAP, WSDL, BPEL i dr. Cilj veb servisa je dostizanje interoperabilnosti između aplikacija korišćenjem veb standarda.Veb servisi su slabo povezani modeli koji omogućavaju fleksibilnu integraciju heterogenih sistema u različitim domenima kao što su B2C, B2B ili EAI. Mogući tipovi veb servisa su [29]:

- **Servisi poslovnih procesa:** Poslovni procesi predstavljaju sekvence aktivnosti koji ispunjavaju jedan poslovni cilj. Na primer, proces prijave za dobijanje kredita od banke, kreiranje porudžbine i sl. Servisi poslovnih procesa se mogu sastojati i iz drugih servisa.
- **Servisi poslovnih transakcija:** Predstavljaju poslovne funkcije koje menjaju stanje poslovanja, kao na primer, nabavka materijala od dobavljača, snimanje nove transakcije klijenta, rezervacija klijenta i sl.
- **Servisi poslovnih funkcija:** Predstavljaju poslovne funkcije koji ne menjaju stanje poslovnih procesa, već vrše jednostavnija izračunavanja ili vraćaju podatke, kao npr. *proračun konverzije valuta* ili *dobijanje cene* itd.
- **Servisi tehničkih funkcija:** Višekratno su upotrebljivi, ali ne obezbeđuju poslovne, već samo tehničke ili infrastrukturne funkcije koje se zahtevaju radi podrške interakcija servisa u IT sistemima, npr. *provera događaja, provera korisničke lozinke ili ovlašćenja.*

Postoje brojni napadi na veb servise, kao što su WSDL/UDDI skeniranje, prisluškivanje grešaka parametara, odgovaranje, ispravljanje XML-a, posredovanje, prisluškivanje saobraćaja, skretanje rute itd. Pored toga, selekcija dinamičkih servisa, koreografija, orkestracija i kompozicija servisa dodatno povećavaju rizike od napada na aplikacije i tokove podataka [33].

Da bi se olakšala forenzička analiza nad poverljivim podacima korisnika, predlaže se razvoj forenzičkih veb servisa - FWS (*Forensic Web Services*,) koji će sačuvati odgovarajući dokaz za ponovno kreiranje poziva ka kompozitnim veb servisima. Takvi dokazi imaju veću šansu da budu prihvaćeni na sudu. FWS treba da obezbedi *online DF istragu* veb servisima, tako što će biti integrisan sa veb servisima koji zahtevaju njegove servise, tzv. klijent vebservisi FWS-a. Da bi se to realizovalo, FWS obezbeđuje centralizovanu tačku pristupa ka klijent veb servisima. Informacije, koje FWS sačuva, mogu se direktno dati forenzičaru na analizu i ispitivanje.

2.2. Digitalna forenzička istraga u virtuelnom okruženju

Virtualizacija je ključni koncept CC sistema, a podrazumeva da se na jednom fizičkom računaru podigne više različitih virtuelnih računara (operativnih sistema - OS) radi boljeg iskorišćenja resursa . Danas je na raspolaganju više alata za virtuelizaciju - *Microsoft Virtual PC* (2007), *VMWare* (2007), QEMU (*Bellard*, 2007, besplatan) i nekoliko drugih.

Virtuelna mašina (VM) je softverski proizvod koji omogućava korisniku da kreira jedno ili više okruženja (platformi) od kojih svako simulira svoj skup hardverskih komponenti (CPU, HD, memoriju, mrežne kontrolere itd.) i ima sopstveni softver. Idealno je kada svaka VM radi i ponaša se kao potpuno nezavisan računar sa sopstvenim operativnim sistemom i hardverom. Korisnik može kontrolisati svako okruženje nezavisno i, ako je potrebno, umrežiti virtuelne računare zajedno ili ih spojiti na eksternu fizičku mrežu. U CC sistemu virtuelizacija omogućava rad velikog broja VM-a različitih klijenata i bezbednosnih ciljeva, sa enormnim porastom obima

digitalnih podataka [10] koje je nemoguće ispitivati metodama konvencionalne *post-mortem* DF-e [28]. Takođe, FWS sugeriše da se za forenzičku mašinu koristi VM-a kao forenzički alat [17].

Proces *post-mortem* DF istrage sadrži brojne korake, a u CC okruženju se može generalno enkapsulirati u četiri ključne faze: *pristup, akviziciju, analizu i izveštavanje* (*prezentaciju*). Posle pristupa izvoru digitalnih podataka, u fazi akvizicije forenzičar sakuplja što je moguće više promenljivih podataka sa aktivnog sistema i iz sistema proaktivne DF, zatim se isključuje računar i kreira forenzički (bit po bit) imidž svih medijuma za skladištenje. Za kreiranje imidža HD-a ispitivani računar se mora butovati iz forenzičkog alata ili nezavisnog butabilnog procesa, da bi se sprečile izmena originalnih podataka (npr. Windows OS-i u procesu butovanja unose stotinu i više promena u fajl sistemu) [27]. Ovakav pristup je nepraktičan za rekonstrukciju originalnog okruženja zbog brojnih mogućih hardverskih kombinacija ispitivanog sistema. Ako se forenzički imidž butuje na forenzičku mašinu sa različitom konfiguracijom hardvera, OS će otkriti ove razlike i pokušati (u nekim slučajevima neuspešno) da instalira nedostajući drajver. Pored toga, može se desiti da se neki instalirani servisi i softverski proizvodi ne mogu pokrenuti, ili se sistem uopšte ne može podići. Sličan problem postoji i u forenzičkoj VM-i, koja simulira samo neke osnovne hardverske komponente. Forenzički imidž se neće moći neposredno instalirati na forenzičkoj VM-i, pošto VM zahteva dodatne fajlove koji sadrže informacije o okruženju u kojem se butuje. Problem mogu rešiti različiti softverski proizvodi koji kreiraju ove dodatne fajlove, sa parametrima zahtevanim za VM-u. Prihvatljivo rešenje je model distribuirane, paralelne DF analize [15].

Na primer, okruženje kreirano sa *VMWare* znatno se razlikuje od originalnog računarskog sistema, a mala je verovatnoća da sam *VMWare* može generisati sudski prihvatljive dokaze. U ovom pristupu, konvencionalno i virtuelno okruženje treba koristiti konkurentno i nezavisno. Posle forenzički ispravne akvizicije imidža HD-a, prave se referentna i dve radne kopije. Jedna kopija se hešuje, čuva i procesira, striktno prema proceduri čuvanja imidža do zaključivanja istrage, a druga kopija imidža se daje tehničaru (ne forenzičaru) na ispitivanje u VM-i, bez osvrtanja na striktne forenzičke procedure. Svaki nalaz se dokumentuje i predaje kvalifikovanom forenzičaru koji nalaze potvrđuje u skladu sa forenzičkim procedurama. Dodatna prednost je ovog modela je što VM-a olakšava demonstraciju nalaza ne-tehničkim licima i zadržava u sebi sve antiforenzičke maliciozne aktivnosti [16].

Iako su postojale sumnje u vrednost *VMWare* kao alata za forenzičku istragu [23], pošto se zahtevaju brojne izmene originalnog okruženja, ako se imidž butuje na VM-i. Takođe, kada se sistem butuje na VM-i novi podaci se upisuju na originalni imidž i menjaju ga, što forenzički nije prihvatljivo. Zlatno pravilo da se forenzička analiza vrši na imidžu originalnog ispitivanog diska, u virtuelnom okruženju je nesumnjivo narušeno. Predložen je novi pristup u kojem se konvencionalno i virtuelno okruženje procesiraju paralelno i nezavisno čime, se skraćuje vreme analize i bolje se koristi manje kvalifikovano osoblje za forenzičku analizu.

Australijski institut za kriminologiju je izdao smernice sa preporukom da proces analize digitalnih dokaza treba da bude usaglašen sa sledećim osnovnim principima [28]:

- Minimalno rukovanje i rad sa originalnim računarskim sistemom i čvrstim diskom
- Dokumentovan nalog za bilo kakvu izmenu i dokumentovanje izmene
- Usaglašenost sa pravilima rukovanja i rada sa digitalnim dokazima
- Ne raditi ništa izvan opsega sopstvenog znanja, veština i tehnika forenzičke analize.

Tačnost procesa analize može se značajno povećati, a vreme analize podataka skratiti ako se proces proširi uključivanjem dve paralelne linije istrage, kao na slici 2 [15].



Slika 2. Proces distribuirane, paralelne analize podataka

U modelu se koriste rezultati analize na dva nivoa forenzičkih kompetencija: *manje iskusnih kompjuterskih tehničara i iskusnih forenzičara.* Forenzički manje iskusan kompjuterski tehničar radi po zadatku, ne mora da striktno sledi procedure metoda forenzičke istrage i nikada ne unosi rezultate istrage direktno u formalni proces izveštavanja. Uloga tehničara je da u kopiji imidža proveri sve što je od potencijalnog interesa i suzi obim forenzičkog ispitivanja, a zatim podnese izveštaj profesionalnom forenzičaru istraživaču. Zadatak kompjuterskog tehničara je da dobijeni imidž butuje na virtuelnoj mašini, tretira je kao normalan *živi* računarski sistem i pretražuje sve detalje relevantne za istragu.Metod kojeg koristi kompjuterski tehničar na vrši validaciju integriteta dobijenog imidža što nema posledica za istragu. Sve nalaze predaje iskusnom forenzičaru na verifikaciju i dalju istragu. Da bi instalirao imidž na VM-u, tehničar treba da instalira dodatne drajvere (npr. *Live View*) koji definitivno kontaminiraju imidž i prema tome rezultati ovog ispitivanja nebi bili prihvatljivi na sudu.

Osposobljeni i iskusni forenzičari rade striktno prema procedurama metoda DF istrage računarskog sistema i koriste standardne forenzičke procedure i tehnike da potvrdi rezultate analize tehničara i u izveštaj unosi samo dokaze koji su forenzički potvrđeni.

2.3. Osiguranje kvaliteta forenzičkih servisa u CC okruženju

Osigurati *kvalitet informacija* i *pouzdanost rada* računarskog sistema, osnovni je princip i cilj servisa DF istrage, jer trajno otklanja uzroke, a ne samo posledice bezbednosnog rizika. U evoluciji pojma *kvaliteta*, razlikuju se tri faze:

- **Kontrola kvaliteta** - QC (*Quality Control*): Tradicionalni pristup sistemu kvaliteta, koji se bavi posledicama, a ne uzrocima problema.
- **Osiguranje kvaliteta** - QA (*Quality Assurance*): Aktivniji pristup sistemu kvaliteta sa elementima planiranja i razvoja kvaliteta u svim fazama nastanka, razvoja, proizvodnje i upotrebe servisa. U domenu servisa DF istrage u CC okruženju poseban značaj ima uključivanje DF servisa u upravljački okvir zaštite – SMF (*Security Managament Framework*) u procesu uspostavljanja ISMS-a u CC okruženju.
- **Sveukupno upravljanje kvalitetom** - TQM (*Total Quality Management*): Predstavlja integraciju svih funkcija i procesa u organizaciji (uključujući i ISMS) u cilju konstantnog poboljšanja kvaliteta poslovanja. TQM, više usmeren na uzroke nego na posledice, je pre

strateška, nego operativna akcija koja podrazumeva proaktivno upravljanje kvalitetom kako bi se preventivno predvideli i sprečili mogući problemi.

Osiguranje kvaliteta može obezbediti kvalitet DF servisa. ISO definiše QA kao skup planiranih i uređenih aktivnosti neophodnih radi obezbeđivanja dovoljnog nivoa poverenja da će servisi dostići željene zahteve za kvalitetom. Osnovni faktori uspeha sistema QA-a su dokumentovani priručnik osiguranja kvaliteta - QAM (*Quality Assurance Manual*) i menadžer kvaliteta - QM (*Quality Manager*) koji osigurava implementaciju i održava sistema kvaliteta. U praksi, često ne postoji dokumentacija koja se analitički bavi politikom i procedurama, kao i praksom održavanja i poboljšavanja sistema kvaliteta. Ovo bi moglo da ima ogromne posledice ukoliko pravne norme proizilaze iz analitičke prakse na kojima se zasniva i forenzički postupak. Menadžer sistema kvaliteta u CC okruženju treba da definiše svoju misiju traženjem odgovora na sledeća pitanja: Da li su obezbeđeni servisi za održavanje i poboljšavanje sistema kvaliteta? Kako se zna da li se sprovode mere kvaliteta? Šta je potrebno da se uradi da bi se demonstrirali rezultati kvaliteta? [1].

3. KRITIČNI FAKTORI KVALITETA FORENZIČKIH SERVISA

U CC sistemu ključno pitanje je, kad organizacija ima proboj sistema zaštite, kome verovati i poveriti istragu - otkrivanje napada i identifikaciju incidenta. Standardni tim za zaštitu informacija u organizaciji, bez forenzičkih znanja i alata, može oštetiti digitalne dokaze o incidentu, a iznajmljivanje poverljivog provajdera DF istrage, može biti neprihvatljivo za neku organizaciju (npr. državnu koja ima vrlo osetljive informacije). Rešenje je da se u tim za zaštitu informacija u organizaciji uključe alati, tehnike i specijalisti za DF osposobljeni za rukovanje digitalnim dokazima ili sertifikovani za DF istragu. *Korporacijski digitalni forenzičari* su odgovorni za čuvanje tajnosti svih informacija o istrazi kompjuterskog incidenta i predaju istih lokalnim zvaničnim organima istrage kompjuterskog kriminala, ako takvu odluku donese menadžment organizacije. Sama DF analiza u korporacijskoj DF istrazi ide dublje od inicijalne istrage incidenta i uključuje [28]:

- Izgradnju čvrstih digitalnih dokaza prihvatljivih na sudu
- Izgradnju dokaza o poreklu e-dokumenata i istragu autentifikacije u istoriji pretraživača
- Rekonstrukciju događaja koristeći uskladištene i kompjuterski generisane dokaze i analizu vremenske linije napada
- Izgradnju dokaza za potvrdu, dokazivanje/osporavanje, tzv. „trojanske odbrane“
- Minimizaciju uticaja posledica napada
- Analizu Internet istorije i baze registara
- Povezivanje digitalnih dokaza za dokazivanje slučaja na sudu
- Priprema digitalnih dokaza za veštačenje i svedočenje pred sudom.

Dobro osposobljen *korporacijski tim* za zaštitu i upravljanje kompjuterskim incidentom, sa osposobljenim forenzičarem može obezbediti sledeće forenzičke servise:

- *Otkrivanje elektronskih informaciju* u e-formatu (*e-mail, instant messaging, chats, accounting databases, CAD/CAM files, websites*).
- *Otkrivanje i oporavak* prethodno obrisanih podataka i informacija.

- *Forenzički konsalting* koji uključuje pregled dokumenata, savete o strategiji rešavanja slučajeva, komunikaciji rezultata i nalaza na ne-tehnički način, sledeći korak u istrazi itd.
- *Konsalting za svedočenje/veštačenje* pred sudom.
- *Tehnički konsalting* (proces kriptozaštite, konverzija fajlova, produkcija e-mejlova itd.).
- *Forenziku čvrstog diska* i drugih medija za skladištenje, uključujući procese imidžovanja, akvizicije i analize uskladištenih podataka u fizičkim medijima (mobilni telefon, PDA uređaji, USB i HD). Ovaj proces uključuje otkrivanje skrivenih i obrisanih podataka kao i identifikaciju fajlova na bazi potpisa fajla, identifikaciju kreatora fajlova ili poruka.
- *Proaktivnu mrežnu forenziku,* uključujući monitoring i ispitivanje mrežnog saobraćaja pomoću snifera i trasera u realnom vremenu i pregled transakcionih logova radi otkrivanja sumnjivog ponašanja i anomalija.
- *Forenziku Interneta,* uključujući status korisnika u toku posete Internetu, kao što je namerno ili slučajno daunlodovanje sa zabranjenih/inficiranih sajtova, nepropisno slanje osetljivih informacija personalnim e-mejlom i nalogom itd.
- *Forenziku e-mejla i drugih sistema za slanje poruka.*

Kritični faktori uspeha forenzičkih servisa u CC okruženju su:

a. **Kvalitet menadžment sistema –** Najznačajniji faktor uspeha korporacijske DF istrage u virtuelnom prostoru je kvalitet *menadžmenta ljudskih resursa* i saradnje svih relevantnih učesnika [31]. Ovaj menadžment mora dati podršku forenzičkom timu organizacije, organizovati izradu i primenu politike i procedura za upravljanje kompjuterskim incidentom i *korporacijskim DF servisima*. Na primer, u slučaju upada u sistem, DF istragu treba da vodi forenzičar i da harmonizuje rad složenog tima programera, administratora sistema, inženjera mrežne opreme, administratora *firewalls-a*, administratora zaštite i dr. Digitalni forenzičar mora voditi profesionalce sa različitim veštinama i izraditi procedure za rad i integritet digitalnih podataka i dokaza u celom lancu istrage. Svi učesnici koji imaju pristup forenzičkim podacima i dokazima moraju voditi evidenciju za svaku aktivnost [12].

b. **Ugovor klijenta i provajdera CC servisa –** DF istraga u CC okruženju zahteva precizan SLA (*Service Level Agreemnt*) ugovor između klijenta i CSP-a [7]. Takav ugovor mora, između ostalog, obavezati provajdera CC servisa na „servis forenzičke istrage“ do određenog nivoa [8,32]. Na taj način klijent može saznati šta će, a šta neće lako dobiti u slučaju DF istrage. Zahtev za ovim CC servisom treba da postane standardni deo zahteva svakog CC klijenta koji postavlja osetljive informacije na CC sistem [24].

c. **Antiforenzički alati i aktivnosti -** Generalno, kompjuterski kriminalci preduzimaju brojne aktivnost, tehnike i alate da ometaju DF istragu. Pored klasičnih tehnika brisanja računarski generisanih tragova upada u sistem (*PC Claner, Evidence Eliminator* itd.), postavljanja vremenskih bombi, korisničkih aplikacija za gašenje računara itd., neke popularne antiforenzičke tehnike uključuju [27].:
   - izmenu vremenskog pečata,
   - promenu hedera i ekstenzija fajlova, parsiranjem fajla i skladištenjem njegovih delova u *slack* prostor fajla, da učini nemogućom identifikaciju fajla i njegovu namenu,
   - izvalačenje *hash* vrednosti lozinki bez traga izvršavanja,
   - napade tipa *Data mule* na rezervisane sektore na čvrstom disku,

- generisanje slučajnih imena fajlova, čime se izbegava detekcija na bazi otkrivanja potpisa fajla.

d. **Individualna odgovornost menadžera:** Menadžerska nebriga i zanemarivanje su česti uzrok brojnih sudskih slučajeva. Posebno, je lako dokazati posledice slučajeva nebrige i zanemarivanja *strategije menadžmenta tehnologija.* Dokumentovani međunarodni standard menadžment sistema bezbednosti informacija - ISMS (ISO/IEC 27001/2) obezbeđuje neophodna uputstva za menadžment sistema zaštite informacija u organizaciji, koja su posredno namenjena i za digitalnog forenzičara. Zbog sve veće forenzičke potrebe za procenu individualne odgovornosti menadžera forenzičar mora poznavati ISMS standard.
e. **Verifikacija kvaliteta izvora podataka:** Za pouzdanu identifikaciju incidenta zahteva se konstantna verifikacija izvora podataka o predznacima i indikatorima incidenta. Standardi dobre prakse preporučuju sledeće aktivnosti [13].
   - Korisnici podataka treba da razviju metod i kriterijume za evaluaciju kvaliteta izvora podataka o incidentu;
   - Korisnici ili provajderi CC servisa treba da verifikuju informacije o incidentu pre unosa u bazu podataka ili u program za upravljanje incidentom, bez kašnjenja toka procesa;
   - Podaci o incidentu treba da su u korelaciji sa eksternim servisima, dopunjeni i filtrirani da spreče dupliranje događaja, bez kašnjenja toka procesa;
   - Ako izvor podataka implementira mehanizam za povratnu vezu, korisnici treba da ga upotrebe u slučaju zahteva za poboljšanje kvaliteta podataka;
   - Eksterni izvori podataka (CERT/CIRT) treba da razviju svoje senzorske mrežu za detekciju malvera i drugih uzročnika incidenta, implementiraju *honeypot* i *sandbox* tehnologije kod klijenata i, ako je moguće, implementiraju pasivnu tehnologiju za monitoring DNS-a.

4. ZAKLJUČAK

Razvoj veb servisa, servisno-orijentisane arhitekture i drugih koncepata novijeg datuma prethodile su pojavi novog poslovnog okružanje nazvanog „*Cloud Computing*“. Poslovanje u CC okruženju zahteva novi pristup menadžmentu servisa, ISMS-u i zaštiti informacija [25], uključujući uspostavljanje sistema proaktivne DF [4,34,35] i razvoj DF veb servisa [2,36]. Još uvek je u fazi istraživanja uvođenje standardnog okvira forenzičkih servisa u CC okruženju [5,6,9]. Uspostavljanje, održavanje i poboljšavanje sistema kvaliteta je neophodna mera u svakom poslovnom procesu. U ovom radu su razmatrani problemi DF istrage u virtuelnom okruženju, kritični faktori kvaliteta DF servisa i njihov doprinos uspostavljanju sistema kvaliteta u CC okruženju..

LITERATURA

[1] Barbara, J.J., *Quality Assurance Practices for Computer Forensics*, Forensic Magazine, http://www.forensicmag.com/ article/quality-assurance-practices-computer-forensics-%E2%80%93-part-2?page=0,0. 2007.
[2] Bem D., Huebner E., *Computer Forensic Analysis in a Virtual Environment,* University of Western Sydney, Australya, 2008.

[3] Biggs, S.J., Vidalis, S., *Cloud Computing & The Impact On Digital Forensic Investigations*, International Conference for Internet Technology and Secured Transactions ICITST, 2009.
[4] Bradford, P. G., Hu, N., *A Layered Approach to Insider Threat Detection and Proactive Forensics*. http://www.acsa-admin.org/2005/techblitz/hu.pdf, 2005.
[5] Buyya, R., et all., *Cloud Computing: Principles and Paradigms*, John Wiley & Sons, Inc., 2011.
[6] Cloud Computing Aliance, *Securing The Cloud*, TechTarget, https://cloudsecurityalliance.org/, 2012.
[7] Costin, R., *Cloud computing and security: SLA compliance and cloud encryption*, Kaspersky Lab Expert, 16.05.2011.
[8] Dinakar, S., Buvaneshwari, S., Prabhu, V., Varshini, B., *Computer Forensic Analysis in Virtual Environment*, International Journal of Communications and Engineering, Vol 4, No 4, Issue 3, pp. 77-82, 2012,.
[9] ENISA (*European Network and Information Security Agency*), *Cloud Computing Information Assurance Framework,* http://www.enisa.europa.eu , 2009.
[10] Erickson, T., *IDS*, *Digital Universe Study*, for EMC Corp., SearchStorage.com, The Security Help Net, 2012.
[11] Gartner, *Assessing the Security Risks of Cloud Computing*, The Help Net Security, June 2008.
[12] Gottlieb, J., *Key challenges in proactive threat management*, The Help Net Securita News, 2012.
[13] Gorzelak, K. et al, *Proactive Detection of Network Security Incidents*", ENISA Report, 12.07.2012.
[14] Grance, T., Chevalier, S., Kent. K., Dang, H., *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*, NIST Special Publication 800-86, 2005.
[15] Grubor, G., *Evolucija modela digitalne forenzičke istrage*, Zbornik radova, Savetovanje ZITEH 2010, Beograd.
[16] Grubor, G., Njeguš, A., *Virtuelna mašinska introspekcija u digitalnoj forenzici,* Singidunum revija, vol. 7, no. 1, 2010.
[17] Hoopes, J., *Virtualization for Security*, Syngress, ISBN: 1597493058, 2012.
[18] IBM, *Cloud Security Guidance document*, http://www.redbooks.ibm.com/abstracts/redp4614.htm, 2012.
[19] ISO/IEC 27001, *IT – Code of practice for information security management,* http://www.iso.org, 2008.
[20] ISO/IEC 27002, *IT – Code of practice for security controls,* http://www.iso.org, 2008.
[21] ISO/IEC 27005, *IT – Code of practice for risk management,* http://www.iso.org, 2009.
[22] Krutz R. L., Vines R. D., *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley Publishing, Inc. http://23510310jarinfo.files.wordpress.com/2011/08/ebooksclub-org__cloud_security__a_comprehensive_guide_to_secure_cloud_computing.pdf, 2010.
[23] Kutz, A., *Monitoring a virtual infrastructure*: *A step-by-step process to successful virtual infrastructure management*, E-Guide, TechTarget, 2012.
[24] Leibolt, G., *The Complex World of Corporate Cyber Forensics Investigations*, Springer's Forensic Laboratory Science Series, 2010.

[25] Miliefsky, G., *Securing the Cloud: Is it a Paradigm Shift in Information Security?,* IT security Magazine, Vol5 No7, 2010.
[26] Miller, M., *Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online,* 2008.
[27] Milosavljević, M., Grubor, G., *Digitalna forenzika računarskog sistema,* Univerzitet Singidunum, 2010.
[28] Milosavljević, M., Grubor, G., *Istraga kompjuterskog kriminala*, Univerzitet Singidunum, 2011.
[29] Njeguš, A., *Servisno orijentisano modelovanje poslovnih procesa*, PPT prezentacija, Fakultet za informatiku i računarstvo, Univerziteta Singidunum, 2012.
[30] Qualis Inc., *Security & Compliance in the Cloud age*, http://www.qualys.com/docs/qualys-overview-paper.pdf , 2012
[31] Rittinghouse J. W., . Ransome J. F., *Cloud Computing: Implementation, Management and Security*, CRC Press Taylor & Francis Group, 2010.
[32] Ruan, K., Carthy, J., Kechadi, T., Crosbie, M., *Cloud forensics: An overview*, http://cloudforensicsresearch.org/ publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf
[33] Singhal, A., Gunestas, M., Wijesekara, D., *Forensics Web Services* (*FWS*)", NIST, http://csrc.nist.gov/ publications/nistir/ir7559/nistir-7559_forensics-web-services.pdf, 2010.
[34] Taylor, P., ***Proactive Forensics in the Workplace,*** Litigation and Forensics, Data Recovery Services, Inc. www.legalforensics.com, 2010.
[35] Zimmerman, S., *Proactive Computer Forensics*, Digital Forensics Magazine, 2010.
[36] Zimmerman, S., Glavach, D., *Cyber Forensics in the Cloud*, The Newsletter for Information Assurance Technology Professionals, Vol.4 No 1, pp. 4-7., 2011.

AN APPROACH IN SOLVING AUTOMATIC RESPONDING IN E-GOVERNMENT SERVICES

JEDAN PRISTUP U REŠAVANJU AUTOMATSKOG ODZIVA U SERVISIMA E-UPRAVE

Goran Šimić
Military Academy, Defense University
Gen.Pavla Jurišića Šturma 33, Beograd, Serbia
Telefon: +381 11 3603 409
Fax: +381 11 3005 130
E – mail: goran.simic@va.mod.gov.rs
Ejub Kajan
State University of Novi Pazar
Vuka Karadžića bb, 36300 Novi Pazar, Serbia
Telefon: +381 20 317 752
Fax: +381 20 337 669
E – mail: kajane@acm.org
Dragan Ranđelović
Academy of Criminalistic and Police Studies
Dušanova 196 Street, 11080 Belgrade, Serbia
Telefon: +381 11 3107188
Fax: +381 11 3161 152
E – mail: dragan.randjelovic@kpa.edu.rs

Abstract
Contemporary e-Government public services lack of response time in answering the citizens' questions. This paper gives one solution of this problem based on specific content model and searching engine. Multilayered clustering of e-government documents based on hybrid combination of Fuzzy-C-mean algorithm, cosine similarity and semantic similarity measures are the techniques used for these purposes. The main solution objective is to reduce time between citizen's questions and government feedbacks, either to completely eliminate or at least minimize the engagement of subject matter experts. The paper describes solution scenario, content model, clustering method and similarity measurement implemented in responding on the citizen questions.

Sažetak
Savremeni javni servisi e-Uprave imaju nedostatak dugog vremena odziva u odgovaranju na pitanja građana. Ovaj rad prikazuje jedno rešenje ovog problema na osnovu specifi;nog modela sadržaja i mehanizma pretrage. Višeslojno klasterovanje dokumenata e-Uprave na osnovu hibridne kombinacije *Fuzzy-C-mean* algoritma, kosinusna sličnosti i mere semantičke sličnosti su tehnike koje se koriste za ovu svrhu. Osnovni cilj je rešenje da se smanji vreme povratne informacije na pitanja građana, i da se time potpuno eliminiše, ili bar smanji angažovanje

eksperata. U materijalu je opisan scenario rešenja, model sadržaja, metod klasterovanja i merenje sličnosti, korišćeno u odgovaranju na pitanja građana.

1. INTRODUCTION

There is a growing amount of information related to the government regulations, announcements, guidelines and similar contents which are sited at the government portals, so that citizens can browse, search and use them by using simple text based searching engines.
The content is different in structure, type and way in which is stored. Therefore, existing searching services are not appropriate to the citizen needs. Citizens, without much knowledge in specified domain, can be disappointed in interacting and using these government portals. In such a situation, domain experts must be engaged to examine the various cases and select the appropriate service or information requested by citizen. Typically scenario should consist of the following: Citizen makes a question (request) for specific information; government officer receives the request, examines the request, clustering the nature of the problem and sends it to specific domain expert; domain expert evaluates the citizen's case and prepares the requested information. Some of the citizen's cases are related to previous and could be easily answered. Others need more time for creating the response. Moreover, the number of requests usually significantly exceeds the available number of government domain experts that process the requests. It produces increasing of the cost of e-Government services. The paper shows the solution for reducing of the time between citizen's questions and government feedbacks as well as eliminating or minimizing the engagement of subject matter experts.

2. CHANGING IN BASIC SCENARIO

Proposed solution provides the citizen – service interaction in three phases [1.]. The scenario is shown in Figure1. At the beginning the system offers groups of key terms (phrases and words) to the citizen. Firstly, citizen chooses the question from the list, or enters a new one.

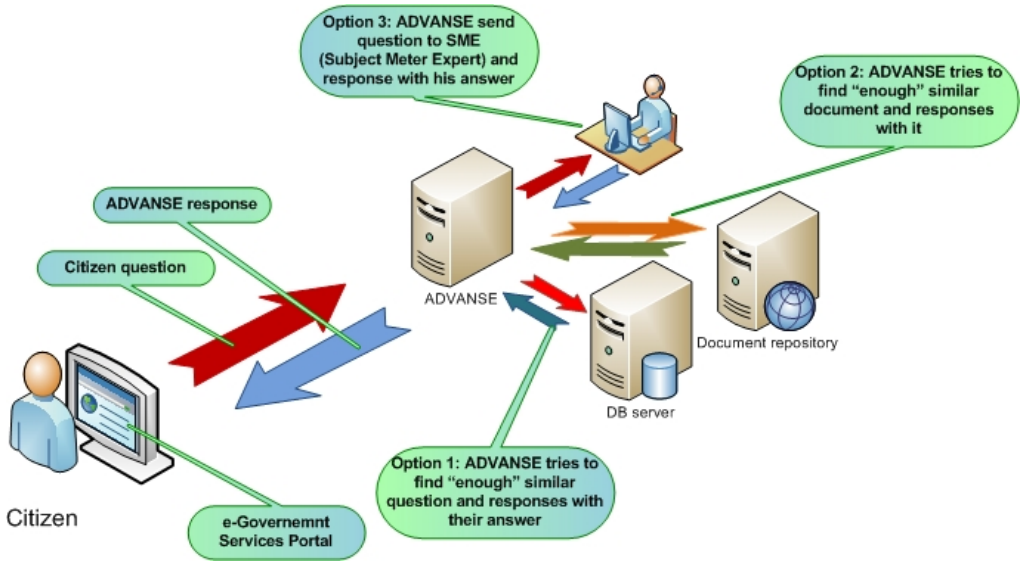


Figure 1: Scenario of use

If the question is selected from the list, the answer which is fully matched to the question is delivered. Otherwise, there are 3 options in which the responding can be performed:

- Option 1 – the system finds existing question in the data base which is the most similar to the new one and responses with its answer.
- Option 2 – the system finds 'enough' similar document at the repository and responses with it.
- Option 3 – if there are not 'enough' similar questions or documents in the system, the citizen's question is forwarded to the subject matter expert (SME); in such a case the announcement about it is delivered to the citizen.

3. CONTENT REPRESENTATION

There are three content types in the system: citizen's questions, governmental documents and SME answers. Therefore the content model is layered into the 3 layers which are shown in the figure 2. The content model for a particular domain (i.e. finance, medicine, or low) represents a corps that is layered. The questions are in the top layer, the answers are in the middle layer and the documents are in the bottom layer. Layers of documents and questions are clustered by 'Key terms'. These terms represent the particular words or phrases extracted from the dictionary of the specific domain.

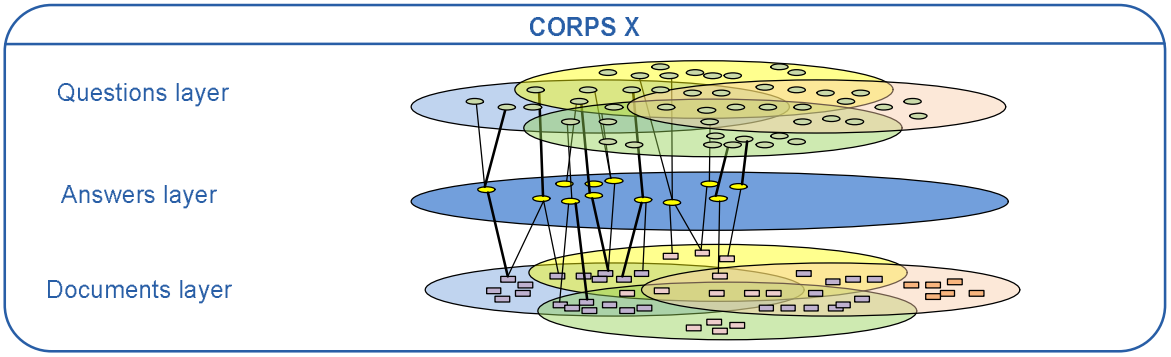


Figure 2: General content model

There are documents and questions that belong to more than one cluster. That means there are several key terms in one document, or in one question. Therefore the clusters are represented as the sets that are intersected with each other. Therefore, the fuzzy C mean algorithm is used for clustering. Every question and document can belong to more than one cluster in some degree. This value is calculated during the clustering process and it is represented by membership function.

The answers represent the real products of the system. They are connected to the questions as well as to the documents. The connections can be many-to-many relation type. It means that each question could have a multiple answers and each answer could be relevant for multiple questions. The similar approach is applied for connection between answers and documents.

4. CLUSTERING AND SIMILARITY MEASURING

Initialization represents the first step of the clustering process. During this phase the system defines or makes cluster centers of gravity (centroids). *Random partition* [2.], *Forgy partition* [3.], *Kaufman partition* [4.] represent the most used methods for this purpose. Random and Forgy partition are based on predefined number of clusters while Kaufman method calculates it. Because of using the predefined set of key terms as number of clusters, Random partition is found as the most appropriate for initialization purpose.
Clustering is performed by using Fuzzy C – mean algorithm (FCM) [5.][6.]. Unlike the most popular K – means algorithm [7.][8.] that forms clusters with the clear boundaries and without intersections, FCM provides possibility that chunks of information can belong to more than one cluster. Next is a functional representation of used clustering method:

$$f_{fcm} = \sum_{i=1}^{n}\sum_{j=1}^{k} m_{ij}^{f}\left\|x_i - c_i\right\|^2$$

, where n stands for number of key terms, k stands for number of clusters, m_{ij} represents the membership function of information chunk x, while c stands for key term (centroid of the particular cluster). Membership function is normalized by using logarithm values of key term frequency [9.] in the information chunk $tf_{t,q}$ and inverse document frequency [9.] represented as a ratio of full number of information chunks in the cluster N_q and number of information chunks that contains particular key term N_{qt}. It is shown in the next equation.

$$m_{t,q} = \log(tf_{t,q} + 1)\log\frac{N_q}{N_{q,t}}$$

The same function is used for measuring similarity between the new citizen's question and existing ones during the exploitation of the system. This way the system becomes adaptive because every new question added into the system change the inverse document frequency and it can be the best fitted candidate for the new asked one.

5. PREPARING RESPONSE

As shown in the figure 2, there are connections between questions, answers and documents. They provide the responding mechanism. This is shortly described in the options 1 and 2 (2nd chapter). Owing to fuzzy approach, there is usually more than one candidate for responding. The decision about which one is the best is based on the pondering of the answers. Beside the measures mentioned in the previous chapter, the citizens' feedbacks are also involved in it. This value provides the system ability to calculate the strength of the question – answer connection (S_{qa}). This value depends on different factors shown in the next equation:

$$S_{qa} = V_{ini} + I_{nf} * R_{pn}$$

When SME makes a new answer, the system assigns initial strength (V_{ini}) to the connection. This value is important immediately the answer is made and there is no one citizen's feedback. Over time, as the number of feedbacks grows up, the importance of the other two factors also grows: feedback importance (I_{nf}) and positive & negative ratio (R_{pn}). Feedback importance is calculated

by using the number of positive and negative feedbacks. Another factor in product is positive & negative ratio. Its value is calculated by dividing the summary result of positive and negative grades with whole number of feedbacks. Responding with the answers represents the favorite scenario.
Responding with documents represents the alternative way. The similarity in this case is calculated by matching key terms in question and document description. The best fitted document would be delivered.

6. CONCLUSION

Hybrid solution proposed in paper is determined by heterogenic nature of e-Government services. Varieties of functionalities and content types have the common characteristic: they are all focused to satisfy citizens' needs and requests. High quality of service basically means two things: responding with really useful content in a reasonable short time. These two is a main objective of presented advanced answering mechanism. Layered model of overlapped clusters produced by Fuzzy-C-mean algorithm, as like as semantically connected questions, answers and documents represent the main achievement of the research. These features provide flexibility and adaptive response of the system. The system provides the conditions for early high – quality responding (for each case). Since deployment, the citizens' satisfaction has grown up because the feedbacks are getting better over time.
Presented solution is a part of wider project aiming to provide intelligent decision support system that will collect, cluster and analyze data from various data sources including, but not limited to, social, biological, and economical systems in order to make government's decisions easier. Further research will take place in improvement of adaptive behavior of the system by evaluating and implementing appropriate algorithms in different domains as well as establishing semantically connections and clustering of heterogeneous data sources.

7. REFERENCES

[1.] Šimić, G., Kajan, E., Jeremić, Z., Randjelović, D., (2012): "An Approach to Document Clustering Using Hybrid Method" in *IADIS International Conference E-Society 2012*, *Proceedings*, Berlin, Germany, pp. 153-159
[2.] Hamerly, G. and Elkan, C., (2002): "Alternatives to the k-means algorithm that find better clusterings" in: *11th international conference on Information and knowledge management*, *Proceedings*, (CIKM), pp. 600-607
[3.] Garijo, F., Riquelme, J., Toro, M., (2002): "A GRASP algorithm for Clustering" in: *IBERAMIA 2002, LNAI 2527, Proceedings*, *Spain*, pp. 214 – 223
[4.] Laan, M., Pollard, K., Bryan, J., (2003): "A New Partitioning Around Medoids Algorithm", *Journal of Statistical Computation and Simulation* Vol. 73, No. 8, pp. 575-584
[5.] Kanzawa, Y., Endo ,Y. and Miyamoto, S., (2010): "Indefinite Kernel Fuzzy C - Means Clustering Algorithm" in: *7th Conference Modeling Decisions for Artifical Intelligence*, *Proceedings, France*, pp. 116 – 128
[6.] Zou, K., Wang, Z., Hu, M., (2008): "A new initialization method for fuzzy c-means algorithm", *Journal of Fuzzy Optimization and Decision Making*, Vol. 7/4 pp. 409 – 416

[7.] MacQueen, J., (1967): "Some Methods for classification and Analysis of Multivariate Observations" in: *5th Berkeley Symposium on Mathematical Statistics and Probability*, *Proceedings*, University of California Press. pp. 281–297
[8.] Vattani, A., (2011): "K-means Requires Exponentially Many Iterations Even in the Plane", *Discrete and Computational Geometry Journal*, Vol. 45, No. 4, Springer, pp. 596 – 616
[9.] Wu, H.C., Luk, R.W.P, Wong, K.F., and Kwok, K.L ., (2008): "Interpreting TF-IDF term weights as making relevance decisions", *ACM Transactions on Information Systems*, Vol. 26, No. 3, Article 13

PROFILISANJE WEB APLIKACIJA I VIZUALIZACIJA REZULTATA

Aleksandar Jevremović
Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: ajevremovic@singidunum.ac.rs
Mladen Veinović
Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: mveinovic@singidunum.ac.rs
Dušan Regodić
Univerzitet Sinergija
Raje Baničića BB, Bijeljina, Republika Srpska
E-mail: dregodic@sinergija.edu.ba
Goran Šimić
Vojna akademija
E-mail: gshimic@gmail.com
Saad Zeid
Faculty of Engineering, Sirte University, Sirte, Libya
E-mail: saad_zeid@hotmail.com

Sažetak
Savremene *Web* aplikacije zahtevaju visok nivo performansi da bi bile prihvaćene od strane korisnika. Arhitektura Veba je veoma složena i postoji veliki broj mogućih „uskih grla“, koja često nije lako locirati i ukloniti. U ovom radu predstavljamo način za profilisanje *Web* aplikacija zasnovanih na PHP programskom jeziku i otklanjanje „uskih grla“ i grešaka u njima.

Ključne reči: performanse, optimizacija, vizualizacija, proflisanje

Abstract
Modern Web applications require high-performance execution in order to be accepted by users. Web architecture is very complex and there are many possible bottlenecks. These are usually not easy to locate and remove. In this paper we present some server-side methods for profiling Web applications based on PHP programming language and removing bottlenecks and bugs.

1.UVOD

Performanse *Web* aplikacija mogu predstavljati ključan aspekt njihovog uspeha. Na primer, dodatnih 500 milisekundi kod prikazivanja rezultata na *Google* pretraživaču rezultovalo bi sa 20% manje poseta, dok svakih 100 dodatnih milisekundi pri odzivu *Web* aplikacije koja pokreće *Amazon.com* umanjuje prodaju za jedan procenat[1]. Yahoo.com beleži pad od 5 do 9 procenata poseta na svakih dodatnih 400 milisekundi potrebnih za učitavanje stranica[2]. Optimizacijom stranica za preuzimanje *Firefox* Web pretraživača i smanjivanjem vremena učitavanja za 2,2 sekunde zabeleženo je povećanje broja preuzimanja pretraživača za 15,4%[3]. Šest dodatnih sekundi za učitavanje stranica *Hotmail* servisa rezultovalo je gubitkom od 40

miliona prikazivanja reklama, odnosno gubitkom od 2,4 miliona dolara[4]. *Shopzilla*, servis za upoređivanje cena zabeležio je porast od 7-12% posetilaca koji su se odlučili za kupovinu nakon smanjivanja prosečnog vremena potrebnog za učitavanje stranice sa 7 na 2 sekunde[5]. Pomenuto smanjivanje vremena je rezultovalo i u porastu broja otvorenih stranica za 25 procenata, kao i u duplo manjem broju mrežnih čvorova potrebnih za isporuku sadržaja.

