

Sekcija 3. INFORMATIKA

“Privredni kriminalitet i savremeno poslovanje”

Specifičnosti veštačenja u informacionim tehnologijama	Gojko Grubor, Nenad Ristić, Ivan Barać	1
The Application of Information Analysis in Forensic Linguistics	Marijana Prodanović, Saša Adamović	2
The Implications of the Maturity Level of Strategic Alignment of ICT Systems Projects on Economic Criminality	Hajrudin Imamović, Gojko Grubor, Dušan Regodić	3
Penetraciono testiranje Android aplikacije	Mladen Veinović, Miroslav Čajić	4
Modelovanje tokova podataka u kazneno-popravnim institucijama Republike Srpske	Bogdan Mirković	5
Višekriterijumski pristup organizaciji rada računara u malim i srednjim preduzećima sa stanovišta zaštite i forenzike	Mališa Žižović, Nada Damljanović, Kosana Vićentijević, Jelena Kaljević, Miodrag Žižović	6
Cyber kriminal i digitalna forenzika	Slađan Soldat, Gojko Grubor	7
Uticaj globalnih mreža i savremenih informacionih sistema na nastanak i razvoj forenzičkog računovodstva u Srbiji	M. Milojević, P.Vukadinović, D. Miletić	8
Tehnike otkrivanja privrednog kriminaliteta	Munir Hadrović, Slavica Pantović	9
Dijeljenje i integracija informacija u kazneno-popravnim institucijama Republike Srpske	Bogdan Mirković, Nenad Mirkonj	10
Održavanje flote: Upotreba data mining-a i statistike u prevenciji zloupotreba	Miloš Dobrojević	11

Specifičnosti veštačenja u informacionim tehnologijama

Specificity of expertise in information technology

Gojko Grubor, Univerzitet Sinergija, Nenad Ristić, Univerzitet Sinergija, Ivan Barać

Sažetak— Sve većom upotrebom računara i razvojem informaciono komunikacionih tehnologija (IKT) rastu i zloupotrebe i novi oblici kriminala i načina izvršenja klasičnih krivičnih dela. Računarska tehnologija je zamenila klasična sredstva izvršenja krivičnih dela. Glavna oružja sada su miš, tastatura, skener, printer itd., oni postaju sve pristupačniji širokom krugu korisnika. Iskušenja i izazovi su veliki, jer se u banku može provaliti iz fotelje, bez izlaganja riziku fizičkog prisustva i ostavljanja otisaka u banci, a mogućnosti ostvarivanja nelegalne koristi su fascinantne. Posledice mogu biti katastrofalnih razmera, jer samo jedna osoba sa hakerskim znanjem i alatima može naneti ogromna materijalna šteta i ugroziti čak i nacionalnu bezbednost. Po pravilu kompjuterski kriminalci su uvek u prednosti ispred istražnih organa - policije, tužilaštva, suda. Kompjuterski kriminalci razvijaju nove sofisticirane metode napada za proboj tradicionalnih, reaktivnih sistema zaštite koji postaju neefektivni. Autori ovog rada su, zbog kompleksnosti procesa digitalne forenzičke istrage, fokusirali istraživanje na odlučujuću fazu rekonstrukcije događaja, dokazivanja i svedočenja/veštačenja digitalnih dokaza kompjuterskog kriminala na sudu.

Ključne riječi – kompjuterski kriminal, izbor veštaka u IKT, iskustva veštačenja, prihvatljivost digitalnog dokaza, funkcionalni model IKT svedočenja/veštačenje

Abstract – Alongside with more computer use and ICT development, computer misuse and new forms of the crime increase, too. Computer technology has replaced traditional means for crime committing. Mouse, keyboard, printer, scanner, etc, are the main weapons in computer crime. They are more and more available to the people connected to the Internet. Temptation and challenges are huge. Someone with hacker's knowledge and tools can get in a bank from the armchair, without entering to the bank and leaving fingerprints. Possibilities for crime and getting illegal benefits are becoming fascinating. Computer crime consequences could be catastrophic, and risky even for national security. As a rule, computer criminals are always in front of law enforcement. They are developing new sophisticated methods for attacks and penetration into traditional and reactive security systems of the users that are becoming ineffective. The authors of this paper focused research to the decisive phase of the incident/crime reconstruction, proofing and digital evidence presentation in a courtroom due to digital forensic investigation complexity and specific environment for digital evidence presentation and expert witness.