Nalazi studije[6] koju je kompanija *Forrester Research* napravila za potrebe *Akamai* mreže za isporuku sadržaja pokazuju da: današnji posetioci *Web* stranica postaju nestrpljivi ukoliko se stranica ne učita u roku od dve sekunde; niske performanse sajta za e-trgovinu izazivaju nezadovoljstvo kupaca i uzrok su odustajanja od njegovog korišćenja; posledice niskih performansi sajtova za e-trgovinu su gubitak profita i loš utisak o kompaniji koja vrši prodaju; performanse sajtova su jedan od ključnih parametara za njihovo korišćenje na mobilnim telefonima.

S obzirom na kompleksnost okruženja u kojima se izvšravaju i koriste *Web* aplikacije, postoji više načina za optimizaciju njihovih performansi. Na primer, američka kompanija *Netflix*, koja pruža uslugu emitovanja audio/video sadržaja putem Internet mreže, zabeležila je rasterećenje komunikacionih kanala od 43% nakon uključivanja kompresovanja sadržaja[7]. Jedan od originalnih načina za smanjenje brzine učitavanja stranica predstavljen je i u radu[8]. Grubo gledano, optimizacija Web aplikacije zasnovane na Internet tehnologijama može da se vrši na serverskoj i klijentskoj strani, kao i komunikacionoj infrastrukturi.

U ovom radu su prikazane neke od metoda za optimizaciju *Web* aplikacija na serverskoj strani, razvijenih u *PHP* programskom jeziku. Obuhvaćene su metode profilisanja *Web* aplikacija, vizualizacija rezultata profilisanja i načini za komunikaciju između razvojnog okruženja i izvršne platforme sa ciljem eliminisanja grešaka.

2.PROFILISANJE WEB APLIKACIJA

Profilisanje softvera je jedan od oblika dinamičke programske analize kojim se utvrđuju različite karakteristike programa koji se analizira - vreme potrebno za izvršavanje funkcija, memorijski prostor potreban za skladištenje sadržaja promenljivih, redosled pozivanja funkcija i slično. Za ovu analizu se koriste posebni alati za profilisanje koji se međusobno mogu značajno razlikovati, u zavisnosti od programskog jezika i okruženja u kojima je program pisan i izvršava se.

Profilisanje *Web* aplikacija je jedna od najsloženijih formi profilisanja softvera. Okruženja u kojima se izvršavaju i koriste *Web* aplikacije su složenija nego kod *desktop* aplikacija zbog heterogenosti i distribuiranosti podataka i funkcionalnosti. Od alata za profilisanje se zahteva da podrže

- profilisanje na nivou slanja zahteva,
- profilisanje izvršavanja na strani servera,
- profilisanje prenosa odgovora i obrade na strani klijenta.

U praksi se najčešće koriste pojedinačni alati za svaki od navedenih načina profilisanja, kako zbog cene sveobuhvatnih rešenja, tako i zbog veće fleksibilnosti u radu.

2.1. Xdebug proširenje PHP interpretera

Jedno od najpopularnijih rešenja za prifilisanje *PHP* programa i otklanjanje grešaka u njima jeste sistem pod imenom *Xdebug*. U pitanju je klasično proširenje *PHP* interpretera sa javno dostupnim izvornim kodom i relativno jednostavnim procesom instalacije. *Xdebug* omogućava dinamičku analizu softvera a rezultat praćenja izvršavanja su tekstualni fajlovi u kojima se nalaze rezultati praćenja izvršavanja.

```
==== NEW PROFILING FILE ==============================================
version: 1
creator: xdebug 2.2.1
cmd: /home/ajevremovic/public_html/index.php
part: 1
positions: line
events: Time
fl=php:internal
fn=php::session_start
3 195
...
```

Listing 1. Izvod iz sadržaja fajla dobijenog prilikom praćenja izvršenja

Ono što treba imati u vidu je i to da izvršavanja *PHP* skriptova koja se prate *Xdebug* sistemom traju znatno duže. U skladu sa tim, ovo proširenje ne treba koristiti na produkcionim serverima, ili ga ne treba držati aktivnim osim u slučajevima kada se prati izvršavanje konkretnih zahteva.

Značajnu karakteristiku *Xdebug* proširenja predstavlja i mogućnost njegovog povezivanja sa *NetBeans* razvojnim okruženjem. To se postiže korišćenjem *DBGP-a*, opšteg protokola za komunikaciju između programskih jezika i sistema koji imaju potrebu za praćenjem izvršavanja. Korišćenjem ove mogućnosti direktno iz integrisanog razvojnog okruženja može se kontrolisati izvršavanje skriptova i pratiti stanje promenljivih.

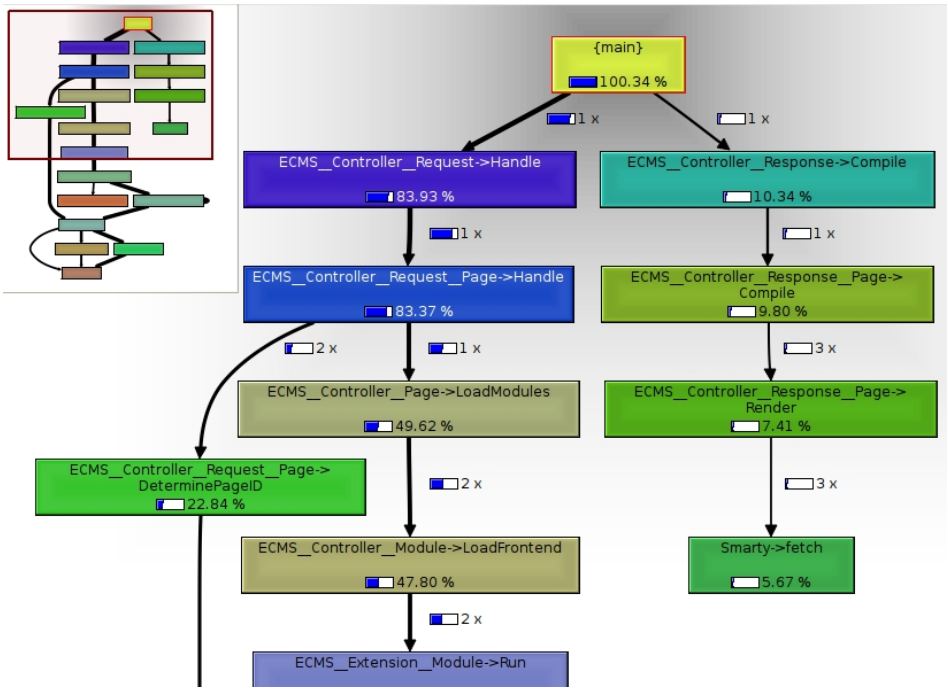
3. VIZUALIZACIJA PODATAKA

Rezultati dobijeni *Xdebug* alatom mogu se analizirati ručno, u svom numeričkom obliku. Međutim, daleko je jednostavnije i informativnije analizu vršiti putem alata za vizualizaciju podataka. Najpopularniji alati ove namene su *WinCacheGrind* (za *Windows* operativni sistem) i *KCacheGrind* (za Linux operativni sistem). Oba alata se besplatno mogu preuzeti sa matičnih lokacija.

Incl.	Self	Distance	Calling	Callee
83.65	0.08	1	1	ECMS__Controller__Request->Handle (Request.class.php)
83.09	0.44	2	1	ECMS__Controller__Request__Page->Handle (Page.class.php)
72.92	8.00	3-8 (8)	37	ECMS__SQL->Select (SQL.class.php)
57.45	57.45	2-10 (10)	133	php::mysql_query (php:internal)
49.45	0.20	3	1	ECMS__Controller__Page->LoadModules (Page.class.php)
47.64	1.76	4	2	ECMS__Controller__Module->LoadFrontend (Module.class.php)
42.63	0.11	5	2	ECMS__Extension__Module->Run (Module.class.php)
42.49	0.15	6	1	ECMS__Extension__Module__Menu__Section2Tree__Frontend->Main (Frontend.class.p...
39.75	6.36	4-9 (9)	37	ECMS__SQL->Describe (SQL.class.php)
34.22	0.66	7	1	ECMS__Controller__Page->LoadTree (Page.class.php)
22.76	0.56	3	2	ECMS__Controller__Request__Page->DeterminePageID (Page.class.php)
16.18	0.64	4-9 (9)	37	ECMS__SQL->SetCharset (SQL.class.php)
10.30	0.07	1	1	ECMS__Controller__Response->Compile (Response.class.php)
9.77	0.50	2	1	ECMS__Controller__Response__Page->Compile (Page.class.php)
7.38	0.54	3	3	ECMS__Controller__Response__Page->Render (Page.class.php)
7.23	0.17	3-7 (7)	2	ECMS__Controller__Page->DetermineRootID (Page.class.php)
5.65	0.13	4	3	Smarty->fetch (Smarty.class.php)

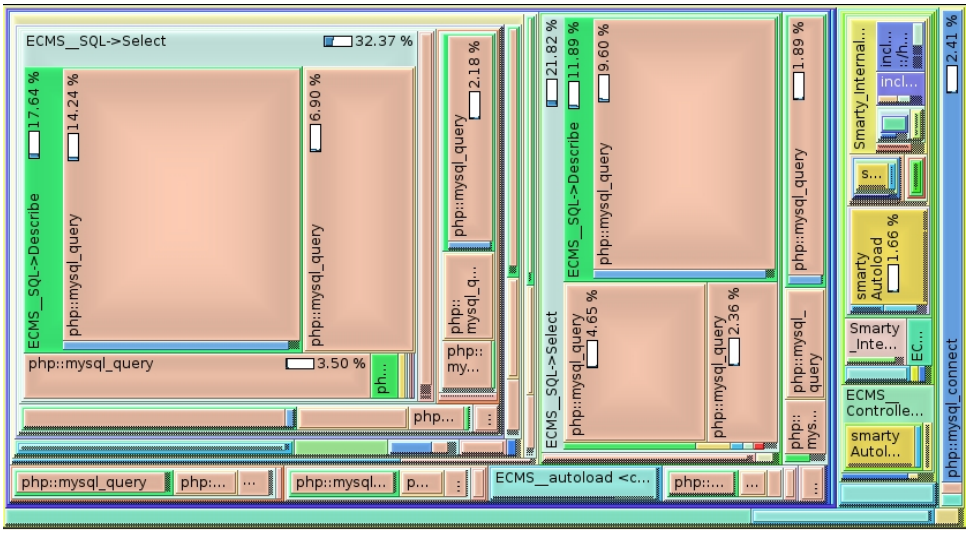
Slika 1. Broj poziva i parametri izvršavanja funkcija

Prvi tip izveštaja koji *KCacheGrind* alat daje jeste sumarna lista funkcija koje su pozivane tokom obrade zahteva. Ova lista, pored naziva same funkcije, sadrži i fajl iz koga je funkcija učitana, zatim koji procenat sveukupnog vremena izvršavanja je rezultat izvršavanja te funkcije (bez i sa podpozivima) i koliko puta je funkcija pozivana



Slika 2. Stablo pozivanja funkcija aplikacije

Sledeći važan tip vizualnog izveštaja jeste dijagram toka izvršavanja zahteva. Iz ovog tipa dijagrama se može brzo i jasno videti koji je aktuelni redosled pozivanja i izvršavanja funkcija (ili metoda), kao i koje funkcije su pozivane od strane kojih funkcija. Opisani dijagrami su i interaktivni, što znači da se nivo apstrakcije može podešavati tokom pregleda.



Slika 3. Grafički prikaz raspodele utrošenog vremena po funkcijama

Grafički prikaz raspodele utrošenog vremena po funkcijama pruža jednu od najkvalitetnijih informaciju o tome kojih funkcija rad treba optimizovati, odnosno optimizacijom kojih funkcija će se postići najveći efekat u smanjivanju sveukupnog trajanja obrade zahteva. U praksi intuitivni pristup za optimizaciju najčešće ne daje nikakve ili čak negativne rezultate jer logička složenost funkcija i broj linija koda u njima često nisu u korelaciji sa vremenom potrebnim za izvršavanje. Nasuprot tome, vizualizacija utrošenog vremena jasno ukazuje na to na koje se delove programa treba fokusirati, odnosno optimizacijom kojih delova se može postići najveći efekat.

4. ZAKLJUČAK

Dinamička analiza softvera je tip analize u kome se karakteristike softvera utvrđuju u toku samog izvšravanja, u realnim ili simuliranim uslovima. Ova analiza ne predstavlja optimalan izbor u ranim fazama razvoja, ali je nezamenljiva u periodu eksploatacije softvera.

Web aplikacije se izvršavaju u složenim i promenljivim okruženjima, što predstavlja dodatan izazov kod njihovog profilisanja i optimizacije. U ovom radu su prikazane softverske komponente i način njihovog korišćenja za profilisanje *Web* aplikacija i vizualizaciju dobijenih rezultata. Njihovim korišćenjem se može precizno utvrditi koji delovi aplikacije predstavljaju „usko grlo“, odnosno na koje delove aplikacije se treba fokusirati prilikom pokušaja njene optimizacije.

LITARATURA

[1.] Greg Linden, „Make Data Useful“, StanfordDataMining.2006-11-29.ppt ;

[2.] Stoyan Stefanov, „Don't make me wait or Building High-Performance Web Apps“;

[3.] Blog of Metrics, Mozilla, https://blog.mozilla.org/metrics/category/website-optimization/

[4.] Alladin Nassar, „Performance-Based Design - Linking Performance to Business Metrics“, Velocity Web Performance and Operations Conference, 2009;

[5.] Philip Dixon, „Shopzilla's Site Redo - You Get What You Measure“, Velocity Web Performance and Operations Conference, 2009;

[6.] Forrester Research, Akamai Technologies, „eCommerce Web Site Performance Today - An Updated Look At Consumer Reaction To A Poor Online Shopping Experience “;

[7.] Bill Scott, „Improving Netflix Performance“, Velocity Web Performance and Operations Conference, 2008;

[8.] A. Jevremovic, R. Popovic, D. Zivkovic, M. Veinovic, G. Shimic, „Improving Web Performance by a Differencing and Merging System“, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012, ISSN (Online): 1694-0814, page 349-355;

NACIONALNA STRATEGIJA INFORMACIONE BEZBEDNOSTI- IMPERATIV ZEMALJA EVROPSKE UNIJE U OBLASTI INFORMACIONE BEZBEDNOSTI

THE NATIONAL STRATEGY OF INFORMATION SECURITY - EUROPEAN UNION COUNTRIES IMPERATIVE OF INFORMATION SECURITY

Ivan Barać[49]**, Gojko Grubor**
Univerzitet Singidunum
Danijelova 32, 11000 Beograd
E-mail: ivan.barac@yahoo.com
E-mail: ggrubor@singidunum.ac.rs

Sažetak
Da bi odgovorile na sajber pretnje u stalno promenljivom okruženju, države članice Evropske unije moraju da imaju fleksibilne i dinamične strategije informacione bezbednosti. Uzimajući u obzir prekograničnu prirodu pretnji, neophodno je fokusirati se na jaku međunarodnu saradnju. Sveobuhvatna nacionalna strategije informacione bezbednosti je prvi korak u tom pravcu. Razumevanje informacione bezbednosti i drugih ključnih uslova varira od zemlje do zemlje, što utiče na veoma različite pristupe strategiji informacione bezbednosti na međunarodnom nivou.

Ključne reči
informaciona bezbednost, sajber prostor, sajber pretnje, kritična infrastruktura.

Abstract
To respond to cyber threats in a constantly changing environment, the member states of the European Union must have a flexible and dynamic strategy for information security. Taking into account the cross-border nature of the threat, it is necessary to focus on the strong international cooperation. Comprehensive national strategy for information security is the first step in that direction. Understanding of information security and other key requirements vary from country to country, affecting a very different approach to information security strategy at the international level.

1. UVOD

Državne institucije, kompanije kao i društvo u celini, zavise od funkcionisanja informaciono komunikacionih tehnologija (u daljem tekstu: IKT) i rada kritičnih infrastruktura koje se oslanjaju na dostupnost, integritet i poverljivost informacija. Zaštita tih *kritičnih informacija* ili *kritične informacione infrastructure* postaje jedan od prioritetnih nacionalnih interesa u brojnim državama EU. Incidenti koji izazivaju poremećaj u funkcionisanju IKT usluga za podršku

[49] doktorant na Univerzitetu Singidunum

kritične infrastrukture mogu izazvati ogromne negativne efekte u funkcionisanju društva i privrede. Tako je informaciona bezbednost postala jedan od najvažnijih izazova 21. veka.

Nacionalna strategija informacione bezbednosti (u daljem tekstu: NSIB) je okvir i sredstvo da se poboljša bezbednost i otpornost nacionalnih kritičnih informacionih infrastruktura. Kroz NSIB definiše se čitav niz nacionalnih ciljeva i prioriteta koji treba da budu ostvareni u određenom vremenskom periodu. NSIB predstavlja strateški okvir za pristup jedne nacije informacionoj bezbednosti.

Evropska agencija za mrežnu i informacionu bezbednost - ENISA (*European Network and Information Security Agency*) razvila je praktičan vodič za razvoj i izvršenje NSIB[50]. Vodič predstavlja pravilo dobre prakse i preporuke o tome kako da države članice EU razviju, implementiraju i održavaju NSIB. Razvoj sveobuhvatne strategije može predstavljati brojne izazove.

2. INFORMACIONA BEZBEDNOST I NSIB

Termin informaciona bezbednost, podrazumeva, primarno, bezbednost informacija i podataka u IKT sistemu, a sekundarno ─ bezbednost informacione imovine, čime se posredno štite informacije, kao njen najvredniji deo. Na nivou države to je stanje zaštićenosti nacionalnih interesa u informacionoj sferi, određenih skupom ličnih, poslovnih i državnih interesa ili zaštićenost informacija od slučajnih ili namernih aktivnosti prirodnog ili veštačkog karaktera, koje mogu naneti neprihvatljivu štetu informacionoj imovini organizacije [1] .

Usvajanje NSIB je prvi korak u uspostavljanju nacionalnog programa za informacionu bezbednost. U NSIB treba objasniti značaj informacione bezbednosti, definisati ciljeve i prioritete, uloge i odgovornosti svih zainteresovanih strana na nacionalnom nivou i posebno naglasiti neophodnost njihove kooperacije. NSIB takođe može poslužiti kao okvir za stvaranje zakona koji se odnose na oblasti kao što su kompjuterski kriminal, zaštita intelektualne svojine, zaštita informacija u IKT sistemima i sajber prostoru, zaštita privatnost itd. [2].

Država je glavni subjekt u oblasti informacione bezbednosti jer poseduje zakonske, ekonomske i diplomatske kapacitete [3] . Kritične informacije, odnosno, *kritična informaciona imovina* upravlja i kontroliše kritične sektore i njihovu fizičku imovinu. Zato je, obezbeđivanje visokog stepena informacione bezbednosti kritičnih infrastruktura, strateški nacionalni cilj.
Imajući u vidu da se pretnje po informacionu bezbednost razlikuju od zemlje do zemlje, međunarodna telekomunikaciona unija - ITU[51] (*International Telecommunication Union)* je razvila opšti model za uspostavljanje sistema nacionalne informacione bezbednosti kroz usvajanje NSIB [4].

2.1. NSIB Nemačke

[50] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national_cyber-security-strategies-an-implementation-guide/at_download/fullReport
[51] http://www.itu.int

Nemačka Vlada objavila je u februaru 2011. godine NSIB[52]. Cilj NSIB je da pruži pun doprinos očuvanju bezbednog sajber prostora i tako očuva i unapredi ekonomski i društveni prosperitet zemlje. Strategija je uglavnom fokusirana na civilni sektor, dopunjena sa merama koje Vlada preduzima da bi zaštitila svoje kapacitete. Poseban akcenat dat je na saradnju sa međunarodnim organizacijama kao što su UN, EU, Savet Evrope, NATO, G8 i dr., sa ciljem da se obezbede koherentnost i kapaciteti međunarodne zajednice za zaštitu sajber prostora. Strategijom su definisani sledeći ciljevi i mere:

1. zaštititi kritičnu informacionu infrastrukturu,
2. zaštititi IKT sisteme u Nemačkoj,
3. ojačati informacionu bezbednost u javnom sektoru,
4. formirati nacionalni sajber centar za odgovore na incidente,
5. formirati nacionalni savet za informacionu bezbednost,
6. obuka kadrova u federalnim organima u oblasti informacione bezbednosti,
7. sprovoditi borbu protiv kriminala u sajber prostoru,
8. sprovoditi evektivne koordinirane akcije sa ciljem jačanja informacione bezbednosti u Evropi i širom sveta.

Vladina agencija za informacionu bezbednost[53] ima ključnu ulogu u razvoju informacione bezbednosti u Nemačkoj, a osnovna funckija je zaštita Vladine infrastrukture od sajber napada. Budžet ove agencije u 2011. godini bio oko 68 miliona eura, što govori o stepenu svesti o značaju ulganja u kapacitete za unapređenje informacione bezbednosti. U aprilu 2011. godine formiran je nacionalni centar za sajber odbranu[54] koji ima osnovni cilj da analizira sajber incidente i da objavljuje obaveštenja, upozorenja i preporuke o sajber pretnjama i ranjivostima svih zainteresovanih strana u nemačkom sajber prostoru.

2.2. NSIB Ujedinjenog Kraljevstva (*The United Kingdom*-UK)

Vlada UK je 25.11.2011. godine objavila najnoviju NSIB[55]. Osnovna premisa strategije je da ona određuje kako će UK podržati ekonomski prosperitet, zaštiti nacionalnu bezbednost i zaštiti javnu dimenziju života svakog građanina u sajber prostoru. Strategijom je predstavljen plan razvoja informacionog društva u UK do 2015. godine i definisana su četiri ključna cilja:

1. da se UK posveti borbi protiv sajber kriminala i da na taj način postane jedno od najbezbednijih područja u svetu za poslovanje u sajber prostoru,
2. da UK postane otpornija na sajber napade, kako bi bolje zaštitila svoje interese u sajber prostoru,
3. da UK pomogne u oblikovanju otvorenog, stabilnog i dinamičnog sajber prostora koji bi javnost mogla da koristi sigurno i koji bi pružio podršku otvorenom društvu i
4. da UK stekne višeslojna znanja, veštine i kapacitete koji su potrebna osnova za rešavanje svih problema iz domena informacione bezbednosti.

[52] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf
[53] https://www.bsi.bund.de
[54] https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Cyber-Abwehrzentrum_01042011.html
[55] http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

Oko 52% građana UK koji imaju pristup Internetu koriste *online* kupovinu kao priliku da uštede[56].
UK je pozitivno usvojila sajber prostor kao sredstvo poslovanja. U 2009. godini oko 608 miliona platnih kartica je korišćeno za online plaćenje, sa ukupnim troškovima od 47,2 milijardi funti [57], a u 2011. godini oko 74% građana UK imalo je pristup Internetu. U UK 93% dece uzrasta od 12-15 godina sada koristi Internet kod kuće[58]. Mesečno se registruje preko 20.000 malicioznih email poruka na Vladinim mrežama, od kojih je 1.000 koji su direktno ciljali tu infrastrukturu[59]. Vlada UK je 2010. godine obezbedila 650 miliona funti za četvorogodišnji program nacionalne informacione bezbednosti, sa ciljem obezbeđenja potrebnih kapaciteta za odgovor države na sajber pretnje.

U septembru 2012. godine Vlada UK je organizovala skup po nazivom "Informaciona bezbednost-smernice za preduzeća", kome su prisustvovali direktori preduzeća iz grupe FTSE 100 (preduzeća sa najvišom tržišnom kapitalizacijom u UK). Smernice uključuju detaljne informacije i savete za deset kritičnih oblasti koje pokrivaju tehničke, procesne i kulturne oblasti za preduzeća[60]. Svi ovi navedeni brojčani pokazetilji govore o visokom stepenu razvijenosti informacionog društva u UK, što sa druge strane donosi ogromne pretnje i rizike, a NSIB je okvir za očuvanje visokog stepena informacione bezbednosti.

2.3. NSIB Francuske

Francuska vlada je 2008. godine procenila da će u narednih 15 godina jedna od glavnih pretnji po nacionalnu bezbednosti biti sajber napadi na kritičnu nacionalnu infrastrukturu. U februaru 2011. godine francuska agencija za mrežnu i informacionu bezbednost objavila je NSIB[61]. kojom su definisani sledeći ciljevi:

1. da Francuska postane svetska sila u oblasti sajber odbrane,
2. zaštiti sposobnost Francuske da, kroz zaštitu informacija, donosi odluke vezane za njen suverenitet,
3. zaštititi kritičnu nacionalnu informacionu infrastrukturu,
4. osigurati bezbednost u sajber prostoru.

Stvaranje agencije za mrežnu i informacionu bezbednost[62] predstavlja prekretnicu u procesu unapređenja kapaciteta Francuske da zaštiti svoju kritičnu informacionu infrastrukturu.

Pošto se u većini savremenih NSIB kao bitna stavka pominje i međunarodna saradnja, dobar primer su sporazumi koje je francuska agencija za mrežnu i informacionu bezbednost potpisala sa nemačkom agencijom za informacionu bezbednost u maju 2010 [63] godine i sa estonskim

[56] Ofcom, Communications Market Report, 2010.
[57] www.theukcardsassociation.org.uk
[58] Ofcom, Children and Parents: Media use report 2011.
[59] Iain Lobban, Director of UK Government Communications Headquarters, 2010.
[60] Tom Neaves and John Yeo-Trustwave: Cyber security needs to be a board level issue, 2013.
[61] http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf
[62] http://www.ssi.gouv.fr/en/the-anssi
[63] https://www.bsi.bund.de/ContentBSI/EN/Press/pressreleases/BSI-ANSSI_050210.html

informatičkim centrom u novembru 2010. godine[64]. Predmet oba sporazuma je razmena znanja u oblasti informacione bezbednosti.

2.4. NSIB Estonije

Vlada Estonije je 2008. godine objavila NSIB[65]. Prvi koordinirani sajber napad na informacionu infrastrukturu jedne zemlje bio je upravo napad na Estoniju 2007. godine. Strategija faktički predstavlja reaktivan odgovor Estonije na navedeni napad, a ustvari strategija ima *proaktivnu* dimenziju za potencijalne napade u budućnosti. Strategijom su definisani sledeći ključni ciljevi:

1. razvoj i implementacija opsežnog sistema mera bezbednosti,
2. povećanje znanja i veština u oblasti informacione bezbednosti,
3. unapređenje pravnog okvira za podršku informacione bezbednosti,
4. jačanje međunarodne saradnje i
5. podizanje svesti o značaju informacione bezbednosti.

NATO, čija je Estonija članica, prepoznao je Estoniju kao strateški bitnu zemlju za informacionu bezbednost i sajber odbranu zemalja članica NATO-a, pa se u toj zemlji nalazi NATO centar za sajber odbranu[66].

2.5. NSIB Finske

Finska vlada je objavila 24.01.2013. godine treću verziju NSIB[67]. Strategija ima za cilj da se svakodnevni život u informacionom društvu učini bezbednim i sigurnim za sve u Finskoj – kako za pojedince, tako i za preduzeća, organe javne vlasti, kao i sve druge aktere u društvu.
Vizija strategije je da:

1. Finska može sačuvati svoju kritičnu infrastrukturu od sajber napada u svim situacijama,
2. građani, vlast i preduzeća mogu koristiti siguran sajber prostor i nadležnosti koje proizilaze iz bezbednosnih mera kako na nacionalnom tako i na međunarodnom planu i
3. do 2016. godine Finska bude vodeća zemlja u svetu u pogledu informacione bezbednosti.

3. ZAKLJUČAK

Razvoj NSIB predstavlja veliki izazov za zemlje članice EU, što zahteva koordinaciju između raznih aktera u nacionalnom sajber prostoru, bez obzira da li se radi o akterima iz javnog ili privatnog sektora. Iako postoje mnoge različite definicije informacione bezbednosti, u radu je kroz konkretne primere NSIB UK, Nemačke, Francuske, Finske i Estonije, pokazano da je NSIB instrument koji pomaže vladi određene države da upravlja naporima svih relevantnih činioca u sajber prostoru u menadžmentu rizika vezanih za informacionu bezbednost na nacionalnom nivou. Veliki značaj se daje i međunarodnoj saradnji, jer informaciona bezbednost definitivno predstavlja globalni problem.

[64] http://www.ssi.gouv.fr/IMG/pdf/2010-11-24-fr-ee-agreement.pdf
[65] http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf
[66] https://www.ccdcoe.org
[67] http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy

Doprinos ovog rada može biti u tome da on može predstavljati putokaz za zemlje bivše SFRJ koje teže da postanu članice EU, kako bi unapredili svoje kapacite i izradom NSIB dosegli nivo nacionalne bezbednosti koji imaju zemlje članice EU.

LITERATURA

[1] Grubor, G. (2012): "*Projektovanje menadžmenta sisteme zastite informacije*", Beograd, Univerzitet Singidunum.
[2] Haller J., Merrell S., Butkovic M., Willke B. (2011): "*Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0*", Hanscom, Carnegie Mellon University.
[3] International Telecommunication Union-ITU (2011): "*The ITU National cybersecurity strategy guide, Geneva, ITU*".
[4] International Telecommunication Union-ITU (2008): "*ITU Global Cybersecurity Agenda (GCA)- A Framework for International Cooperation in Cybersecurity*", Geneva, ITU.

ISTRAŽIVANJE PODATAKA U TEHNOLOGIJI OBLAKA (CLOUD) POMOĆU SISTEMA R I REVOLUTION R

CLOUD-BASED DATA MINING USING SYSTEM R AND REVOLUTION R

Vladislav Miškovic
Singidunum University, Department of Informatics and Computing
Danijelova 32, Belgrade, Serbia
Phone: +381 11 3121 351
Fax: +381 11 3093 294
E-mail: vmiskovic@singidunum.ac.rs

Abstract

This paper considers the high memory space and time demands problem of data mining methods, which is resolved using cloud computing technology. It presents capabilities of a free business analysis and data mining system R and a commercial system Revolution R in large-scale data mining tasks using cloud technology. It demonstrates common knowledge discovery methods on a large problem in field of finance. Finally, it gives comparison to other systems for cloud-based business analysis and data mining.

Keywords: data mining, machine learning, system R, Revolution R, classification, regression

Sažetak

U radu se razmatra problem visokih memorijskih i vremenskih zahteva metoda istraživanja podataka, koji se rešava tehnologijom računarstva u oblaku (cloud computing). Izlažu se mogućnosti programskog sistema R, besplatnog alata za poslovne analize i istaživanje podataka i komercijalnog sistema Revolution R u istraživanju veoma velikog obima podataka korišćenjem tehnologije oblaka (cloud). Demonstriraju se poznati metodi otkrivanja znanja na obimnom primeru iz oblasti finansija. Na kraju se daje poređenje sa drugim sistemima za poslovne analize i istraživanje podataka koji koriste tehnologiju oblaka.

Ključne reči: istraživanje podataka, mašinsko učenje, sistem R, Revolution R, klasifikacija, regresija

1. INTRODUCTION

Data Mining methods are used for extracting potentially useful information from available data [1], [2], [3] not only for analytics specials, but for anyone who need it for its everyday activities, for example marketing or other businesses needs. Data mining techniques require a lot of data to ensure statistical significance of conclusions, but a large sets of data require enough computing resources. Cloud computing tehnology allows users to perform data mining with a reduced costs for infrastructure and storage.

The main problems of data mining are potential complexity of mining algorithms and huge amounts of data to be processed. Typically both problems can be solved by space and time decomposition using *parallel* and *distributed* computing methods on distributed computer systems. The main difference between parallel and distributed computing is in memory usage: in parallel computing, all processors may have access to a common shared memory in contrast to distributed computing, where each processor has its own private or distributed memory. Information exchange in distributed systems is obtained by passing messages between processors [4].

A distributed computer system consists of multiple computers (or *nodes*) which communicate through a computer network and interact with each other in order to achieve a common goal. An example of tool for building such systems is *Apache Hadoop*, an open-source software framework that supports data-intensive distributed applications. It is based on *MapReduce* distributed computing model and *Hadoop Distributed File System* (HDFS) to store data on the nodes [4]..

System R is a programming language and a working environment for statistical computing [5], but it is currently considered as popular open source data mining tool [3], [6]. The actual development of R is carried out by a core team composed of people from different institutions around the world. There are versions of R for different computer architectures (*Intel* 32/64, *PowerPC*, *Alpha*, *and Sparc*) and several families of operating systems (*Unix*, *Windows*, *Mac*). The commercial version of R is built by *Revolution Analytics* and it is powered by *Microsoft Visual Studio* development environment [7].

The most important reason for the success of commercial data mining tools like SAS *Enterprise Miner* or IBM *SPSS Modeler* is their efficiency in using and analyzing large data sets. But, access to these tools is limited despite high initial software cost and additional cost in cloud computing environments, based on the number of CPUs.

Open source data mining software as system R is a useful alternative solution, but the basic system R has limited abilities because all computations are carried out in computer's main memory and are single-threaded. There are several existing additions or R *packages* which can be used to solve these problems, for example by using a parallelized loop statement *foreach*, parallelized *apply* functions, or *MapReduce* model of parallel processing [4].

2. DATA MINING USING MACHINE LEARNING METHODS

Machine learning methods are rote learning, learning by being told, learning by analogy, and *inductive learning*, where methods of learning by examples and learning by experimentation and discovery belong [1], [2], [8].

Inductive learning method is often considered as a process where software system improves its performances on a specific task without additional programming [1]. Formal definition of inductive learning is that it is the process of estimating an unknown function or (input, output) dependency or structure of a system S using a limited number of observations $\mathbf{x}$ [1]. Set of functions which can be learnt and estimation method for its best approximation is predefined, by selection of a basic algorithm A and some background knowledge about the system S.

Induction is performed on a set of empirical data which is commonly called a *training set* (or a *data set*). Problem domain model creation is based on background knowledge about the problem

under consideration and often ends by specification of a set of attributes or variables $\mathbf{x}_i$, $i=1..n$. Some of these attributes are irrelevant or redundant, and deterate performances of majority of learning algorithms. Irrelevant and redundant attributes removal is performed by attribute/feature selection methods [1], [2], [9].

Frequently used methods are *learning classifications* (learning to predict some discrete value) and *regression* (to predict a numeric quantity). Learning classifications includes learning mathematical or logical expressions, decision trees, rules, decision tables, graphs, networks, hypersurfaces and other useful knowledge representations. In this work, *Random Forests* and *Support Vector Machines* methods will be used.

2.1 Random Forests machine learning method

Random forest is method of machine learning composite models consisted from many redundant decision tees [10]. In addition, Random Forests method can provide estimation of attributes *importance* [10], by calculating the increase of a prediction error estimate of the random forest created after removing each attribute from the problem definition.

2.2 Support Vector Machines method

Support Vector Machines (SVM) is a very successful method of machine learning from examples [11] which is based on mapping of learning examples from input space to a new high dimensional, potentially infinite dimensional feature space in which examples are linearly separable. The method then finds an optimal hyperplane

$$\langle \mathbf{w}, \Phi(x) \rangle + b = 0$$

where $\mathbf{w}$ is a matrix of coefficients, $\Phi(x)$ is a mapping function, and b is a constant. This hypersurface separates learning examples with a maximal margin or distance to the nearest learning example [11], [12]. Support vectors are a small set of critical border examples of each class best separated by this hyperplane. Construction of an optimal hyperplane is performed using iterative algorithm which minimizes the error estimation function:

$$\frac{1}{2}\mathbf{w}^{\mathrm{T}}\mathbf{w} + C\sum_{i=1}^{N}\xi_i$$

with the constraints

$$y_i(\mathbf{w}^{\mathrm{T}}\Phi(x_i) + b) \geq 1 - \xi_i,\ i = 1,..N, \xi_i \geq 0\ ,\ i = 1,..N$$

where $\mathbf{w}$ is a vector of coefficients, b is a constant, ξ is a slack variable (tolerance of overlapping linear nonseparable classes of examples), N is a number of learning examples and C is a regularization parameter. SVM method uses linear functions to create non-linear discrimination borders in a high-dimensional space using non-linear transformations. Returning to the original space using inverse transformation, we get a non-linear discriminant function in an input space (*kernel trick*).

3. DATA MINING USING SYSTEM R

System R can be used for different data mining tasks because there are thousands libraries for many analytic tasks, including data mining, machine learning and parallel programming [4].

3.1 Parallelization capabilities of system R

There are three class of methods which can be used to make parallel large scale software solutions using R:

- *Explicit parallelization methods* are based on programmer's responsibility to divide the problem into independent pieces to run in parallel, and then to aggregate the results from each piece.
- *Implicit parallelization methods* are easier to use than explicit parallelism. These methods are based on parallel execution of looping structures. For example, *foreach* loop statement from *Revolution Analytics' foreach* package.
- *Map-Reduce method* is the most recent parallelization method. It uses *MapReduce* model, popularized by Google, which is a way to process large data sets in parallel across a cluster built of inexpensive, commodity server machines [4]. *Revolution Analytics' RHadoop* project implements *MapReduce* for *Hadoop* using *R* and provides parallel implementations of several important methods, for example for learning *decision trees* and *K-means* clustering.

There are several existing additions or *R* packages which can be used for parallel execution and large datasets, based on (1) a parallelized loop statement *foreach*, (2) variants of *R* apply functions, or (3) *MapReduce* model of parallel processing [4].

3.2 Cloud Computing approach support in R

Cloud computing is a form of distributed computing. The approach is an extension of an object-oriented programming concept of abstraction, which hides complex implementation details. The term cloud computing comes from the fact that a cloud is often used to describe inexact knowledge of internal functioning. The most important R packages for parallel implementations for cloud computing are [4].:

- *snow* – a simple package for multithreading and big memory, using variants of standard R *apply* functions; it supports many platforms, but can be difficult to configure;
- *multicore* – a simple and efficient package which allows developers to parallelize R code without leaving the R interpreter, but only on one machine, and doesn't support Windows;
- *parallel* – a package which merges *snow* and *multicore* packages and is built into R from November 2011;
- *R+Hadoop* – it runs R programs in an internal or a cloud-based Hadoop cluster; it breaks up a single logical process into multiple scripts and steps;
- *RHipe* – it uses Hadoop without ever leaving the R interpreter. It is closer to a native R experience than R+Hadoop. It uses pure R code for *MapReduce* operations, but requires extra setup and cannot process standard files;
- *Segue* – it abstracts developers from *MapReduce* management using only R *apply*-like calculations, but cannot use an internal Hadoop cluster and require Amazon's Elastic *MapReduce*.

A newer approaches uses *MapReduce* model, an implementation of *divide-and-conquer* computing strategy, but programmer must supply the code for the *Map* and *Reduce* task [4].

3.3 Cloud Computing approach support in Revolution R

The commercial *Revolution R Enterprise* have two products to support parallelism:

- The commercial *RevoScaleR* package enables distributed computing to *R*. Its functions work on large datasets and include functions to run code across several local cores, or across a cluster of machines running *MS Windows HPC Server*.
- More recently, the open-source solution *RevoConnectR* is introduced for connecting *Hadoop* and *R*. Package *rmr* provides the *MapReduce* functionality. Its method *rhdfs* enables developers to manage data in HDFS and its method *rhbase* can communicate with *HBase*, the *Hadoop*-backed database.

Both *RevoScaleR* and *rmr* packages are created for typical data analysis work. First, they use special functions and constructs to get the essence of a larger dataset, and then pass those results to standard *R* functions for further analysis and plotting.

The simplest method to do parallel or distributed computing is to boot a multi-core instance and use the *multicore* package. If a single machine is not powerful enough, one can boot up multiple instances and link them as a *snow* cluster or a Linux cluster. In all cases, one can use the *foreach* framework to write a single version of code, which is able to run on all platforms.

In this work, data size is not too high and we can take a much simpler approach, using built-in package *parallel* for classical parallel programming, or a simpler R looping statement. For example, standard *foreach* loop statement over dataset *X* can be executed sequentially using %do% construct

```
foreach (n=1:1000,.combine=combine) %do% {... somefunction(X, n,...)}
```

or in parallel by using %dopar% construct

```
foreach (n=1:1000,.combine=combine) %dopar% {...somefunction(X, n,...)}
```

4. EXAMPLE OF USING MACHINE LEARNING METHODS FOR DATA MINING

In this work usage of machine learning methods for data mining will be demonstrated on a problem of making decisions during stock market trading [3].

4.1 The stock market trading problem

Stock market trading is a challenging data mining problem, because there is a large amount of historical data which humans use for decision making. Also, there are research results that the markets change so rapidly in terms of price adjustments and that it is impossible to obtain profits in a consistent way, but more realistic statement is that there is some space for trading opportunities due to temporary market inefficiencies [3].

The general goal of stock trading is to maintain a portfolio of assets based on buy and sell orders in order to achieve as much profit as possible from these trading actions. According to [3], given a single security in the form of market index and initial capital, we will try to *maximize profit* over future testing period using trading actions *buy*, *sell* and *hold*. Decision making is based on indications provided by the data mining process.

The *Standard&Poor's 500* is a stock market index based on the market capitalizations of 500 leading companies publicly traded in the U.S. stock market which is determined by

Standard&Poor's. It is one of the most commonly followed equity indices and many consider it the best representation of the market as well as the U.S. economy [3]. Dataset description of the original S&P500 stock market data is in Table 1.

Table 1: Original stock market data attributes

Field	Meaning
Date	Date of the stock exchange session
Open	Open price at the beginning of the session
High	Highest price during the session
Low	Lowest price
Close	Closing price of the session
Volume	Volume of transactions
AdjClose	Adjusted close price, adjusted for stock splits, dividends/distributions, and rights offerings

This initial set of attributes is not good enough to make trading decisions [Torgo]. Actual stock trading data are taken from the Yahoo!Finance site [13].

4.2 Problem solution using R

Attributes for defining the trading decision problem will be percentages of variations of stock prices over the last *k* days (positive or negative). These values, calculated from the quotes data, can be seen as indicators of the tendency in the following *k* days. Positive variations will lead us to *buy*, while negative variations will trigger decision to *sell*. The whole analysis is based on the *Close* quote, because buy or sell decisions is made at the end of each daily session [3].

Following the methodology and R code described in [3], the initial set of analysis attributes is created from (1) past returns on the *Close* price performed in last *k* days, for *k*=1..10, and (2) values derived from the set of technical indicators, available in *R* package TTR (*Technical Trading Rules*) [14].



Fig. 1: S&P stock trading for last 3 months

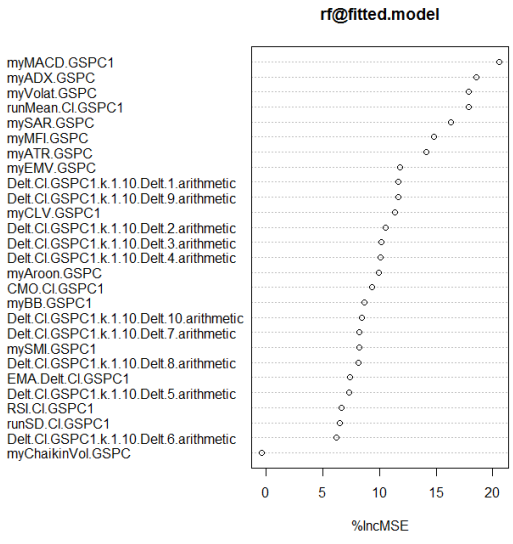


Fig. 2: Attribute importance by Random Forest

The data available depends on time and this is time series data [15], which can be analyzed by methods of R packages *zoo* and *xts* [14]. The actual daily prices of S&P500 stocks for last 3 months and indicator value are described in Fig. 1.