Keywords – computer crime chose of the expert witness in ICT, expert witness testimony experience, digital evidence

admissibility in courtroom, functional model of expert witness testimony

I. UVOD

Raznovrsnost i stalno usavršavanje pojavnih oblika kompjuterskog kriminala onemogućava, precizno i opšte prihvaćeno definisanje tog fenomena. I pored definicija brojnih autora, još nema međunarodno priznate, globalne definicije kompjuterskog kriminala. Takođe, još uvek nije postignuta potpuna saglasnost ni oko njegovog naziva: kompjuterske zloupotrebe (computer abuse), kompjuterske prevare (computer fraud), kriminal povezan sa kompjuterom (computer-related crime), kriminal podržan kompjuterom (computer-assisted crime), sajber (kiber) kriminal (cyber crime) i konačno, kompjuterski kriminal (computer crime), koji se najčešće koristi.

Ekspertska grupa Organizacije za ekonomsku saradnju i razvoj (OECD) definiše kompjuterski kriminal kao „svako ilegalno, neetičko ili neautorizovano ponašanje koje uključuje automatsku obradu podataka ili njihov prenos”. Interpol definiše kompjuterski kriminal (decembra 1981.) kao “svaki ilegalan akt za čije je uspešno izvršenje, istragu, gonjenje ili kažnjavanje esencijalno poznavanje kompjuterske tehnologije”. Sveobuhvatnu i opšteprihvaćenu definiciju u domaćoj literaturi dao je profesor Đorđe Ignjatović, određujući kompjuterski kriminal kao poseban vid inkriminiranih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekt krivičnog dela, ukoliko se delo na drugi način, ili prema drugom objektu, uopšte ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.

U istrazi kompjuterskog kriminala učestvuju klasični organi istrage i organi digitalne forenzičke (DF) istrage koji imaju tri osnovne uloge – forenzičar istražitelj, forenzički analitičar i forenzičar stručni svedok/veštak. U većini slučajeva, posebno u modelu korporacijske DF istrage, sve tri uloge izvršava ekspert za sisteme informaciono komunikacionih tehnologija (IKT), specifično za DF. U modelu javne (zvanične) DF istrage sve tri uloge su pokrivene različitim specijalistima. Tako fizičku akviziciju osumnjičenog sistema/uređaja mogu vršiti obučeni policajci, a DF analitičar u forenzičkoj laboratoriji ispituje digitalne podatke (DP), otkriva tragove digitalnih dokaza (DD), analizira koraborativne DD i izgrađuje čvrsti, neoboriv DD,

relevantan za slučaj i prihvatljiv na sudu. Najčešće se DF analitičar javlja u ulozi eksperta svedoka/veštaka na sudu. Iznošenje DD na sudu, razumljiva i jasna interpretacija za tehničko osoblje suda postaje ključna faza DF istrage za pravosnažnu presudu i sankcionisanje kompjuterskih kriminalaca.

II. CERTIFIKACIJA EKSPERTSKIH ZNANJA I FORENZIČKIH KOMPETENCIJA

Postoji dilema o tome ko treba da odlučuje da li je neki IKT ekspert, stvarno ekspert za svedočenje i veštačenje slučajeva zloupotreba i kompjuterskog kriminala pred sudom ili drugim državnim organima i telima. Pitanje je da li sudije mogu odlučivati da li je neki IKT ekspert dovoljno kvalifikovan, kad ne poznaju pitanja o kojima se raspravlja. U svetu je debata razrešena na osnovu nivoa obrazovanja (npr. doktor DF) ili prihvatanja sertifikata sa konsenzusom profesionalnog strukovnog udruženja ili profesionalne interesne zajednice. U svakoj nacionalnoj državi treba da postoje akreditovana tela za sertifikaciju, koja daju različite sertifikate iz predmetne oblasti. Sud prihvata da je određeni IKT ekspert kvalifikovan ako ima neki relevantni sertifikat ovih tela i institucija ili univerzitetsku diplomu. Kredibilitet i reputacija institucija i tela koje daju sertifikate svakako se procenjuje u svakom konkretnom slučaju, ali obično sud ne

sumnja u takve preporuke. Priroda naučne ekspertize je da se organizuje u strukovna udruženja, zainteresovana da štite standarde koji se zahtevaju u određenoj naučnoj oblasti. Nažalost, u IKT oblasti tipovi ekspertskih grupa i udruženja su sasvim različiti po formi i funkcijama od drugih naučnih i profesionalnih zajednica. Ovo nije akademska ili filozofska teza. Jedan kompetentan ekspert lako može ugroziti otkrivanje činjenica iz digitalnih podataka, ako u suštini greši, menja podatke iz neznanja, pravi činjenice i izmišlja nepostojeće standarde u toku DF veštačenja.

Problem može postati neprijatan i otežati se kontroli kada zbog istinskog moralnog stava jedan IKT ekspert ne može zauzeti suprotan stav od drugog u toku svedočenja/veštačenja. Ili, IKT veštak (ekspert) se suočava sa teškim moralnim i praktičnim problemom kada se, zbog legalnog zahteva da svedoči krajnje objektivno, mora suprostaviti drugom veštaku (često iz iste interesne grupe ili udruženja). Zato većina IKT eksperta odbiju svedočenja/veštačenja na sudu ili umesto toga nude konsultantske usluge, ako sa druge strane sedi drugi nedovoljno kvalifikovan i iskusan ekspert.

A. Iskustva veštačenja iz drugih naučno-tehničkih disciplina

Iskustva veštačenja iz drugih disciplina su dragocena za veštačenje u oblasti DF istrage kompjuterskog kriminala. Ključna iskustva veštačenja u tehničkim i drugim disciplinama sumirana su u Tabeli 1.

Tabela 1. Forenzička iskustva u drugim disciplinama

Disciplina veštačenja	Ključna iskustva
Forenzika saobraćajnih udesa	Veštak je često automehaničar, SSS, koje advokati odvrću od veštačenja, strahom od unakrsnog ispitivanja i napada na pristrasnost, predrasude, neobjektivnost i korupciju veštaka. Uticaj advokata u pripremi veštaka za glavni pretes je najopasniji po integritet svedoka, postepen je, delikatan i svedok ga obično nije svestan [1].
Forenzika umetničkih dela	Kao u proceni falsifikata umetničkih dela, IKT ekspert mora rekonstruisati DD - podatak u kompjuteru, ponašanje RM u slučaju upada, testiranje upada i rekonstrukciju sistema zaštite, identifikaciju i autentifikaciju DD i njihovih autora ili korisnika u slučaju kompjuterskog kriminala. Velika je sličnost u određivanju autentičnosti umetničkog dela i DP iz log datoteke sistema za detekciju upada (IDS) u računarsku mrežu.
Forenzički arheolozi	Iskustva o tome kako izneti svoja naučna saznanja drugim ekspertima i zvaničnim organima, koji nemaju njihova znanja i iskustva, dragocena su za DF eksperte. Ovi eksperti potpisuju i sprovode u praksi mnogo etičkih i drugih kodeksa ponašanja i moraju poštovati brojne procedure i standarde. Moraju održati svoju akademsku i profesionalnu reputaciju na najvišem nivou, jer će suprotna strana uvek pokušavati dovesti u pitanje pojedine delove kredibiliteta eksperta. DF ekspert, kao i forenzički arheolog, mora biti familijaran sa nizom prostorno distribuiranih konfiguracija na terenu u pokušaju rekonstrukcije ponašanja RM u slučaju kompjuterskog napada sa Interneta.
Forenzički entomolozi	Forenzički entomolozi pomažu u utvrđivanju vremena ubistva i lokaciji tela u trenutku ubistva, analizom dokaza koji se odnose na insekte. U kompjuterskom svetu reč bug (buba) označava seriju softverskih grešaka i problema vezanih za tokove podataka u kompjuterima, gde je osnovno pravilo da su sve informacije na raspolaganju svim korisnicima. Suviše mnogo dokaza je često glavni problem za DF analitičare. Postoji potreba opšte edukacije o potencijalnim rezultatima forenzičke analize digitalnih dokaza i to: pravosudnih organa (sudija i tužioca); organa za istragu kompjuterskog incidenta i digitalnih dokaza i zajednice forenzičkih analitičara DD.
Forenzička medicina	U sudskoj medicini, uspostavljeni standardi su podvrgnuti proverbi naučne javnosti, što se zahteva i za DF, uključujući uspostavljanje pouzdanih standarda iz oblasti DF istrage, ekspertskog svedočenja/veštačenja. Kao patolog sudske medicine, koji skuplja uzorke tela za analizu, tako i digitalni forenzičar treba da uzme fizičku kopiju (tzv. forenzički imidž) podataka sa medija računarskog sistema i drugih uređaja za skladištenje podataka za forenzičku analizu i ispitivanje. Sudnica je strana i negostoljubiva sredina za IKT eksperta – naučnika.