To select the most important from this set of attributes, feature selection method is used. An estimation of importance of attributes is performed using Random Forests method [10]. Importance of attributes and feature selection threshold is showed in Fig. 2 (n=100 trees).

Prediction model is created from the part of trading data using SVM method.

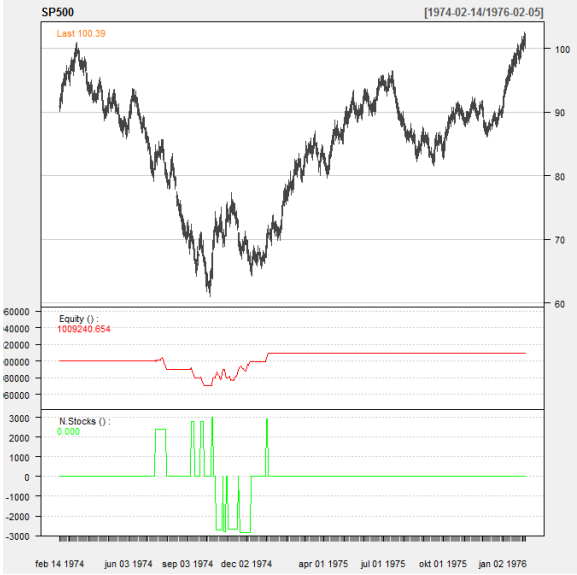


Fig. 3: The results of trading using Policy 1 based on the signals of an SVM

The main evaluation criteria is the performance of a developed trading system, that is, the *profit* or *loss* resulting from the actions of the system, instead of the predictive accuracy of the developed data mining models, Fig. 3. It is tested using Monte Carlo trading simulation experiments for 500 days to obtain reliable estimates of the evaluation criteria.

4.3 Cloud-based solution using R

Cloud-based data mining using R and Revolution R can be performed as folows:

1. Prepare the cloud
   - Create an account and sign in (for example, to Amazon or Windows Azure);
   - Login to provider, for example http://manage.windowsazure.com;
   - Create and manage resources (for example Virtual Machines) and define running in by providing configuration options: number and type of processors, operating system and storage requirements and password;
   - Download, install and configure open source *R* from [14] or commercial *Revolution R* from [7] (it is free for academics).
2. Prepare and upload the data for mining
3. Run parallelized R code

In this work, paralelization is provided and tested for the time-consuming RandomForest method which is used for selection of important attributes:

```
nts    <- 100
ncores <- detectCores()
clusts <- makeCluster(ncores)
registerDoParallel(clusts)
rf<-foreach(nl=rep(nts,ncores),.combine=combine,.packages='randomForest') %dopar%
          randomForest(mydata.train, ntree=nl, importance=T)
stopCluster(clusts)
```

For small or moderate data sets, the parallelized code is the same for multi-threaded execution on a multicore computers and massive cloud-based server configurations.

5. CONCLUSION

The problems of high memory and time demands of data mining methods, which are important in real applications, are considered in this paper. The proposed resolution uses cloud computing approach to achieve a high level of abstraction for potential users.

The capabilities of system R, a free business analysis and data mining tool, and a commercial system Revolution R in large-scale data mining tasks using cloud technology are briefly compared.

Important knowledge discovery methods, which are common for both systems, but have different implementations for standard and parallel computations, are used for a data mining task from the field of finance. The performances for standard and parallel versions of these methods are demonstrated under Windows operating system.

Finally, the process of cloud-based data mining is briefly described. The parallelized solution is in the same time a cloud-based solution.

6. REFERENCES

[1] Cherkassky V., Mulier F. M., *Learning from Data: Concepts, Theory, and Methods*, 2nd edition, John Wiley - IEEE Press, 2007
[2] Witten I.H., Frank E., Hall. M.A., *Data Mining: Practical machine Learning Tools and Techniques*, 3rdEd, Elsevier Inc, 2011
[3] Torgo L., *Data Mining with R: Learning with Case Studies*, Chapman & Hall/CRC, 2011
[4] McCallum E., Weston S., *Parallel R*, O'Reilly Media, Inc, 2012
[5] Maindonald J., Braun J., *Data Analysis and Graphics Using R*, 2nd Edition, Cambridge University Press, Cambridge, 2007
[6] Karatzoglou A., Meyer D., Hornik K., "Support Vector Machines in R", Journal of Statistical Software, Volume 15, Issue 9, 2006
[7] Revolution R Enterprise and RevoScaleR: http://www.revolutionanalytics.com
[8] Michalski, R.,Carbonell,J., Mitchell T. (Eds.), *Machine learning: An artifcial intelligence approach (Vol. I)*, San Francisco, CA: Morgan Kaufmann,1983
[9] Miškovic V., *Inductive Learning of Understandable Knowledege from Sparse Learning Sets* (in Serbian), Phd thesis, Singidunum University, Belgrade, 2008
[10] Breiman L., "Random Forests", *Machine Learning*, 45, pp. 5-32, 2001
[11] Vapnik V., Statistical Learning Theory, John Wiley&Sons, 1998
[12] Shawe-Teylor J.,Cristianini N., Kernel Methods for Pattern Analysis, Cambridge University Press, 2004

[13] Yahoo!Finance http://finance.yahoo.com
[14] The Comprehensive R Archive Network http://cran.r-project.org/
[15] Miškovic V., "Application of Support Vector Machines Method to Classification of Time Sequences" (in Serbian), *Proc. 56th ETRAN Conference*, Zlatibor, June 11-14, 2012
[16] Annual Survey http://www.RexerAnalytics.com
[17] RHadoop: https://github.com/RevolutionAnalytics/RHadoop/wiki

PROCJENA RIZIKA BEZBJEDNOSNIH MEHANIZAMA ANDROID OPERATIVNOG SISTEMA

ASSESSMENT RISK OF SECURITY MECHANISMS OF ANDROID OPERATING SYSTEM

Mladen Veinović[1], Miroslav Ćajić[2], Bogdan Brkić[3]
[1]Univerzitet Singidunum, Beograd; mveinovic@singidunum.ac.rs
[2]O.Š. "Sveti Sava", Istočno Novo Sarajevo; miroslavcajic@gmail.com
[3]Fond za zaštitu životne sredine, Banja Luka; bogdan.brkic@gmail.com

Sažetak
U ovom radu izvršena je kvalitativna analiza bezbjednosnih mehanizama Android operativnog sistema. Urađena je procjena rizika koji utiče na stabilnost datog sistema na osnovu čega su date preporuke za podizanje nivoa bezbjednosti. Poštovanjem ovih preporuka moguće je uticati na napade koji djeluju na stabilnost operativnog sistema kao i na potencijalne povrede integriteta podataka koji bi sistem učinile ranjivim ili manje stabilnim. Na osnovu dobijenih rezultata na kraju rada dat je zaključak.
Ključne riječi: Android, bezbjednost, integritet, podatak, sigurnosne prepreke

Abstract
In this paper is presented a qualitative analysis of safety mechanisms Android operating system. Performed is assessment risk, who affects the stability of that system on the basis which recommendations were made to raise the level of security. Strict adherence to these recommendations can be affect on the attacks that affect the stability of the operating system and the potential violation of the integrity of the data that would have made the system vulnerable and less stable. At the end of the paper's conclusion is based on the results.
Key words: Android, security, integrity, data, firewall

UVOD

Android operativni sistem prvenstveno je namijenjen za korisnike mobilnih uređaja, bilo da su to telefoni ili računari. Platforma je programski otvorena i kao takva izložena je velikom broju tipičnih napada koji mogu izazivati niz neželjenih radnji, od potpune ili djelimične neupotrebljivosti mobilnog uređaja, slanja SMS ili MMS-ova, ili čak do krađe ličnih podataka iz računara [1]. Pomenuti napadi se mogu ostvariti preko GSM, 3G ili 4G mreže, bluetooth konekcije, putem WiFi-a, preko USB priključaka, Access point-a i sl [2].

Potencijalni napadači prilikom napada najčešće upotrebljivaju programe koji su dizajnirani za određenu vrstu napada. Neki od zlonamjernih programa za Android su : Lasco [3] i Commwarrior, Mabir [4], FlexiSpy, RedBrowser, Skulls Trojans, i CardTrap [5]. Stepen bezbjednosti u mobilnim uređajima pod Android opertivnim sistemom sličan je nivou bezbjednosti u računarima pod nekim drugim operativnim sistemom [6].

Da bi se napad izvršio eksterno, odnosno izvana, uređaj treba da bude povezan na Internet ili na lokalnu mrežu. Prvi korak prilikom napada je osluškivanje komunikacionog kanala što u ovom slučaju eliminiše Interenet. Zbog toga smatramo da je uređaj više ranjiv iz lokalne mreže, odnosno, na lokalnom host-based nivou. Drugi problem se odnosi na aplikacije koje korisnici nesvjesno instaliraju, a koje nose određene rizike po operativni sistem. Korisnik je u mogućnosti da promijeni dozvolu i da dâ određenoj aplikaciji niži nivo sigurnosti. Pored toga, dijeljeni, odnosno, zajednički ključ omogućava dijeljenje dozvola između aplikacija bez interakcije korisnika.

Neki od ovih napada baziraju se na memorijski overflow i određene ranjivost u XSS dijelu koje su nastale zbog upotrebe zastarjelih naslijeđenih biblioteka. Ovaj napad omogućavava potencijalnom napadaču izvršavanje malicioznih programa na uređaju i dobijanje dozvole za pristup određenoj web aplikaciji [7].

PROCJENA BEZBJEDNOSTI

Sa nivoa bezbjednosti sistem je dobro zaštićen od SQL napada, međutim, neki dijelovi su u potpunosti izloženi potencijalnoj modifikaciji, kao što je slučaj sa SD memorijskom karticom. Cilj ovog rada je svakao procjena identifikacije potencijalnih opasnosti i prijetnji. Procjena se bazira na uticaju i mogućnosti različitih prijetnji koje koriste određene ranjivosti u Android frameworku, a koje onemogućavaju ili zloupotrebljavaju povjerljivost, dostupnost i integritet dijelova Android frameworka [8].

Najvažnije prijetnje koje se spominju u radu podjeljene su u tri grupe: malo vjerovato, moguće i vjerovatno, dok su tri moguća uticaja klasifikovani u takođe tri grupe: manji, umjereni i teški.

2.1. PRIJEDLOZI BEZBJEDNOSNIH RJEŠENJA

Na osnovu analize bezbjednosti utvrđeno je više grupa potencijalnih opasnosti. U ovom radu će biti prezentovane samo tri. Ove opasnosti nastale su grupisanjem više prijetnji sa višim nivom sigurnosti. U ovom radu su izloženi određeni prijedlozi za rješavanje bezbjednosnih propusta.

Opasnost 1.: Ugrožavanje pristupa i (ili) integriteta i (ili) povjerljivosti podataka pomoću dozvole da se instalira određena aplikacija. Ovaj scenario ima veliku mogućnost da se dogodi i ima potencijalno veliki rizik po uređaj.

Rješenja mogu biti sledeća:

-Otkrivanje i detekcija napada, IDS predstavlja dobro prilagođeno rješenje za definisanje normalnog ponašanja sistema, programa ili korisnika u cilju otkrivanja odstupanja ili za otkrivanje zlonamjernih programa koje potencijalni napadač nastoji izvršiti. IDS može poslužiti i kao djelotvorno sredstvo u otkrivanju nepoznate prijetnje. Međutim, budući da se zlonamjerni program može brzo prilagoditi svoje ponašanje u skladu sa aktuelnim sigurnosnim alatom, djelotvornost IDS-a može se smanjiti tokom vremena. Na osnovu analize, postojeći IDS bi trebao se modifikovati u cilju unapređenja njegovih bezbjednosnih osobina [9].

-Podizanje sigurnosnih prepreka (Firewall), predstavlja jedno bezbjednosno rješenje koje se bavi mrežnim prijetnjama. Cilj je da spriječi protok podataka usljed izvršavanja zlonamjernih programa koji su već instalirani u uređaju. Međutim, budući da nisu svi napadi mrežno orjentisani, firewall može veoma korisno da utiče i na djelimične skupove napada. Kao rezultat navedenog možemo odrediti nizak napor prilikom sprečavanja izvršavanje ove akcije.

-Sertifikovanje korisničkih aplikacija, predstavlja idealnu kontra-mjeru prilikom pokušaja izvršavanja zlonamjernih programa. To podrazumijeva da svaki program treba biti detaljno testiran i analiziran prije procesa sertifikacije i davanja korisničkih dozvola. Samo u tom slučaju zlonamjerni programi će biti presretnutu već u ranoj fazi izvršavanja. Takođe, upotrebom sertifikata osigurano je zahtijevanje za izvršavanje određene aplikacije kao i kalkulacija potencijalnog rizika. Uloženi napor pri izvršavanju ove radnje treba označiti visokim nivom.

-Određivanjem korisnički dozvola, pruža se mogućnost davanja određenih dozvola samo za određenu grupu aplikacija u cilju smanjenja rizika od korišćenja zlonamjernih programa sa granted korisničkim dozvolama. Ovo rješenje zahtijeva modifikovanje i dodavanje određene napredne osobine u radu programa za instaliranje aplikacija, tako da korisnik ima mogućnost odbacivanja određene dozvole. Ove dozvole se ne miješaju sa dozvolama već instaliranih aplikacija. Rješenje ima za cilj zaštitu od dodjeljivanja nepotrebnih dozvola koje bi se mogle zlonamjerno koristiti. Uz određene izmjene u samom sistemu potreban napor za izvršavanje ove akcije može se označiti kao nizak.

Opasnost 2.: Ugrožavanje pristupa i (ili) integriteta i (ili) povjerljivosti podataka upotrebom nedostataka u Linux kernel ili određenim bibliotekama. Iako ovaj scenario ima malu vjerovatnoću događaja, velika je mogućnost nanošenja potencijalne štete.
Rješenja mogu biti sledeća:
-Upotreba Security-Enhanced Linux-a, predstavlja pogodno rješenje za ograničavanje mogućnosti određenog subjekta ili procesa tokom izvršavanja u operativnom sistemu. Ovo se posebno ogleda u situacijama kada potencijalni napadač iz određenog razloga stekne mogućnost određenih privilegija ili dozvola. Ograničavanjem mogućnosti izvršavanja procesa koji se pokreću sa root-a osigurava se manja efikasnost u slučaju napada na sistem. Međutim, pošto svaki proces zahtijeva mogućnost izvršavanja određenih komandi za normalan režim rada, ove komande ne smiju biti blokirane od strane SELinux-a. U slučaju da je određeni proces kompromitovan, odnosno napadnut, potencijalni napadač će još uvijek imati priliku da izvrši potrebno skeniranje za izvršavanje određenog napada. To podrazumijeva da će napad biti samo skrenut ili djelimično uništen. Upotrebom SELinux-a postiže se ograničena upotreba resursa i nastaje vrlo nizak pritisak na sistem. U ovom slučaju jedino ostaje otvoreno pitanje odgovarajuće SElinux politike za Android operativni sistem [10].

-Prijavljivanje korisnika na sistem na osnovu korisničkog imena i lozinke ili na osnovu njegovih biometrijskih parametara je već dobro poznata i provjerena sigurnosna metoda u slučaju zaštite privatnih podataka. U slučaju otuđenja uređaja koji na sebi ima implementiran sistem korisničke prijave smanjuje se mogućnost narušavanja integriteta pomenutih podataka. Ipak,

sigurnosni mehanizam je beskoristan u slučaju da je uređaj otuđen nakon provjere korisničkih parametara. Zbog navedene sigurnosne činjenice potreban je manji trud za razvijanje drugog sigurnosnog rješenja kako bi se klasični sigurnosni mehanizam za prijavu korisnika poboljšao.

-Šifrovanje podataka pri zapisivanju, je još jedno vrlo pouzdano sredstvo za zaštitu privatnih podataka. Šifrovani podaci su čitljivi samo vlasniku ili vlasnicima ključa. U slučaju otuđenja uređaja podaci ostaju nečitljiv bez upotrebe ključa u razumnom vremenskom intervalu. Primjena šifrovanja u Androidu podrazumijeva izmjenu aplikacija za pristup SMS/MMS, e-mailu, kontaktima i sl. Realizacija navedenog podrazumijeva manji uloženi rad za podizanje većeg nivoa sigurnosti.

-Kontrola pristupa sistemu, sa ciljem razvijanja mehanizma za kontrolu pristupa podacima korisnik ima mogućnost ograničenja pristupa svojim privatnim podacima, zavisno od situacije, odnosno, uslova u kojima se nalazi. Uslovi za pristup mogu biti mjesto korisnika, vrijeme i vrste mobilne mreže, konekcija na Wi-Fi mrežu i sl. Ovakva konstrukcija sistema može biti djelotvorna u različitim situacijama. Ako se uređaj nalazi u uslovima koji dozvoljavaju pristup podacima onda će ti podaci biti čitljivi za trenutng korisnika. U slučaju otuđenja uređaja mijenjaju se uslovi u kojima uređaj radišto uzrokuje da na osnovu očitanih vrijednosti podaci neće biti dostupni za upotrebu. Zadatak ovakvog rješenja je definisati uslove u kojima će mehanizam raditi i način aktiviranja, bilo da je to ručno ili automatski.

Opasnost 3.: Ugrožavanje pristupa i (ili) integriteta i (ili) povjerljivosti podataka na SD memorijskoj kartici. Ne postoji mehanizam kontrole pristupa memorijskoj kartici tako da ovi podaci mogu biti izloženi kompromitaciji od neovlaštene strane. Takođe, bežična komunikacija može biti prisluškivana i na daljinu.

Rješenja mogu biti sledeća:

-Sistem upravljanja resursima predstavlja sigurnosni mehanizam koji ima zadatak ograničavanja resursa sistema zbog zlonamjerne upotrebe memorijskog prostora i procesorske snage uređaja. Rad sistema se bazira na raspodjeli sistema zavisno od potrebe određenih aplikacija u skladu sa njihovim potrebama i važnošću izvršavanja. Bez ovakvog nadzora memorijske i procesorske snage nije moguće osigurati smanjenje uticaja izvršavanja zlonamjernih aplikacija. Implementacija ovakvog sigurnosnog mehanizma zahtijeva određenu modifikaciju sistema, a uloženi napor može biti ocijenjen od srednje do visoke ocjene, zavisno od korisničkog podešavanja i željenog nivoa zaštite.

-Otkrivanje i detekcija „loših“ aplikacija predstavlja sistem za praćenje i otkrivanje stanja uređaja, odnosno, promjena u njemu na osnovu stanja baterije, memorije, CPU-a i abnormalnih primjena koje se dešavaju u sistemu. Prilikom izvršavanja na ciljnom uređaju zlonamjerna aplikacija ima za cilj da ostane neprimjećena. Zbog toga profil samog sistema treba konstantno održavati ispravnim, a samo određene radnje treba da budu potvrđene od strane sistema.

4. ZAKLJUČAK

U ovom radu izvršena je procjena bezbjednosti za Android operativni sistemu u cilju utvrđivanja sigurnosnih propusta. Istaknute su određene slabe tačke u sistemu koje se trebaju uzeti u obzir prilikom implementacije sigurnosnih mehanizma. Neke od njih su problem

sigurnosnih mehanizama za dodjeljivanje dozvola, sigurnosni propusti u Linux kernel jezgru, korisničkim bibliotekama, izvršnim datotekama, povezanošću između medija i hardvera, i sl. Potencijalne opasnosti su povećane činjenicom da je Android operativni sistem konstruisan kako za mobilne telefone tako i za personalne računare, čime mobilnog korisnika izlažu svim napadima koji se dešavaju i na personalnom računaru.

Glavni problem koji smo naveli je taj što je kôd za Android operativni sistem javno dostupan, te je nakon proizvodnje prvog uređaja softver puštan na tržište u slobodnu prodaju. Mora se istaći i to da većina kôda još uvijek nije pregledana od strane open-source asocijacije. Takođe, još uvijek ne postoji određeno sertifikaciono tijelo koje bi sistemom javnih ključeva povezalo instalacione aplikacije sa njihovim vlasnicima, pri čemu bi se znatno smanjio rizik od potencijalno zlonamjernih upada u sistem prilikom instaliranja aplikacija. Naravno, vrlo je važno da se uključi sigurnosni mehanizam kao što je LinuxSecurityModule (LSM) koji je namijenjen za kontrolu pristupa, odnosno, za sprječavanje potencijalne štete koja proizlazi iz eksploatacije ranjivostiu Linux kernel jezgra. Ipak, najviši prioritet dat je upotrebi SELinux-a uz određeni zaštitni zid, kao i sistemu detekcije napada, kontroli pristupa podacima, filtriranju podataka i dodjeljivanju dozvola. Implementacijom određenih bezbjednosnih riješenja koja su pomemuta u ovom radu podiže se nivo bezbjednosti u cilju osiguranja prednost mobilnih operatera na tržištu GSM veza.

LITERATURA

[1] Dagon, C., Martin, T., and Starner, T., 2004. Mobile phones as computing devices the viruses are coming. *PervasiveComputing,* pp. 11-15.

[2] Cheng, J., Wong, S.H., Yang, H., and Lu, S., 2007. SmartSiren: virus detection and alert for smartphones. In *Proceedings ofthe 5th international Conference on Mobile Systems, Applications and Services (MobiSys'07).*

[3] B. K. Bose, Sliding mode control of induction motor, In. *Proc. IEEE Ind. Appl. Soc. Annu. Meeating, pp. 479-486, 1985.*

[4] Schultz, E.E., 2006. Where have the worms and viruses gone?-new trends in malware. *Computer Fraud and Security*, pp. 4-8.

[5] Leavitt, N., 2005. Mobile phones: the next frontier for hackers? *Computer,* 38(4): 20-23.

[6] Muthukumaran, D., et al., 2008. Measuring integrity on mobile phone systems. In *Proceedings of the 13th ACM Symposiumon Access Control Models and Technologies.*

[7] Enck, W., Ongtang, M., and McDaniel, P., 2009. Understanding Android security, *IEEE Security and Privacy*, vol. 7, no. 1,pp. 50-57

[8] Schmidt, A.D., Schmidt H.G., Clausen J.H., Yükse,l K.A., Kiraz, O., Camtepe, S.A., Albayrak, S. "Enhancing Security of Linux-based Android Devices". 15th International Linux Kongress, 2008, Hamburg, Germany.

[9] Shabtai, A., Fledel, Y., Elovici, Y., 2010. Securing Android-Powered Mobile Devices Using SELinux, to appear in *IEEE Security and Privacy.*

[10] Ongtang, M., McLaughlin, S., Enck, W., and McDaniel, P. Semantically Rich Application-Centric Security in Android. *Proceedings of the 25th Annual Computer Security Applications Conference* (ACSAC) Honolulu, Hawaii, 2009.

UTICAJ UVOĐENJA ELEKTRONSKIH SERVISA NA POBOLJŠANJE KVALITETA USLUGA U LOKALNOJ SAMOUPRAVI

THE EFFECTS OF ELECTRONIC SERVICES ON IMPROVING THE QUALITY OF SERVICE IN LOCAL INSTITUTIONS

Tijana Radojević
Univerzitet Singidunum
Danijelova 32
E-mail: tradojevic@singidunum.ac.rs
Marko Šarac
Univerzitet Singidunum
Danijelova 32
E-mail: msarac@singidunum.ac.rs
Dalibor Radovanović
Univerzitet Singidunum
Danijelova 32
E-mail: dradovanovic@singidunum.ac.rs
Jelena Srejić
Gradska uprava za finansije
E-mail: jelenasrejic@yahoo.com

Sažetak
Zadatak ovog rada je sagledavanje nužnosti i neophodnosti uvođenja i upotrebe elektronskog poslovanja u rad državnih službi, kako bi se obezbedili novi vidovi komunikacije i poslovanja. U ovom radu izvršena je analiza sajtova gradova i opština, odnosno utvrđivanje stepena informaciono tehnološke razvijenosti pojedinih jedinica lokalne samouprave. E-servis čija primena je u većini gradova na visokom nivou je servis Virtuelni matičar. Prikazan je broj podnetih zahteva i izdatih izvoda iz matičnih knjiga u periodu od 2009-2011 godine i izvršena je analiza koliko je dokumenata izdato podnošenjem zahteva elektronskim putem, a koliko je podneto lično, odnosno, dolaskom na šalter Gradske uprave.
Ključne reči: e-uprava, e-servis, e-poslovanje

Abstract
This paper aim is to provide the overview of the need and necessity of implementing and using e-services in the work of state institutions, which will provide the new means of communication and business. The paper presents a comparative analysis of the websites of municipalities and cities and determines the level of information technology development in certain local governments. The E-service that was being developed in most of the cities, is Virtual Registry service. This paper presents the number of applications and issued Birth Certificates in the period of 2009-2011. Also, two ways of filing requests have been analyzed: the electronic way and the traditional way.
Key words: e-government, e-services, e-business

1. UVOD

Elektronsko poslovanje i e-uprava doprinose modernizaciji i profesionalizaciji državne uprave i lokalne samouprave u Republici Srbiji. U dosadašnjoj organizaciji rada gradskih i opštinskih uprava, građani su bili prinuđeni da se radi dobijanja svih informacija vezanih za rešavanje nekog zahteva obraćaju većem broju službi, pri čemu su pored nepotrebnog gubitka vremena dobijali i nepotpune i kontradiktorne informacije. Poslednjih godina velika pažnja se posvećuje informacionim tehnologijama i razvoju elektronskog poslovanja kako bi se stvorile mogućnosti da svi građani koji koriste Internet mogu na jednostavniji i brži način rešiti svoje administrativne probleme.

Pored tradicionalnog poslovanja koje je zasnovano na korišćenju papirnih dokumenata i opšte prihvaćenoj komunikaciji između učesnika u procesu poslovanja, neophodno je razviti i nov oblik poslovanja-elektronsko poslovanje. Elektronsko poslovanje smanjuje troškove poslovanja i poboljšava rad administracije, podstiče ekonomski razvoj jer savremene tehnologije omogućavaju razvijanje boljih odnosa sa poslovnim organizacijama, menjaju način rukovođenja i komunikaciju [3.].

U mnogim gradovima e-servisi pružaju samo obaveštenja i informacije o postupcima rešavanja nekih problema, ali je još uvek nedovoljan broj servisa preko kojih se može vršiti potpuno elektronsko poslovanje i koji pružaju brži, jednostavniji i efikasniji rad.

2. E-UPRAVA

2.1. Značaj e-uprave

Snažan i brz razvoj elektronskog poslovanja ubrzao je uvođenje i implementaciju elektronske uprave. Uvođenjem elektronskog poslovanja u javnu upravu dolazi do sve većeg broja transakcija koje se obavljaju po uzoru na e-poslovanje, a to podrazumeva krupne promene u unutrašnjoj proceduri rada administracije [2.]. E-uprava podrazumeva upotrebu informaciono komunikacionih tehnologija, a naročito upotrebu Interneta kao instrumenta za postizanje dobre uprave. „Dobra uprava“ treba da omogući lakšu, jeftiniju, transparentniju interakciju između vlade i građana, vlade i kompanija, i samih vladinih agencija. Termin „dobra uprava“ podrazumeva postizanje efikasnosti birokratije, odnosno optimizovanje rada uprave. Dobra uprava danas funkcioniše preko umreženih pravnih baza podataka, odnosno automatizovane administracije, a cilj e-uprave je da građani što više administrativnih procedura obave putem Interneta, što bi isključilo čekanje i uštedelo vreme.

Elektronska država je bitna da bi obezbedili:

- postavljanje države kao servisa građana i države,
- jeftiniju i efikasniju državnu administraciju,
- transparentnost u radu države.

Ključni elementi Elektronske države su:

- pravni okvir,
- jedinstveni državni registri,
- platforma za razmenu elektronskih dokumenata između državnih organa i građana.

2.2. Pravni okvir

U našoj zemlji postoji pravni okvir za funkcionisanje E-države: Zakon o elektronskom potpisu, Zakon o elektronskom dokumentu, vremenski žig, sertifikaciona tela za izdavanje

kvalifikovanog elektronskog potpisa i vremenskog žiga. Ovaj pravni okvir treba upotpuniti sa Zakonom o arhivskoj građi. Ovo je jedan od najvažnijih zakona za E-državu jer treba da izjednači u pravnom smislu orginalni dokument koji je nastao u papirnoj formi i njegovu digitalnu kopiju. Ta kopija naravno mora biti potpisana kvalifikovanim digitalnim potpisom (jednoznačno određuje ko je kreirao kopiju dokumenta) i overena vremenskim žigom koji definiše kada je kopija nastala. Elektronski potpis je tehnologija koja omogućava autentičnost, zaštitu integriteta i neporecivost podataka i dokumenata u elektronskom poslovanju.[68] Tehnologija može da odgovara svojeručnom potpisu u klasičnom poslovnju, pri čemu se štiti integritet potpisanih dokumenta. Po zakonu o elektronskom potpisu razlikuju se elektronski i kvalifikovani elektronski potpis. Kvalifikovani e potpis je potpis kojim se pouzdano garantuje identitet potpisnika, integritet potpisanog elektronskog dokumenta i onemogućava naknadno poricanje potpisa. Upotreba kvalifikovanog elektronskog potpisa elektronskog dokumenta, osnov je za njihovu punovažnost i dokaznu snagu u pravnim poslovima, upravnim, sudskim i drugim postupcima. Kvalifikovani elektronski potpis ima isto pravno dejstvo i dokaznu snagu kao svojeručni potpis i pečat.

Zakon o elektronskom dokumentu[69] dodatno određuje uslove i način postupanja sa elektronskim dokumentom. Propisi o elektronskom dokumentu regulišu uslove za formiranje i čuvanje dokumenata u elektronskom obliku, određuju pojam orginala elektronskog dokumenta i mogućnost pretvaranja dokumenta iz papirnog oblika u elektronski i obrnuto. Elektronski dokument koji je izvorno nastao u elektronskom obliku smatra se orginalom i elektronski dokument koji je nastao digitalizacijom izvornog dokumenta čija forma nije elektronska, smatra se kopijom izvornog dokumenta. Digitalizovana kopija dokumenta u papirnom obliku ima istu pravnu snagu kao i izvorni dokument, a elektronski dokument je potom potpisan kvalifikovanim elektronskim potpisom od strane ovlašćenog lica. Zakonom o elektronskom dokumentu uvodi se pojam i upotreba vremenskog žiga kao postupka za pouzdano označavanje da su elektronski podaci postojali pre označenog trenutka.

Na ovaj način stvoreni su preduslovi da počne razmena elektronskih dokumenata između državnih organa (G2G), državnih organa i građana (G2C), države i privrede (G2B) kao i građana između sebe (C2C). Ta razmena predstavlja usluge koje pružaju razni državni organi [1.].

2.3. E-uprava u jedinicama lokalne samouprave

Internet usluge javne administracije postoje na lokalnom nivou – u velikom broju gradova i opština koje su to same uvele. U Srbiji je stanje dosta različito, jer pojedine jedinice lokalne samouprave koriste tok-centre, neke komuniciraju sa građanima preko Interneta, ali ima i opština koje su u velikom tehnološkom zaostatku i to su uglavnom male i siromašne opštine koje vrlo malo ulažu u izgradnju i unapređenje informaciono komunikacionih tehnologija. U ovakvim opštinama građani gube mnogo vremena za dobijanje usluga. Svako odeljenje funkcioniše nezavisno i retko postoji razmena informacija između službi. Podaci se vode i pretražuju na staromodan način, bez elektronske obrade podataka.

Uvođenjem elektronskog poslovanja u gradske i opštinske uprave znatno se utiče na efikasniji rad službi, racionalnost u potrošnji sredstava što dovodi do smanjenja troškova i uštede vremena. E-uprava nije samo alternativni način ostvarivanja servisa javne administracije, ona mora biti efikasnija i jeftinija i vremenom mora potisnuti klasičan način šalterskog pružanja servisa.

[68] Zakon o elektronskom potpisu, „Sl.glasnik RS“, br. 135/2004

[69] Zakon o elektronskom dokumentu, „Sl.glasnik RS“ br. 51/2009

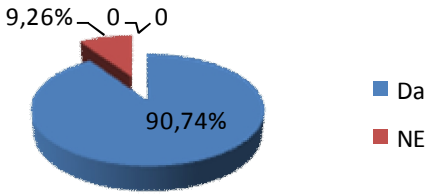
Ukidanjem administrativnih barijera olakšavaju se svakodnevni postupci građana pred organima lokalne samouprave.
Zahvaljujući velikim promenama u oblasti informacionih tehnologija omogućena je realizacija dinamičkih web aplikacija koje mogu da ponude podršku u radu različitih službi na nivou opštine. Nova internet prezentacija treba da ubrza dobijanje informacija i usluga od grada preko interaktivnih servisa. Implementirani e-servisi omogućili su da građani većinu zahteva u potpunosti mogu da podnesu putem Interneta, a posledica primene je efikasniji i transparentniji rad službenika [5.].
Građanima i pravnim licima potrebno je olakšati pristup bazama podataka od javnog značaja za koje su nadležni organi lokalne samouprave i svi sadržaji moraju biti u funkciji ciljeva Internet prezentacije, a koji se ogledaju u pružanju servisa i informacija široj javnosti, unapređenju komunikacije sa građanima, privrednim subjektima i drugim organima državne uprave, ali i stvaranju pozitivne slike o lokalnoj samoupravi. Internet prezentacija gradova i opština trebalo bi da sadrži što više obrazaca koji mogu da se štampaju u popunjavaju elektronski, pri čemu format dokumenata mora biti čitljiv i prilagođen upotrebi.
Pojedine jedinice lokalne samouprave uvele su veb portale koji su aktivni i dostupni. U većini gradova i opština Internet portal daje mogućnost podnošenja zahteva, proveru stanja predmeta, informacije o opštinskim službama. Komunikacija se ogleda u vidu samog internet portala kao i putem elektronske pošte i sms-a.

3. SERVISI E-UPRAVE

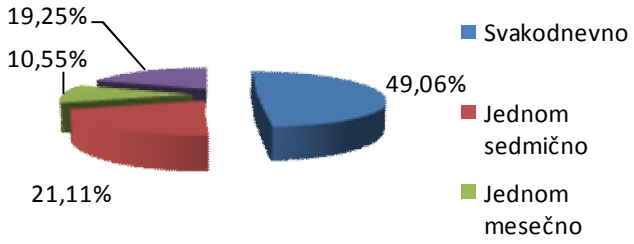
U našoj zemlji izvršen je Projekat Ministarstva za telekomunikacije i informaciono društvo „Procena IKT infrastrukture gradova i opština u Srbiji“ koji je imao za cilj jasno definisanje potreba lokalne samouprave. Rezultati koji su dobijeni u tom istraživanju bi trebalo da daju smernice za dalje unapređenje servisa e-uprave, što bi doveleo do približavanja građana i privrede lokalnoj samoupravi, povećanja efikasnosti rada lokalne samouprave i veću transparentnost u radu lokalne samouprave [6.].
U okviru ovog projekta je u saradnji sa Stalnom konferencijom gradova i opština (SKGO) izvršeno anketiranje gradova i opština. Anketa je izvršena korišćenjem veb portala koji su popunili službenici lokalnih samouprava nadležni za IT. Upitnik je sadržao četiri grupe pitanja.

- Stanje servisa e-uprave
- Stanje infrastrukture
- Ljudski resursi
- Socioekonomska analiza

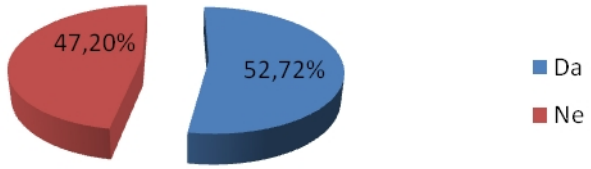
Istraživanje je uključivalo sledeća pitanja kako bi se ustanovio stepen razvijenosti e-servisa opština i gradova.



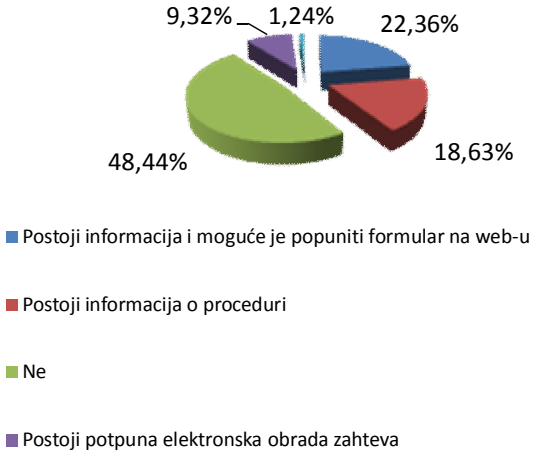
Slika 1. Da li Vaša opština ili grad imaju web prezentaciju?



Slika 2: Koliko često postavljate nove sadržaje na Vašu veb prezentaciju



Slika 3: Da li u vašoj opštini postoji servis elektronske pisarnice?



Slika 4: Da li postoji savremeni elektronski sistem za izdavanje izvoda iz matičnih knjiga?

Analizom ovog istraživanja utvrđeno je da samo u pojedinim opštinama (oko 20%) izvedena su kvalitetna rešenja e-servisa. Ovaj upitnik imao je za cilj i uvođenje nove prakse komunikacije bez papira i u tom smislu projekat je uspeo obzirom da su svi gradovi i opštine izvršili popunjavanje upitnika na vebu [6.].
Poslednjih godina intezivirale su se aktivnosti na polju uvođenja informacionih tehnologija, ali je implementacija svih nivoa elektronskih usluga prema građanim i pravnim licima još uvek niska [7.]. Pojam „elektronska uprava“ označava jedan od glavnih instrumenata za povećanje efikasnosti i pouzdanosti rada javne uprave. Povezivanje svih gradskih službi u jedinstvenu mrežu predstavlja osnovu za efikasniji i efektivniji rad administracije. Građani i pravna lica ne

smeju biti opterećeni teretima administracije i potrebno je olakšati puteve i načine rešavanja administrativnih problema.
Iako je od poslednjeg istraživanja e-servisa opština i gradova prošlo dosta vremena, upoređivanjem sajtova jedinica lokalnih samouprava može se videti da je broj javnih servisa koji su pristupačni online na veoma niskom nivou. Sa ciljem da s skrati put do dokumenata kao i redovi ispred šaltera i poboljša komunikacija sa lokalnim organima, obezbeđena je mogućnost informisanja o potrebnim dokumentima i načini kako da se najbrže dođe do njih. Ideja E-uprave je da se omogući građanima da na jednom mestu saznaju kako izgleda procedura za pribavljanje dokumenata [7.]. Mnogi gradovi i opštine kao što su Niš, Kragujevac, Kruševac, Inđija imaju svoje Internet prezentacije. ali je potrebno raditi na razvijanju e-servisa i omogućiti dvosmernu komunikaciju, jer se i dalje na veb sajtovima nude samo informacije o radu organa grada ili opštine i obaveštenja. U gradovima kao npr. Niš, Užice, Inđija omogućeno je da se putem e-servisa provere stanja na finansijskim karticama u lokalnoj poreskoj administraciji i u Javnim preduzećima, što je dovelo do pomaka u elektronskom poslovanju jer je došlo do povezivanja rada više službi. Uz korisničko ime i lozinku na veb adresi građani mogu imati uvid u svoje komunalne račune, ali i u zahteve i žalbe koje su uputili call-centru.
Servis čija je primena dostigla najviši nivo u svim jedinicama lokalne samouprave je servis virtuelni matičar. Virtualni matičar je e-servis koji se nalazi na svim portalima gradova. Preko njega mogu se naručiti izvodi i uverenja iz matičnih knjiga. Sadrži sve obrasce koji se popunjavaju direktno i sve žiro račune na koje treba uplatiti određene takse šte predstavlja ogromnu uštedu vremena. U pojedinim gradovima neophodno je popuniti direktno zahteve za izdavanje dokumenata, a dokaze o uplati određenih taksi poslati poštom, faksom Gradskoj upravi. U pojedinim lokalnim samoupravama proces izdavanja dokumenata je potpuno automatizovan, dovoljno je da se direktno popuni zahtev, a plaćanje se vrši pouzećem. Veliki značaj servisa je u tome što je sada omogućeno i licima koja su raseljena, izbeglim licima da u vrlo kratkom roku dobiju potrebnu dokumentaciju poštom.

3.1. E-servis Grada Kragujevca - Virtuelni matičar

Stranice Virtuelnog matičara predviđene su da omoguće građanima koji su upisani u matične knjige koje se vode na području grada Kragujevca, da putem Interneta naruče i na kućnu adresu dobiju naručene izvode ili uverenja iz matične službe grada Kragujevca.
Matične knjige su osnovne službene evidencije o ličnom stanju građana. O ličnom stanju građana vode se matična knjiga rođenih, matična knjiga venčanih i matična knjiga umrlih. Sve tri knjige vode se po dva primerka Prvi primerak – izvornik matične knjige je knjiga tvrdog poveza. Drugi primerak matičnih knjiga vodi se primenom elektronskih sredstava za obradu i skladištenje podataka. Poslovi vođenja matičnih knjiga poveravaju se opštinama, odnosno gradovima, a poslove izvršava opštinska, odnosno gradska uprava[70].
Sa portala može se direktno popuniti i proslediti obrazac zahteva za izdavanje izvoda ili uverenja iz matičnih knjiga i knjiga državljana koje se vode za matično područje Grada Kragujevca, ali i za matično područje Peć, Istok i Klina jer po čl. 6 stav 3 Zakona o matičnim knjigama poslovi vođenja matičnih knjiga za područje Autonomne pokrajne Kosovo i Metohija poveravaju gradu Kragujevcu za opštine Peć, Istok i Klina. Naručene isprave šalju se na kućnu adresu isključivo na području Republike Srbije i iste se plaćaju pouzećem pošti prilikom njihovog prijema.