B. Priprema digitalnih dokaza za sudski process

U toku pripreme za prezentaciju slučaja na sudu koji uključuje DD treba imati na umu razna pitanja. Najznačajnije je, svakako, da prezentacija digitalnih dokaza zahteva poznavanje specijalizovanih i kompleksnih alata za forenzičku analizu i prezentaciju DD. Zato je za tužioce i istragu važno [3, 8]:

- da obezbede osnovna znanja o tehničkim aspektima DD u opštim crtama, i
- da dopuste dovoljno vremena za menadžment raspoloživih DD u slučaju.

Kako efikasne priprema za glavni pretres počinju već nakon završetka istražnog postupka, potreba za kompetentnim tehničkim znanjima održava se kroz ceo tok slučaja. U predistražnom postupku, u procesu pripreme treba obratiti pažnju na:

- Preliminarna razmatranja tužioca, o obimu istrage koji se odnosi na DD.
- Efikasnu komunikaciju između tužioca, organa istrage i forenzičkog analitičara.
- Menadžment DD (autentifikacija DD, DF alata/tehnika i posrednost DD).

Idealno, slučaj sa DD treba da razvije i priprema tim koji se sastoji od najmanje tri lica [5]: (1) tužioca, (2) kriminalističkog inspektora (vodećeg organa istrage) i DF istražitelja. Često slučaj sa DD predstavlja specijalno proceduralno i materijalno pitanje. Jedan od prvih zadataka tužioca naimenovanog za slučaj, je pregled obima istrage, što uključuje nekoliko ključnih pitanja:

- Priprema i prezentacija razumljive i prihvatljive teorije slučaja za glavni pretres.
 - Razjašnjavanje tehnološke prirode kriminala (visokotehnološki ili ne?)
 - Ako slučaj ne uključuje kriminal visoke tehnologije, da li je DD ipak važan za slučaj?
 - Da li je DD uključen u istagu ili prezentaciju slučaja (npr. animacija ubistva)?
 - Identifikacija i objašnjenje izvora i prirode DD u slučaju:
 - Da li su kompjuterski memorijski uređaji dokazi, kontradokazi ili instrumenti KK?
 - Koji hardver, softver, OS i sistem konfiguracije su korišćeni za napad?
 - Da li je DD pronađen na izolovanom računaru ili na RM?
 - Identifikovanje potencijalnih izvora koraborativnih DD.
 - Razmatranje svih odgovarajućih kazni za slučaj.

C. Svedočenje/veštačenje IKT eksperta (expert opinion testimony)

Procedura za postavljanje zahteva i veštačenje/svedočenje digitalnog forenzičara na sudu odvija se u tri glavne faze:

- Identifikacija pitanja koja zahtevaju svedočenje/veštačenje;
- Identifikacija kvalifikovanog eksperta/veštaka, i

3. Obezbeđivanje da kvalifikovani ekspert/veštak koristi prihvatljive (naučne) metode.

U međunarodnoj praksi razvijeno je više preporuka za ispitivanje mišljenja IKT veštaka i prihvatanje istih kao dokaza na sudu. U praksi IKT veštačenje u SAD-u najčešće se prihvataju Daubert principi, koji su zamenili Fry test u pravosudnoj praksi [2]. Po ovim principima sudija prihvata DD na osnovu njegove relevantnosti i težine, kao i pouzdanosti korišćenih naučnih metoda i tehnika akvizicije i analize DD za konkretan slučaj. Sud odlučuje da li je svedočenje/veštačenje IKT eksperta bilo od pomoći za utvrđivanje činjenica i istine i da:

- su forenzičke tehnike i alati naučne testirane i da mogu biti verifikovane,
- su podvrgnute višestrukoj recenziji naučnih krigova u eminentnim stručnim časopisima,
- postoji poznat ili potencijalni stepen grešaka forenzičkih tehnika i alata, i
- da su generalno prihvaćene u naučnoj zajednici.