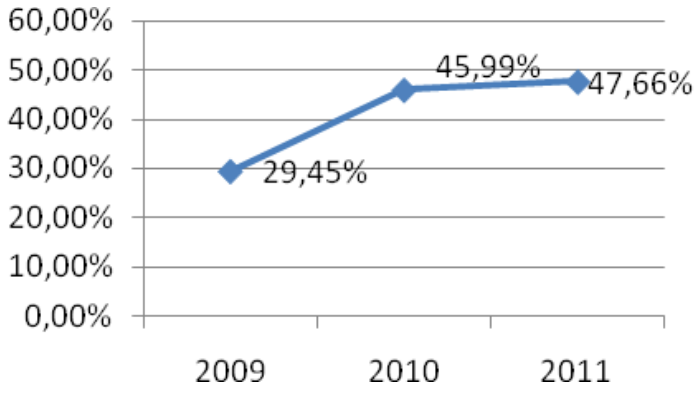
[70] Zakona o matičnim knjigama „Sl. glasnik RS“ br. 20/2009, čl.4

Servis virtualni matičar u gradu Kragujevcu jedan je od najposećenijih servisa jer pored toga što građani mogu dobiti informacije za dobijanje izvoda, mogu i naručiti dokumenta elektronskim putem.
Gradska uprava za mesnu samoupravu i opštu upravu na osnovu podnetih zahteva i izdatih izvoda iz matičnih knjiga sastavlja izveštaje o svom radu svake godine. Na osnovu službene evidencije i na osnovu zavedenih i popisanih akata u delovodnicima došlo se do sledećih podataka:

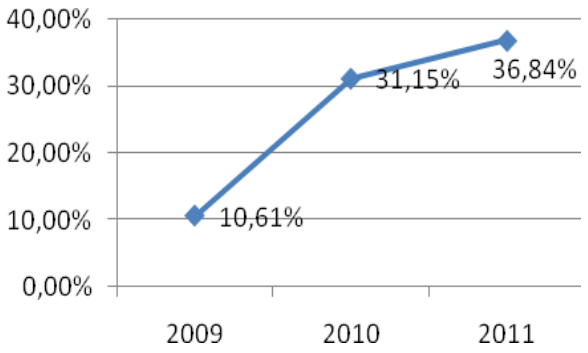
Tabela 1: Broj zahteva koji su podneti elektronski i lično

	Kragujevac		**Peć, Istok, Klina**	
	elektronski	lično	elektronski	lično
2009	14747	35325	1943	16375
2010	31867	37428	12655	27975
2011	28765	31587	10643	18250

U 2009. godini ukupan broj izdatih izvoda iz matičnih knjiga za matično područje grada Kragujevca iznosio je 50 072. Od tog broja 35 325 dokumenata je izdato na osnovu pismeno podnetih zahteva na šalteru Gradske uprave, dok je 14 747 izvoda izdato na osnovu zahteva koji su podneti preko e-servisa - Virtuelni matičar. Od ukupnog broja izdatih dokumenata 29,45% izdato je elektronskim putem.
Za matična područja Peć, Istok i Klinu ukupan broj izdatih dokumenata bio je 18 318, od tog broja 16 375 izdato je šalteru Gradske uprave, dok je 1 943 izdato elektronskim putem. Od ukupnog broja izdatih dokumenata, preko servisa Virtualni matičar izdato je 10,61% .
U 2010. godini ukupan broj izdatih dokumenata za Grad Kragujevac iznosio je 69 295, a u 2011. godini 60 325. U 2010. godini elektronski je podneto 31 867 zahteva, što je 45,99% od ukupnog broja, dok je u 2011. godini elektronski podneto 28 765 što predstavlja 47,66 % od ukupnog broja podnetih zahteva i izdatih dokumenata.
Za matična područja Peć, Istok i Klinu broj podnetih zahteva u 2010. godini iznosio je 40 630 i od tog broja elektronski je izdato 12 655 odnosno 31,15% od ukupnog broja, dok je u 2011. godini broj izdatih dokumenata 28 893 a od tog broja preko servisa izdato je 10 643 odnosno 36,84% od ukupnog broja.



Slika 5 : Zahtevi podneti preko e-servisa virtualni matičar matično područje grad Kragujevac



Slika 6: Zahtevi podneti preko e-servisa virtualni matičar matično područje Peć, Istok, Klina

Upoređivanjem izveštaja po godinama može se videti da je u 2009. godini elektronsko podnošenje zahteva i dobijanje dokumenata bilo na niskom nivou. Razvojem informacionih tehnologija, ali i povećanjem svesti građana za korišćenjem Interneta, kao i isticanje Virtuelnog matičara na sajtu grada može se videti povećanje korisnika elektronskih usluga u 2010. godini. Tendencija rasta nastavljena je tokom 2011. godine, iako je manji broj dokumenata izdat, jer broj izdatih dokumenata ne mora pratiti rast iz godine u godinu, potrebe za vađenjem izvoda su različite. Primetno je da se broj elektronskih zahteva povećava iz godine u godinu, a naročito je primetno povećanje korisnika koji su raseljenji sa teritorije Kosova i Metohije. Može se primetiti da je za opštinu Peć, Istok i Klinu u 2009. godini 10,60% izvoda izdato elektronski dok je u 2010. godini taj broj dostigao 31,14%. Do sada su raseljena lica morala da dolaze u mesto gde su izmeštene matične knjige iz njihovih matičnih područja ili da angažuju prijatelje, rodbinu da podnose zahteve i uzimaju dokumenta, a sada je dovoljno da znaju samo mesto gde su knjige izmeštene i da na sajtu grada kome su povereni poslovi za teritoriju Kosova i Metohije pronađu servis Virtuelni matičar, popune zahtev i čekaju da izvodi stignu na kućnu adresu.

3.2.Centralni registar matičnih knjiga

Najznačajniji projekat u razvoju e-uprave je Centralni registar matičnih knjiga. Projekat je veoma ambiciozan i predstavlja prekretnicu u razvoju e-uprave. U ovom projektu učestvovalo je Ministarstvo za ljudska i manjinska prava, državnu upravu i lokalnu samoupravu i Pošta Srbije [8.]. Centralni registar matičnih knjiga podrazumeva kompletno unošenje svih podataka iz starih matičnih knjiga u jedinstvenu elektronsku bazu podataka. Projekat bi trebalo da bude završen do kraja 2014. godine. U vrlom kratkom periodu omogućeno je građanima Srbije da dobiju izvode iz matičnih knjiga u bilo kojoj opštini ili matičnom području, što znači da sada ne mora da se ide po izvod iz matične knjige rođenih u mesto gde je lice rođeno, već se izvod može izvaditi u bilo kojoj gradskoj ili opštinskoj upravi u Srbiji. Postupak izdavanja dokumenata je vrlo jednostavan. Sertifikovani matičari imaju pristup centalnoj bazi podataka i izdaju tražena dokumenta. Od 09.05.2011. godine omogućeno je da se iz centralnog sistema izdaju izvodi iz matičnih knjiga u svim gradovima i opštinama Srbije. U centralnom sistemu se nalaze podaci iz većine gradova i opština koje su predale na čuvanje drugi primerak matičnih knjiga, ali kako to nije jednostavna procedura jer podrazumeva detaljnu proveru podataka, postoje gradovi koji još nisu dostavili podatke. Pošta Srbije je za potrebe Ministarstva obezbedila sve informatičke, tehničke i infrastrukturne preduslove za uspostavljanje centalnog sistema za elektronsku obradu, skladištenje podataka i čuvanje drugog primerka matičnih knjiga. Mnoge opštine nisu kadrovski

i tehnički spremne da koriste novu uslugu tako da je Pošta Srbije pomogla tim opštinama tako što je poklonila programe za pristup centralnom registru.
Kada Projekat bude u potpunosti realizovan, svi građani će moći u bilo kojem gradu ili opštini da elektronskim putem naruče izvode iz matičnih knjiga i državljanstva. Tako će administrativni poslovi biti obavljeni bez papira, a ušteda za državu će biti ogromna, ali i za građane jer sadašnji izvodi imaju holograme, pa je samim tim njihovo trajanje neograničeno i neće morati svaki put da se iznova vade i neće se plaćati administrativana taksa za njihovo vađenje.
Projekat e-Uprave u kojem učestvuje Pošta Srbije je Elektronska razmena podataka o građanima i uspostavljanje elektronske evidencije o državljanima Republike Srbije koji su pokrenuli Ministarstvo unutrašnjih poslova i Ministarstvo ljudskih i manjinskih prava. U skladu sa postavljenim ciljevima projekta, očekuje se da će zaživeti razmena podataka o građanima između ministarstava, tako da će na primer građanima biti dovoljno da se pojave na šalteru MUP-a prilikom vađenja biometrijskih pasoša, dok će se izvodi iz matičnih knjige rođenih i uverenja o državljanstavu povlačiti u elektronskoj formi.

ZAKLJUČAK

U uslovima savremenog života i eri informacionih tehnologija pored klasičnog načina poslovanja neophodno je uvesti i nove oblike poslovanja i komunikacije. Mnogi gradovi i opštine imaju svoje Internet prezentacije, ali je potrebno raditi na razvijanju e-servisa i omogućiti dvosmernu komunikaciju, jer veliki broj gradova na veb sajtovima nudi samo informacije, obaveštenja ili preuzimanje obrazaca. Jedini servis koji je dostigao visok nivo primene u svim gradovima je servis Virtuelni matičar. Mora se više raditi i na podizanju svesti građana da ne pružaju otpor novim tehnologijama i novim uslugama. Novo vreme nosi i nove načine poslovanja, a elektronsko poslovanje je nužno i neophodno kako bi se što brže i jednostavnije rešili mnogi poslovni procesi.

LITERATURA

[1.] Arsovski, Z., Ranković, B., Kolin, Z.(2011): *Elektronsko poslovanje*, Ekonomski fakultet, Kragujevac
[2.] Vuksanović, E. (2009): *Elektronski sistemi plaćanja*, Ekonomski fakultet,Kragujevac
[3.] Stankić, R. (2009): Elektronsko poslovanje, Ekonomski fakultet, Beograd
[4.] Radojević, T., Radovanović, D. (2010): „The impact of electronic banking on offer of financial services“, in 33rd International Convention MIPRO, Proceedings, Opatija, Croatia, May 24th-28th, 2010, 1131 - 1136
[5.] Kujačić, M., Tasić, M., Ćuk, D., Šolaja, M., Branisavljević, I. (2009): “*Priručnik za IKT u jedinicama lokalne samouprave*“, (pristup 17.01.2013) [dostupno na http://www.digitalnaagenda.gov.rs/]
[6.] Republički zavod za informatiku i Internet (2009): „Analiza stanja IKT infrastrukture“, (pristup 15.01.2013) [dostupno na http://www.digitalnaagenda.gov.rs/]
[7.] Vlašković, S. (2010): „Merenje eSpremnosti lokalnih samouprava u Srbiji“, (pristup 20.01.2013) [dostupno na http://www.digitalnaagenda.gov.rs/]
[8.] Portal eUprava Republike Srbije (pristup 22.01.2013) [dostupno na http://www.euprava.gov.rs/]

POBOLJŠAVANJE KVALITETA I NIVOA ZAŠTITE KORISNIČKIH PODATAKA U WEB OKRUŽENJU

IMPROVING QUALITY AND LEVEL OF USER DATA PROTECTION IN WEB ENVIRONMENT

Nenad Ristić
Fakultet za računarstvo i informatiku, Univerzitet Sinergija
Bijeljina, Bosna i Hercegovina
nristic@sinergija.edu.ba

Aleksandar Jevremović, Mladen Veinović
Univerzitet Singidunum, Beograd, Srbija
ajevremovic@singidunum.ac.rs
mveinovic@singidunum.ac.rs

Sažetak
U ovom radu analiziraju se postojeća i predlaže novo rešenje problema vezanog za zaštitu korisničkih podataka u Web okruženju. Metoda koja se predlaže je zasnovana na korišćenju slučajnih i složenih *salt* vrednosti pri individualnom generisanju heš vrednosti za lozinku koju je uneo korisnik, kao i upotreba segmentnog hešovanja za šifrovanje lozinke uz standardnu metodu hešovanja SHA512. Lozinka se nakon šifrovanja deli u dva dela koja se čuvaju u dve zasebne baze podataka skladištene na različitim platformama.
Ključne riječi- *zaštita podataka, Web aplikacije, šifrovanje, baze podataka*

Abstract
In this paper we analyze existing solutions and propose a new solution to the problem of the protection user data. The method is based on the use of random and complex salt values of the individually generated hash value of the password entered by the user as well as the use of segmented hashing to encrypt passwords with SHA512 hash method. Password after encryption is divided into two parts and the parts are stored in two separate databases that are on different platforms.
Key words – Data protection, Web applications, encoding, data bases

1.UVOD

Jedan od sve značajnijih bezbednosnih problema u savremenoj upotrebi *Web*-a je otkrivanje lozinki korisnika prilikom kompromitovanja servera baze podataka u kojoj se one nalaze. Skorašnji slučajevi kompromitovanja baza *LinkedIn*, *Twiter* i *Sony* korporacije [1] pokazuju da čak i veći sistemi imaju ranjivosti koje se mogu iskoristiti za dobijanje pristupa bazi podataka. Čak i kod čuvanja heš vrednosti lozinki savremeni rečnici omogućavaju relativno brzo dolaženje do originala. Primena tzv. „soljenja“ pri izračunavanju heš vrednosti takođe nije rešenje, jer se u slučaju *Web* aplikacije, pri kompromitovanju baze podataka, najčešće kompromituje aplikativni server na kome se nalazi korišćena *salt* vrednost.

2.RANJIVOSTI SISTEMA ZA UPRAVLJANJE BAZAMA PODATAKA

U bazama podataka skladište se brojne informacije iz mnogih domena. Različiti programi i različite namene zahtevaju različite informacije, a one se skladište u bazama podataka. Skladištenje i čuvanje podataka je glavna namena SUBP, podataka koji mogu biti izuzetno vredni i tajni. Zbog toga za tim sistemima raste zanimanje zlonamernih napadača, a samim time i potreba da ih se učini sigurnijim. Osim velike količine informacija koje čuvaju, postoji još nekoliko faktora koji doprinose ranjivosti baza podataka. Uz današnje trendove Interneta, SUBP-ovi koji su tradicionalno bili smešteni u zatvorene mreže i iza zaštitnih barijera, postaju sve otvoreniji prema udaljenim korisnicima, a time i sve podložniji napadima. Takođe, značajan faktor predstavlja i javna dostupnost izvornog koda poznatih SUBP, što zlonamernim korisnicima daje mogućnost istraživanja i pronalaženja sigurnosnih propusta.

Koncept bezbednosti u bazama podataka sličan je bezbednosti u računarskim mrežama. U oba slučaja nastoji se da se korisniku daju samo neophodne privilegije da bi se time smanjila ranjivost sistema, onemogućavanje nepotrebnih funkcionalnosti, obavezno odobravanje izmena i nadzor pristupa, odvojiti funkcionalne blokove, obavezna upotreba šifrovanja, itd. Jedina stvarna razlika je u tome što kod baza podataka svi ovi mehanizmi djeluju unutar samog SUBP-a.

Ranjivosti baza podataka mogu proizaći iz neispravne konfiguracije SUBP-a, programskih propusta ili bezbednosnih nedostataka unutar aplikacija povezanih sa njima. Iako SUBP često ne podržavaju bezbednosne mogućnosti tradicionalno prisutne kod drugih sistema, pravilno postavljanje postojećih mogućnosti može podići nivo bezbednosti podataka, te ukloniti veliki broj ranjivosti. SUBP uglavnom nemaju mogućnosti zaštite korisničkih naloga koje su prisutne kod operativnih sistema. Tu se prvenstveno misli na nedostatak kontrole lozinki proverama u rečniku i na nemogućnost određivanja perioda aktivnosti korisničkog naloga.

Često se tokom instalacije SUBP-a izvorno postavljeni i opšte poznati korisnički nalozi i lozinke ostavljaju aktivni bez promene. Na području upravljanja bazama podataka nema uloge administratora za sigurnost. Zbog toga administratori baza podataka moraju voditi računa o korisničkim nalozima i lozinkama, u isto vrijeme osiguravajući ispravan rad i zadovoljavajuće performanse baze podataka. Evidentiranje događaja na SUPB najčešće se formira tako da je visokih performansi, a sa što manjom upotrebom prostora diskovima. Zbog ovakvih podešavanja otežava se utvrđivanje odgovornosti kao i potencijalna forenzička analiza baze. Takođe, sigurnosni propusti u SUBP predstavljaju veliku ranjivost u SUBP i omogućavaju zlonamernom korisniku izvođenje napada uskraćivanjem usluge (engl. *DoS - Denial of Service*) ili izvršavanje zlonamernog koda.

Činjenica da se baze podataka nalaze iza zaštitne barijere ne čine ih potpuno sigurnim. Napad umetanjem ili ubrizgavanjem (engl. *SQL injection*) predstavlja najčešći napad na bazu podataka. Ovaj napad nije direktan napad na bazu, već predstavlja pokušaj izmene parametara koji se šalju *Web* aplikaciji sa namerom da se izmeni SQL upit koji će se poslati bazi podataka.

Napad umetanjem najprimenjiviji je u procesu prijavljivanja korisnika na neku *Web* lokaciju [2]. Korisnik unosi svoje podatke za verifikaciju, korisničko ime i lozinku, pomoću kojih se kreira upit koji proverava tabelu u bazi sa korisničkim podacima. Ako se u tabeli pronađu podaci korisnik postaje autorizovan.

Ako je korisničko ime Nenad a lozinka test123 upit će izgledati

```
SELECT*
FROM Korisnici

WHERE KorisnickoIme='Nenad' AND Lozinka='test123'
```

Napadač može u polje predviđeno za lozinku upisati par karaktera, zatim upis završiti jednostrukim navodnikom, te u nastavku polja dodati logički izraz koji je uvek tačan i kao odgovor iz baze može dobiti poverljive tabele sa podacima, u nastavku vidimo primer takvog unosa. Upisivanjem umesto lozinke niza karaktera *Aa' OR 'A'='A* sql upit postaje

```
SELECT*
FROM Korisnici
WHERE KorisnickoIme=’Nenad’ AND Lozinka=’Aa’ OR ’A’=’A’
```

Ovakav upit će vratiti podatke svih korisnika pa čak i administratorskog naloga. Još veću opasnost predstavlja mogućnost izvršavanja više upita pa unošenjem izraza *a'; DROP TABLE Korisnici; SELECT * FROM KorisniciInfo WHERE 't' = 't* umesto korisničkog imena dobija se upit

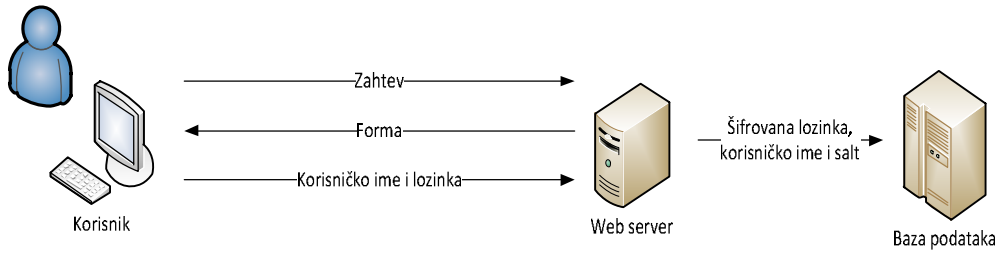
```
SELECT * FROM Korisnici WHERE ime = 'a'; DROP TABLE Korisnici; SELECT * FROM KorisniciInfo WHERE 't' = 't';
```

Ovakav upit će obrisati tabelu Korisnici i prikazivanje svih podataka iz tabele KorisniciInfo.

Svi SUBP-ovi sadrže ranjivosti i nije moguće odrediti koji je najsigurniji niti koji je najranjiviji među njima. Jedino se sa sigurnošću može tvrditi, a to je da je najsigurniji onaj sistem koji se najbolje poznaje. Dobro poznavanje arhitekture i funkcionalnosti sistema od strane administratora, omogućuje siguran rad SUPB.

3.MEHANIZMI ZAŠTITE PODATAKA U UPOTREBI

U ovom poglavlju biće analizirani mehanizmi zaštite korisničkih podataka koji se trenutno koriste kroz primer *Web* aplikacije za registrovanje i logovanje. Na slici 1 prikazan je klasični sistem zaštite korisničkih podataka.



Slika 1. Klasični system zaštite korisničkih podataka

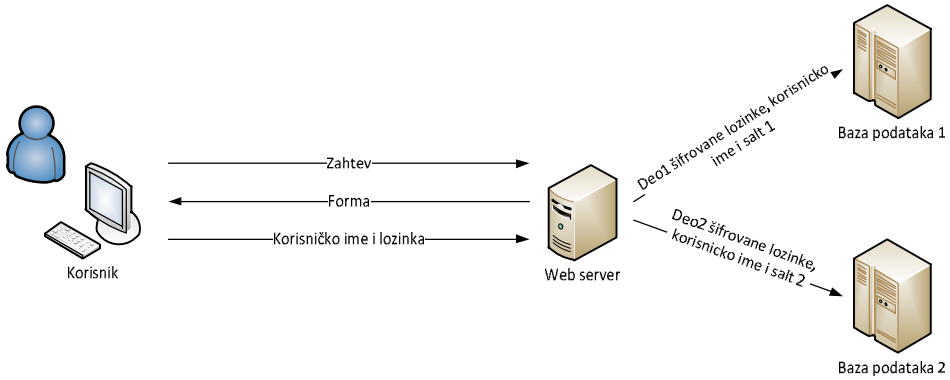
Tokom procesa registrovanja korisnik unosi željeno korisničko ime i lozinku. Upotrebom npr. php programskog koda korisničko ime i lozinka se skladište u bazu podataka. Nakon unosa podataka u *Web* formu lozinka se šifruje i kreira se upit bazi podataka kojim se podaci smeštaju u bazu. U nastavku je primer dela koda potreban za šifrovanje kao i generisanje upita za bazu.

```
<?php
$lozinkahash = sha1($_POST['lozinka']);
$sql = 'INSERT INTO korisnici (korisnickoime, lozinkahash) VALUES (?,?)';
$result = $db->query($sql, array($_POST['username'], $passwordHash));
?>
```

U ovakvom slučaju lozinka se šifruje SHA1 algoritmom zatim se skladišti u bazu podataka zajedno sa korisničkim imenom. Prilikom sledećeg logovanja korisnika koristi se sličan interfejs kao i kod za proveru korisničkih podataka. Nakon unosa podataka u formu vrši se šifrovanje unesene lozinke zatim provera pristupnih podataka sa podacima koji se nalaze u bazi. Ovakav princip registrovanja korisnika i čuvanja lozinke u šifrovanom obliku pruža određen nivo sigurnosti za podatke koji su u bazi. Osnovna slabost ovakvog sistema je u slučaju dobijanja pristupa bazi podataka napadač može napadom sirovom silom (engl. *Brute Force*) doći do odgovarajuće heš vrednosti koja predstavlja lozinku [3]. Napadač će porediti šifrovane lozinke iz baze sa listom generisanih heš vrednosti dok ne pronađe podudaranje. Ranije su ovakvi napadi zahtevali mnogo vremena pa je nivo zaštite običnim šifrovanjem lozinke sažimanjem bio dovoljan. Razvojem tehnologija došlo je do naprednih napada koji su koristili grafičke čipove za napade sirovom silom [4] kao i mogućnost zakupljivanja resursa, samim time ovakav sistem zažtite podataka postaje izuzetno nesiguran.

• IMPLEMENTACIJA SISTEMA SEGMENTOVANE ZAŠTITE KORISNIČKIH PODATAKA

U ovom poglavlju biće prikazana praktična primena sistema segmentovane zaštite korisničkih podataka. Sistem je baziran tako da nakon unosa korisničkog imena i lozinke, lozinku šifruje sha512 algoritmom i zatim „umotava“ u dve slučajno generisane *salt* vrednosti. Postoje dva osnovna pristupa za generisanje slučajnih brojeva korišćenjem računara: pseudo slučajni generatori brojeva (*PRNG*) i istinito slučajni generatori brojeva (*TRNG*). Svaki od navedenih pristupa ima svoje prednosti i mane [5]. Salt vrednosti se dodaju pre i posle lozinke. Nakon toga dobijeni blok se šifruje segmentnim hešovanjem. Na kraju se dobijena šifrovana lozinka deli se na dva dela. Delovi lozinke zajedno sa po jednom salt vrednošću se čuvaju u zasebnim bazama podataka. Baze podataka su na različitim platformama što nudi dodatni nivo sigurnosti. Pored dela lozinke čuva se i jedna od salt vrednosti, što znači da kompromitovanjem jedne baze napadač ima samo deo šifrovane lozinke kao i deo salt vrednosti. Na slici 2 je prikazan je šematski prikaz sistema segmentovane zaštite korisničkih podataka.



Slika 2 . Sistem segmentovane zaštite korisničkih podataka

Klasični sistemi čuvaju u jednoj bazi šifrovanu lozinku kao i *salt* vrednost dok ovaj sistem pored dvostrukog šifrovanja, deli šifrovanu lozinku i skladišti je u dve različite baze podataka. Baze podataka mogu biti na dva različita SUBP kao i različitim platformama operativnih sistema (*Unix*, *Linux*, *Windows* ..). Ovakav princip čuvanja podataka predstavlja veliku prepreku u potencijalnom napadu. Napadač bi morao da pronađe slabosti na različitim

platformama da ih iskoristi kao i da nakon toga izvrši sklapanje lozinke i generisanje potpisa za poređenje sa postojećim *salt* vrednostima što zahteva velike hardverske resurse kao i nerealan vremenski period.

Za pokazni model korišten je php programski jezik, *MYSQL* SUPB na *Linux* platformi, MSSQL na *Windows* 2008 platformi. Php je izabran prije sveg jer u trenutku kada korisnik poseti php kreiranu stranicu, *Web* server automatski obrađuje php kod na osnovu kog određuje šta će prikazati korisniku. Sve ostalo npr. operacije sa fajlovima, promenljive, različite funkcije i operacije, ne prikazuju se korisniku već korisnik dobija generisanu HTML stranicu bez php koda. Modeli platformi kao i SUPB mogu biti zamenjeni bilo kojom drugom platformom i sistemom za upravljanje bazama uz minimalne izmene u programskom kodu i prilagođavanje upita.

Za početak kreirana je forma za registrovanje sa neophodnim poljima, ova forma preuzima podatke i prosleđuje ih skripti koja vrši obradu i kreiranje upita za baze podataka. Prilikom generisanja salt vrednosti koristi se php funkcija *mcrypt_create_iv* za generisanje inicijalnih vektora dužine 768 bita zatim se vrši pretvaranje u oblik za upotrebu kao salt. Kod kojim dobijamo salt 1 i salt 2 je u nastavku

```
$salt1=bin2hex(mcrypt_create_iv(768, MCRYPT_DEV_URANDOM));
$salt2 = bin2hex(mcrypt_create_iv(768, MCRYPT_DEV_URANDOM));
```

Primer jedne generisane salt vrednosti je :

ced3f282b04a63333e57946a079025be89ee7601f93cd9ea4891da2f69ca43f58921475db91c58042
7bfd4b10ee43ccb94268918af6b65037eea1a0081ff9a4b19ae0fdc0c45c4cb5e74d089a7c7c73a661
f3891c6b1bcc0c5ef2795bb85bd6d0c75dcc00674e35f290a52f3dfd890012730e33607cdfd05776b
0c3fde814349a0a1a1dbd5ca72f692cd21415a6b9463a49bfc29efe7872ddfacd20e5d8b9b0031ec6
bc4418f0c4edd8e4e0d2246d7ec016ca98a70827516408d1db401b59aaacca874729f764d6cc3bfc9
d5c86cc621ae6895fb4e239d723ea3e086abcf7b0e9fd68772ebfe7bc4e3c8813f2e40c1391bef21ad
1905148dd9e35d2ad8cac3b7fdd140057d60bd62be57489ae9f8f3a5ee5802267a2eef4144267274
24a925a07ee8626efdc823fff03452ece14422ddef7341860af7cd108bec69be4c7d9a6d12fee51f1fd
deff018a6ecba7ccaa112234bf98ba28c1aee6e57395c5f4d1028c02c73bb59ab6abd027f83488925
984799ad6b33c5ff025ad5c7c0096c2331ab

Na ovaj način generišu se dve različite slučajne vrednosti koje se koriste kao *salt* prije završnog šifrovanja lozinke. Ove salt vrednosti će biti različite za svakog novog korisnika. U sledećem koraku vrši se kreiranje bloka za šifrovanje koji sadrži salt1 vrednost zatim šifrovanu lozinku sha512 algoritmom i salt 2 vrednost.

```
$blok = $salt1 . hash ('sha512', $lozinka) . $salt2;
```

Na kraju formiranja šifrovane lozinke vršimo sažimanje/šifrovanje dobijenog bloka upotrebom ssdeep funkcije.

```
$lozinka = ssdeep_fuzzy_hash ($blok);
```

Rezultat šifrovanja je:

96:40cCjDoMAN34W4KijkSy2jaKnZwfWCB7m5nN0Wr:l7pu4WMkJ0VZlCB7m5N0Wr

Ovako dobijena lozinka se deli na dva dela i vrši se smeštanje u baze podataka. Uz prvi deo lozinke u bazu podataka 1 skladišti se salt 1 kao i korisničko ime. Drugi deo lozinke se uz salt 2 i korisničko ime smešta u bazu podataka 2. Lozinku delimo tako što prvo određujemo dužinu a zatim delimo promenljivu u kojoj je lozinka na dva dela i smeštamo u zasebne promenljive koje će se uskladištiti u baze podataka. U nastavku je primer koda za podelu lozinke na dva dela.

```
$polovina = (int) ( (strlen($sifra1) / 2) );
```

```
$deo1 = substr($sifra1, 0, $pola);
$deo2 = substr($sifra1, $pola);
```

Nakon ovog koraka definišu se upiti i podaci se upisuju u baze podataka. Baze podataka pored toga što mogu biti na različitim platformama mogu biti i na različitim lokacijama time se dodatno umanjuje ranjivost sistema. Kod autentifikacije korisnika koji je registrovan na osnovu korisničkog imena iz baza podataka uzimaju se salt1 i salt2 vrednosti, lozinka koju je korisnik uneo prolazi proces šifrovanja kao i prvobitna lozinka a zatim se vrši poređenje delova u bazama. Nakon uspešne provere segmenata lozinke korisnik je završio proces logovanja i uspešno je autentifikovan.

4.ZAKLJUČAK

Trenutno jedan od značajnijih sigurnosnih problema u savremenoj upotrebi *Weba* je otkrivanje lozinki korisnika prilikom kompromitovanja servera baze podataka na kome se one nalaze. Trenutni mehanizmi zaštite uglavnom ne pružaju dovoljan nivo sigurnosti.

U ovom radu predloženo je i analizirano novo rešenje problema zaštite korisničkih podataka zasnovano na korišćenju složenih i slučajnih *salt* vrednosti pri individualnom generisanju heš vrednosti za lozinku koju je uneo korisnik kao i upotreba segmentnog hešovanja za šifrovanje lozinke uz standardnu metodu hešovanja SHA512. Lozinka se nakon šifrovanja deli u dva dela i delovi se čuvaju u dve zasebne baze podataka koje se nalaze na različitim platformama. Smeštanje delova lozinke na različite baze podataka koje su na različitim platformama obezbeđuje podatke u slučaju kompromitovanja jedne platforme napadač dolazi u posed samo dela šifrovane lozinke. Da bi se izvršilo kompromitovanje obe baze neophodno je izvršiti napad na različite platforme (*Linux*, *Windows*, *Unix* …) kao i na različite

Metoda koja se koristi u ovom radu je nova i kombinuje više standardnih mehanizama kao i novih metoda koji zaštitu korisničkih podataka podižu na viši nivo i čine bazu otpornijom na napade. Savršeno siguran sistem ne postoji, ali postavljanjem dovoljno prepreka i otežavanjem procesa napadaču možemo nivo sigurnosti korisničkih podataka postaviti na visok nivo uz minimum ulaganja i promena u postojećim sistemima.

LITERATURA

[1] http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html
[2] Anley C. „Advanced SQL Injection In SQL Server Applications“, An NGSSoftware Insight Security Research (NISR) Publication, 2002
[3] Bertino, E. Sandhu, R. „Database security - concepts, approaches, and challenges“ Dependable and Secure Computing, IEEE Transactions, vol.2, no.1, pp.2-19, Jan.-March 2005
[4] Zonenberg A. „Distributed Hash Cracker: A Cross-Platform GPU-Accelerated Password Recovery System“, Rensselaer Polytechnic Institute, 2009
[5] Adamović S. Milenković M. Šarac M. Radovanović D. “Generatori slučajnih sekvenci i njihov uticaj na sigurnost”, INFOTEH-JAHORINA Vol. 9, Ref. E-VI-1, p. 820-822, March 2010.

PRIMENA NUMERIČKI UPRAVLJIVIH MERNIH MAŠINA U RAČUNARSKI INTEGRISANOJ PROIZVODNJI

APPLICATION OF NUMERICAL CONTROL MEASUREMENT MACHINES IN COMPUTER INTEGRATED MANUFAKTURING

Slobodan Jovanović
Univerzitet Singidunum, Departman za poslediplomske studije, Beograd, Srbija
Dušan Regodić
Univerzitet Singidunum, Danijelova br.32, Beograd
dregodic@singidunum.ac.rs
Aleksandar Jevremović
Univerzitet Singidunum, Danijelova br.32, Beograd
ajevremovic@singidunum.ac.rs
Radomir Regodić
Univerzitet Singidunum, Departman za poslediplomske studije, Beograd, Srbija

***Rezime**: Izmeriti neku veličinu, znači utvrditi njen brojni odnos sa nekom drugom istorodnom veličinom, pri čemu je usvojena merna jedinica. Pri merenju je potrebno obezbediti podatke o različitim fizičkim veličinama: diskretnim i neprekidnim, konstantnim i promenjivim, zavisnim i nezavisnim. Izuzetno kompleksni radni predmeti kao i tendencija smanjenja tolerancija postavljaju vrlo visoke zahteve, pred numerički upravljanjim mernim mašinama (NUMM) u pogledu efikasnosti i tačnosti. Pored provere tačnosti i parametara kvaliteta NUMM prilikom njenog istalisanja potrebno je vršiti i periodične provere.Istorijski gledano u proizvodnim procesima, merenje i kontrola su predstavljali usko grlo proizvodnje.*

***Ključne reči**: numerički upravljane merne mašine, greške merenja*

***Abstract**: Measure the size of a means to determine its relationship with many other homogeneous size, where the unit of measurement adopted. When measurement is necessary to provide information on different physical sizes: discrete and continuous, constant and variable, dependent and independent. Extremely complex cases working as well as the tendency to reduce tolerances set very high standards, the Nummi in terms of efficiency and accuracy. In addition to checking the accuracy and quality parameters during its NCMM istalisanja should perform periodic checks. Historically in the production processes, measurement and control were a bottleneck in production.*

***Key words:**numerically controlled measuring machines, measurement error*

Na taj način rezultat merenja se predstavlja kao kvantitativna informacija o osnovnim svojstvima mernog objekta, dobijena kao rezultat fizičkog procesa sa određenim stepenom tačnosti

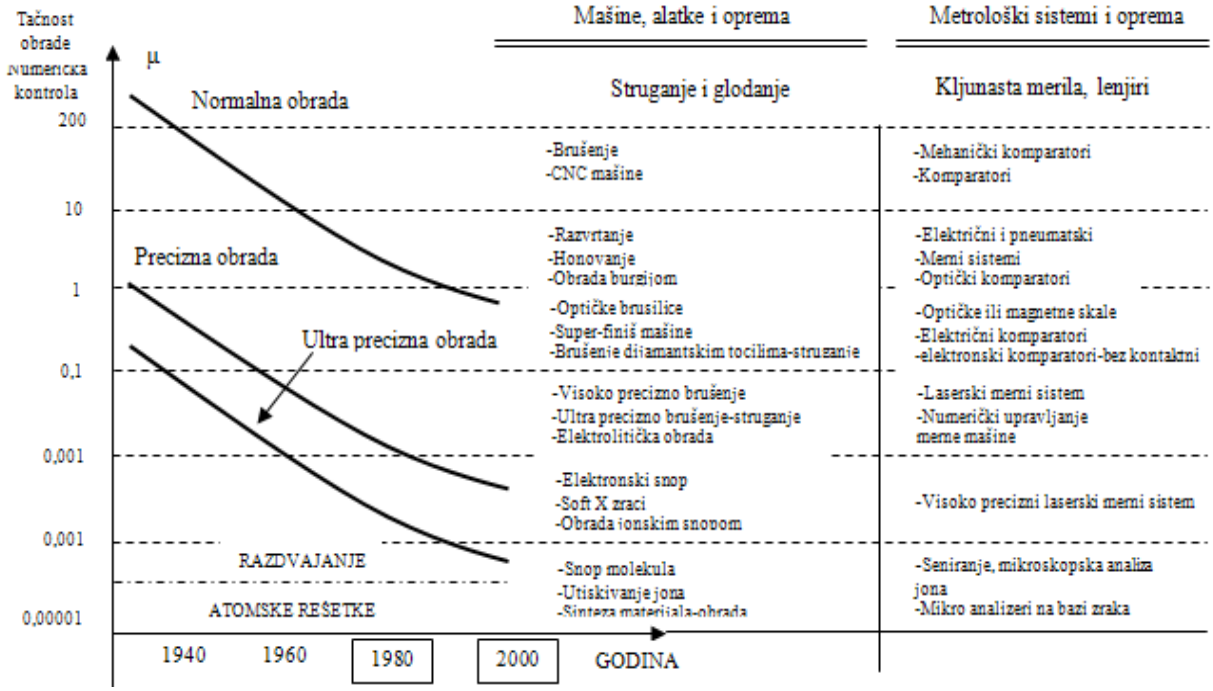
Danas možemo reći da je pod uticajem veštačke inteligencije otpočela nova etapa razvoja proizvodno metroloških sistema koji u inženjerskom merenju omogućavaju dalje korake ka inteligentnom naučno zasnovanom (uz pomoć baze znanja) i potpuno asocijativnom merenja

Tehnologije merenja i kontrole čine integralni deo svake proizvodnje i po značaju koji im u proizvodnom procesu pripada ni malo ne zaostaju za tehnologijama obrade. Ako se izvrši komparacija razvoja obradnih sistema sa aspekta tačnosti obrade koja se njime može ostvariti i metroloških sistema kojima se za te metode obrade identifikuju parametri kvaliteta konfornosti dolazi se do relacija i odnosa prikazanih na slici 1.

Ako se zaista želi automatizovati proizvodnja, neophodno je da metrološka identifikacija ima isti stepen fleksibilnosti i automatizacije kao i mašine alatke koje se koriste za izradu delova. U skladu sa ovim, potrebno je da metrološki sistem vrši nadzor nad celokupnim procesom i da obezbedi povratnu spregu i to u realnom vremenu, te tako održi proces u okviru zadatih karakteristika [Rodi94].

Izuzetno kompleksni radni predmeti kao i tendencija smanjenja tolerancija postavljaju vrlo visoke zahteve, pred NUMM u pogledu efikasnosti i tačnosti. Na tačnost rezultata merenja, utiču razne greške. Izvori ovih grešaka mogu se podeliti u dve osnovne grupe [Rodi96]:

- greške koje potiču od pojedinih funkcionalnih elemenata same NUMM i
- izvori grešaka koji nisu vezani za MM.



Slika 1. Razvoj obrade metala rezanjem i metroloških sistema

1. NUMERIČKE UPRAVLJANJE MERNE MAŠINE

Memi ili metrološki sistemi najviše klase tačnosti su fleksibilni metrološki sistemi kao što su NUMM fleksibilni metrološki moduli, ćelije, centri, stanice i informacioni metrološki sistemi (CIQ, CAQ i sl.), računarom integrisani sistemi. Osnovu gradnje fleksibilnih metroloških sistema čine NUMM i/ili merno kontrolni roboti.

NUMM se odlikuju visokim ili najvišim metrološkim karakteristikama. Ova ocena proizilazi iz sledećih osnovnih karakteristika koje poseduju NUMM [Stan88i; Majs86, Zaim03]: metrološka univerzalnost, visoka rezolucija, tačnost i pouzdanost merenja, visoka proizvodnost, potpuna automatizacija skoro svih ciklusa rada, visoka fleksibilnost, niski ukupni troškovi metroloških procesa, relativno jednostavan i brz proces pripreme, kalibracije, nameštanja mernog predmeta, programiranja i rukovanja numm sistemom, jednostavne i lake komunikacije sa nadređenim računarom, itd.

1.1 Osnovne strukturne jedinice NUMM

Osnovne hardverske strukturne jedinice NUMM su: noseća struktura, pogonski sistem, merni sistem, merna glava, upravljački sistem I dodatni uređaji, slika 2.



Slika2. *Razvoj obrade metala rezanjem i metroloških sistema*

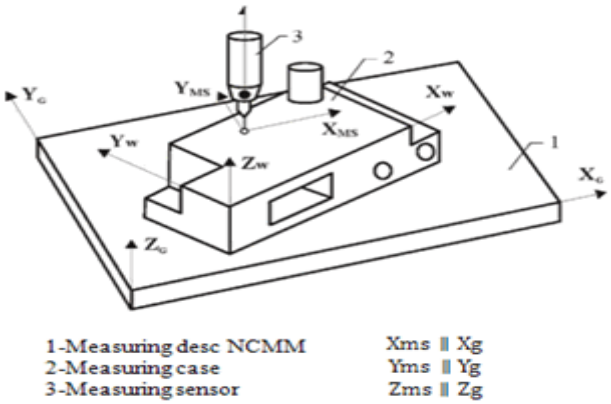
Noseća struktura ima zadatak da obezbedi statičku i dinamičku krutost celog sistema i da uležišti sve pokretne elemente NUMM.

Pogonski sistem obezbeđuje snagu i obrtni moment za kretanje pokretnih elemenata NUMM radi dovođenja mernog senzora u poziciju opipavanja mernog predmeta određenom vrednosti merne sile. Merni sistem jednoznačno identifikuje položaj pokretnih elemenata noseće strukture NUMM.

Merni senzor je prvi element mernog lanca. Pomeranje mernog senzora iz jednog u drugi položaj izvodi se ručno ili po programu, a u skladu sa metrološkim

zadatkom koji treba izvršiti. U trenutku kada merni pipak dodirne merni predmet, generiše se signal koji se predaje pogonskom sistemu odgovarajuće ose radi zaustavljanja klizača, na kome se nalazi merni senzor.

Ovaj signal se istovremeno predaje i upravljačkoj jedinici, a ona mernom sistemu NUMM radi očitavanja koordinata dodirne tačke. Rezultati očitavanja se prenose u računar, gde se izračunava posmatrana metrološka karakteristika mernog predmeta.



Slika3. *Koordinatni sistem kog NUMM*

Upravljački sistem koji čine upravljačka jedinica i/ili računar obezbeđuje upravljanje pokretnim elementima NUMM, obradu električnih signala koje dobija od mernog senzora, obradu, prikaz i distribuciju izmerenih vrednosti. Takođe vrši kontrolu o izvršenju CNC programa merenja mernog predmeta i o opterećenju mernog senzora. U širem smislu pored navedenog sistem se može koristiti i za automatizovano programiranje, za integraciju MM u CIM koncept itd. Može se slobodno reći da je primenu i razvoj upravljačkog sistema MM pratio razvoj softvera za njihovu podršku.

Softverska podrška MM obuhvata:

- sistemski softver (operativni sistem) i
- korisničke softvere (metrološke).

1.2 Princip rada NUMM

Proces metrološke identifikacije različitih vrsta tolerancija, zasniva se na poređenju njihovih nominalnih i stvarnih vrednosti, koristeći različite vrste transformacija između koordinatnih sistema: merne mašine, mernog senzora i mernog predmeta, slika 3.

Koordinatni sistem merne mašine se definiše preko koordinatnog sistema mernog stola, koji predstavlja referentni koordinatni sistem, i njegove vrednosti predstavljaju merne opsege osa merne mašine. Merni predmet ima dva koordinatna sistema: uravnjavanja i merenja. Prvi od njih, vrši uspostavljanje veze između koordinatnog sistema merne mašine i mernog predmeta. Drugi koordinatni sistem mernog predmeta, daje veze između metroloških zadataka na njemu i drugih koordinatnih sistema (mašine i mernog senzora).