Ova lista zahteva (preporuka) nije konačna niti iscrpljena i na tome treba da rade pravosudni sistem i nauka o IKT. Pravosudni sistem mora da zahteva da sudovi ograniče primenu ovih principa na prihvatanje DD dobijenih tzv. pseudonaučnim metodama i tehnikama i da ohrabre razvoj pouzdanih naučnih i tehnoloških tehnika DF akvizicije i analize DD. Sličnost je prihvatanje dokaza u slučaju ubistva, kada sud ne dovodi u pitanje naučnu zasnovanost detektora metala kojim je otkrivena čaura iz oružja iz kojeg je ubistvo izvršeno. Tehničko ekspertsko mišljenje je prihvatljivo (amandman FRE 702, SAD) ako je:

- Svedočenje zasnovano na dovoljno činjenica i podataka;
- Svedočenje je rezultat pouzdanih principa i metoda, i
- Svedok prezentira principe i metode pouzdano na suđenju.

Forenzički analitičari koji uvode nove softverske metode i nove verzije starijih softverskih alata za analizu digitalnih medija, moraju primenjivati ove principe na nove softverske alate. Takođe, tehnike za primenu alata za akviziciju i analizu digitalnih dokaza, na osnovu kojih forenzički analitičari izvlače zaključke, moraju biti za sud relevantne i pouzdane, u skladu sa usvojenim principima. Za međunarodnu razmenu rezultata DF istrage, potrebna je standardizacija principa, procesa, alata i tehnika DF istrage

Postojeći industrijski standardi kvaliteta i zaštite informacija (ISO 9004, ISO 31000, ISO 26000, ISO/IEC 27001, 27032, 27033, 27034 i 27035), takođe, treba da se primenjuju u okviru menadžmenta bezbednosti informacija, uključujući DF istragu. Razvijeni su ili u razvoju novi međunarodni standardi namenjeni za DF istragu. Standard ISO/IEC 27037 pokriva samo tri komponente procesa DF istrage: akviziciju, čuvanje integriteta DD i analizu. Namena ISO/IEC 27041 standarda je da opiše mehanizme, metode i procese za prvi odgovor na kompjuterski incident ili kriminal, čime se obezbeđuju relevantni DD za kasniju DF istragu. Standard ISO/IEC 27042 opisuje smernice za proces analize, interpretacije i koraborativne izgradnje čvrstog DD. Primenom smernica standarda obezbeđuju se jednaki rezultati analize

forenzičara koji rade na istim DP i sa različitim DF alatima. Standard daje osnove za izbor DF alata i kompetencija forenzičara. Harmonizovan proces DF istrage je predstavljen u standardu ISO/IEC 27043. Namena ovog standarda je primena principa i procesa DF u istrazi kompjuterskog incidenta, koji obezbeđuju proaktivnu zaštitu i izvlačenje forenzički relevantnih podataka za DF istragu.

D. Prezentacija digitalnih dokaza na sudu

Suđenja koja uključuju DD razlikuju se od svih drugih suđenja sa dva glavna aspekta:

1. Gotovo uvek se pokrene pitanje legalnosti prihvatanja DD, i

2. Proces može uključiti kompleksni skup nepoznatih pojmova, termina i koncepata.

Zato je pažljiva priprema DD i planiranje svedočenja/veštačenja od posebnog značaja. Ako je slučaj kompleksan, upoznavanje svih u sudnici u svakoj fazi suđenja treba da obuhvati najmanje pitanja provere usklađenosti sa principima i standardima prihvatljivosti DD i princip prihvatljivosti posrednih DD. Iako je važno sudiju (i porotu) održavati na minimalnom nivou razumevanja, nije cilj da se od njih stvaraju eksperti za kompleksnu problematiku IKT veštačenja. Osnovno pravilo je da se svedočenje/veštačenje izvodi što jednostavnijim i razumljivijim jezikom i drugim neverbalnim i vizuelnim metodama. Imajući na umu da će druga strana uvek pokušavati da stvari učine složenijim negi što jesu, treba razmotriti koja pitanja prezentirati u glavnom pretresu, a koja ostaviti za unakrsno ispitivanje.

Svaki slučaj zahteva da se pažljivo ispitaju elementi optužnice i forenzičkih zahteva da bi se obezbedilo svedočenje/veštačenje uverljivih dokaza za svaki elemenat optužnice. Slučaj sa DD često zahteva da tužilac odredi šta se može i šta treba eliminisati uz razumno objašnjenje DD. Ključna pitanja su treba li opovrći sva alternativna objašnjenja i da li sva razumna alternativna objašnjenja mogu biti opovrgnuta? U tom kontekstu značajno je razmotriti sledeća pitanja [3]:

1. Tehničke anomalije vezane za prirodu DP kada postoji konflikt između praktičnih ograničenja na to šta se može dokazati ili opovrći (pobiti) i šta od alternativnih objašnjenja druga strana može iskoristiti da unese razumnu sumnju u postupak ili DD.

2. Alternative osporavanja DD zavise od samog pitanja i snage preostalih dokaza u slučaju. Na primer: u slučaju dečije pornografije, osumnjičeni tvrdi da su slike uskladištene bez njegovog znanja, tzv. trojanska odbrana. Ili, kada se razlikuju hash vrednost između originalnog dokaza i forenzičkog duplikata, ali ako postoji preovlađujući broj dokaza u računaru (na primer, hiljade porno slika), onda se razlika heš vrednosti može opisati i komentarisati kao nebitna za stvarni slučaj.

3. Pravovremenost pobijanja tvrdnji druge strane je suština uspeha i najbolje je uraditi to na glavnom pretresu.

E. Veštačenje visokotehnološkog kriminala i naučne metode dokazivanja

Sudija i tužilac u svakom slučaju donose odluku o tome da li je IKT veštak potreban u slučaju koji uključuje kompleksne tehnologije i ekstenzivnu forenzičku analizu DD i da li je veštak kvalifikovan. Pri tome, treba imati na umu da IKT ekspert može da svedoči o ekstremno kompleksnim stvarima, a da ne bude stalni sudski veštak. U tom slučaju ekspert iznosi samo otkrivene činjenice, a ne iznosi svoje mišljenje. Stalni sudski veštak, pak, iznosi otkrivene činjenice i svoje stručno mišljenje o posebnim pitanjima u slučaju. Na primer po pitanju da li je DD bio ili ne na računaru osumnjičenog, forenzički analitičar je samo običan svedok za utvrđivanje činjenice i ne mora da iznosi svoje mišljenje. Slično je u slučaju gde se metal detektor koristi za otkrivanje čaura na mestu zločina, gde nema potrebe određivati "naučni" nivo metal detektora. U ovom primeru, iako ekspert ne treba da objašnjava kako je čaura ili metak pronađen, ipak, odgovor da li nađeno zrno odgovara zrnu ispaljenom iz oružja osumnjičenog, zahteva posebno mišljenje veštaka balističara. Na sličan način mogu se posmatrati mnogi slučajevi koji uključuju DD i kada je potrebno mišljenje IKT veštaka [7].

U radu sa IKT veštacima u slučajevima sa DD, pravosudni sistem treba da obrati pažnju na:

1. Identifikovanje zajednice kvalifikovanih eksperata - forenzičara iz oblasti IKT.

2. Objašnjenje legalnih ograničenja u istrazi i ispitivanju raspoloživih DD.

3. Planiranje rada u skladu sa usvojenim principima i međunarodnim standardima.

U pripremi svedoka/veštaka za suđenje advokat strane koja zahteva veštačenje treba da:

- Nauči svedoka/veštaka da ispriča tehničku priču na prihvatljiv način.

- Učini direktno saslušanje jednostavnim i interesantnim.

- Inicira primenu pomoćnih vizuelnih sredstva za kompleksne koncepte DF istrage.

- Nauči svedoka/veštaka kako da izbegava greške u ponašanju i svedočenju.

- Upozna svedoka/veštaka sa svojom hipotezom slučaja.

- Podrži izradu nacrt svedočenja/veštačenja sa vlastitim izveštajem.