Najzad, koordinatni sistem mernog senzora, uspostavlja vezu između generisane koordinate osnovnog geometrijskog oblika, metrološkog zadatka i ostalih koordinatnih sistema mašine i mernog predmeta.

Ovakav princip rada NUMM omogućuje merenje položaja prostornih tačaka na površinama mernog predmeta, da bi se na osnovu njih odredila numerička slika površina, koje ograničavaju merni predmet, slika 3. Numerička slika realnog oblika mernog predmeta upoređuje se sa modelom traženog oblika, koji je memorisan u računaru, nakončega se mogu utvrditi poklapanja i eventualna odstupanja između modela i stvarnog oblika mernog predmeta.

Može se reći da merenje sa NUMM uvek obuhvata sledeće korake [Tala03]:

- kalibracija mernog pipka (uzimajući u obzir i mernu glavu na osnovu uzete merne tačke sa npr. kalibrisane kugle),
- metrološko određivanje pozicije mernog predmeta u cilju usaglašavanja koordinatnog sistema uravnavanja mernog predmeta Xw, Yw i Zw, u odnosu na koordinatni sistem merne mašine Xm, Ym i Zm),
- merenje tačaka na površini mernog predmeta u koordinatnom sistemu mašine i
- obrada geometrijskih parametara izmerenog mernog predmeta i prezentacija izmerenih rezultataposle izvršene transformacije koordinata.

Kod merenja na NUMM koristi se indirektna metoda, tj. mere se koordinate diskretnih tačaka. Kod konvencionalne merne tehnike merenjem se direktno određuju merne veličine.

2. GREŠKE REZULTATA MERENJA

Rezultat svakog merenja javlja se kao funkcija dve nezavisne veličine, jedne koja odražava pravu vrednost merene veličine, i druge, koja predstavlja grešku njenog merenja. Prema tome, pod greškom merenja neke veličine treba smatrati razliku između rezultata merenja i prave vrednosti izmerene veličine.

Ako se prava vrednost izmerene veličine označi sa Q, a greška njenog merenja sa dx, tada se rezultat merenja x može predstaviti relacijom x = f(Q, dx), odnosno x = Q + dx, odakle, sledi:

$$dx = x - Q \qquad (2)$$

U tehnici merenja prava vrednost merene veličine je nepoznata. Razlog za to je nesavršenost merila. Smanjenjem greške merenje mi se sve više približavamo pravoj vrednosti merene veličine.

Klasifikacijom grešaka merenja prema određenim kriterijumima olakšava se njihova analiza, a takođe i matematička obrada rezultata merenja.

Greške merenja mogu se podeliti prema [Stan88]:

1) Zakonomernostima nastajanja grešaka na:
   - sistematske greške,
   - slučajne greške i
   - grube greške.
2) Izvorima ili poreklu nastanka na:
   - greške mernog uređaja,
   - metodske greške,
   - subjektivne greške i
   - greške vezane za stanje i uticaj spoljašnje okoline (temperatura, vlaga, vibracije, udari i sl.) na proces i rezultate merenja.
3) Karakteru vremenske promene veličine na:
   - statičke greške i
   - dinamičke greške.

2.1 Tačnost i preciznost merenja

Sa pojmom greške merenja neke veličine, direktno je povezana tačnost (T) i preciznost (P) merenja.

Pod tačnošću merenja podrazumeva se, u opštem slučaju, kvalitet ili valjanost merenja, tj. stepen bliskosti (slaganja) između rezultata merenja i prave vrednosti merene veličine.Tačnost merenja neke veličine utoliko je veća, ukoliko je manja greška njenog merenja. Otuda se preko greške merenja kvantitativno izražava tačnost merenja date veličine. Preciznost merenja definiše se ponovljivošću mernih rezultata, odnosno stepenom rasipanja ili uzajamnog podudaranja pojedinih mernih rezultata. Ti rezultati dobijeni su uzastopnim, višestrukim ponavljanjem merne operacije nad nekom mernom veličinom,čija je vrednost vremenski nezavisna (konstantna). To znači da je preciznost nekog merenja veća, ukoliko je manje međusobno rasipanje pojedinih vrednosti rezultata merenja u skupu rezultata ponovljenih merenja, ili ukoliko je međusobno podudaranje ovih vrednosti veće.

Osnovne razlike između tačnosti, preciznosti, netačnosti (NT) i nepreciznosti (NP) merenja pokazuju dijagrami na slici 4. [Stan88].

Pažljivom analizom slike 4. zaključuje se da je za potrebnu i dovoljnu tačnost, neophodna i odgovarajuća preciznost merenja (merenje u slučaju 4.c može biti netačno prilikom jednokratnog merenja, bez ponavljanja). To ne važi za preciznost, jer se relativno visoka preciznost može postići i pri maloj tačnosti merenja

Karakteristika rasipanja rezultata merenja, definisana graničnim greškama predstavlja mernu nesigurnost [NN96]. Granične greške jednog merenja proračunavaju se kao proizvod srednjeg kvadratnog odstupanja jednog merenja *s*, iz niza merenja i broja *t*, utvrđenog u funkciji verovatnoće da greška neće premašiti granične vrednosti.

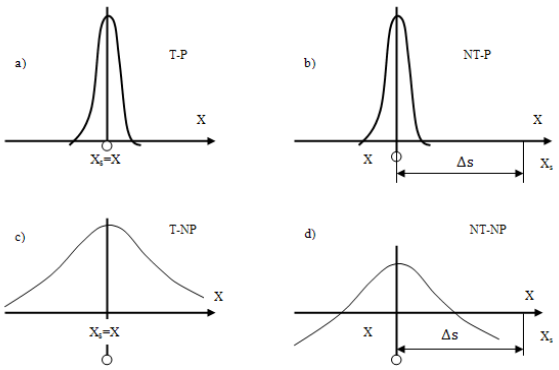
Srednje kvadratno odstupanje određuje se prema obrascu:

$$s = \sqrt{\frac{\sum_{i=1}^{\infty}(x_i - \bar{x})^2}{n-1}} \qquad (3)$$

gde je:

X_i- -ti rezultat merenja,

X - aritmetička sredina n rezultata merenja.



Slika4.*Mogući slučajevi tačnosti i preciznosti merenja, odnosno netačnosti i nepreciznosti nekog merenja*

3. TAČNOST MERENJA NUMM

Merne mašine poslednje generacije, predstavljaju složene mehatronske proizvode, koji imaju svoje parametre tačnosti.Kod NUMM nije moguće specificirati tačnost merenja opšte primenjivu za sve tipove merenja, zbog sledećih razloga [Neum00]:

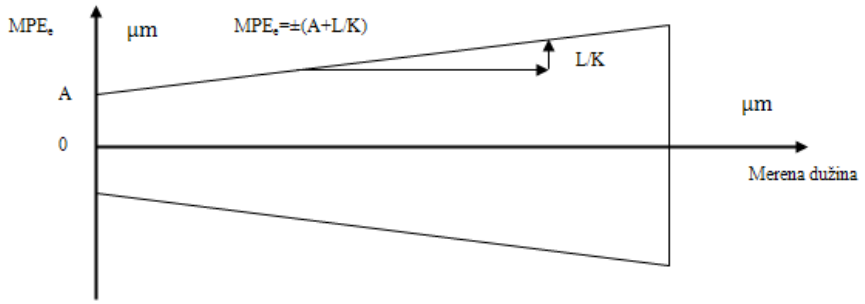
- NUMM imaju mogućnost merenja svih geometrijskih obeležja radnog komada, za razliku od jednonamenskih mernih instrumenata koji su pogodni za samo jedan zadatak;
- Rezultati nastaju analitičkom obradom mnoštva proizvoljnih tačaka sa površine radnog komada;
- Objekti se mogu meriti primenom različitih mernih strategija i na različitim mestima unutar merne zapremine mašine i
- Način na koji je definisan koordinatni sistem mernog predmeta utiče na prikupljanje podataka.

4.1 Procena merne netačnosti

Standardi koji daju preporuke za procenu merne netačnosti odnose se na maksimalno dozvoljenu grešku za jasno definisan merni zadatak (kao npr. ISO 10360). Ove vrednosti su označene sa MPE i dodatno su označene indeksom. U ovom kontekstu, "greška" ne treba da bude shvaćena kao nešto što je "pogrešno" većkao odstupanje koje može biti potpuno dozvoljeno.

Maksimalno dozvoljena greška za dužinsko merenje paralelnih i stepenastih merki označena je sa MPE_e(slika 5).

Prema važećim međunarodnim standardima, pred NUMM se postavljaju zahtevi začije je izvršenje ona pogodna sa stanovišta merne netačnosti. Merne netačnosti su za definisane uslove okoline, izdvojene za svaki pojedinačni merno kontrolni zadatak od strane proizvođača i stoje u specifičnoj vezi sa tolerancijama, utvrđenim od strane korisnika.



Slika5.Maksimalno dozvoljena dužinska greška MPE_e je funkcija merne dužine L. Svi rezultati moraju ležati unutar ograničene površine

4.2 Izvori grešaka merenjea kod NUMM

Greške od kojih zavisi tačnost MM mogu se podeliti u dve grupe [Kolj87]:

- Greške čiji je izvor sama MM i
- Greške čiji su uzroci okolni uslovi i merni predmet.

Glavni uzroci koji dovode do geometrijskih grešaka NUMM su sledeći [Kolj87]:

- greške pravosti i normalnosti elemenata pri izradi i montaži,

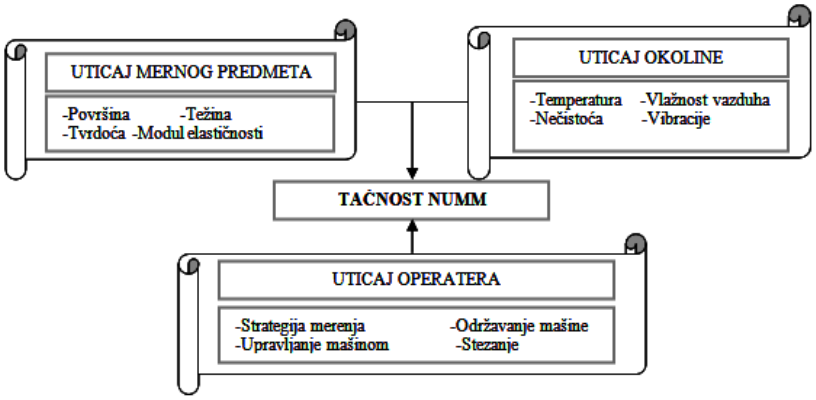
- greške prouzrokovane nestabilnošću usled unutrašnjih napona,
- greške prouzrokovane trenjem elemenata za vođenje u eksploataciji,
- greške zbog plastične deformacije uzrokovane dejstvom mase, sile trenja i inercije,
- greška položaja odstupanja koordinatnog sistema NUMM u odnosu na referentni koordinatni sistem. Ovo odstupanje je prouzrokovano usled nesavršenosti konstrukcije i položaja vođica i sastavnih elemenata od kojih su vođice komponovane, itd.

Greške čiji su izvori uslovi okoline i merni predmet mogu se podeliti na tri vrste u zavisnosti od izvora i to na greške čiji su izvori prostorni uslovi (uslovi okoline), merni predmet i operater, slika 6.

Greške usled prostornih uslova i mernog predmeta su uglavnom zbog:

- temperaturnih promena u prostoriji u kojoj je instalisana NUMM,
- vibracija pri merenju,
- vlažnosti vazduha,
- nečistoće,
- kvaliteta površine mernog predmeta,
- tvrdoće površine mernog predmeta,
- težine,
- modula elastičnosti mernog predmeta,

Greške uticaja operatera se prevashodno odnose na: izbor merne strategije, upravljanje mašinom, stezanja i održavanje mašine.



Slika 6. Uticajni faktori na tačnost NUMM nezavisno od merne mašine

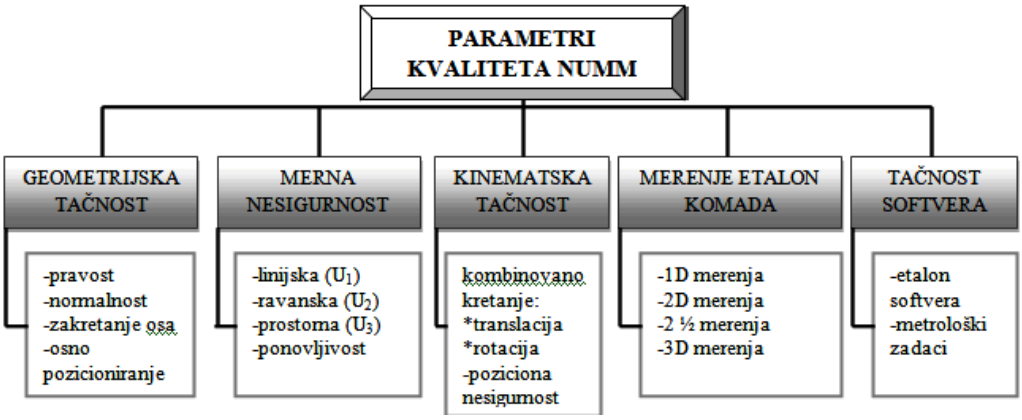
4. PARAMETRI KVALITETA NUMM

Parametri prikazani na slici 7, određuju kvalitet jedne NUMM i to su:

- geometrijska tačnost osa,
- merna nesigurnost,
- kinematska tačnost,
- merenja etalon komada i
- tačnost softvera.

Element klasifikacije parametara kvaliteta sa slike 7, koji se odnosi na kinematsku tačnost, posebno je uzet kao preporuka firme OPTON, koja svoje novo- proizvedene NUMM proverava i na ovaj način. Proizvođači NUMM preporučuju proveru tačnosti pomoću:

geometrijske tačnosti osa, merne nesigurnosti, i merenje etalon komada. Povećanje tačnosti merenja NUMM i mogućnost tog povećanja, na osnovu periodične provere parametara kvaliteta NUMM je složen problem. Realizacija povećanja tačnosti merenja odnosi se pre svega na geometrijsku tačnost osa.

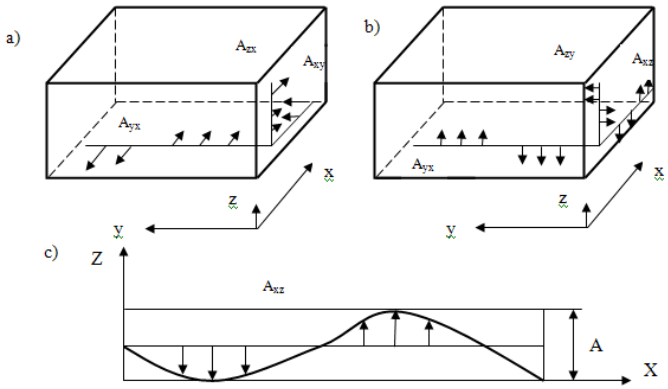


Slika7.*Elementi parametara kvaliteta NUMM-a*

4.1 Geometrijska tačnost osa

Parametri geometrijske tačnosti osa su: pravost ose, normalnost osa, zakretanje ose i osno pozicioniranje.

Ovde se ispituje provost osa kordinatnog sistema NUMM, i ona predstavlja odstupanje toka njene linije u dve upravne ravni, slika 8 (a i b).



Slika8.Parametri i način predstavljanja rezultata merenja pravosti osa

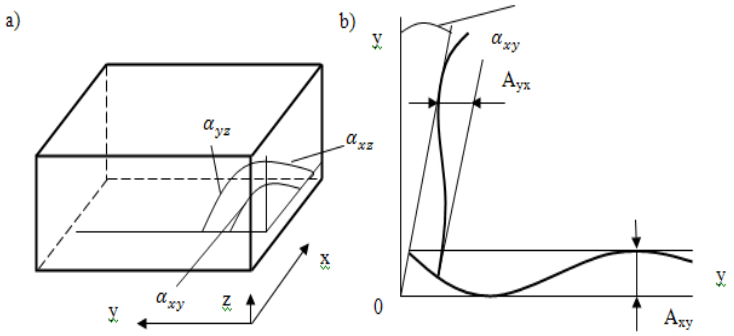
Na ovaj način dobija se 6 parametara pravosti i to:

- A_{xy} – pravost ose *X* merena u *Y* pravcu,
- A_{zx} – pravost ose *Z* merena u *X* pravcu,
- A_{yx} – pravost ose *Y* merena u *X* pravcu,
- A_{xz} – pravost ose *X* merena u *Z* pravcu,
- A_{zy} – pravost ose *Z* merena u *Y* pravcu i
- A_{yz} – pravost ose *Y* merena u *Z* pravcu.

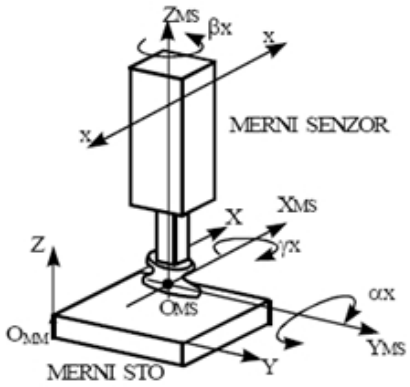
Normalnost dveju osa koordinatnog sistema MM predstavlja odstupanje od 90^o, pojasa širine A_{ik}, koji definiše pravost osa *i* i *k* i izražava se u lučnim sekundama, slika 9. Mere se tri parametra normalnosti, slika 9a:

- - normalnost između osa X i Y,
- - normalnost između osa Y i Z,
- - normalnost između osa X i Z.

Rezultat merenja normalnosti osa X i Y je prikazan na slici 9b.



Slika9.Parametri i način predstavljanja rezultata merenja normalnosti osa



Slika 10. Zakretanje ose X oko osa X, Y i Z

Pokretni elementi noseće strukture NUMM, koji se preko koordinatnog sistema mernog senzora (X_{MS}, Y_{MS}, Z_{MS}) sa koordinatnim početkom u tački O_{MS}, vezuju za koordinatni sistem MM (X, Y, Z) sa koordinatnim početkom u tački O_{MM}, slika 10, u svakom položaju u mernom opsegu generišu greške zakretanja osa koordinatnog sistema mernog senzora. Ovo odstupanje se iskazuje sledećim parametrima: Ugao nagiba (savijanja), ugao uvijanja (skretanja) i ugao valjanja.

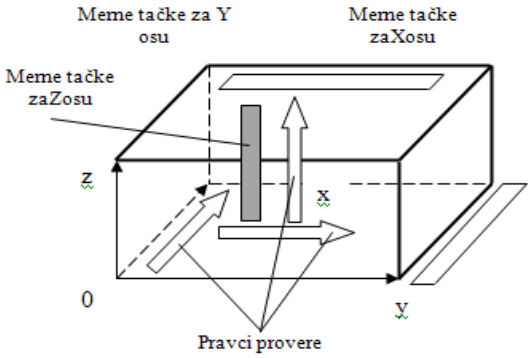
Odstupanja se mere u odnosu na pravac kretanja. Za pravac kretanja po X osi, prema slici 10, ovi parametri imaju sledeće oznake: α_x - ugao nagiba (savijanja) ose X u odnosu na osu Y, β_x - ugao uvijanja (skretanja) ose X u odnosu na osu Z, γ_x - ugao valjanja ose X u odnosu na osu X.

Provera ovog parametra kvaliteta, vrši se pri zauzimanju definisane pozicije pokretnog elementa duž ose koordinatnog sistema MM. Razlika između veličine pomeranja, dobijenog posredstvom mernog sistema NUMM iIi stvarnog pomeranja određenog etalonom (granično merilo, laserski interferometar), predstavlja odstupanje od tačnosti pozicioniranja.

Merenje se vrši u mernom opsegu, duž osa koordinatnog sistema, kako je prikazano na slici 11. Prema ISO standardu, netačnost osnog pozicioniranja se definiše sledećim izrazima:

$$OP_x = H_x + J_x \cdot L_x \leq DOP_x$$
$$OP_y = H_y + J_y \cdot L_y \leq DOP_y$$
$$OP_z = H_z + J_z \cdot L_z \leq DOP_z$$

gde su: OP_i-izmerene vrednosti osnog pozicioniranja, H_i, J_i-konstante osnog pozicioniranja koje definiše proizvođač NUMM, L_i-dužina pomeranja i DOP_i-dozvoljena vrednost odstupanja za osno pozicioniranje.



Slika11.*Šema provere osnog pozicioniranja kao parametra kvaliteta NUMM*

5.2 Vrste provere kvaliteta NUMM

Proizvođač NUMM izdaje atest za novu NUMM, sa tačno definisanim parametrima kvaliteta. Nova NUMM stiže parcijalno rastavljena i propisno upakovana, da ne bi došlo do oštećenja prilikom transporta. Posle odmašćivanja i pripreme delova monter proizvođača izvodi montažu.

Nakon izvršene montaže NUMM, sprovodi se njena obavezna verifikacija. Pri tome je važno naglasiti sledeće: verifikacija se sprovodi od strane tehničkog osoblja proizvođača NUMM, a uz prisustvo predstavnika korisnika I provera karakteristika NUMM vrši se primenom odgovarajuće merne instrumentacije.

Razlikuju se tri vrste provere parametara kvaliteta NUMM: nakon proizvodnje NUMM, prilikom preuzimanja NUMM i periodične provere tokom upotrebe NUMM.

Sve metode za proveru parametara kvaliteta dele se na: standardne metode, metode korisnika NUMM i metode proizvođača NUMM.

1. ZAKLJUČAK

Ulaganje u CAD/CAM rešenja je ozbiljan poduhvat.Odabir odgovarajućeg proizvoda direktno utiče na metode mašiniranja a često određuje produktivnost i profitabilnost određene kompanije.U današnjem svetu proizvodnja je poboljšana lakoćom upotrebe (rada), automatizovanjem, pojednostavljivanjem, inoviranjem (stalnim unošenjem novina) i radom.

Mane današnjih tehnologija u odnosu na nekadašnje tehnologije su male odnosno nikakve. Ali ono što jeste problem kod današnjih tehnologija jeste cena. Cena tehnologija, pri tom računajući u tehnologije kako softverska rešenja tako i tehnička rešenja, je velika. Što je tehnologija mlađa njena cena je veća. To je najveći problem kod današnjih tehnologija.

S druge strane, prednosti koje se dobijaju korišćenjem savremenih tehnologija su ogromne. Lakši je rad sa savremenim tehnologijama, njihov interfejs je poboljšan, komande su olakšane, obuka za rad na novim tehnologijama je kraća itd. Sve ovo ide u prilog današnjem razvitku jer poboljšanje na bilo kom polju skoro da uslovljava poboljšanje na drugim poljima.

Nakon izrade delova dat je prikaz i same numeričke kontrole na numerički upravljanim mernim mašinama, kao i prikaz grešaka rezultata i njihovih potencijalnih izvora, njihova klasifikacija, zatim tačnost merenja i ono najvažnije, parametri kvaliteta na osnovu kojih se vrši samu kontrola.

LITERATURA

[1] Jovanović P. i dr, „Upravljanje razvojnim i investicionim projeketima”, Zbornik radova, Fakultet organizacionih nauka, Beograd, 1996.
[2] Regodić D., Cvetković D., Automatizacija i računarski integrisana proizvodnja, Univerzitet Singidunum, Beograd, 2011.
[3] Cleland, David I. and Roland Gareis „Global Project Management Handbook, Planning, Organizing and Controlling International Projects, second edition”, 2006.
[4] James P.Lewis, „Fundamentals of project management,second edition,„ New York, 2002.
[5] Samardžić G., Mašiniranje složenih delova (Surface machining)”, Kragujevac, 1998.
[6] John Ridley and John Channing, „Safety at work – Seventh edition”, Burlington, 2008
[7] Radivojević G., Miljuš M.,Upravljanje informacijama u logistici – Sistemi za podršku odlučivanju, Beograd, 2002.
[8] Upotreba materijala iz predužeća „Hidromatik d.o.o.” Sremska Mitrovica

INFORMACIONE TEHNOLOGIJE I ENERGETSKA EFIKASNOST KROZ PRIMJENU STANDARDA ISO 50001:2011

INFORMATION TECHNOLOGY AND ENERGY EFFICIENCY BY USING ISO 50001:2011

Momčilo Kokić
MD - Perić Company Bijeljina
Petrove Gore 8, 76300 Bijeljina
Telefon: +387 65 661 385
Fax: +387 55 202 743
E – mail: kokicm@gmail.net

Sažetak
Posmatrajući sa ekonomskog stanovišta, cilj svake ljudske djelatnosti je utrošak što manje resursa za ostvarenje što boljih rezultata. Nema djelatnosti u kojoj se ne koristi određeni vid energije. Smanjenje potrošnje energije utiče na povećanje ekonomičnosti. Efikasno korišćenje energije ima pozitivan doprinos očuvanju životne sredine. Efikasno korišćenje energije podrazumijeva realizaciju niza procesa od definisanja svih potrošača energije, izvora energije do definisanja niza procesa usmjerenih ka smanjenju potrošnje energije. Ostvarenju cilja, efikasna potrošnja energije, veliki doprinos mogu dati savremene informacione tehnologije inkorporisane u procese kroz koje se ostvaruje energetska efikasnot u skladu sa ISO 50001:2011 -Sistem menadžmenta energijom.
***Ključne riječi**: energetska efikasnost, informacione tehnologije, ISO50001.*

Abstrakt
Observing from an economic point of view, the goal of every human activity is the consumption of fewer resources to achieve the best possible results. There is no activity which does not use a specific type of energy. Reducing energy consumption increases efficiency. Efficient use of energy has a positive contribution to the environment. Efficient use of energy is the realization of a number of processes from defining all energy consumers, energy sources to defining a series of processes aimed to reduction energy consumption. The goal, efficient energy consumption, can make a major contribution to modern information technology incorporated into the processes through which the energy efficiency in accordance with ISO 50001:2011 - Energy Management System.
***Keywords**: energy efficiency, information technology, ISO50001.*

1. UVOD

Nema ekonomske aktivnosti bez utroška određenih resursa, odnosno nema ostvarenja ekonomskog cilja bez utroška energije u nekom obliku. Obzirom da su resursi uglavnom ograničeni neophodno je upravljanje resursima. To je posebno važno za one resurse koji su rijetki ili se teško do njih dolazi, koji su skupi ili je njihova proizvodnja povezana sa procesima

koji imaju znatna štetna djelovanja po okolinu. Sve nabrojane osobine ima energija kao resurs, zato je težnja ka efikasnoj proizvodnji i potrošnji energije imperativ današnjice. Da bi se ove težnje ostvarile, u sve procese proizvodnje i potrošnje energije, potrebno je implementirati određene procese koji doprinose ostvarenju postavljenih ciljeva. O kojim procesima je riječ najbolje govori standard ISO 50001:2011. U radu su analizirani procesi koji doprinose energetskoj efikasnosti u skladu sa zahtjevima ISO 50001:2011 i naznačene mogućnosti primjene informaciono komunikacionih tehnologija u tim procesima.

2. ENERGETSKA EFIKASNOST

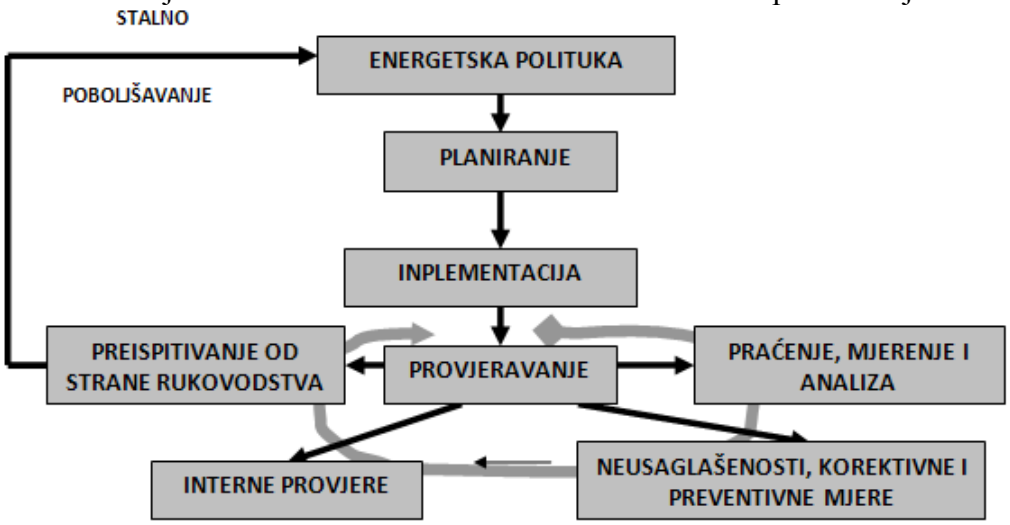
Energetska efikasnost je jedan od osnovnih ekonomskih pokazatelja, a ukazuje na ostvarivanje nekog ekonomskog cilja uz minimalne troškove za energiju, minimalan gubitak energije i minimalno zagađenje okoline. Procesi za ostvarenje energetske efiksnosti moraju obezbijediti optimalanu potrošnju energije za kvalitetno zadovoljenje potreba u pogledu energije uz minimalno zagađivanje okoline. Neki procesi proizvodnje energije su veliki zagađivači okoline.
Upotreba obnovljivih izvora energije ima ključnu ulogu u smanjenju zagađivanja, zato se do 2020. godine u Evropskoj Uniji planira 20% potrošnje energije iz obnovljivih izvora (2005. godine taj udio je bio 8,5%). Na primjer, potencijal obnovljivih energetskih resursa Srbije procenjuje se na više od 4,3 miliona tona ekvivalentne nafte godišnje. [4.]
Mnoge zemlje bilježe rekordan porast upotrebe biomase, najistaknutiji primjer je Švedska kod koje je zabilježen veći udio biomase u ukupnoj energiji nego nafte. [5.]
U današnjem vremenu, vremenu globalne ekonomske krize, cilj poslovnih sistema jeste unapređenje poslovanja uz smanjenje proizvodnih i operativnih troškova u kojima je učešće energije neizbježno. Primjena koncepta energetske efikasnosti, za mnoge sisteme, postaje jedno od glavnih rješenja za efikasnije i bezbolnije prevazilaženje negativnih efekata prouzrokovanih ekonomskom krizom, a suština ovog koncepta je ušteda i smanjenje troškova za energiju. Mnogi veliki poslovni sistemi u svijetu vide svoju veliku šansu za proširenje poslovanja nudeći tržištu proizvode, kako u domenu proizvodnje energije tako isto i u sistemu potrošnje energije, zasnovane na principima energetske efikasnosti. Jedan od poznatih je i konpanija SIMENS.[6.] Oko 40% ukupnog godišnjeg dohodka ove konpanije u 2012. godini otpadalo je na tz. zelene proizvode i tehnologije.[6.]
Energetska efikasnost započinje definisanjem energetske politike. Energetska politika kao dio ukupne ekonomske politike definiše se kroz: načela, ciljeve, zadatke, mjere i instrumente, počevši od istraživanja i razvoja, dobijanja, distribucije i korišćenja energije. Za pdsticanje energetske efikasnosti mogu se koristiti različiti instrumenti politike kao što su: [8.]

- Zakonska regulativa - zakoni, lokalni zakonski i podzakonski akti, standardi, pravila;
- Ekonomske mjere - porezi, subvencije, tarife;
- Istraživanje i razvoj - aktivnosti usmjerene na razne segmente;
- Informisanje i obrazovanje – potrošača energije kako da efikasnije koriste energiju;
- Podaci i statistika - obezbjeđenje podataka i statistike o energiji, itd.

U sprovođenju energetske politike, posebno onog njenog dijela koji se odnosi na sistemski pristup upravljanju energijom, veliki doprinos može dati implementacija standarda ISO 50001-Sistem menadžmenta energijom.

3. ISO 50001- SISTEM MENADŽMENTA ENERGIJOM

ISO 50001 Sistem menadžmenta energijom (*Energy Management System*) je jedan od najnovijih standarda iz oblasti sistema menadžmenta. Nastao je kao odgovor na zahtjeve za očuvanje životne sredine, energetsku efikasnost i održivi razvoj. Sveobuhvatni cilj standarda za sistem menadžmenta energijom ISO 50001:2011 je da se pomogne organizacijama da uspostave sistemski pristup poboljšanju energetske efikasnosti. Standard je primjenljiv na sve vrste organizacija, nezavisno od njihove djelatnosti i veličine. On je namijenjen i za sertifikaciju.[10.] Ovaj standard je kompatibilan sa svim standardima iz oblasti sistema menadžmenta koje je objavio ISO i baziran je na PDCA sistemu. Suština ISO 50001:2011 prikazana je na slici 1.



Slika 1. Model sistema menadžmenta energijom prema standardu ISO 50001

ISO 50001 zahtieva da organizacija utvrdi za koje sve potrebe koristi energiju i u kojim količinama, iz kojih izvora, kao i da definiše mjere za smanjenje upotrebe na prihvatljiv nivo. U standardu se izričito zahtijeva da organizacija utvrdi indikatore preko kojih će pratiti učinak na polju energetske efikasnosti, slično kao što ISO 9001 zahtieva uspostavljanje sistema za praćenje i mjerenje efektivnosti procesa. Zahtjevi ISO 50001 su vrlo slični zahtjevima ostalih standarda iz oblasti sistema menadžmenta i kao minimum podrazumijevaju postojanje: energetske politike, ciljeva, i procedura. [11.]

Implementacijom standarada se postiže sledeće:

- pomaže se organizacijama da bolje koriste svoju opremu koja koristi energiju;
- dobiju se uputstvo za procjenu, mjerenje, dokumentovanje i izvještavanje;
- bezbjeđuje se transparentnost u vezi sa upravljanjem energetskim resursima;
- pruža se okvir za promovisanje energetske efikasnosti kroz lance snabdijevanja;
- omogućavanje unapređenja u upravljanju energijom;
- integracija sa drugim sistemima upravljanja; itd.

Značajne koristi od razvoja i implementacije ISO 50001- sistema za upravljanje energijom su: smanjenje upotrebe energije, kontrola i smanjenje troškova, smanjenje negativnog uticaja na životnu sredinu, priprema za praćenje i izvještavanje o emisiji štetnih gasova, itd.

Za sprovođenje usvojenog sistema menadžmenta energijom, a u cilju ostvarenja energetske efikasnosti veliku pomoć pruža implementacija IT u procese vezane za energetsku efikasnost.

4. INFORMACIONE TEHNOLOGIJE U PROCESIMA OSTVARENJA ENERGETSKE EFIKASNOSTI

Kao i u mnogim drugim procesima i u procesima ostvarenja energetske efikasnosti primjena informacionih tehnologija je neizostavna. Iako u globalnoj emisiji CO_2 učestvuju sa samo 2%, IT su izuzetno bitan faktor u smanjenju negativnih efekata po okolinu. Kada je u pitanju energetska efikasnost, IT imaju mogućnost dvostrukog djelovanja. Prvi put, IT kao efikasni potrošači energije sa minimalnim zagađenjem okoline i drugi put, kao sistemi za podršku procesima ostvarenja energetske efikasnosti od proizvodnje do potrošnje energije. IT kao efikasni potrošač energije smatra se onda kada uz minimalnu potrošnju energije obezbjeđuje maksimalan doprinos sistemima u koje je implementirana. IT industrija se odavno svesrdno uključila u sve procese energetske efikasnosti i zaštite životne okoline kroz realizaciju programa green IT. Među 10 najbolje rangiranih kompanija na svijetu u pogledu zaštite okoline 5 je koje se bave IT i telekomunikacijama, a ostalih 5 su kompanije kod kojih je implementacija IT tehnologija na najvišem nivou, to su finansijske i osiguravajuće institucije.[12.] Sa stanovišta značaja energetske efikasnosti u ovim industrijama to su izuzetni rezultati, ali to nije dovoljno kada je u pitanju globalna energetska efikasnost. Zato, mnoge IT kompanije kombinujući softverske i hardverske proizvode sa IT uslugama nude takozvana Green IT rješenja. Primjeri takvih rješenja su: skalabilni modularni data centri, virtualizacija- servera, memorija i desktopa, cloud kompjuting, itd. Kao kuriozitet IBM ističe da 60% menadžera informacionih sistema (CIO) sada planira da koristi cloud u svojim poslovnim sistemima, što predstavlja porast od 30% u udnosu na dvije godine ranije. [13.] Virtualizacija, SOA (*Service Oriented Architecture*), WOA (*Web Oriented Architecture*) i *Cloud Computing* su uzdanice na savremenom terenu informacionih tehnologija. Njihova implementacija daje značajne rezultate na polju energetske efikasnosti u IT domenu, ali najveći rezultati procesa energetske efikasnosti se očekuju u energetski zahtjevnijim sektorima.

Za moderne nacionalne ekonomije odlučujuću važnost imaju sektori: energetike, saobraćaja, građevinarstva i sirovine kao što su: čelik, aluminijum, cement i papir. Postizanje energetske efikasnosti u ovim sektorima je imperativ nacionalnih ekonomija.

Pa u čemu IT mogu dati doprinos energetskoj efikasnosti u najvažnijim sektorima? Posmatrajući energetsku efikasnost kroz prizmu zahtjeva ISO50001:2011može se zaključiti da je implementacija *Green* IT u procese energetske efikasnosti dvostruko korisna.

Prvo, IT kroz softverska rješenja usklađena sa zahtjevima standarda obezbjeđuju lakšu implementaciju zahtjeva standarda, a dosledna primjena standarda daje mogućnost uštede energije i do 60%. Drugo, implementacija informacionih tehnologija u same procese koji se odvijaju u pojedinim industrijama doprinosi efikasnosti tih procesa. Na primjer, implementacija IT u procese mjeranja, prikupljanja, obrade i distribucije podataka o utrošenoj energiji i načina trošenja energije iz različitih izvora u zgradama višestruko smanjuje gubitke energije, smanjuje potrošnju energenata i štiti okolinu. Implementacija IT u procese ostvarenja energetske efikasnosti u zgradama dovela je do uvođenja pojma pametna građevina-zgrada*(Smart Building)*. Ostvarena energetska efikasnost u zgradama direktno se odražava na potrošnju energije u saobraćaju zbog manjih potreba za putovanjima zaposlenih, kao i na energetsku efikasnost u

procesima proizvodnje, transporta energenata i distribucije energije. Znači, implementacija IT u bilo kome segmentu, proizvodnji, transportu ili potrošnji energije doprinosi energetskoj efikasnosti u svim segmentima.

5. ZAKLJUČAK

Čovječanstvo se mora pomiriti sa činjenicom da nekontrolisanom eksploatacijom neobnovljivih prirodnih resursa ugrožava prirodno okruženje i svoj opstanak dovodi u pitanje. Zato je neophodno shvatiti da su proizvodnja energije iz obnovljivih prirodnih izvora, štednja energije kroz procese optimizacije proizvodnje i korišćenja energije ključ za opstanak i bolju budućnost čovječanstva. Ovakvo ponašanje je prepoznato kao energetska efikasnost. Na putu ka ostvarenju što većeg stepena energetske efikasosti stoji nam mnoštvo alata, a jedan od njih je i ISO 50001:2011. Efikasnoj primjeni ovog i mnogih drugih alata veliki doprinos daju savremene informacione tehnologije te njihovu inkorporaciju u procese menadžmenta energijom treba svesrdno podržavati i unapređivati.

LITERATURA

[1] Balaban N.: *Informacione tehnologije i informacioni sistemi*, Univerzitet u Novom Sadu, Ekonomski fakultet Subotica, Subotica, 2007.

[2] Marković D.: *Procesna i energetska efikasnost*, Univerzitet Singidunum, Beograd, 2010.

[3] Turban, McLean, Wetherbe: *Informaciona tehnologija za menadžment*, John Wiley, prevod 3. izdanje Zavod za udžbenike i nastavna sredstva, Beograd, 2003

[4] „Obnovljivi izvori**",** (pristup 06.02.2013.), [dostupno na http://glassrbije.org/].

[5] „Obnovljiva energija" (pristup 03.02.2013.), [dostupno na http://www.profitiraj.hr/].

[6] http://www.energy.siemens.com, (pristup 03.02.2013.).

[7] http://www.personalmag.rs/ (pristup 23.01..2013).

[8] Mikić M., „Strategija razvoja energetike do 2015", *Build br. 2*, jun 2007., Infonet Group d.o.o. Beograd, (pristup 28.01.2013.), [dostupno na http://www.buildmagazin.com].

[9] Jelena, J., Krivokapić Z., (2012): "Implementacija standarda ISO 50001-Sistem menadžmenta energijom", *Kvalitet i izvrsnost*, Godina I- Broj 7-8/2012, 24-29, FQCE-Beograd.

[10] „ISO 50001:2011 i EN 16001:2009 (pristup 01.02.2013. [dostupno na http://victoriaconsulting.co.rs].

[11] „ISO 50001 Sistem menadžmenta energijom", (pristup 01.02.2013.) [dostupno na http://www.tdconsulting.rs/].

[12] „Green rankings 2012 global 500 list", (pristup 06.02.2013.), [dostupno na http://www.thedailybeast.com/newsweek/].

[13] IBM: "Reinvent your business with the power of cloud computing", (pristup 08.02.2013.), [dostupno na http://www-935.ibm.com/services].

INTEGRISANI SISTEM ZAŠTITE I SPASAVANJA U VANREDNIM SITUACIJAMA

INTEGRATED PROTECTION AND RESCUE SYSTEM IN EXTRAORDINARY SITUATIONS

Branko Babić
Visoka tehnička škola strukovnih studija u Novom Sadu
Školska broj 1
Telefon: +381 69 4892 540
Fax: +381 21 4892 500
E – mail: babic@vtsns.edu.rs

Sažetak
Donošenje Zakona o vanrednim situacijama i Zakona o zaštiti od požara, krajem 2009. godine, doprinelo je povećanju bezbednosti građana i materijalnih dobara imajući u vidu činjenicu da je u poslednjih 30 godina višestruko povećan broj katastrofa kao i njihov razarajući efekat na društvo i okolinu. Najsnažnije i najviše su pogađane zemlje u razvoju koje su najranjivije i imaju najmanje kapaciteta da se sa njima izbore. Doneti zakoni su usklađeni sa najvišim standardima Evropske unije i omogućavaju formiranje jedinstvene službe za zaštitu i spasavanje i integrisanog sistema upravljanja u vanrednim situacijama koji obuhvata spremnost, ublažavanje, prevenciju i ima za cilj jačanje otpornosti na vanredne situacije.
Ključne reči: integrisani sistem, vanredne situacije, snage i sredstva sistema

Abstract
Passing the Emergency Management Law and Fire Protection Law in 2009 raised the level of security of population and material goods bearing in mind that the number of catastrophes and their devastating effects on society and environment has multiplied in the last thirty years. The biggest impact was with the developing countries as they are the most vulnerable and unable to cope with them. The passed Laws are in accordance with the highest standards of the European Union and enable the formation of a unique protection and rescue service and an integrated system of control in extraordinary situation that includes preparedness, mitigation and prevention, and its goal is to strengthen resistance to extraordinary situations.
Keywords: integrated system, extraordinary situations, system strength and resources

1. UVOD

U okviru Ministarstva unutrašnjih poslova, 2006. godine formirana je posebna organizaciona celina ***Sektor za zaštitu i spasavanje*** koji je direktno bio odgovoran ministru unutrašnjih poslova. U okviru Sektora prvobitno je formirana Uprava za preventivu, Uprava za vatrogasno-spasilačke jedinice i Glavni trening centar. Na osnovu urađene analize organizacije službi za zaštitu i spasavanje, koja je pokazala da u 26 evropskih država ova Služba funkcioniše kao nezavisna u okviru Ministarstva unutrašnjih poslova, doneta je odluka da se postojeći Sektor za

zaštitu i spasavanje reorganizuje u **Sektor za vanredne situacije**. Sektor za vanredne situacije dobija još dve nove uprave - Upravu za upravljanje u kriznim situacijama i Upravu za civilnu zaštitu. Takođe, Sektor postaje glavni nosilac i koordinator aktivnosti u oblasti vanrednih situacija u Republici Srbiji čime se počeo stvarati **integrisani sistem zaštite i spasavanja**. Glavni zadaci Sektora za vanredne situacije su prevencija, spasilačke aktivnosti, upravljanje zaštitom u vanrednim situacijama, koordinacija između republičke i lokalne uprave i drugih organizacija, sprovođenje mera na otklanjanju posledica vanrednih situacija, pripremanje građana za vanredne situacije, opremanje i obučavanje operativnih jedinica, nadzor, informisanje o događajima i međunarodna saradnja. Na ovaj način je izvršen prelazak na novi sistem upravljanja i reagovanja u vanrednim situacijama u Srbiji. Ministarstvo odbrane R.Srbije je do donošenja Zakona o vanrednim situacijama [1.] bilo nosilac aktivnosti civilne zaštite, upravljanja i reagovanja na vanredne situacije.

2. POTREBNI USLOVI ZA FORMIRANJE INTEGRISANOG SISTEMA ZAŠTITE

Da bi se što pre ustrojio i formirao integrisani sistem zaštite i spasavanja u vanrednim situacijama bilo je potrebno stvoriti potrebe uslove. Prioritetni uslov je bio hitno usvajanje **Zakona o vanrednim sutuacijama** [1.] koji će obezbediti stvaranje pravne osnove za uvođenje novog sistema zaštite u vanrednim situacijama. Ovaj zakon će omogućiti uspostavljenje jedinstvenog sistem za organizovan odgovor u vanrednim situacijama jer prethodni zakon iz 1977. godine na to nije mogao odgovoriti. Paralelno sa usvajanjem zakonske regulative bilo je neophodno i pristupiti izradi **Nacionalne strategije za zaštitu i spasavanje u vanrednim situacijama** [2.] čiji je cilj da stviri povoljne uslova za brzo reagovanje i spasavanje lica i imovine, da omogući izradu planova delovanja u vanrednim situacijama i sprovodjenje mera pre, tokom i posle vanrednih situacija i da omogući angažovanje građana na planu zaštite. U skladu sa novim zakonskim rešenjima neophoodna je izmena postojećih **Zakona o odbrani i Zakona o vojsci**, kao i unošenje izmena u **Strategiju nacionalne bezbednosti** i **Strategiju odbrane** [4.] i sve druge zakone po sektorima, čije su izmene potrebne da bi novouspostavljeni sistem reagovanja u vanrednim situacijama zaživeo. Učešće u **aktivnostima međunarodnih institucija** i organizacija je jedan od presudnih uslova. Republika Srbija na polju vanrednih situacija ima potpisane brojne međunarodne sporazume i članica je Inicijative za prevenciju i spremnost za vanredne situacije (DPPI[71]) regionalne inicijative koja funkcioiše pod okriljem Regionalnog saveta za saradnju i čiji je glavni cilj saradnja država Zapadnog Balkana i prevenciji i reagovanju na prirodne katastrofe. Očekuje se **formiranje operativnog centra za dojavu svih vanrednih događaja (112)**, čilj je cilj lakša komunikacija sa organima za delovanje u svim situacijama I eliminisanje slabosti iz prethodnog sistema jer se jako malo pažnje posvećivalo komunikaciji sa javnošću. Od presudnog značaja za efikasno funkcionisanje sistema za upravljanje vanrednim situacijama je i saradnja i komunikacija između ministarstava, službi Vlade, **sa NVO i lokalnom samoupravom**. **Komunikacija i informisanje** jednako su važni kako u fazi pripreme zakona i podzakonskih akata, tako i u fazi implementacije usvojenih propisa. Ministarstvo unutrašnjih

[71] Misije i organizacije u kojima još učestvuje Sektor za zaštitu i spasavanje su: EUROPA - Saveta Evrope, Saveta za regionalnu saradnju za region jugoistočne Evrope, Međunarodna strategija za smanjenje posledica vanredne situacije Ujedinjenih nacija (UNISDR), Program razvoja pri Ujedinjenim nacijama (UNDP), UN biro za humaniratne poslove (UN-OCHA), Civilno vojno planiranje u vanrednim situacijama (CMEP), Partnerstvo za mir PfP, Balkanska vatrogasna sportska federacija (BFSF), USAID, OSCE, ICDO i dr.

poslova treba da identifikuje potencijalne partnere i obezbedi ekspertsku podršku u procesu edukacije lokalne samouprave i građana o novom institucionalnom mehanizmu kojim se uspostavlja novi sistem upravljanja i reagovanja u vanrednim situacijama. **Podizanje nivoa svesti kod građana o značaju i ozbiljnosti vanrednih situacija** ali i o njihovoj ličnoj ulozi i saradnji sa državnim organima u ovakvim situacijama je od izuzetnog značaja. Novi sistem upravljanja i reagovanja u vanrednim situacijama treba da dostigne nivo efikasnosti koji postoji u evropskim državama. Zbog klimatskih promena, biće sve više I više novih tipova virusa, što će biti najveća pretnja u narednim godinama. Svetska zdravstvena organizacija je uvela stepenovanje opasnosti, tako da se sada tačno zna na kom nivou je epidemija i da li se drži pod kontrolom. Srbija nema te kapacitete ali je stvaranje novog institucionalnog I zakonskog okvira za reagovanje u vanrednim situacijama prilika da se postojeće manjkavosti isprave i sistem uobliči tako da **odgovara standardama koji postoje u EU,** kao i potrebama sopstvenih građana. **Pitanje finansiranja sistema za zaštitu i spasavanje** u vanrednim situacijama u prethodnom period je bilo iz vojnog budžeta-samo 0,08 %. Sa izmenama u nadležnostuma preispitaće se postojeći i uspostaviti novi okvir i osnov za finansiranje nadležnosti iz ove oblasti koje prelaze iz resora odbrane u resor unutrašnjih poslova.
Zaključak Radne grupe koja je radila na uspostavljanju novog sistema zaštite I spasavanja je bio da nebriga države i neadekvatan tretman sistema, koji treba pre svega da prevenira nastanak vanrednih situacija I katastrofa, ne samo ugrožava elementarnu bezbednost građana, već dugoročno posmatrano proizvodi rizik za nastanak štete koja je uvek desetostruko veća od ulaganja u prevenciju.

3 NACIONALNA STRATEGIJA ZA ZAŠTITU I SPASAVANJE U VANREDNIM SITUACIJAMA

Skupština Srbije je 05.10. 2011. godine prihvatila Nacionalnu startegiju za zaštitu i spasavanje u vanrednim situacijama [2.] prouzrokavanih prirodnim nepogodama ili ljudskim faktorom. Svrha strategije je zaštita života, zdravlja i imovine građana, životne sredine i kulturnog nasleđa. U tom dokumentu se navodi da će uvođenje univerzalnog broja „112 za hitne pozive" u Srbiji obezbediti koordiniranu, bržu i efikasnu intevenciju i pomoć u vanrednim situacijama, događajima i katastrofama u skladu sa standardom i praksom u zemljama EU. Taj dokument definiše i određuje mehanizme koordinacije i smernice programa za smanjenje katastrofa izazvanih prirodnim pojavama i opasnosti od nesreća, kao i zaštitu, odgovor i sanaciju posledica. Kao nedostaci potojećeg sistema navode se nepostojanje sveobuhvatnih mapa rizika, zastarela i nepouzdana oprema, sredstva i vozila za reagovanje u vanrednim situacijama, nedovoljna koordinacija i saradnja, nedovoljna obučenost i nerazvijena kultura prevencije. U strategiji je ukazano da je koordinacija među hitnim službama - policija, vatrogasci i hitna pomoć nedovoljno efikasna i da u Srbiji ne postoji jedinstven broj koji građani mogu da pozovu u hitnim situacijama. **U cilju razvoja integrisanog sistema zaštite i spasavanja**, neophodno je veće tehničko inoviranje i opremanje, kao i unapređenje infrastrukturnog, informacionog i tehnološkog sistema uz primenu savremenih tehnologija i standarda EU. Sistem obuke za reagovanje u vanrednim situacijama treba proširiti, modernizovati i poboljšati jer postojeći ne može na adekvatan način da odgovori svim zahtevima integrisanog sistema upravljanja u oblasti vanrednih situacija. Daljem razvoju i poboljšanju integrisanog sistema zaštite i spasavanja doprinosi podsticanje nevladinih, neprofitnih organizacija i građana na obrazovanje za postupanje pre, tokom i posle vanrednih situacija. U dokumentu se upozorava da je region

Jugoistočne Evrope sve više ugrožen poplavama, sušom, ekstremnom vrućinom, zemljotresima, klizištima i olujama. Vlada je odgovorna za sve apsekte upravljanja vanrednim situacijama, a odgovornost za planiranje i sprovođenje preventivnih mera i otklanjanje posledica zajednička za organe državne uprave, autonomne pokrajina i jedinice lokalne samouprave. Predviđeno je donošenje akcionog plana za sprovođenje strategije koje će pratiti Republički štab za vanredne situacije, o čemu će objavljivati godišnje izveštaje koji će biti javni. Realizacija strategije finansiraće se sredstvima iz državnog budžeta i Budžetskog fonda za vanredne situacije. Prilikom izrade strategije uzete su u obzir Strategija unutrašnje bezbednosti EU i Strategija EU za podršku smanjenju rizika od katastrofa u zemljama u razvoju, a jedan od prioriteta je uključivanje Srbije u Mehanizam civilne zaštite EU.

4. ZAKLJUČAK

Za uspešno funkcionisanje integrisanog sistema zaštite u vanrednim situacijama neophodno je formirati štabove za vanredne situacije, izraditi planove zaštite i izvršiti edukacija subjekata sistema zaštite i spasavanja. Proces formiranja je dug i teče uz manje ili veće poteškoće što negativno utiče na bezbednost građana i povećava rizik od vanrednih situacija. Za koordinaciju i rukovođenje zaštitom i spasavanjem građana, obrazovani su štabovi za vanredne situacije [5.], od republičkog do opštinskog nivoa (obrazovanje završeno do polovine marta 2011. godine). Štabovi rukovode i koordiniraju rad subjekata i snaga sistema zaštite i spasavanja; rukovode i koordiniraju sprovođenje mera i zadataka civilne zaštite; prate stanje i organizaciju zaštitu i spasavanja i predlažu mere za njihovo poboljšanje; naređuje upotrebu snaga, sredstava pomoći i drugih sredstava koja se koriste u vanrednim situacijama; razmatraju organizaciju, opremanje i obučavanje jedinica civilne zaštite, ovlašćenih, osposobljenih pravnih lica; sarađuju sa nadležnim organima zaštite i spasavanja susednih država u vanrednim situacijama [2]. Članove Republičkog štaba za vanredne situacije imenovala je Vlada R.Srbije [6.], iz reda rukovodilaca državnih organa u čijem delokrugu su poslovi od značaja za zaštitu i spasavanje, stručnih radnika Ministarstva, Vojske Srbije, Crvenog krsta Srbije, Gorske službe spasavanja Srbije, direktora javnih preduzeća u oblasti saobraćaja, šumarstva i vodoprivrede i rukovodilaca drugih organa, organizacija i ustanova čiji su poslovi u vezi sa zaštitom i spasavanjem. Uredbom o sadržaju i načinu izrade planova zaštite i spasavanja [7.] uređen je sadržaj i način izrade Nacionalnog Plana zaštite i spasavanja u vanrednim situacijama na nivou R.Srbije i Plan zaštite i spasavanja organa državne uprave, autonomnih pokrajina, jedinica lokalne samouprave, privrednih društava i drugih pravnih lica, i drugih organizacija. Nacionalni plan ima cilj: da definiše rizike; da planira preventivne i operativne mere za sprečavanje i umanjenje posledica elementarnih nepogoda, tehničko-tehnoloških nesreća - udesa i katastrofa; da planira snage i sredstva subjekata sistema zaštite i spasavanja; da planira njihovo organizovano i koordinirano angažovanje i delovanje u vanrednim situacijama u cilju zaštite i spasavanja ljudi, materijalnih i kulturnih dobara i obezbeđenja osnovnih uslova za život. Plan se izrađuje se na osnovu Procene ugroženosti (rok za izradu-februar 2012. godine na nivou R.Srbije, odnosno oktobra za jedinice lokalne samouprave i decembar 2011. godine za Autonomne pokrajine). Da bi formirani sistem imao uspeha u rukovođenju rizikom u vanrednim situacijama, neophodno je izvršiti edukaciju stanovništva u cilju sticanja potrebnih znanja za preventivnu zaštitu iz oblasti lične i kolektivne zaštite. Po odgovarajućem programu, obučavanje će se vršiti i u okviru osnovnog i srednjeg obrazovanja radi sticanja znanja o opasnostima od prirodnih i drugih nesreća i zaštiti od njih [1.].

LITERATURA

[1.] Zakon o vanrednim situacijama, "Službeni glasnik Republike Srbije" broj 111/2009
[2.] Nacionalna startegija za zaštitu i spasavanje u vanrednim situacijama,"Službeni glasnik Republike Srbije", br. 86/2011
[3.] Strategija nacionalne bezbednosti Republike Srbije, "Službeni glasnik Republike Srbije" broj 88/2009
[4.] Strategija odbrane Republike Srbije, "Službeni glasnik Republike Srbije" broj 88/2009
[5.] Uredbova o sastavu i načinu rada štabova za vanredne situacije, "Službeni glasnik Republike Srbije" broj 98/2010
[6.] Odluka o obrazovanju Republičkog štaba za vanredne situacije, "Službeni glasnik Republike Srbije" broj 32/2011
[7.] Uredba o sadržaju i načinu izrade planova zaštite i spasavanja, "Službeni glasnik Republike Srbije" broj 8/2011

UNAPREĐENJE KVALITETA NASTAVE KORIŠĆENJEM SOFTVERSKIH POSLOVNIH SIMULACIJA

IMPROVING EDUCATION QUALITY USING SOFTWARE BUSINESS SIMULATIONS

Marko Marković
Poslovni fakultet Valjevo, Univerzitet Singidunum
Železnička 5, 14000 Valjevo
Telefon: +38114-292-610
Fax: +38114-292-611
E-mail: mmarkovic@singidunum.ac.rs
Boško Nikolić
Elektrotehnički fakultet Beograd, Bulevar kralja Aleksandra 73, 11120 Beograd
Telefon: +38111-3218-392
Fax: +38111-324-8681
E-mail: bosko.nikolic@etf.bg.ac.rs

Ovaj rad je delimično finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije (TR32054).

Apstrakt
Zbog velikog značaja za unapređenje kvaliteta nastave u oblasti poslovnog odlučivanja u obrazovnim ustanovama, do sada je razvijen veliki broj softverskih simulatora. Upravo se zbog toga ukazala potreba da se u ovom radu simulacije predstave kao jedno od najmodernijih rešenja u obrazovanju uz prikaz načina na koje se mogu primeniti u nastavi. Predstavljen je i opis simulatora razvijenog da pomogne izučavanje oblasti poslovnog odlučivanja na Poslovnom fakultetu Valjevo Univerziteta Singidunum u cilju razumevanja načina funkcionisanja određenih algoritama mašinskog učenja koji se koriste u ovoj oblasti.
Ključne reči: softverske poslovne simulacije, poslovno odlučivanje, mašinsko učenje

Abstract
Because of great importance in improving business decision making teaching process in educational institutions, there is a large number of software simulators developed. Based on that information, it was necessary to present simulations as one the most modern educational solutions, with possibilities of their usage. The basic features of a software system developed to support the teaching of business decision making and machine learning algorithms used in this field at the the Singidunum University Faculty of Business Valjevo, have been presented in the paper.
Keywords: software business simulations, business decision making, machine learning

1. UVOD

Savremeno poslovanje se ne može ni zamisliti bez procesa poslovnog odlučivanja, a primena savremenih tehnologija se u tu svrhu nameće kao obavezan alat. S obzirom na to da je ova oblast

zbog velike ekspanzije sve interesantnija za proučavanje, posvećuje joj se i sve više pažnje u edukativnom smislu. Razvija se sve više tehnika za njeno lakše izučavanje, a softverski sistemi su upravo jedna od njih. Zbog toga je u ovom radu detaljno obrađena primena takvog softvera u edukaciji. Tačnije, obrađeni su softverski poslovni simulatori. Ovaj pristup je sve popularniji jer omogućuje učesnicima potpuno aktivan pristup učenju u okviru kontrolisanog i bezbednog okruženja.

Korišćenjem softverskih simulacija moguće je koristiti modele situacija iz realnog sveta uz strogo definisane uloge svih učesnika u okruženju bogatom parametrima koji pomažu u donošenju poslovnih odluka. Na ovaj način je moguće steći praktičan uvid u način funkcionisanja poslovnih procesa u modernom preduzeću.

Upravo zbog navedenih prednosti korišćenja softverskih simulacija, na Poslovnom fakultetu Valjevo Univerziteta Singidunum razvijen je Sistem za simulaciju algoritama poslovnog odlučivanja (SAPO) koji je i predstavljen u ovom radu. Simulator je zamišljen da studente zainteresuje za poslovno odlučivanje i da im omogući dalje usavršavanje u ovoj oblasti.

2. ULOGA INFORMACIONIH TEHNOLOGIJA U SAVREMENOM POSLOVNOM ODLUČIVANJU

Savremeno poslovanje se u velikoj meri oslanja na korišćenje modernih tehnologija, tako da se u informacionim sistemima prikupljaju ogromne količine podataka. Da bi ovi podaci postali upotrebljivi za donošenje odluka, koriste se tehnike *data mining*-a koje predstavljaju skup metoda pomoću kojih računari trebaju da podrže rešavanje problema pomoću analiziranja (učenja) postojećih podataka. Naravno, ovaj posao nije jednostavan. Za ove potrebe, koriste se algoritmi mašinskog učenja.

Kompanije idu i korak dalje u prikupljanju informacija pa se, na primer, prilikom kupovine generišu informacije o proizvodu koji je potrošač naručio, broju platne kartice, veličini porudžbine i vremenskom intervalu između prethodne i trenutne narudžbine. Transakcije obavljene putem interneta mogu da pruže još više informacija, obzirom da potrošač prilikom kupovine ostavlja niz podataka o sebi i svojim navikama, a podaci u vezi sa transakcijama potrošača lako mogu biti povezani i sa podacima o ponašanju prilikom pretrage veba. Niz podataka o istoriji kupovine putem interneta, finansijskoj istoriji i drugi lični podaci o potrošaču samo su nekoliko klikova mišem daleko. Kao što je navedeno, prvi korak procesa *data mining*-a je upravo prikupljanje ovakvih podataka o ponašanju potrošača, bilo da su izvor internet transakcije, kupovina u prodavnici ili se koriste neki drugi izvori podataka o korisniku.[72]

3. SOFTVERSKE POSLOVNE SIMULACIJE U POSLOVNOM ODLUČIVANJU

3.1. Istorijat softverskih poslovnih simulacija

Od sredine 1950-ih godina, upotreba softverskih poslovnih simulacija je u stalnom porastu. Danas je ovaj metod izvođenja nastave dostigao visok stepen upotrebe na mnogobrojnim univerzitetima. Iako postoje zapisi o borbenim igrama u Kini, 3000. godine pre nove ere, prva moderna softerska poslovna simulacija je predstavljena tek 1955. godine. Radi se o simulacionoj vežbi *Monopologs* koja se fokusirala na sistem logističke podrške vazduhoplovstva SAD-a, a

[72] Pražić J., Bukvić B., Torbica V., Šćepanović I. (2010): Marketing informacioni sistemi, Novi Sad: Fakultet za menadžment, p. 4.

razvila ju je *Rand* korporacija. Zadatak učesnika bio je da rukovode lancem snabdevanja i po strukturi je bio sličan onome što nude savremena rešenja.[73]
Brz porast broja poslovnih simulacija desio se između 1958. i 1961. godine. Procenjuje se da je do 1961. godine razvijeno preko 100 rešenja i da ih je koristilo više od 30000 rukovodilaca iz raznih kompanija. Do 1969. godine broj simulacija je porastao na oko 200. Neprestani porast je, još u to vreme, ukazivao na sve veću popularnost ove oblasti.[74]
Brz razvoj oblasti simulacija koje se koriste u edukaciji doveo je do sve veće potražnje za složenim rešenjima. Zahvaljujući tome, danas postoji izuzetno veliki broj modela za razne oblasti. Sve veći broj obrazovnih ustanova se opredeljuje da svojim studentima na ovaj način obezbedi praktično razumevanje oblasti kojima se bave.

3.2. Korisnost softverskih simulacija

Simulacija se definiše kao interaktivna apstrakcija realnog života, ili kao bilo koji pokušaj da se oponaša neko okruženje ili sistem.[75] Praktično, simulacije predstavljaju vežbe u okviru kojih se moraju primeniti određena znanja, veštine i strategije u cilju ispunjavanja određenog zadatka. One predstavljaju igre otvorenog kraja u kojima se kroz određene situacije prolazi korišćenjem mnogobrojnih promenljivih. Potrebno je da svaki učesnik, preuzimanjem određene uloge, prouči određena stanja, pretnje ili probleme, da na osnovu toga donese određene odluke, kao i da vidi efekte svojih odluka. Simulacija se može odvijati u raznim pravcima, u zavisnosti od odluka koje su preduzimane.
Simulacije su posebno korisne u objašnjavanju složenih poslovnih situacija koje se mogu javiti u praksi jer predstavljaju *aktivan* edukativni alat. One predstavljaju kontrolisano okruženje u kome ne postoji rizik od pravljenja štete. Zahvaljujući tome, studenti mogu razumeti veze između svojih poteza i njihovih efekata na funkcionalne oblasti u okviru preduzeća.
Svakako, uz odgovarajući način korišćenja, simulacije predstavljaju izvanredan metod elektronskog učenja koji čini osnovu modernog obrazovanja. Na ovaj način se može podstaći aktivniji rad studenata, pri čemu će im biti omogućeno da uče iz ličnog iskustva. Praktično, pruža im se mogućnost da se nađu u realnim situacijama koje ih mogu očekivati i na radnom mestu. Tokom rada, nastavnik ima tačan uvid u sve aktivnosti što mu omogućava da se u svakom trenutku uključi i usmeri učesnike ukoliko naiđu na problem.
Kako bi sama simulacija bila na najbolji način prilagođena učesnicima, potrebno je voditi računa o njenoj kompleksnosti. Potrebno je uvideti vezu između složenosti igre i percepcije stvarnosti. Ukoliko je simulacija suviše jednostavna, biće shvaćena kao nerealna, pogotovo od strane učesnika koji su napredniji po nivou znanja. Sa druge strane se nalaze izuzetno složene igre, za koje se može reći da su izuzetno realistične. Ali, u slučajevima da je složenost igre na većem nivou od pripremljenosti njenih učesnika, može se raširiti stav da je nerealna upravo zato što je izvan njihovih mogućnosti.[76] Potpuno realistična simulacija ozbiljnog preduzeća bi imala

[73] Faria J. A., Nulsen R. (1996):, "Business simulation games: Current usage levels", Developments in Business SImulation & Experiental Exercieses, p. 22.
[74] Faria. J. A (1990): "Business Simulation Games After Thirty Years", Guide to Business Gaming and Experiental Learning, p. 37.
[75] Gibson D., Aldrich C., Prensky M. (2007): Games and Simulations in Online Learning, Hershey: Information Science Publishing, p. 4.
[76] Dittrich J. E. (1977): Realism in Business Games: A Three Game Comparison, Lexington, Kentucky: University of Kentucky, p. 273.

ogroman broj promenljivih i stoga bi sigurno bila nepraktična. Zbog toga njihov broj treba ograničiti na neku razumnu meru. Sa druge strane, simulaciji je potrebno dati više dinamike – zbog toga se u igru mogu postepeno uvoditi, na primer, nova tržišta ili novi proizvodi.

3.3. Značaj vizuelnih softverskih simulacija u poslovnom odlučivanju

Postoji drevna kineska poslovica koja glasi: *Reci mi - zaboraviću, pokaži mi – zapamtiću, uključi me – razumeću.* Ova tvrdnja se pokazuje posebno istinitom u oblasti kao što je poslovno odlučivanje. Korisnici mogu razumeti kako određena tehnika radi ukoliko im se da odgovarajuća literatura, ili na tabli ispiše postupak rešenja nekog primera. Ali, ukoliko im se omogući da to sami isprobaju i da se uključe, onda mogu razumeti mnogo lakše, ali i bolje.

Softverske poslovne simulacije u poslovnom odlučivanju su značajan metod praćenja i razumevanja poslovnih procesa u modernom preduzeću. Zahvaljujući njima, podstiče se razvijanje preduzetničkih stavova i učenje tehnika savremenog menadžmenta. Za studente je stvorena mogućnost da postanu, na primer, poslovni menadžeri koji moraju da donose odluke u strogim tržišnim uslovima. Preuzimanjem takve uloge, učesnik se nalazi u situaciji u kojoj je neophodno preuzeti finansijski rizik sopstvenih odluka - upravo zbog ovog razloga je korišćenje simulacija značajno.[77]

U današnje vreme, simulacije zauzmaju sve važnije mesto u nastavi. Jedna od vodećih strukovnih organizacija, *ACM*, preporučuje korišćenje odgovarajućeg softvera na laboratorijskim vežbama u oblasti računarskog inženjerstva kao izuzetno važnog načina da se studentima omogući da prate, istražuju i rukuju karakteristikama i ponašanjima uređaja, sistema i procesa. Preporučuje se korišćenje aplikacija i simulacija u cilju modelovanja i proučavanja realnih sistema koje nisu praktični za fizičku implementaciju.[78] Pogodne oblasti za ovakvu primenu su i poslovno odlučivanje i mašinsko učenje, tako da se svi navodi vezani za računarsko inženjerstvo i korišćenje simulacija mogu primeniti i u ovom slučaju.

4. OPIS SOFTVERSKOG SIMULATORA RAZVIJENOG NA POSLOVNOM FAKULTETU VALJEVO

Postoji dosta softverskih simulatora razvijenih da pomognu učenje algoritama mašinskog učenja u oblasti poslovnog odlučivanja. Međutim, svaki od njih je razvijen sa ciljem da zadovolji veoma specifične zahteve. Zato je nakon sprovedene analize dostupnih simulatora, na Poslovnom fakultetu Valjevo razvijen sistem koji će pomoći u motivisanju studenata i usmeravanju njihovog razmišljanja i ambicija u ovoj oblasti.

Sistem za simulaciju algoritama poslovnog odlučivanja (SAPO) je podeljen na četiri logičke celine - modula. Svaki od modula zadužen je za simulaciju jednog algoritma, a obrađeni su stabla odlučivanja (ID3), klasterovanje (k-means), Naive Bayes i perceptron. Prvi korak u radu sa simulatorom je izbor korisnika koju simulaciju želi da pokrene. Nakon izbora, učitava se odgovarajuća radna površina, kao i potrebne linije sa alatkama.

Za simulaciju svakog algoritma, prilagođena je posebna radna površina, u skladu sa potrebama tog algoritma. Površina se sastoji od obaveznih delova, kao što su grafički prikaz simulacije i okvir za ispis poruka, i neobaveznih delova, kao što su polje za prikaz početnog skupa podataka, polja za unos dodatnih podataka itd.

[77] Wawer M., Milosz M., Muryjas P., Rzemieniak M. (2010): "Business Simulation Games in Forming of Students' Enterpreneurship", International Journal of Euro-Mediterranean Studies, p. 49.

[78] ACM (2004): "Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering", (pristup: 13.2.2013.), [dostupno na http://www.acm.org/education/education/curric_vols/CE-Final-Report.pdf]

Opcije pomoću kojih se korisniku omogućava postupno kretanje kroz algoritam su: napred, nazad – pokretanje algoritma za jedan korak unapred ili unazad, respektivno; na početak – izvršenje algoritma se vraća na početak; na kraj – simulacija prelazi na poslednji korak algoritma.
SAPO sistem omogućava korisnicima da vide kako određeni algoritmi poslovnog odlučivanja rade. Moguće je zadati ulazni skup podataka i na njega primeniti izabrani algoritam, a potom, korak po korak, pratiti na koji način se izvršava. Tokom same simulacije, prikazuju se detaljne informacije o tome u kojoj se trenutno fazi nalazi algoritam kako bi se lakše razumeo način njegovog rada. Zahvaljujući postupnom prikazu rada algoritama i njihovoj odgovarajućoj vizuelnoj prezentaciji olakšano je razumevanje načina rada algoritama mašinskog učenja.

5. ZAKLJUČAK

U ovom radu predstavljena je oblast softverskih poslovnih simulacija u oblasti poslovnog odlučivanja, a prikazani su i njihov značaj i primene u edukaciji. Objašnjeno je i zašto su simulacije pogodne za prikazivanje modela iz realnog sveta. Kao primer njihovog korišćenja, prikazan je sistem razvijen na Poslovnom fakultetu Valjevo Univerziteta Singidunum. Ovaj sistem omogućava korisnicima da vide kako određeni algoritmi poslovnog odlučivanja rade. Moguće je zadati ulazni skup podataka i na njega primeniti izabrani algoritam, a potom, korak po korak, pratiti na koji način se izvršava. Tokom same simulacije, prikazuju se detaljne informacije o tome u kojoj se trenutno fazi nalazi algoritam kako bi se lakše razumeo način njegovog rada.

LITERATURA

[1] Pražić J., Bukvić B., Torbica V., Šćepanović I. (2010): Marketing informacioni sistemi, Novi Sad: Fakultet za menadžment
[2] Faria J. A., Nulsen R. (1996):, "Business simulation games: Current usage levels", Developments in Business SImulation & Experiental Exercieses
[3] Faria. J. A (1990): "Business Simulation Games After Thirty Years", Guide to Business Gaming and Experiental Learning
[4] Gibson D., Aldrich C., Prensky M. (2007): Games and Simulations in Online Learning, Hershey: Information Science Publishing
[5] Dittrich J. E. (1977): Realism in Business Games: A Three Game Comparison, Lexington, Kentucky: University of Kentucky
[6] Wawer M., Milosz M., Muryjas P., Rzemieniak M. (2010): "Business Simulation Games in Forming of Students' Enterpreneurship", International Journal of Euro-Mediterranean Studies
[7] ACM (2004): "Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering", (pristup: 13.2.2013.), [dostupno na http://www.acm.org/education/education/curric_vols/CE-Final-Report.pdf]

PREGLED KARAKTERISTIKA I OSNOVNIH ZAHTEVA 4G MREŽA

Suzana Miladić
Saobraćajni fakultet Doboj
E-mail: miladics@hotmail.com

Sažetak
Četvrtu generaciju IP umrežavanja karakteriše ogroman rast mobilnog širokopojasnog pristupa, video usluge, globalni roaming i mogućnost povezivanja raznovrsnih uređaja. 4G mreže su heterogene mreže bazirane na IP protokolu koje omogućavaju korisnicima isporuku svih servisa koje moderne telekomunikacije mogu da ponude. U radu su u kraćim crtama predstavljene karakteristike i dva osnovna zahteva u razvoju ove mrežne infrastrukture, a to su obezbeđenje sigurnosti i kvaliteta servisa.
Ključne reči: 4G sistem, sigurnosni zahtevi, QoS

Apstract
The fourth generation telecommunications networks are characterized by tremendous growth in mobile broadband, video services and the ability to connect various devices. 4G networks are heterogeneous networks based on IP protocol, allowing users to deliver all the services that modern telecommunications can offer. In short, the review outlines the characteristics and the two main requirements in the development of heterogeneous network infrastructures, to ensure the safety and quality of service.

1. UVOD

Stalna potreba korisnika za sve većim brzinama prenosa podataka i kvalitetom servisa uslovljava mobilne operatere da unaprede postojeće mreže, što predstavlja skup i složen posao pri čemu bi trebalo obezbediti povezanost sa postojećim GSM/EDGE i WCDMA/HSPA sistemima [4.]. Zbog toga je sadašnja arhitektura mreža kompleksna i različita kod raznih operatera. Sledeće generacije mreža treba da omoguće IP bazirane servise (govor, video, multimedija, podaci...) za sve vrste korisničkih terminala dok se kreću između fiksnih (optika, DSL, kabl) i bežičnih tehnologija pristupa (baziranih na 3GPP, 3GPP2, IEEE), kao i roming između mreža različitih operatera [5.].
U telekomunikacijama, 4G je četvrta generacija standarda mobilnih mreža. Za razliku od 3G sistema koji se baziraju na razvoju novih standarda i hardvera, 4G sistemi podrazumevaju integraciju postojećih bežičnih tehnologija [6.]. Ovim radom su obuhvaćene telekomunikacione mreže četvrte generacije koje predstavljaju otvoreno okruženje gde različite bežične tehnologije i provajderi usluga dele IP bazirano jezgro mreže da bi obezbedili neprekidnu uslugu svojim pretplatnicima sa gotovo istim kvalitetom servisa. U [1.] je pokazano da 4G karakterišu tri reči: svestranost, širokopojasni pristup i mobilnost. Kratak pregled prihvaćenih karakteristika i elemenata teorije na kojoj počivaju tehnologije 4G mreža kao i uporedne karakteristike sa 3G mrežama prikazane su u drugom poglavlju rada. U trećem i četvrtom poglavlju ukratko su predstavljena dva osnovna zahteva 4G mreža koja se odnose na ostvarivanje sigurnosti i QoS.

2. KARAKTERISTIKE I OSNOVNE TEHNOLOGIJE 4G MREŽA

Od bežičnih 4G sistema se očekuje da pruže sveobuhvatno IP rešenje gde će se multimedijalne aplikacije i usluge isporučivati korisnicima uvek i svuda a osnovni cilj je visoka brzina prenosa podataka i visoka sigurnost što nije ostvarivo korišćenjem trenutne 3G bežične infrastrukture. Mobilni sistemi četvrte generacije koriste OFDM u sprezi sa višeantenskim sistemima. Prednosti 4G u odnosu na 3G date su u tabeli 1. Poboljšanja 4G u odnosu na 3G sisteme su značajna ne samo u pogledu propusnog opsega, pokrivenosti i kapaciteta, već i u mnogim naprednim funkcijama kao što su QoS, malo kašnjenje, visoka mobilnost, sigurnosna podrška itd.

Tabela 1.Uporedne karakteristike 3G i 4G mreža

	3G	***4G***
Kapacitet prenosa	prenos glasa, podataka	prenos podataka i multimedijalnih usluga preko IP
Mrežna arhitektura	WAN	integracija: bežični LAN i WAN
Propusni opseg (Bps)	384 K-2 M	100 M za mobilne uređaje 1 G za fiksne
Frekvencijski opseg (GHz)	1,8 – 2,4	2 – 8
Način prenosa	komutacija kola i komutacija paketa	komutacija paketa
Pristupna tehnologija	CDMA	OFDMA
QoS i sigurnost	ne podržava	podržava
MIMO	ograničena podrška	podržava
Multicast/broadcast usluge	ne podržava	podržava

Generalno, neke od prihvaćenih karakteristika bežičnih mreža četvrte generacije su:

- mrežna arhitektura kompletno bazirana na IP protokolu
- veći propusni opseg
- podrška za različite pristupne tehnologije, uključujući WLAN tehnologiju i standarde 802.11
- podrška za sve multinedijalne aplikacije
- obezbeđen kvalitet usluge

U globalu, kako su tehnologije, infrastrukture i terminali u bežičnim sistemima evoluirali od 1G, 2G, 3G do 4G i od bežičnog LAN-a do širokopojasnog bežičnog pristupa, 4G sistem će sadržati sve standarde koje su ranije generacije implementirale. Među nekoliko tehnologija koje se trenutno razmatraju u 4G mrežama uključujući 3GPP LTE/LTE-Advanced, 3GPP2 UMB i mobilni WiMAX baziran na standardu IEEE 802.16e, u radu su ukratko navedene dve tehnologije koje imaju širu primenu.

2.1. 3GPP LTE

Long Term Evolution (LTE) je predstavljen u 3GPP (3rd Generation Partnership Project) specifikaciji R8 kao sledeći značajan korak UMTS-a (Universal Mobile Telecommunications System). Podržava fleksibilan propusni opseg od 1,4-20 MHz kao i mogućnost rada u FDD (Frequency Division duplex) i TDD (Time Division Duplex) modu. Prema 3GPP okviru LTE

treba da obezbedi vršnu brzinu od 100 Mb/s u direktnom kanalu i 50 Mb/s u povratnom kanalu. Bitna karakteristika radio kanala je da trenutni kvalitet radio kanala varira u vremenu, prostoru, i po frekvenciji [7.]. To se odnosi na varijacije usled višestruke propagacije, koja se manifestuje kao selektivni feding, koji se u okviru korelisanog opsega može zanemariti. Da bi se ispunili visoki zahtevi koje je pred sebe postavila LTE izabran je radio pristup drugačiji od onoga kod WCDMA. Za direktan kanal je usvojen OFDM (Orthogonal Frequency Multiple Access), a za povratni SC-FDMA (Single Carrier FDMA). Osnovna ideja je da se ukupni prenosni opseg podeli na niz podopsega odnosno da se uvede niz podnosilaca koji su međusobno ortogonalni. Budući da su podopsezi relativno uski, to se selektivni feding, tamo gde postoji, manifestuje kao običan ravni feding i mnogo je lakša ekvalizacija kanala. Primena OFDM u povratnom kanalu nije optimalna zbog osobine OFDM-a da amplitude signala imaju veliki dinamički opseg zbog čega se u povratnom kanalu koristi jedan nosilac. Što se tiče broja antena, LTE podržava MIMO tehniku koja se realizuje tako što na predajnoj i prijemnoj strani postoji više antena.

2.2. Mobilni WiMAX

Mobilni WiMAX je dio WiMAX (Worldwide Interoperability for Microwave Access) tehnologije i predstavlja širokopojasno bežično rešenje koje omogućava konvergenciju mobilne i fiksne mreže kroz zajedničke širokopojasne radio pristupne tehnologije i fleksibilnu mrežnu arhitekturu. WiMAX obezbeđuje prosečan protok od oko 24 Mb/s i kašnjenje manje od 50 milisekundi. Korišćenje OFDM tehnike omogućilo je WiMAX-u spektralnu prilagodljivost. Tehnologija mobilnog WiMAX-a je projektovana tako da se može skalirati kako bi radila u kanalima različite širine od 1,25-20 MHz i mogla se uskladiti s različitim zahtevima širom sveta [8.]. Sistemski profil mobilnog WiMAX-a omogućava mobilnim sistemima da budu kofigurisani na uobičajen način što osigurava baznu funkcionalnost terminala i baznih stanica koje su potpuno interoperabilne. WiMAX ima ogroman potencijal, ali je cena njegove implementacije još visoka, dok LTE zahteva jednostavnu nadogradnju 3G opreme i omogućava interoperabilnost sa postojećim standardima. U [3.] je pokazano da, iako kasni nekoliko godina za WiMAX-om, zbog pažljivo odabranih tehničkih rešenja LTE predstavlja ravnopravnog konkurenta u borbi za tržište širokopojasnih bežičnih komunikacija.

3. QoS 4G MREŽA

QoS se opisuje nizom kvantitativnih i kvalitativnih opštih parametara kao što su bitski protok bilo maksimalni, bilo garantovani, kašnjenje pri prenosu, varijacija kašnjenja, kvalitet govora i slike, kao i nizom parametara koji zavise od konkretne aplikacije. U tehničkom pogledu QoS predstavlja skup merljivih performansi odnosno karakteristika jedne multimedijalne mreže. Obezbeđenje kvaliteta servisa je jedna od najzahtevnijih karakterisitika bežičnih mreža četvrte generacije zbog različitih brzina prenosa, propusnih opsega, karakteristika kanala, tolerancije grešaka i handoff podrške među heterogenim bežičnim mrežama. Efektivno obezbeđen QoS omogućava simultanu upotrebu različitih servisa sa različitim zahtevima, omogućavajući da saobraćaj manje zahtevnih aplikacija ne utiče negativno na osetljiviji saobraćaj. Propusni opseg, protok, vremenska ograničenja, pouzdanost, percipirani kvalitet i cene su osnovni elementi koji čine QoS. Da bi QoS efektivno funkcionisao mora se tretirati s kraja na kraj veze i njime se moraju baviti svi komunikacioni slojevi. Zbog osiguranja kvaliteta servisa mreža prepoznaje ili klasifikuje različite tipove saobraćaja i prosleđuje ih različito da bi se postigao zahtevani nivo usluge za svaku klasu saobraćaja. Efikasnost svake QoS šeme se bazira na njenoj sposobnosti da

osigura odgovarajući nivo usluge za klasičnu kombinaciju klasa saobraćaja. Svaka klasa saobraćaja u mreži uvodi određene garancije za QoS, koje se odnose na parametre kvaliteta servisa kao što su kašnjenje, džiter, gubitak paketa i propusni opseg. U 4G okruženju sa nekoliko dostupnih mreža korisnicima, QoS mora biti usko povezan sa mobilnošću kako bi se omogućilo korisnicima da izaberu najprikladniju mrežu. Postoji više komponenti i funkcionalnosti kvaliteta servisa u end-to-end mrežama nego preko vazdušnog interfejsa. End-to-end servis je mrežni servis posmatran s kraja na kraj veze od jednog korisničkog terminala do drugog korisničkog terminala i na aplikacionom nivou koristi nosioce usluga. End-to-end servis može imati određeni QoS koji je obezbeđen korisniku od strane mrežnog operatera, na osnovu čega korisnik može jasno potvrditi stepen izvršenja usluge. Postoje tri osnovne komponente uključene u koncept QoS s kraja na kraj veze, na nivou krajnjeg korisnika, a to su: ono što korisnik očekuje, ono što aplikacija zahteva i ono što mreža isporučuje. Sa aspekta krajnjeg korisnika percepcija QoS se može podeliti u dve kategorije, i to: kvalitet uspostave poziva i kvalitet poziva [9.]. Da bi se obezbedio kvalitet servisa, potrebna je modifikacija postojećih QoS šema, uključujući kontrolu pristupa, dinamičnu rezervaciju resursa i mogućnost podrške QoS za različite zahteve 4G korisnika. Implementacija ovih QoS šema na različitim nivoima zahteva pažljivu procenu. Bežična mreža daje informacije o svom trenutnom kvalitetu servisa koje treba da budu dostupne ostalim bežičnim mrežama.

4. SIGURNOST U 4G MREŽAMA

Sigurnost u 4G mrežama uglavnom uključuje autentifikaciju, poverljivost, integritet i autorizaciju za pristup povezivanju u mrežu. Pored zaštite krajnjih korisnika i mreža jednih od drugih kroz autentifikaciju i autorizaciju komponente ovakvog jednog koncepta mreža bi trebalo takođe da budu zaštićene od bilo kakvih upada ili zlonamernih napada [10.]. Trenutna 3G arhitektura ne može biti zastupljena u 4G mrežama zbog svojih slabih tačaka kao što je nezaštićena veza između žičnih delova, loša skalabilnost simetrične autentifikacije i izlaganje identiteta korisnika putem vazdušnog interfejsa. Sigurnosni okvir u 4G mrežama odnosi se na korisnika i mobilnu opremu kao dva glavna faktora [10.]. Uzimajući u obzir četiri vrste sigurnosnih pretnji na 4G bežične mreže, koji se odnose na napad na ME/SIM (Mobile Equipment/Subscriber Identity Model), radio interfejs, mrežnog radio operatera i pojedinačne delove IP mreže, ovde su navedeni zahtevi za sigurnost ovih elemenata. Sigurnosni zahtevi koji se odnose na SIM i mobilnu opremu su:

- zaštita integriteta hardvera, softvera i operativnog sistema u mobilnoj platformi
- kontrola pristupa podacima u ME[79]/SIM
- zaštita poverljivosti i integriteta podataka koji se nalaze na ME/SIM ili se prenose između mobilnog uređaja i SIM kartice
- zaštita od krađa ili od zloupotrebe mobilne opreme

Sigurnosni zahtevi koji se odnose na radio interfejs i mrežnog operatera su:

- entitetska autentičnost: uzajamna autentifikacija između korisnika i mreže se implementira zbog sigurnog pristupa i snabdevanja uslugama
- obezbediti poverljivost podataka uključujući korisnički saobraćaj i signalizaciju podataka u žičnom i bežičnom interfejsu

[79] ME – mobile equipment (mobilna oprema)

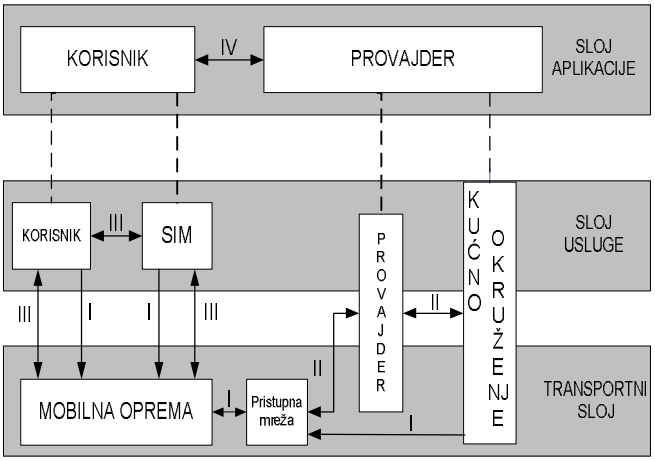
- obezbediti integritet i poreklo autentifikacije korisničkog saobraćaja, signalizacije i kontrole podataka
- zaštita identiteta i lokacije korisnika
- zakonito praćenje i presretanje poziva

Zaštita transparentnosti, poverljivosti i skalabilnosti obuhvata:

- sigurnosne funkcije posećene mreže treba da budu transparentne korisniku
- sigurnosni mehanizmi moraju biti proširivi da podrže povećanje korisnika i elemenata mreže

Sigurnosna arhitektura 4G mreža uključujući sigurnosne karakteristike na različitim slojevima prikazana je na slici 1. i obuhvata:

- sigurnost pristupa mreži - skup sigurnosnih karakteristika koje omogućavaju korisnicima siguran pristup 4G uslugama i onemogućavaju napade na radio pristupnu vezu (I)
- sigurnost u domenu mreže - skup sigurnosnih karakteristika koje omogućavaju čvorovima u domenu provajdera da sigurno razmenjuju podatke i štite od napada na žičnu mrežu (II)
- sigurnost u domenu korisnika - skup sigurnosnih karakteristika koje omogućavaju siguran pristup i okruženje u mobilnoj opremi i SIM- u (III)
- sigurnost aplikacija - skup sigurnosnih karakteristika koje omogućavaju aplikacijama iz domene korisnika i provajdera da sigurno razmenjuju poruke (IV)



Slika 1. Sigurnosna arhitektura 4G mreža

4. ZAKLJUČAK

U ovom preglednom radu ukratko su opisane karakteristike koje se odnose na 4G mreže i dva najvažnija elementa koja su bitna za korisnike ovih mreža a podrazumevaju osiguranje kvaliteta servisa i sigurnosti. Radom nije obuhvaćena detaljnija analiza ovih karakteristika i zahteva već samo osvrt na sadašnje stanje iz te oblasti.

LITERATURA

[1.] Young, K.K., Ramjee, P., (2006): "4G Roadmap and Emerging Communication Techologies", London, Artech House, 1-2.
[2.] Wang, H., Kondi, L., (2009): "4G Wireless Video Communications", Wiley, 2-5.

[3.] Kovačević, Đ. M., (2008): "Pregled aktuelnih tehnologija za mobilne i širokopojasne bežične komunikacije", Telekomunikacije, br.2.
[4.] Bašić, A., (2011): "LTE- Evolucija arhitekture mreže", 11. Međunarodni naučno-stručni skup „Infoteh", Zbornik radova, Jahorina: Elektrotehnički fakultet Istočno Sarajevo, mart, 134-138.
[5.] Drajić, D., Tomić, I., (2010): "Paralelni razvoj HSPA i LTE- fizički sloj", 18. Telekomunikacioni forum TELFOR, Zbornik radova, Beograd: Elektrotehnički fakultet, novembar 23-25, 514-520.
[6.] Popović, R., Petrović, Z., (2004): „Arhitekture protokola za obezbjeđenje kvaliteta servisa kod mreža četvrte generacije", 12. Telekomunikacioni forum TELFOR, Zbornik radova, Beograd: Elektrotehnički fakultet, novembar 23-25.
[7.] Muškatirović, T., (2011): "LTE radio interfejs", 11. Međunarodni naučno-stručni skup „Infoteh", Zbornik radova, Jahorina: Elektrotehnički fakultet Istočno Sarajevo, mart, 129-133.
[8.] Glamočanin, D., Šunjevarić, M., (2007): "Rezultati planiranja mreže mobilnog WiMAX sistema za područje grada Banja Luka", 15. Telekomunikacioni forum TELFOR, Zbornik radova, Beograd: Elektrotehnički fakultet, novembar 20-22, 207-210.
[9.] Cvijanović, M., Jevtović, M., (2005): "Nominalni QoS parametri s kraja na kraj veze buduće UMTS mreže Telekoma Srpske", 13. Telekomunikacioni forum TELFOR, Zbornik radova, Beograd: Elektrotehnički fakultet, novembar 22-24.
[10.] Zheng, Y., He, D., Yu, W., Tang, X., (2005): "Trusted Computing- Based Security Architecture For 4G Mobile Networks", Proceedings, PDCAT.
[11.] Fu, X., Hogrefe, D., Narayanan, S., Soltwisch, R., (2004): „QoS and Security in 4G Networks", Global Mobile Congress, Proceedings, Šangaj.

JEDNO REŠENJE MODELA ZA UČENJE NA DALJINU PRILAGOĐENO STUDENTIMA EKONOMSKOG PROFILA

A SOLUTION FOR THE DISTANCE LEARNING SYSTEM MODE ADAPTED FOR STUDENTS OF ECONOMICS

Jelena Stanković
Univerzitet Singidunum
Danijelova 32, 11000 Beograd, Srbija
011 3093-238
jstankovic@singidunum.ac.rs
Jelena Gavrilović, master
Univerzitet Singidunum
Danijelova 32, 11000 Beograd, Srbija
011 3093-059
jgavrilovic@singidunum.ac.rs

Sažetak:
Kontinuirano obrazovanje je jedan od važnih faktora koji utiču na razvoj ekonomskog društva. Istraživanjem koje je sprovedeno u okviru predmeta Trgovina na uzorku studenata, koji su u radnom odnosu, dobijeni su rezultati koji ukazuju na ekonomske aspekte realizacije sistema učenja na daljinu. U radu je predstavljen predlog rešenja nedostataka, izazova i ograničenja, koji učenje na daljinu nosi u svom kontinuiranom razvoju. Fokus predloženog rešenja modela za učenje, stavljen je kontekst faktora za primenu adaptivnog načina učenja u skladu sa potrebama, vremenom, stečenim znanjem budućih studenata ekonomskog profila.
Ključne reči: učenje na daljinu, ekonomsko društvo, adaptivno učenje, studenti, istraživanje.

Abstract:
Continuing education plays an important role in development of an economic society. The research conducted on a group of students who attended the course in Trade, and who are employeed, showed some economic aspects of the distant learning system. This paper presents a suggestion for improvements in this learning mode. We are focusing our attention to applications of adaptive learning mode in accordance with needs, time, and level of acquired knowledge of our future students of economics.
Key words: distance learning system, economic society, adaptive learning, students, reaserch.

UVOD

Obrazovanje na daljinu je vid obrazovanja koji je nastao prvenstveno kako bi se prevazišle različite prepreke, među kojima su faktori vreme, prostor, skromna finansijska sredstva. Jedan od ciljva je, prevashodno, da se izađe u susret pre svega marginalizovanim grupama, kao što su na primer žene, koje u tadašnjem obrazovnom sistemu nisu imale adekvatan pristup obrazovnim sadržajima. Poslednjih dvadeset godina, kompjuterski zasnovani sistemi učenja značajno su uspeli da poboljšaju i, što je još važnije, oporave univerzitetsko obrazovanje. Samim tim postali su neka vrsta ikone sistema edukacije u svetu, ali i u pojedinim ekonomijama [7]. Razlog ovome,

u prvom redu leži u mogućnostima koje pruža informaciona tehnologija, a to su komunikacija, interakcija i kolaboracija [3].
U ovom radu dat je pregled primenljivih oblika obrazovanja na visokoškolskim ustanovama, sa fokusom na Univerzitet Singidunum. Analiza ovakvog vida učenja urađena je kroz anketu sprovedenu na 42 studenta, u okviru predmeta Trgovina, treće godina osnovnih studija Studijskog programa Poslovna ekonomija Univerziteta Singidunum, za koje se nastava realizuje učenjem na daljinu.

UČENJE NA DALJINU

Prilikom realizacije tradicionalnog načina edukacije, studenti su usmereni ka predavaču. U tom smislu, studenti i predavači, kako bi učestvovali u procesu, moraju biti u isto vreme na istom mestu, usmereni ka istoj temi. Primer ovakve nastave je nastava u učionicama. Svaki oblik nastave van ovih okvira i standarda, smatra se dodatnim aktivnostima. Pri tome, nastavne aktivnosti studenata su vremenski ograničene, odigravaju se najduže na nedeljnom nivou, što je najčešći period između dva predavanja. U ovakvim uslovima, neophodno je održavati kontinuitet u radu, koji isključivo kontroliše predavač. Studenti, u ovakvim okolnostima, predstavljaju pasivne učesnike u nastavi, koji nemaju mogućnost njenog kreiranja, modifikovanja toka, ali i samostalnog motivisanja i samokontrole kada je održavanje kontinuiteta učenja u pitanju.
Razvoj savremenih informacionih tehnologija donosi i mogućnost da predavač i studenti ne budu na istom mestu u isto vreme, ali da, pri tome, zajednički učestvuju u obrazovnom sistemu. Ovakav pristup učenja započeo je svoj razvoj i napredak prihvatanjem činjenice da nastavnici nisu jedini medijum za prenos znanja. Uvođenjem novih obrazovnih tehnologija, kao što su različiti oblici sinhronog i asinhronog elektronskog učenja [6] dobija se novi kvalitet koji se pre svega ogleda u adekvatnoj razmeni svih aktera obrazovnog procesa [1]. Sinhrono elektronsko učenje podrazumeva interakciju nastavnika i studenata u istom vremenskom periodu (npr. video-konferencije, web seminari), dok se pod asinhronim elektronskim učenjem podrazumeva interakcija nastavnika i studenata na različitim lokacijama, u različito vreme (npr. testiranje studenata prema unapred pripremljenim testovima od strane nastavnika, pregledanje snimljenih tutorijala, e-mail korespodencija).
Razvoj kvaliteta se podstiče upotrebom različitih multimedijalnih sadržaja, koji se mogu primenjivati u samom kreiranju materijala ili u njihovoj distribuciji. On-line, a posebno web-zasnovani kursevi, jedinstveni su, usled toga što kombinuju tekst, sliku, video i audio zapise u okviru istog sistema, pojednostavljujući pristup bazama podataka, i omogućavajući fleksibilnu interakciju između korisnika i tehnologije [5]. Bitno je istaći da je organizovanje samog načina realizacije ovakve vrste obrazovanja zasnovano i na sticanju i razmeni iskustava u toku procesa učenja, na sagledavanju i povezivanju potreba studenata, na mogućnosti razvoja sadržaja od strane programera, a uz koordinaciju od strane stručnjaka.

ANALIZA KURSA TRGOVINA

Učenje na daljinu se realizuje kroz pristup različitim platformama za savlađivanje gradiva. Studentima su dostupni video snimci predavanja, platformi za učenje, kao i informativni sajt. Komunikacija sa nastavnim i nenastavnim osobljem odvija se na različite načine, od kojih su najčešći putem elektronske pošte ili u terminima konsultacija, odnosno putem otvorenih vrata. Tehnička služba je zadužena za organizaciju sajta i video snimaka, a ono što nastavno osoblje uređuje jeste sadržaj platforme koju studenti koriste za učenje.

Moodle platforma za učenje predstavlja tzv. Open-source sistem [8] koji sadrži u sebi sistem za upravljanje sadržajem i sistem za upravljanje učenjem. Sistemi obezbeđuju paletu mogućnosti kreiranja edukativnih materijala nastavnicima, a na osnovu kojih oni sami kreiraju nastavne sadržaje namenjene: podučavanju, praćenju toka učenja, proveru znanja.
Jedan od mogućih načina organizovanja resursa namenjenih učenju na daljinu, a kojim se nudi organizovana forma kurseva sa sadržajima koji ovakav sistem učenja predviđa, pruža i predmet Trgovina. Ovaj predmet koncipiran je na Moodle platformi tako da studenti u okviru kursa imaju pristup sledećim ključnim edukativnim sadržajima: informacijama namenjenim kontinuiranom toku nastave i komunikacije, nastavnim materijalima za učenje, sadržajima za proveru znanja. Važno je naglasiti da pristup učenja na daljinu na predmetu Trgovina, pruža mogućnost sinhronog i asinhronog učenja.
Mogućnosti interaktivne komunikacije, slanje i prikupljanje povratnih informacija, testiranje studenata u realnom vremenu, što poznaje i visoko vrednuje praksa u svetu [2], sprovodi se i u okviru DLS nastave predmeta Trgovina.
U višegodišnjoj koordinaciji predmetom Trgovina, rađena je i evaluacija rada, koja je uključivala analizu korišćenih materijala, sprovođenih aktivnosti u okviru kursa, a u odnosu na potrebe studenata definisane planom i programom nastave na Univerzitetu. Akcenat analize stavljen je na kategorizaciju materijala u odnosu na angažovanje studenata na platformi. Pridržavanje standardima izvođenja nastave koji su postavljeni na Univerzitetu, predstavljalo je, prilikom izvođenja analize, veoma važan faktor kontrole, ali i meru objektivnosti prilikom interpretacije rezultata.
Postoje ključni razlozi razvoja i korišćenja sistema učenja na daljinu u okviru podizanja efikasnosti, ekonomske isplativnosti, ali i podizanja kvaliteta informatičke edukacije, i kvalitetnog savlađivanja gradiva. Među značajne faktore kvaliteta ovoga sistema treba uvrstiti:

- visoku i pozitivnu stopu odgovora od strane studenata, što potvrđuje i visoka stopa odgovora (response rate) na anketu postavljenu na platformu;
- jednostavnost korišćenja, koju potvrđuje činjenica da se platformi i sadržajima može pristupiti na svakom mestu na kojem postoji pristup Internetu;
- podizanje nivoa edukacije studenata uopšte u oblasti informacionih sistema i tehnologija, što dalje vodi njihovoj lakšoj adptaciji i prihvatanju novih rešenja;
- racionalizaciju sistema učenja i podizanje kvaliteta sadržaja i brzine rešavanja poslovnih zadataka, što je za studente ekonomskog profila naročito dragoceno (ovo se posebno odnosi na predmete kao što su Kvantitativni metodi, i predmete iz oblasti Finansija).

Ograničavajući faktor organizovanju sistema učenja na daljinu, svakako je dugotrajna priprema, čime se vreme organizovanja aktivnosti učenja može dovesti u pitanje. Takođe, veoma snažan faktor je i preferiranje pohađanja tradicionalne nastave, koja studentima omogućava lični kontakt sa predavačem i direktnu komunkaciju sa kolegama. Video-konferencije predstavljaju sistem koji uspeva da nadoknadi pomenuti nedostatak. Nedovoljno poznavanje informacione tehnologije, nepoznavanje rada na računaru i nemogućnost pristupa platformi (npr. neposedovanje računara ili nepostojanje bežičnog Interneta), svakako su ograničavajući faktori koje treba imati u vidu.

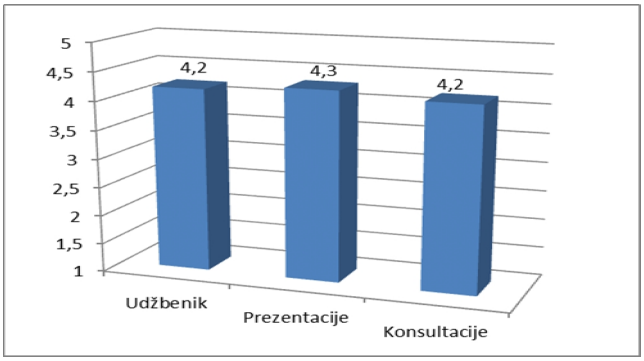
ANKETA I OPIS REŠENJA

U okviru predmeta Trgovina na platformi za učenje, u toku zimskog semestra školske 2011/2012. god., urađeno je istraživanje nad studentima, putem upitnika sa sedam pitanja

zatvorenog tipa. Anketa je sprovedena tokom trajanja zimskog semestra. U anketi je učestvovalo 42 studenta što je oko 70% od ukupnog broja studenata Studijskog programa Poslovna ekonomija. Upitnik je postavljen u okviru predmeta na platformi za učenje nadaljinu. Na osnovu urađene statističke analize prikupljenih odgovora, predlažemo rešenja za uspešniju realizaciju nastave ovakve i sličnih oblika nastave.

Podaci koje smo prikupili i obradili, pokazali su sledeće:

- 73% anketiranih studenata odgovorilo je da se nalazi u radnom odnosu;
- 58% studenata smatra da je predmet Trgovina, sa svojim planom i programom, koristan za posao koji obavljaju;
- 65% ocenjuje sadržaj kursa Trgovine veoma značajnim u pripremi završnog ispita;
- 60% studenta smatra da je uloga samostalnih aktivnosti u formi eseja, zasnovanih na praktičnim problemima, veoma bitna za pripremu ispita, razumevanje i praktičnu upotrebu gradiva.
- Interesantan je podatak visokog poverenja studenata u power point prezentacije, pri čemu se one, za pripremu ispita, moraju koristiti isključivo kao podsetnik, dok se sam ispit sprema iz udžbenika.



Slika 1: Ocena upotrebe različitih oblika pripreme ispita

Na osnovu prezentovanih podataka, možemo izvesti sledeće zaključke, koji nam mogu pomoći u kreiranju jednog rešenja za učenje na daljinu:

- Kurs Trgovina sadrži sve potrebne uslove za pripremanje gradiva za studente koji ga pohađaju, a pri tome ima potrebe da paralelno primenjuje stečeno znanje u okviru delatnosti kojom se bavi. Rezultati, takođe, navode na zaključak da se za nedoumice i konsultacije studenti rado obraćaju nastavnika, putem elektronskih poruka ili na samom fakultetu.
- Za pripremu ispita studenti koriste koncept paralelnog korišćenja prezentacija i udžbenika. Predlog je da prezentacije zbog svog obima i elektronske forme sadrže i podatke o praktičnim mogućnostima primene teoretskih delova gradiva, pri čemu nisu dovoljne za pripremu ispita.
- Samostalan rad studenata je veoma bitan u procesu što boljeg razumevanja celine nastavnih jedinica, pa je u skladu sa tim potrebno ispitati različite načine provere znanja.

Kurs treba kontinuirano pratiti kroz evaluaciju studenata na osnovu čijih rezultata će se kurs prilagođavati znanju i veštini studenata.

ZAKLJUČAK

Sama mogućnost da se predavanja i nastava mogu pratiti sa različitih lokacija u različito vreme, dakle asinhrono, kao i da se mogu ponavljati, što čini proces realizacije nastave dostupnim svim potencijalnim kategorijama korisnika, i to u pogledu različitih aspekata: sociooloških, društvenih, ekonomskih i drugih. Među najčešće kategorije DLS studenata na Univerzitetu Singidunum su: zaposleni ljudi, sportisti koji zbog treninga i putovanja nemaju mogućnost čestog fizičkog boravka na fakultetu, kao i ljudi koji često putuju, žive i borave u inostranstvu. Proces napretka realizacije ovakvog načina učenja je uslovljen spremnošću nastavnog osoblja da svoje predmete adaptira na osnovu potreba studenata kroz upotrebu informacionih tehnologija.

LITERATURA

1. Bajčetić, M., Lazarević, B., (2006) "Online edukacija-nove nastavničke veštine."
2. Colaric, S., Johanssen, D.H., (2001) Information equals knowledge, searching equals learning, and hyperlink is good instruction, myths about learning from the World Wide Web. Computers in the School, 17 (3-4), 159-169.
3. Harasim, L., Hiltz, S. R., Teles, L., Turoff, M. (1995). *Learning Networks, A Field Guide to Teaching and Learning Online*. Cambridge MA. The MIT Press.
4. Holsapple, C.W., Lee-Post, A. (2006) Defining, assessing, and promoting e-learning success: an inforormation systems perspective. *Decision Sciences Journal of Inovative Education*, 4 (1), 67-85.
5. Jung, I., (2001) Building a Theoretical Framework of web-based instruction in the context of distane education. British Journal of Educational Technology. 32 (5), 525-534
6. Littlefield, J., (2013) Synchronous Distance Learning vs. Asynchronous Distance Learning, http://distancelearn.about.com/od/choosingaschool/p/LearningTypes.htm, posećeno 18.02.2013.
7. Selwyn (2007) Selwyn, N. (2007). The use of computer technology in university teaching and learning: a critical perspective. *Journal of Computer Assisted Learning, 23*(2), 83–94.
8. Simonson, M., (2007) Course Management Systems. The Quarterly Review of Distance Education, 8 (1), vii-viii

PRIMENA SOFTVERSKIH APLIKACIJA EVINAS I KPF U OKVIRU POSLOVNOG INFORMACIONOG SISTEMA OBRAZOVNE USTANOVE

IMPLEMENTATION OF EVINASANDKPFSOFTWAREAPPLICATIONS WITHIN BUSINESS INFORMATION SYSTEM ATEDUCATIONAL INSTITUTION

Jelena Kaljević
Poslovni fakultet Valjevo, Univerzitet Singidunum Beograd
Železnička 5, 14000 Valjevo
Telefon: +381 14 292610, +381 65 3122213
Fax: +381 14 292 611
E-mail: jkaljevic@singidunum.ac.rs
Ivan Pantelić
Poslovni fakultet Valjevo, Univerzitet Singidunum Beograd
Železnička 5, 14000 Valjevo
Telefon: +381 14 292610, +381 64 3349811
Fax: +381 14 292 611
E-mail: ipantelic@singidunum.ac.rs
Stojan Milovanović
Poslovni fakultet Valjevo, Univerzitet Singidunum Beograd
Železnička 5, 14000 Valjevo
Telefon: +381 14 292610, +381 64 1586918
Fax: +381 14 292 611
E-mail: smilovanovic@singidunum.ac.rs

Sažetak
U sve većem razvoju informacionih tehnoologija dolazi i do potreba uvođenja novih softverskih rešenja u sam proces rukovođenja organizacija. Vođenje kadrovske politike i sistemi evidentiranja kadrova podižu se na viši nivo uvođenjem i primenom već gotovih rešenja ili se razvijaju nove softverske aplikacije.
Za što efikasnije vođenje evidencije kao i za kasniju analizu podataka o realizovanosti nastave na visokoškolskoj instituciji razvijena je aplikacija koja omogućava menadžmentu uvid u ostvarivanje predviđenog nastavnog plana i programa.
U radu je predstavljena softverska aplikacija KPF za evidenciju zaposlenih na visokoškolskoj ustanovi, kao i EVINAS za elektronsku evidenciju nastave. Analiza je rađena na primeru Poslovnog fakulteta Valjevo i prikazana je kompletna aktivnost razvoja softvera i procesa održavanja u cilju zadovoljavanja kriterijuma kvaliteta.
Ključne reči: softversko rešenje, EVINAS, KPF, kvalitet nastavnog procesa

Abstract
Thegrowingdevelopment of informationtechnologies leadstothe need to introducenew softwaresolutionsinthe process oforganization management. Human Resource Policyand

Systemsof recordingemployeesare builtto a higher levelby introducing andimplementation of theready-madesolutionsor development ofnewsoftware applications.
For more efficientrecord-keepingas well asfor subsequentdata analysis of teaching performance at a highereducationinstitution, an application that enables management toget insight into theplannedcurriculum is developed.
This paper presentsa software applicationforrecords of employeesof a higher educationinstitution - KPF,as well aselectronic recordsof teaching process - EVINAS.The analysis was performedon the exampleof the Facultyof BusinessValjevoandthe complete activityof software developmentandmaintenance process is showninorder to meet thequality criteria.
Keywords:software solution, EVINAS, KPF, the quality of teaching process

1. UVOD

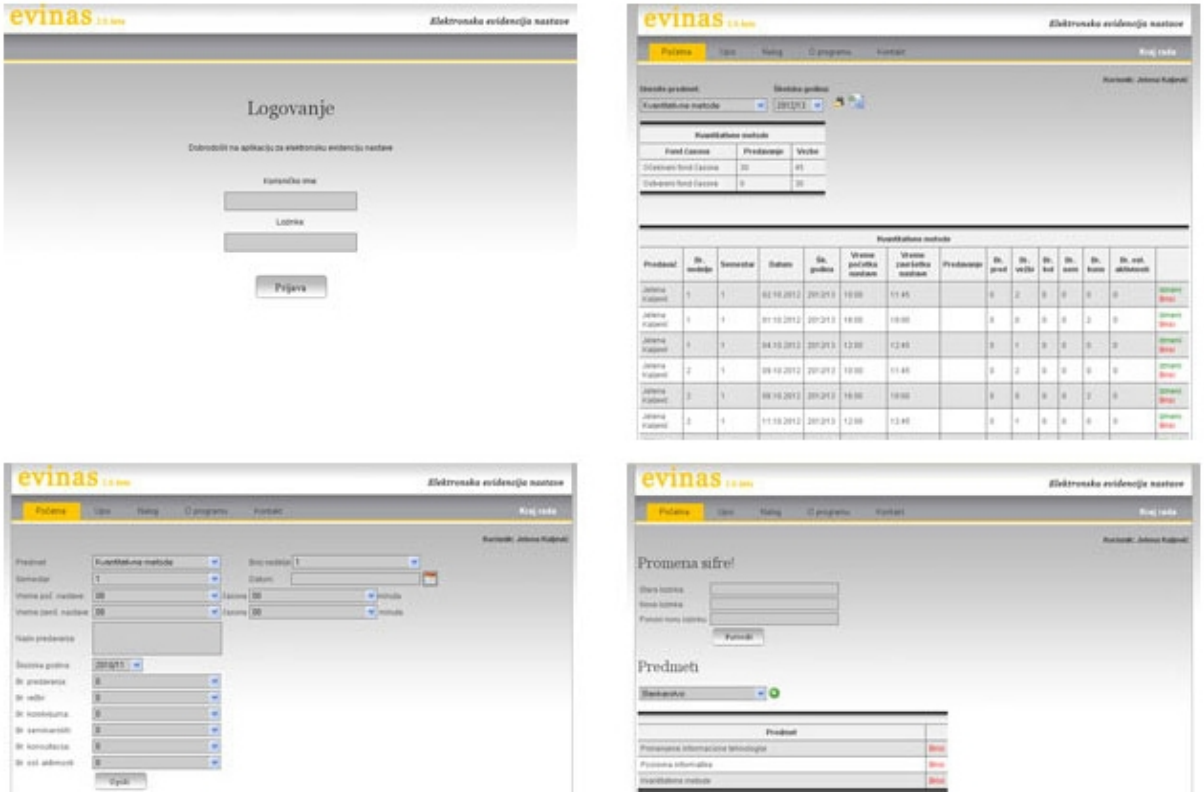
Suština svakog poslovanja je da se identifikuju potrebe na tržištu i razvijaju sposobnosti da služi te potrebe. U okviru ove oblasti stvoren je opšti okvir za pomoć klijenata, menadžment timovi brzo uspostavljaju mehanizme za preduzeća i daju smisao odnosno "misiju" razjašnjavanja i komuniciranja i jasnu viziju trajne svrhe kompanije, osnovne vrednosti, ciljeve i ključ uspeha strategije.
Sa jedne strane, razvijaju se ciljevi i strategije koja postaje od vitalnog značaja za kaskadno vođenje kroz organizaciju gde se sa druge strane svaki pojedinačni element performansi menja u zavisnosti od potreba obrazovne ustanove.
U današnjem poslovnom okruženju ubrzanih promena zahteva se da rukovodstvo kontinuirano usavršava strategiju poboljšanja kvaliteta poslovnih procesa i da se uskladi sa promenama na tržištu.
Postojeća softverska rešenja korišćena u poslovnim procesima Poslovnog fakulteta Valjevo nisu obuhvatala sistematsko elektronsko vođenje podataka o nastavnom osoblju kao ni elektronsku evidenciju realizovane nastave. Ta dva osnovna procesa koje je trebalo sistematizovati sastojala su se u sledećem: ručno vođenje evidencije realizovanih i planiranih časova nastave-predavanja, vežbe, konsultacije i njihova dalja analiza, koji su ne samo menadžmentu ove visokoobrazovne institucije bili potrebni već i Komisiji za akreditaciju i proveru kvaliteta koja je na taj način vršila reviziju realizovane nastave, i unutar same institucije vođenje kadrovske evidencije. Posebna pažnja na Poslovnom fakultetu je upravo posvećena ljudskim resursima, koji su često u poslovnoj informatici zapostavljeno područje.
Vođenje različitih evidencija o radnicima rezidentima ili nerezidentima, koji mogu da imaju različite oblike zaposlenja: stalno zaposleni nastavnici, asistenti i saradnici, nenastavno osoblje, nastavnici po ugovoru i drugo.
U cilju unapređenja kvaliteta na tom polju pristupilo se razvoju softverskih aplikacija koje bi učinile ovaj deo poslovanja što efikasnijim.

2. PRIMENA SOFTVERSKIH APLIKACIJA

2.1.Softverska aplikacija EVINAS

Prvi je razvijen softverski paket za elektronsku evidenciju nastave. Na slici 1. je prikazan izgled korisničkog interfejsa aplikacije. U samoj izradi su korišćene tehnologije: JSF (Java Server Faces)

tehnologija za izgradnju korisnički baziranih interfejsa za web aplikacije, JSP (Java Server Pages) tehnologija za izradu dinamičkih generisanih web starnica i MySQL.
Program se sastoj iz korisničkog i administratorskog dela. Deo kojem korisnik pristupa zavisi od naloga koji korisnik poseduje. Administratorski deo sadrži opcije za upravljanje korisničkim nalozima (dodavanje, brisanje, izmene), upravljanje kursevima (naziv, fond časova, vežbi, konsultacija, i td.) i pregled evidencije nastave svakog kursa posebno. Korisnički deo ima mogućnosti da korisnik dodeli sebi kurs, da vrši unos održanih predavanja i vežbi iz izabranog kursa kao i pregled unetih podataka. Takođe korisnik na svom nalogu može promeniti i svoju pristupnu lozinku. Sistem omogućava i dobijanje različitih vrsta izveštaja vezanaih za održanu nastavu i može se definisati po svim kriterijumima koji su definisani u sistemu. Postoji i mogućnost generisanja izveštaja za određeni vremenski period.



Slika 1. Prikaz korisničkih formi aplikacije EVINAS

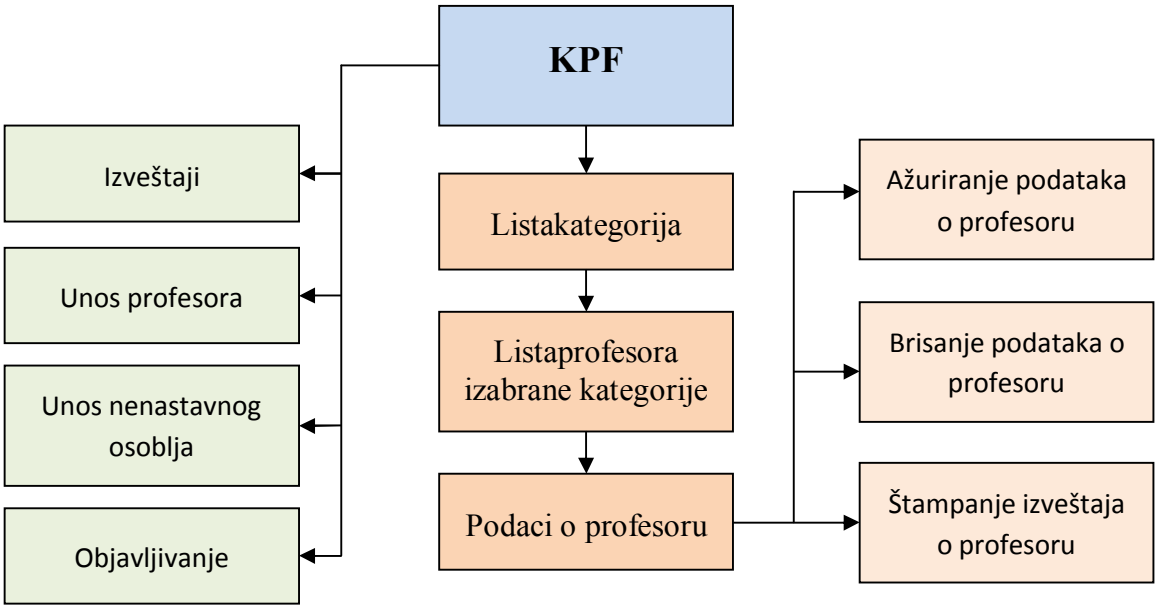
2.2.Softverska aplikacija KPF

Program za evidenciju zaposlenih prvenstveno je urađen za evidenciju zaposlenih na fakultetu. Za njegovu izradu korišćene su tehnologije kao i za prethodni softverski sistem. KPF poseduje i dodatni modul koji koristi deo koda koji obrađuje preostalo vreme do isteka ugovora o radu. Na slici 2. je data blokovska struktura aplikacije iz koje se mogu sagledati glavni procesi u sistemu. Za svakog zaposlenog u sistemu se kreira personalni dosije u koji se unose lični podaci, evidencija radnog staža, kretanje radnika po radnim mestima na fakultetu, kao i podaci o radnom stažu. Tu su i podaci o odmoru i korišćenju odmora, kao i evidencija odsutnosti radnika. Takođe, u sistemu se može voditi evidencija zdravstvenih pregleda radnika, obavljenih kurseva i obuka.

Osnovni delovi koje sadrži ovaj softverski paket su:

- Evidencija zaposlenih (lični podaci, adrese, članovi porodice ...)
- Praćenje podatata iz radne knjižice (radni staž, institucije ...)
- Evidencija obrazovanja zaposlenih, kako u okviru obrazovnih institucija tako i interno
- Evidencija koeficijenta za izračunavanje plate zaposlenog (opcione mogućnosti)
- Praćenje karijere zaposlenog i kretanje u preduzeću
- Evidencija naučnih radova za profesore
- Upozorenja na događaje (istek ugovora o radu, zdravstveni pregledi, rođendani ...)
- Modul za sistematizaciju radnih mesta
- Praćenje godišnjih odmora
- Praćenje radnog vremena
- Podaci o zdravstvenom stanju zaposlenog
- Zdravlje i zaštita na radu
- Zakonski šifarnici
- Izveštaji
- Izvoz podataka u različitim formatima (pdf, xls, xml)

Program je modularnog tipa tako da se na njega mogu nadograditi i drugi moduli ako za njima bude potrebe u budućnosti.



Slika 2. Prikaz blokovske strukture aplikacije KPF

3. ZAKLJUČAK

Kao što se može videti iz prethodnog dela, unapređenje pojedinih poslovnih procesa unutar samog informacionog sistema visokoobrazovne ustanove moguće je kroz razvoj softverskih aplikacija. Ove dve aplikacije su znatno doprinele kvalitetnijem, ekonomičnijem i efikasnijem poslovanju kako nastavnog osoblja tako i kadrovske službe. Znatno je olakšana i analiza

unesenih podataka ali i stvorena mogućnost lakše pretrage, pregleda i pravljenja statističkih izveštaja.
To je pokrenulo i podstaklo ideju o daljem unapređenju kvaliteta drugih nastavnih i vananstavnih procesa na Poslovnom fakultetu Valjevo.

LITERATURA

Knjige:

[1.] Nikolić, B.: *Internet programiranje pomoću programskog jezika JAVA*, Univerzitet Singidunum, Beograd, 2008.
[2.] Živković, D.:*Java programiranje*, Univerzitet Singidunum, Beograd, 2013.
[3.] Njeguš, A.: *Poslovni informacioni sistemi,* Univerzitet Singidunum, Beograd, 2009.
[4.] Heleta, M.: *Projektovanje menadžment sistema kvaliteta,* Univerzitet Singidunum, Beograd, 2012.
[5.] Welling, L. and Thomson, L.:*PHP i MySQL: razvoj aplikacija za Web,*Mikroknjiga, 2009.

Članci u časopisu:

[6.] Jovanović, V. i Veljović, A. (2009): „Reinžinjering poslovnih procesa u visokoškolskim ustanovama korišćenjem standarda IDEF0“,*Singidunum revija*, VOL.6/NO.2, 99-110

Internet izvori:

[7.] Adizes (2011): „Understanding the Corporate Lifecycle“, (pristup 26.01.2013.), [dostupno na http://www.adizes.com/]

UNUTRAŠNJI RAZVOJ INFORMACIONOG SISTEMA ZA UPRAVLJANJE KVALITETOM SIROVINA

IN-HOUSE INFORMATION SYSTEM DEVELOPMENT FOR RAW MATERIALS QUALITY MANAGEMENT

Bogdan Mirković
Fakultet za informacione tehnologije, Slobomir P Univerzitet
PF 70, Slobomir, 76 300 Bijeljina, Republika Srpska, Bosna i Hercegovina
Telefon: +387 65 664 957
Fax: +387 55 251 444
E-mail: bogdanmirkovic@yahoo.com

Sažetak: *Kvalitet proizvoda dobijenih na kraju proizvodnog ciklusa u velikoj mjeri zavisi od kvaliteta sirovina koje se koriste. Upravljanjem kvalitetom sirovina u prehrambenoj industriji predstavlja jedan od najbitnijih činalaca proizvodnog procesa. Korištenjem informacionih tehnologija u ovom segmentu proizvodnog procesa omogućava se pravovremeno dobijanje informacija o kvalitetu i kvantitetu sirovina koje se koriste u proizvodnom procesu. Primjenom informacionih tehnologija informacije koje se dobijaju omogućavaju pravovremeno i svrsishodno donošenje odluka o načinu izvršenja proizvodnog procesa sa sirovinama.*

Summary: *The quality of the product obtained at the end of the production cycle is largely dependent on the quality of raw materials used in the production. Quality management of raw mateials in the food industry is one of the most important factors of manufacturing process. Using information technology in this segment of the manufacturing process is very important to obtain timely information on the quality and quantity of raw materials used in the production process. Usage of information technology to gain information enabling timely and appropriate decisions about the manner of execution of the production process from raw materials.*

Key words*: information system, in-house development, quality*

1. UVOD

Pravovremena, tačna, ažurna i dostupna informacija je osnova savremenog poslovanja. Uz ostale aspekte poslovanja kao što su orjentacija na kupce i zadovoljenje njihovih potreba, povećanje kvaliteta proizvodnje i stroga primjena standarda kvaliteta, efikasnije i rentabilnije poslovanje uz maksimalno skraćenje rokova isporuke proizvoda[80], posjedovanje informacija o sirovinama i njihovom kvalitetu koje su inputi za proizvodni proces je najvažnija. Ovo se posebno odnosi na proizvodne procese koji kao inpute imaju sirovine različitog kvaliteta (primarne sirovine za proizvodnju u osnovnom obliku kao što su žitarice). Informacioni sistemi u ovom segmentu proizvodnje imaju veoma bitnu ulogu u savremenom poslovnom okruženju. Informacioni sistem je skup komponenti organizovanih tako da omogućavaju registrovanje, prikupljanje, prenos,

[80] M. Nikolić, Z.Nikolić, Ž.Petrović: ''Razvoj jednog rešenja fabričkog informacionog sistema', YUInfo2009, 2009.

obradu, skladištenje, analizu i distribuciju informacija za različite namjene. Informacioni sistem je usklađen i oblikovan skup personalnih, organizacionih i tehničkih elemenata koji obezbjeđuju koordinaciju i protok informacionih tokova u okviru sistema i sa okruženjem[81] u kome se sistem nalazi. Razvoj informaciono-komunikacionih tehnologija, poboljšavanje performansi računarske opreme, sve veći broj sistema koji omogućavaju brži i kvalitetniji rad na računarima (operativni sistemi, sistemi za upravljanje bazama podataka, razvojni alati) doveo je do razvoja relativno jeftinih a kvalitetnih informacionih sistema baziranih na platformi personalnih računara koji se mogu naći na informacionom tržištu. Veći dio tih rješenja obuhvata osnovne komponente koje se nalaze u svim poslovnim subjektima (knjigovodstvo, personalne evidencije i slično) i mogu se primjenjivati u bankama, organima javne uprave, proizvodnim preduzećima, osiguravajućim kompanijama, ugostiteljskim i turističkim organizacijama. Drugi dio aplikativnih rješenja koji se odnose na specifične zahtjeve korisnika (posebno se to odnosi na proizvodnu djelatnost) zadovoljava potrebe malog, veoma ograničenog po broju, korisnika. U takvim sistemima, za podršku radnim procesima, potrebno je razviti određene, specifične po zahtjevima, informacione sisteme ili aplikativna rješenja koja bi bila prilagođena krajnjem korisniku.

2. UNUTRAŠNJI (IN-HOUSE) RAZVOJ INFORMACNIH SISTEMA

Unutrašnji (in-house) razvoj informacionog sistema u organizaciji predstavlja razvoj informacionog sistema od strane zaposlenih osoba u toj istoj organizaciji. Koristi od in-house razvoja informacionog sistema mogu se podijeliti u četiri grupe[82]:

- pravovremenost: pravovremensot je najčešće od krucijalnog značaja prilikom procesa implementacije tehnoloških rješenja. Svako novo uvođenje savremenih poslovnih rješenja zahtijeva od organizacije određena prilagođavanja novim tehnologijama i procesima. Sa zaposlenim u samoj organizaciji, mogućnost kontrole u procesu uvođenja je veća u odnosu na spoljne saradnike. U slučaju kritičnih situacija u toku implementacije rješenja, mnogo je lakše izvršiti prilagođavanje novonastaloj situaciji sa zaposlenim u organizaciji nego sa drugim stranama. I sama činjenica da pojedicni i grupe zaposlenih vrše obuku drugih zaposlenih olakšava osbosobljavanje zaposlenih i daje i druge parametre za buduće procese.
- kontrola kvaliteta: dok se razvojni timovi izvan organizacije mogu usredrediti na razvoj informacionog sistema bez prekidanja, oni najčešće nisu dovoljno obučeni u svim segmentima poslovanja u kojima će se razvijani sistem primjenjivati. Spoljni saradnici ne znaju da „čitaju između redova„ i posvete se sitnim detaljima koji se nalaze u poslovnom procesu a koji mogu uticati na kvalitet krajnjeg proizvoda. Manjak spoznaje o načinu korištenja informacija uzrokuje nastajanje većeg broja verzija nakon početne implementacije sistema i odlaganje primjene konačne verzije sa svim zadovoljenim zahtjevima koje sistem treba da posjeduje. Veći nadzor nad sistemom u toku njegovog razvoja omogućava i otkrivanje grešaka i nelogičnosti u samoj kasnijoj implmenetaciji sistema. Razvojni timovi unutar organiazcije bolje razumiju organizaciju, njeno funkcionisanje i potrebe nego što to čine spoljni saradnici tako da će više pažnje posvetiti interesima organiazcije u kojoj su zaposleni. Razvoj stabilnog sistema visokog kvaliteta, koji je ujedno i lak za korištenje obezbjeđuje organizaciji dugoročne koristi.

[81] D. Regodić: ''Logistika'', Univerzitet Singidunum, Beograd, 2011.
[82] J. Wilder: ''The Case for In-house development'', Hospitality Upgrade, Fall 2009. str 20

- transfer znanja: u slučaju razvoja sistema izvan organizacije, potrebno je određeno vrijeme da se znanja koja postoje u organizaciji prenesu spoljniim saradnicima. U slučaju razvoja sistema unutar organizacije, dobija se na tranferu znanja u samoj organizaciji, poboljšava se odnos među zaposlenim stvaranjem timova koji zajedno rade što doprinosi boljem poslovnom okruđenju u samoj organiazciji. Samim transferom znanja preko dokumenata, ličnim kontaktima[83] dolazi do toga da se znanje onoga koji posjeduje može i primjeniti.
- finansijski faktor: angažovanje spoljnih saradnika za razvoj informacionih sistema je najčešće uzrokovano cijenom ponuđenom za izvršenje tih usluga. Međutim, iako je cijena razvijanog inicijalnog projekta od strane spoljnih saradnika manja, uvijek će postoojati potreba za određenim brojem zaposlenih u organizaciji koji će raditi na održavanju sistema. Uslovi za promjenu načina rada sistema ili njegovih pojedinih dijelova podrazumijevaju dodatne troškove spoljnim saradnicima koje utiču na cjelokupno poslovanje organizacije.

3. INFORMACIONI SISTEM ZA UPRAVLJANJE KVALITETOM SIROVINA ZA PROIZVODNJU

3.1. Proizvodni i skladišni kapaciteti u posmatranom preduzeću

"Žitopromet" a.d. Bijeljina osnovano je 01.02.1961.godine. Do 21.02.2002.godine poslovalo je kao državno preduzeće. Rješenjem o upisu u sudski registar pod brojem 1-1490 u Osnovnom sudu u Bijeljini od 21.02.2002.godine registrovano je kao akcionarsko društvo. Osnovna djelatnost "Žitopromet" a.d. Bijeljina je: proizvodnja mlinskih proizvoda, proizvodnja gotove hrane za uzgoj životinja i proizvodnja hljeba i peciva. Pored ovih proizvodnih djelatnosti društvo se bavi i prevozom robe u drumskom saobraćaju, trgovinom na malo kao i uslužnom meljavom. "Žitopromet" a.d. zapošljava 236 radnika od toga[84]: u proizvodnji 196 radnika, u prodaji 14 radnika, u administraciji 16 radnika i u službi obezbjeđenja objekata 10 radnika. Industrijska proizvodnja je tradicionalna i vezana je za sirovinsku bazu područja na kome je locirana. Za normalno obezbjeđenje proizvodnih pogona osnovnim sirovinama i skladištenje gotovih proizvoda preduzeću su potrebni i odgovarajući skladišni kapaciteti. Sadašnji skladišni kapaciteti se sastoje od: silosnih skladišnih prostora kapaciteta 25.000 tona i podnih skladišta kapaciteta 10.000 tona.

Silosni skladišni prostor se sastoji od tri silosa:

- stari betonski silos kapaciteta 5.000 tona;
- novi betonski silos kapaciteta 10.000 tona;
- metalni silos kapaciteta 10.000 tona.

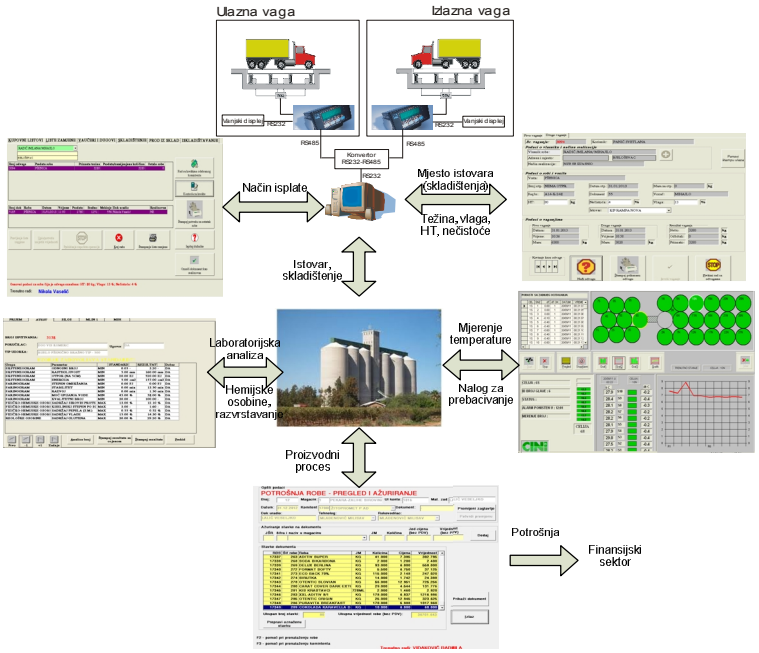
3.2. Komponente integrisanog informacionog sistema za upravljanje kvalitetom sirovina

Sistem za upravljanje kvalitetom sirovina koji se koriste u proizvodnji mora imati određene podatke o kvalitetu[85] i kvantitetu tih istih sirovina s posebnom naznakom da ti podaci moraju biti

[83] P.Jovanović, N.Dragomanović, V.Mišković, S.Drobnjaković: ''Transfer znanja kao podproces menadžmenta znanja'', VIII skup privrednika i naučnika, FON, Beograd, 2011.
[84] ''Godišnji izvještaj o radu Žitopromet ad Bijeljina za 2012.godinu'', Bijeljina, 2013.
85 I. Beker: ''Upravljanje zalihama'', Fakultet tehničkih nauka Univerziteta u Novom Sadu, Novi Sad, 2011.

tačni i raspoloživi svim onim faktorima kojima su potrebni. Osnovne karakteristike sirovina koje se koriste u "Žitopromet" a.d. su te da se radi o zrnastim sirovinama te da se njihovo skladištenje obavlja u silosnim kapacitetima. Za proizvodnju proizvoda od ovih sirovina bitne su dvije vrste karakteristika: fizičko-hemijske i reološke osobine (sadržaj vlage, hektolitarska težina, sadržaj primjesa, proteina, glutena, kiselinski stepen) na osnovu kojih se vrši početno i naknadno razvrstavanje sirovina u silosu. U "Žitopromet" a.d. je razvijen informacioni sistem za upravljanje kvalitetom strateških sirovina koje se koriste u proizvodnji (pšenica, kukuruz, soja, ječam) koji je podijeljen u segmente u zavisnosti od mjesta nastanka i raspoloživosti informacija u skladišno-proizvodnom procesu. Ukupno je implementirano 5 segmenta informacionog sistema (slika 1):

- Pripremanje naloga za isplatu ili druge vrste naknade za dobavljače sirovina vrši se u drugom segmentu informacionog sistema. U ovom segmentu se vode evidencije o zalihama (kvantitetu) pojedinih vrsta sirovina.
- Nakon skladištenja sirovina u silosu vrši se dalja analiza sirovina koje su uskladištene i njihovo dalje razvrstavanje nakon procesa odvajanja sirovina od primjesa. Sirovine koje imaju slične osnovne karakteristike (vlaga, hektolitarska težina) mogu se bitno razlikovati na osnovu ostalih osobina (hemijskih i reoloških) te je potrebno njihovo dalje analiziranje. Uzorci koji se dostavljaju u laboratoriju uzimaju se svakodnevno iz silosa te se na osnovu njihovih osobina razvrstavaju u procesu skladištenja.



Slika 1: Kompnente informacionog sistema

- U toku skladištenja vrlo je bitno u svim skladišnim kapacitetima imati temperaturu koja zadovoljava uslove sirovine koja se čuva. Mjerenje temerature obavlja se na 270 mjesta u silosima (po 10 temperaturnih senzora u svakom od silosa). Povećanjem temperature na pojedinim mjestima dolazi do smanjenja kvaliteta sirovine pa je potrebno na osnovu tih rezultata izvršiti prebacivanje sirovine.

- Nakon iskladištavanja sirovine i korištenja sirovine u proizvodnom procesu, koristi se segment informacionog sistema kojim se vrši evidentiranje potreošnje sirovine o čemu se šalje izvještaj finansijskom sektoru.

ZAKLJUČAK

Savremeno poslovanje nije moguće zamisliti bez upotrebe računarske opreme i softvera koji su napisani bilo u opštem obliku da ih mogu koristiti svi korisnici računara (opšti softverski paketi i aplikacije) bilo u specijalovanim i posebno dizajniranim softverima koji odgovaraju potrebama preduzeća u konkretnom slučaju. Danas je oprema (pa i softver) "jeftin" i predstavlja vrlo malo stavku u rashodima a mogućnosti za dobitak njihovim radom su velike. Zato ih treba pravilno dizajnirati i iskoristiti. Pogrešna procjena potreba za informatičkom tehnologijom ne samo da vodi trenutnom finansijskom gubitku nego može doprinjeti i mnogostruko većim gubicima ukoliko odabrane komponente daju pogrešne rezultate ali i uticati na donošenje pogrešnih poslovnih odluka.

LITERATURA

[1.] M. Nikolić, Z.Nikolić, Ž.Petrović: "Razvoj jednog rešenja fabričkog informacionog sistema', YUInfo2009, 2009.
[2.] D. Regodić: "Logistika", Univerzitet Singidunum, Beograd, 2011.
[3.] J. Wilder: "The Case for In-house development", Hospitality Upgrade, 2009.
[4.] P.Jovanović, N.Dragomanović, V.Mišković, S.Drobnjaković: "Transfer znanja kao podproces menadžmenta znanja", VIII skup privrednika i naučnika, FON, Beograd, 2011.
[5.] "Godišnji izvještaj o radu Žitopromet ad Bijeljina za 2012.godinu", Bijeljina, 2013.
[6.] I. Beker: "Upravljanje zalihama", Fakultet tehničkih nauka Univerziteta u Novom Sadu, Novi Sad, 2011.

KRIPTOGRAFSKA SMENA GENERACIJA

Dragan Vidaković
Poslovni fakultet Valjevo –odeljenje Ivanjica
dragan.vidakovic@open.telekom.rs
Duško Parezanović
Klub mladih matematičara i programera INFOMAT, Ivanjica
infomat@open.telekom.rs
Jelena Kaljević
Poslovni fakultet, Valjevo
jkaljevic@singidunum.ac.rs

Sažetak
Činilo se da će se upravljanje ključevima i digitalno potpisivanje neprekidno odigravati na terenu RSA ili DH (Diffie-Hellman) i to tako što će svaki novi algoritam za napad biti odbijen jednostavnim povećanjem broja bitova ključa-kao glavne mere sigurnosti. Stvar se drastično promenila radovima Koblica i Milera (Neal Koblitz and Victor Miller) uvođenjem eliptičnih krivih u kriptografiju (Eliptic Curve Criptography -ECC) o čemu će i biti reči u ovom radu.

Ključne reči: Kriptografija, Digitalni potpis, RSA, ECC

Abstract
It seemed to be the key management and digital signatures are played continuously on the ground RSA or DH (Diffie-Hellman), such that each new algorithm for the attack to be rejected simply by increasing the number of bits as the major-key security measures. Thing has changed dramatically works Neal Koblitz and Victor Miller in introducing elliptic curve cryptography (eliptics Curve Criptography-ECC) which will be discussed in this paper.

1. UVOD

The US National Institute for Standards and Technology (NIST) 2009. g. doneo je preporuku [1] da su 1024-bitni parametri za RSA i DH dovoljno sigurni do 2010. g. Posle toga NIST preporučuje nadogradnju na nešto što donosi više sigurnosti. Mogli bi reći i iste sigurnosti ali značajne uštede na resursima i znatno većoj primenljivost i koristi naročito za mnoge nove tehnologije koje nisu ni postojale u vreme kad su Miler i Koblic još 1985. uočili mogućnost korišćenja osobina eliptičnih krivih u kriptografiji.
Za NIST i NSA (National Security Agenci) nema nikakve dileme da ECC obezbeđuje veću sigurnost i bolje perormanse nego tehnike prve generacije javnog ključa (RSA i DH) koji su i danas u upotrebi, te da je u skladu sa tim potrebno ozbiljno razmotriti ECC alternativu koju ona nudi u računskom i propusnom opsegu pri komparabilnoj sigurnosti.

2. RSA PARAMETRI

Ko se ozbiljnije bavio sa RSA zna kako je teško isprogramirati i pronaći 1024 bitni broj, jedan niz 0 i 1 i pri tome još biti uveren da je on prost ili bar broj sa ogromnim prostim faktorima ako sam nije prost.

Potrebno je pre svega pronaći taj broj (testirati ga Miler-Rabinovim algoritmom) i pri tome isprogramirati veliki broj osnovnih i mnogih pomoćnih funkcija, samo da bi se dobio jedan broj p, a potreban je još jedan, pa ih treba pomnožiti, deliti, vršiti eksponencijaciju što je dosta teško i zamorno. [2] Jedan takav broj postoji u [3] a izgleda ovako:
100000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000010000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000001000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000100000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000001000000000000000000000000000001000000000000
000000000000000000000000000000000000010000000000000000000000000000000000000000000000000011
0010111011.
Pomnožiti ovakav broj sa još jednim istim takvim i izvršiti još niz operacija je ono što je NIST preporučio do 2010. a zatim, savetuje da se, gde god je to moguće, pređe na ECC.

3. RAZLOZI ZA SMENU GENERACIJA

Već su iz gornjeg očigledni razlozi koji govore u prilog korišćenja alata zasnovanih na ECC, ali sledeća tabela pokazuje to isto.
Tabela1 predstavlja NIST-ovu preporuku broja bitova potrebnih za zaštitu ključeva u konvencionalnim algoritmima za šifrovanje (npr. DES i AES) pomoću RSA, DH i ECC u cilju obezbeđenja ekvivalentne sigurnosti.

Tabela 1.Poređenje broja bita za istu sigurnost

Simetričan ključ- u bitima	RSA i DH ključ- u bitima	ECC ključ- u bitima
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Dakle, 256-to bitnim ECC parametrom štitimo 128 bitni AES ključ istom sigurnošću kao da ga RSA ili DH štitimo parametrom od 3072 bita.

4. OSNOVE ECC

Eliptičnim krivima nazivamo kubne jednačine tipa (1) $Y^2 = x^3 - ax - b$, pri čemu su a i b celi brojevi (Weistrass-ova jednačina) i najstandardniji je prikaz eliptičnih krivih koje se koriste u teoriji brojeva.

Kriptosistem realizovan na eliptičnim krivama (ECC) zasnovan je na Abelovoj grupi koju formiraju eliptične krive na konačnom polju. Ovo esencijalno znači da „sabiranje“ dve tačke sa krive kao rezultat daje treću tačku koja je takođe na krivoj.
Jedna od najbitnijih operacija za sve aplikacije eliptičnih krivih je skalarna multiplikacija, što označava „množenje“ celog broja tačkom sa eliptične krive. Taj broj je veoma veliki pa je veoma bitno efikasno izvršiti pomenuto „množenje“ koje je veoma složen proces koji se sastoji od niza malih operacija. Preciznije rečeno na eliptičnim krivama postoje samo dve operacije: dupliranje tačke i sabiranje dve tačke. Dakle, skalarno množenje velikog broja i tačke sastoji se od serije dupliranja i sabiranja tačaka sve dok se ne nađe tačka k*P=Q [5]

5. SABIRANJE DVE RAZLIČITE TAČKE

Neka su $P(x_p,y_p)$, $Q(x_q,y_q)$ i $R(x_r,y_r)$ tačke krive (1) tako da je P+Q=R. Tada važi: (2) $y-y_p=s(x-x_p)$, gde je s koeficijenat pravca prave PQ(R).
Takođe važi: (3) $y_p^2 =x_p^3 –ax-b$, (4) $y_q^2 =x_q^3 –ax-b$ i (5) $y_r^2 =x_r^2 –ax-b$.
Iz (3) i (4) dobijamo:
(5) $(y_p - y_q) (y_p + y_q)= (x_p – x_q) (x_p^2 +x_px_q + x_q^2) –a(x_p –x_q)$
Iz (3) i (5) dobijamo:
(6) $(y_r – y_p) (y_r + y_p) = (x_r – x_p) (x_r^2 +x_rx_p + x_p^2) –a (x_r –x_p)$
Ako podelimo (6) sa $(x_p –x_q)$ a (7) sa $(x_r –x_p)$ dobijamo
(8) $s(y_p + y_q) = (x_p – x_q)^2 - x_px_q –a$
(9) $s(y_r + y_p) =(x_r + x_p)^2 - x_rx_p –a.$
Ako od (8) oduzmemo (9) dobijamo
(10) $s (y_q - y_r) = (2x_p + x_p + x_q) (x_q – x_r) –x_p (x_q –x_r)$
Ako (10) podelimo sa $(x_q –x_r)$ dobićemo
(11) $s^2 =2x_p + x_q +x_r – x_p$ i odavde dobijamo
(12) $x_r = s^2 –x_p - x_q$
Kako R pripada pravoj (PQ) tada $s=(y_r – y_p)/(x_r – x_p)$, a odavde dobijamo
(13) $y_r = y_p +s(x_r –x_p)$
(12) i (13) daju koordinate tačke R=P+Q

6. SABIRANJE DVE ISTE TAČKE

Izračunaćemo P+P=R
Ako (6) podelimo sa $(x_r –x_p)$ dobićemo
(14) $s (y_r + y_p)= x_r^2 + x_r x_p +x_p^2 –a$
Kako je sa druge strane $s= y'(x_p)$
i $y'= (3x^2 – a)/2sqrt(x^3 –ax-b)$ tada
(15) $y' (x_p) =(3x_p^2 –a)/2y_p$
Kako je $s=y' (x_p)$ tada je
(16) $s=(3x_p^2 –a)/2y_p$ i odavde je
(17) $- a=2sy_p-3x_p^2$ i kako je $(y_r – y_p)/(x_r – x_p)=s$ tada je
(18) $y_r= y_p +s (x_r – x_p)$
Ako (17) i (18) zamenimo u (14) dobijamo
(19) $s(2y_p +s(x_r – x_p)) =x_r^2 +x_r x_p +x_p^2 +2sy_p-3x_p^2$
Odnosno kad sredimo, dobijamo kvadratnu jednačinu po x_r
(20) $x_r^2 + (x_p – s^2)x_r + s^2x_p – 2x_p^2=0$
Diskriminanta je $D= (3x_p – s^2)^2$

Tada su njena rešenja
(21) $x_r = s^2 - 2x_p$, i $x_r = x_p$ koje odbacujemo.
Iz (13) i (21) dobijamo i y_r a time i koordinate tačke P+P=R.

ZAKLJUČAK

Kako je najbolja zaštita sopstvenim znanjem i sopstvenim alatima [4] bilo bi dobro napraviti sopstvene mehanizme zaštite koji će nas bar u prvom koraku zaštititi od onih koji preko proizvoda koji se mogu naći na tržištu mogu da nadgledaju našu komunikaciju koja je sigurna zaštita od svih osim od onih koji nas štite svojim znanjem i svojim tehnologijama. Niko verujem nema iluziju da se možemo takmičiti sa onima koji su daleko ispred nas ali da je neophodno da povećamo sopstvena znanja i usavršimo svoje alate u to nema nikakve sumnje. Doprinos u tom pravcu je i ovaj rad koji može poslužiti kao podstrek za formiranje sopstvenog alata za digitalno potpisivanje tehnologijom eliptičnih krivih.

LITERATURA

[1.] National Sesurity Agency-NSA,"The Case for Elliptic Curve Cryptography", (pristup 09.02.2013.g.) [dostupno na http://www.nsa.gov/business/programs/elliptic_curve.shtml]

[2.] Dragan Vidakovic[1], Olivera Nikolic[1] and Dusko Parezanovic[2], [1]Singidunum University, Belgrade, Serbia and [2]INFOMAT Ivanjica, Serbia "Acceleration detection of large (probably) prime numbers" International Journal of UbiComp (IJU), Vol.4, No.1, January 2013.

[3.] D. Vidakovic, "Analysis and implementation of asymmetric algorithms for data secrecy and integrity protection", Master Thesis (mentor J. Golic), Faculty of Electrical Engineering, Belgrade, 1999.

[4.] D. Vidakovic, D. Simic :"A Novel Approach to Building Secure Systems", Second International Conference on Availability, Reliability and Security, In 1th IEEE International Workshop on Secure Software Engineering (SecSE 2007), Vienna, 2007., Austria, pp 1074-1081

[5.] Vinay S. Iyengar, "Novel elliptic curve scalar multiplication algorithms for faster and safer public-key cryptosystems" International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012

MEĐUORGANIZACIONI INFORMACIONI SISTEM ZA UPRAVLJANJE POŠILJKAMA

INTERORGANIZATIONAL INFORMATION SYSTEM FOR CONSIGNMENT MANAGEMENT

Bogdan Mirković
Fakultet za informacione tehnologije, Slobomir P Univerzitet
PF 70, Slobomir, 76 300 Bijeljina, Republika Srpska, Bosna i Hercegovina
Telefon: +387 65 664 957
Fax: +387 55 251 444
E-mail: bogdanmirkovic@yahoo.com

Cica Jovanović
Preduzeće za poštanski saobraćaj Republike Srpske ad
Ul. Kralja Petra I Karađorđevića 93, 78000 Banjaluka, Republika Srpska, Bosna i Hercegovina
Telefon: +387 65 395 095
E-mail: cicamirkov@yahoo.com

Sažetak: *Kvalitet proizvoda i usluga koje pruža određeni privredni subjekt direktno utiče na njegov opstanak u savremenom poslovnom svijetu. Upravljanjem kvalitetom pruženih usluga u poštanskom sabraćaju posvećuje se velika pažnja. Primjenom informacionih tehnologija u poštanskom saobraćaju postižu se povećanje produktivnosti, poboljšanje kvaliteta usluga, razvijanje novih usluga, poboljšava se povezanost sa korisnicima. U radu su prikazane osnovne karakteristike sistema za upravljanje pošiljkama zasnovanom na korištenju informaciono-komunikacione tehnologije.*

Summary: *The quality of goods or services provided by a business entity, directly affect its survival in today's business world. In the postal, much attention is paid on quality management of services. Usage of information technology in the postal service provides an increase in productivity, improved service quality, developing new services, improving the relationship with customers. In this paper is present the main characteristics of the system for consignment management based on the use of information and communication technology.*

Key words*: information system, quality, consignment management, interorganizational*

1. UVOD

Svjetski poštanski kongres koji je održan u Vašingtonu 1989. godine je donio Opšti akcioni plan. Ovaj plan je na prvo mjesto stavio zadovoljnog korisnika i kvalitetnije ostvarenje usluga. Svjetski poštanski kongresi održani 1994. godine u Seulu i 1999. godine u Pekingu su još veći akcenat stavili na kvalitet izvršenja usluga. Teži se ka što većem razvoju pošta i od svih poštanskih službi se zahtjeva da što više djeluju na komercijalnoj osnovi. Utvrđene su četiri prioritetne oblasti koje su od velikog značaja za opstanak poštanske djelatnosti: potrebe korisnika

i komercijalna strategija; kvalitet usluga i bolje poslovanje pošta; nezavisnost u upravljanju i razvoju pošta i razvoj ljudskih resursa. Dosadašnje poslovanje pošte se vršilo pod zaštitom države i pružanje javnih usluga se vršilo po fiksnim cijenama. Međutim, sada su ciljevi pošte usmjereni u drugom pravcu. Pošta se razvija u konkurentno preduzeće.

2. SISTEMI ZA IDENTIFIKACIJU POŠILJKI I RAZMJENU PODATAKA

Često postavljana pitanje od strane korisnika poštanskih usluga je u vezi sa statusom pošiljke (trenutna pozicija, lokacija). Korisnike usluga zanima gdje se pošiljka u datom trenutku nalazi, zašto nije prispjela na odredište ili ko ju je primio. Danas se veliki značaj pridaje identifikaciji poštanskih pošiljaka u prenosu. Da bi se obezbjedilo kvalitetno izvršenje usluga u poštanskom saobraćaju, vrši se praćenje pošiljaka u transportu. Na osnovu ovog praćenja bi se moglo doći do podataka zašto se javljaju zastoji na pojedinim mjestima, pa bi se oni mogli otkloniti za veoma kratko vrijeme što utiče na poboljšanje kvaliteta pruženih usluga. Već sada postoji mnogo savremenih sistema za automatsku identifikaciju poštanskih pošiljaka. Veliki broj tih sistema se zasniva na primjeni bar koda. Bar kod se koristi kada ID sistem (Identification Data System) zahtjeva brz i tačan unos podataka. U poređenju sa bar kodom RFID[86] sistemi nude više raznovrsnosti nego bar kodovi. Predajnik sa sposobnošću čitanja/pisanja kao portabl baza podataka, dozvoljava informacijama da budu prihvaćene i identifikovane u bilo kom položaju gdje je čitač osposobljen.

U ranim devedesetim IPC87 (International Post Corporation) započinje razvoj prijedloga za standardne poštanske operacije. To je rađeno u okviru Svjetskog Poštanskog Saveza[88] (UPU), da bi se proizveo niz EDI[89] (Electronic Data Interchange) poruka koje bi bile specifične za poštanske operacije, ali koje bi bile podešene priznatim međunarodnim EDIFACT90 standardima. CAPE projekat je instaliran 1991. godine sa dijelom novčanih sredstava iz Evropske Komisije. Njegova svrha je bila da izgradi informacionu tehnologiju koja bi povezivala izmjenične pošte duž Evrope sa putem od nacionalnih centara, koji su povezani sa svakom poštom. Projekat je počeo sa radom 1993. godine, a tada se vršila razmjena poruka između male grupe pošta, koje su bile od početka partneri u projektu. Danas, CAPE tehnologija prikazuje prenos od 7 miliona poštanskih zaključaka godišnje, između IPC članica u Evropi i Sjevernoj Africi. Od septembra 1996. godine, prenos robe se pratio na oko 1100 međunarodnih ruta. U 1995. godini IPC je pokrenuo incijativu nazvanu CAPE 2000, koja bi podržala razmjenu poruka između aerodroma i pošta. I projekat CAPE 2000 je finansijski podržan od strane Evropske Komisije. Pošte su korišćenjem CAPE 2000 u mogućnosti da prikažu veći stepen saradnje u međunarodnom poštanskom distributivnom lancu. Pošte će imati informacije o identifikaciji i popravljaće uska grla koja utiču na kvalitet obavljanja usluga. Pošte će biti u mogućnosti da usklade veličinu planiranog kapaciteta prema kratkom izvještaju. Korišćenje EDI podataka za finansijski obračun će takođe donijeti uštedu i garantovat će veću tačnost u računima napravljenim od strane aerodroma za tonažu i učestanost prenosa.

[86] Karen L. Jones, James F. Davis & Arthur D. Little: ''RFID frequent solutions for the millennium'', Postal technology '99
[87] www.ipc.be
[88] www.upu.int
[89] Ross Hinds: ''EDI- the key to efficiency'', Postal technology '97
[90] UN: UN/EDIFACT, UN Directories for EDI for Administration, Commerce and Transport

3. MEĐUORGANIZACIONO UPRAVLJANJE POŠILJKAMA

3.1. Poštanski saobraćaj u Republici Srpskoj

Razvoj poštansko-telefonskog-telegrafskog (PTT) saobraćaja u Republici Bosni i Hercegovini treba posmatrati sa stanovišta istorijskih, društveno-političkih i ekonomskih odnosa. Na teritoriji Republike Srpske nakon izbijanja ratnih dejstava u BiH 1992.godine su ostala samo dva poštanska centra: Poštanski centar Banja Luka i Poštanski centar Bijeljina. U to vrijeme, tj. u aprilu i maju 1992. godine organizovani poštanski sistem Republike Srpske nije ni postojao. Upravo iz ovog razloga, Vlada Republike Srpske je 24. maja 1992. godine je u skladu sa Zakonom o preduzećima donijela odluku o formiranju Jedinstvenog javnog preduzeća PTT saobraćaja Republike Srpske. U narednim mjesecima je vršeno stvaranje jedinstvene poštanske mreže, a formirani su i novi poštanski centri. Od 01.01.1997.godine JODP "Srpske pošte" posluje kao samostalno Javno osnovno državno preduzeće. JODP "Srpske pošte" na osnovu Zakona o preduzećima[91], mijenja naziv u Preduzeće za poštanski saobraćaj Republike Srpske AD (skraćeno JP "Srpske pošte" a.d.). Skupština Društva, na sjednici, održanoj dana, 04.12.2002., donijela je Statut Preduzeća za poštanski saobraćaj Republike Srpske AD koji je poslednji put mijenjan u martu 2012.godine[92] u skladu sa Zakonom o privrednim društvima[93] i Zakonom o poštanskim uslugama Republike Srpske[94]. Djelatnosti Društva su: prenos poštanskih pošiljaka, usluge novčanog poslovanja, usluge elektronske pošte i prenos podataka za korisnike poštanskih usluga, internet usluge, izdavačka djelatnost, pružanje savjeta u vezi sa kompjuterskom opremom, obrada podataka, izgradnja baza podataka, prevoz robe i putnika u drumskom saobraćaju, održavanje i popravka motornih vozila, trgovina na malo proizvodima od duvana, knjigama, novinama i pisaćim materijalom i ostala trgovina na malo u prodavnicama mješovite robe.

3.2. Osnovne karakteristike sistema Track and Trace

"Track and Trace" predstavlja sistem za praćenje pošiljaka. Uz pomoć sistema za kontrolu i praćenje mogu se pratiti pošiljke unutar poštanskog operativnog sistema od momenta prijema do uručenja. "Track and Trace" je projektovan da zadovolji potrebe poštanske administracije i korisnika. Sistem "Track and Trace" je prilagođen jednostavnoj i efikasnoj poštanskoj tehnologiji, a može se koristiti u automatizovanim i u neautomatizovanim poštama. On predstavlja ključnu komponentu logističkog sistema pošte, jer ima za cilj pružanje kvalitetnih usluga i zadovoljenje potreba korisnika. Kao osnovna karakteristika poštanskog saobraćaja može se smatrati velika brzina izvršavanja poštanskih usluga. Sistem za kontrolu i praćenje povećava brzinu i tačnost unosa podataka, a vjerovatnoća nastanka greške se svodi na minimum. Sistem podržava stvaranje velikog broja izvještaja, neophodnih za postupak donošenja upravljačkih odluka kao i veliki broj razumljivih i prevashodno čitljivih izvještaja. Proces pretraživanja pošiljaka je efikasniji i mnogo kraći. Na osnovu ovog sistema možemo znati u svakom trenutku gdje je pošiljka. Postoji mogućnost praćenja pošiljke putem interneta. Zanimljivo za ovaj sistem je praćenje zaključaka, a ne samo pošiljaka. Praćenje pošiljke unutar poštanskog operativnog sistema se postiže upotrebom bar koda. Sve informacije koje korisnici kao i radnici pošte žele da

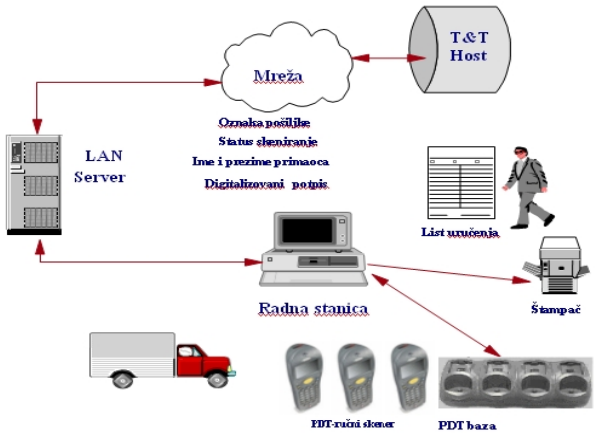
[91] Zakon o preduzećima, Službeni glasnik RS 24/98 i 62/02
[92] Statut preduzeća za poštanski saobraćaj Republike Srpske ad Banjaluka, mart 2012.godine
[93] Zakon o privrednim društvima, Službeni glasnik RS 127/08, 58/09 i 100/11
[94] Zakon o poštanskim uslugama Republike Srpske, Službeni glasnik RS /10

dobiju su pristupačne na osnovu jedinstvenog broja bar koda. Sistem "Track and Trace" ima tri glavne komponente, a one su:

- Portabl terminali za podatke (PDT);
- Radna stanica za kontrolu i praćenje (T&T W/S);
- Host računar za kontrolu i praćenje (T&T Host).

3.3. Obrada podataka

U T&T sistemu svaki PDT ima svoj identifikacioni broj na osnovu kog se vrši prepoznavanje u mreži. Većina podataka se prikuplja preko PDT-a. Svi prikupljeni podaci se prosleđuju do radne stanice za kontrolu i praćenje, a zatim do host računara. Osnovne komponente, odnosno način njihovog povezivanja je prikazan na slici 1.



Slika 1. Način povezivanja komponenti sistema Track and Trace

Na osnovu slike se može uočiti da se svi podaci koje prikupi PDT, šalju na radnu stanicu za kontrolu i praćenje radi dalje obrade. Prenos se vrši preko komunikacione podloge, koja je direktno povezana sa personalnim računarom radne stanice. Podaci se sa T&T W/S prenose na host računar za kontrolu i praćenje na tri načina:

- Svi podaci unijeti sa PDT-a se direktno unose u host računar za kontrolu i praćenje, čim se podaci sa PDT-a prenesu na T&T W/S;
- Status uručenja sa dokumenta List uručenja, kao i ime primaoca se na host računar prenose po unaprijed određenom redosledu (koji je utvrdio administrator);
- Prenos obrađenih podataka sa Lista uručenja je planirani zadatak T&T W/S, a može se izvršiti preko odgovarajućih tastera.

Podaci se u okviru radne stanice čuvaju u periodu predviđenom za tu radnu stanicu. Ne postoji pravilo u kome bi se naveo tačan podatak o periodu čuvanja podataka za sve radne stanice. Za određena radna mjesta je neophodno imati neke podatke i do par mjeseci. Međutim, isti ti podaci su za drugo radno mjesto od veoma malog značaja i njihovo čuvanje nema posebnu važnost. Ako posmatramo podatke u okviru host računara za kontrolu i praćenje, imamo drugo pravilo. Na T&T host računaru se podaci čuvaju koliko i manipulativne isprave, tj. period čuvanja zavisi od vrste isprava.

Mali je broj pošiljaka kod kojih je odredišna i prijemna pošta ista pošta. Na osnovu ovoga možemo zalkjučiti da će gotovo sve pošiljke upravo i ići preko poštanskog centra, a na taj način će se one i evidentirati u T&T sistem. Podaci o pošiljkama, kod kojih je prijemna pošta i

odredišna pošta, su na posebnim dokumentima koji se otpremaju do poštanskog centra (PC) zajedno sa ostalim zaključcima u vrijeme otpreme. Poštanski centar je u ovom slučaju dužan da te podatke preko svojih radnih stanica unese u T&T sistem. PC je dužan da unese podatke o pošiljkama, samo za one pošte koje pripadaju njegovom gravitacionom području. Korišćenjem intranet mreže postoji mogućnost izbora velikog broja izvještaja, među kojima je i "Izvještaj o istoriji pošiljke". Pri biranju željenog prijemnog broja pošiljke dobija se potpun pregled o kretanju pošiljke. Na slici 2 je prikazan pregled o istoriji pošiljke.
Međunarodni saobraćaj je organizovan preko izmjenične pošte u Banja Luci. Sve pošiljke koje glase za Srbiju i Crnu Goru se direktno iz izmjenične pošte u Banja Luci otpremaju za izmjeničnu poštu u Beogradu. U PC Bijeljina se zaključci, koji glase za Srbiju i Crnu Goru, pretovaraju i dalje GPC Beograd organizuje prevoz do izmjenične pošte u Beogradu. Isto važi i za pošiljke koje glase za Republiku Srpsku, a pristižu iz izmjenične pošte u Beogradu.
Pošiljke, koje glase za druge zemlje, se otpremaju ka GPC Sarajevo ili GPC Mostar. Dakle, cjelokupan međunarodni saobraćaj, izuzev sa Srbijom, Crnom Gorom, Slovenijom, Hrvatskom i Austrijom, se obavlja preko GPC Sarajevo i GPC Mostar. Radi praćenja pošiljaka u međunarodnom saobraćaju, radne stanice za IPS su postavljene u izmjeničnoj pošti u Banja Luci.

SRPSKE POŠTE T&T: Izvještaj o istoriji pošiljaka

22.12.2012 15:04:43

Izvještaj o istoriji pošiljaka

Oznaka pošiljke	Opis tipa skeniranja	Datum i vrijeme	JPM	Status isporuke	Potpis
RR489637715RS	Prijem pošiljaka	18.12.2012 11:44:47	76300 Bijeljina		
RR489637715RS	Pošiljke u kontejneru	18.12.2012 12:05:58	76300 Bijeljina		
RR489637715RS	Otprema	18.12.2012 12:35:43	76300 Bijeljina		
RR489637715RS	Prispjeće kontejnera	18.12.2012 13:05:23	76300 Bijeljina		
RR489637715RS	Pošiljke u kontejneru	18.12.2012 18:21:25	76300 Bijeljina		
RR489637715RS	Otprema	18.12.2012 18:30:13	76300 Bijeljina		
RR489637715RS	Prenos	18.12.2012 18:36:52	76300 Bijeljina		
RR489637715RS	Prispjeće kontejnera	19.12.2012 00:24:25	78000 Banjaluka		
RR489637715RS	Pošiljke u kontejneru	19.12.2012 06:03:36	78000 Banjaluka		
RR489637715RS	Otprema	19.12.2012 06:23:18	78000 Banjaluka		
RR489637715RS	Prispjeće kontejnera	19.12.2012 07:49:05	78000 Banjaluka		
RR489637715RS	Dostava u toku	19.12.2012 09:56:21	78000 Banjaluka		
RR489637715RS	Status uručenja	19.12.2012 14:59:35	78000 Banjaluka	0	
RR489637715RS	Dostava u toku	19.12.2012 15:23:08	78000 Banjaluka		
RR489637715RS	Pošiljke u kontejneru	19.12.2012 18:06:23	78000 Banjaluka		
RR489637715RS	Otprema	19.12.2012 19:23:40	78000 Banjaluka		
RR489637715RS	Prispjeće kontejnera	20.12.2012 06:27:06	78000 Banjaluka		
RR489637715RS	Pošiljke u kontejneru	20.12.2012 12:16:49	78000 Banjaluka		
RR489637715RS	Otprema	20.12.2012 13:09:04	78000 Banjaluka		
RR489637715RS	Prispjeće kontejnera	20.12.2012 13:45:21	78000 Banjaluka		
RR489637715RS	Pošiljke u kontejneru	20.12.2012 18:57:40	78000 Banjaluka		
RR489637715RS	Otprema	20.12.2012 19:03:08	78000 Banjaluka		
RR489637715RS	Prispjeće kontejnera	21.12.2012 07:32:23	78000 Banjaluka		
RR489637715RS	Status uručenja	21.12.2012 09:38:08	78000 Banjaluka		

Slika 2. Izvještaj o istoriji pošiljke iz sistema Track and Trace

Prerada pošiljaka se vrši preko radnih stanica koje su povezane sa IPS serverom preko LAN-a. LAN uz to omogućava i štampanje potrebne dokumentacije i bar kod naljepnica. Server je konektovan na nacionalnu informatičku poštansku mrežu. Svi podaci se prenose u nacionalnu IPS bazu podataka, koja se nalazi u Banja Luci. Podaci su dostupni preko Web site-a Srpskih pošta ili preko Intraneta.

ZAKLJUČAK

Poštanski saobraćaj u svijetu razvija se uporedo s razvojem proizvodnih snaga i s razvojem ostalih saobraćajnih grana. Nekadašnja spora vozila (diližanse) zamjenjena su na kopnu željeznicom i motornim vozilima, na moru trgovačkom flotom, a koriste se i sredstva

vazduhoplovnog saobraćaja. Karaketristike poštanskog saobraćaja u savremenom svijetu su: brzina, regularnost, relativno niske cijene uz veoma visok kvalitet pruženih usluga.
"Track and Trace" sistem je prilagođen poštanskoj tehnologiji. Njegov cilj je zadovoljenje korisnika, kao i kvalitetnije pružanje usluga. Korišćenjem ovog sistema povećava se brzina i tačnost unosa podataka, a vjerovatnoća pojave greške je svedena na minimum što u krajnoj mjeri poboljšava kvalitet usluga koje se pružaju korisnicima.

LITERATURA

[1.] Karen L. Jones, James F. Davis & Arthur D. Little: *RFID frequent solutions for the millennium*, Postal technology '99, 1999.
[2.] www.ipc.be
[3.] www.upu.int
[4.] UN Economics Commission for Europe: *UN/EDIFACT*, UN Directories for Electronic Data Interchange for Administration, Commerce and Transport
[5.] Ross Hinds: *EDI- the key to efficiency*, Postal technology '97, 1997.
[6.] Zakon o preduzećima, Službeni glasnik RS 24/98, 1998.
[7.] Zakon o preduzećima, Službeni glasnik RS 62/02, 2002.
[8.] Preduzeće za poštanski saobraćaj Republike Srpske ad, *Statut preduzeća za poštanski saobraćaj Republike Srpske ad Banjaluka*, mart 2012.
[9.] Zakon o privrednim društvima, Službeni glasnik RS 127/08, 2008.
[10.] Zakon o privrednim društvima, Službeni glasnik RS 58/09, 2009.
[11.] Zakon o privrednim društvima, Službeni glasnik RS 100/11, 2011.
[12.] Zakon o poštanskim uslugama Republike Srpske, Službeni glasnik RS /10, 2010.