- Pripremi svedoka/veštaka za unakrsno ispitivanje.

- Vežba sa svedokom/veštakom za nastup u sudu.

Iako se svaki slučaj sa DD međusobno razlikuje, postoje neki zajednički elementi koje se javljaju u odnosu na osnovne elemente optužnice i prirodu računara i RM, a to su:

- utvrđivanje identiteta osumnjičenog,
- dokazivanje znanja osumnjičenog o DD,
- utvrđivanje hronologije događaja kompjuterskog kriminala.

Identitet osumnjičenog može se otkriti na više načina ali se zahteva direktno povezivanje osumnjičenog sa računarom sa kojeg je napad izvršen. Osumnjičeni može lično biti povezan za informacije nađene u računaru na razne načine, uključujući: lično priznanje ili izjavu; posredno (jedini stanovnik na

lokaciji računara, ili registrovani korisnik); bitne informacije u računaru postoje jedino sa znanjem osumnjičenog; analiza sadržaja ukazuje na jedinstvenu sličnost između gramatike i spelinga ili drugih karaktersistika dokaza, sa drugim pisanim dokumentima za koje se zna da ih je pisao osumnjičeni.

Znanje osumnjičenog o DD u računaru, potrebno je dokazati u slučaju tzv. trojanske odbrane kada se osumnjičeni izgovara da je DD u računar uneo trojanac. Ovakva tvrdnja osumnjičenog se često može opovrći sa: brojem takvih fotografija; strukturom direktorijuma koji je logički povezan sa slikama (npr: C:/Pictures/young/girls/sex); imenima datoteka, koja su najčešće jedinstvena i tačno opisuju sadržaj datoteke (npr: 8yrolld.jpg, baby.jpg) itd.

Hronologija događaja je moćan dokaz koji povezuje osumnjičenog sa računarom i kompjuterskim incidentom. Tipičan dokaz su vremena i datumi pristupa računaru i drugim mrežnim uređajima. Iako se ovi podaci mogu lako manipulirati i zavise od tačnosti internog časovnika i vremenske zone, mogu se objasniti uspostavljanjem vremenske linije upada u RM.

Forenzički analitišar (veštak) može na sudu dokazati tačnost ili netačnost vremena i datuma koristeći sledeće forenzičke tehnike:

1. Konzistentnost vremena i datuma štampanja sa istim u fajlovima,
2. Tačnost Internet fajlova ili konzistentnost kreiranja datuma fajla sa datumom u fajlu,
3. Poređenjem datuma e-mail hедера sa vremenom i datumom kojeg upisuje sistem,
4. Poređenjem poznatih vremena i datuma sa vremenom i datumom kojeg upisuje sistem,
5. Upoređivanjem mrežnih podataka o vremenu i datumu (forenzička vremenska linija),
6. Obrazac kreiranja vremena i datuma fajlova (svi kreirani u isto vreme) itd.

F. Funkcionalni model svedočenja/veštačenja DD na sudu

U istrazi kompjuterskog kriminala od pronevera, do krađe intelektualne svojine i dečije pornografije DD-i igraju sve značajniju ulogu. Pošto su DD vrlo laki za manipulaciju, ako

forenzičar ostavi nedokumentovanu prazninu u pristupu DD u fazi akvizicije ili analize, DD neće biti prihvatljiv na sudu. Bez dokaza o uspostavljanju adekvatnog lanca fizičkog čuvanja i dokaza o integritetu (autentičnosti) DD, sud će odbaciti DD kao neprihvatljiv zbog sumnje u korupciju i kontaminaciju. Sledeći izazov za forenzičara svedoka/veštaka je kako da saopšti kompleksne tehničke detalje na sudu ljudima koji su tehnički neobrazovani. Za prezentaciju DD na sudu forenzičar mora početi pripremu znatno ranije kroz sve faze procesa DF istrage - od trenutka privremenog oduzimanja fizičkih uređaja i akvizicije DP do svedočenja/veštačenja na sudu.

Da bi obezbedio prihvatljivost DD na sudu, DF istražitelj mora imati sudski nalog za DF istragu i ispitivanje DD i dokumentovati sve aktivnosti nad fizičkim izvorima DD od trenutka fizičke i logičke akvizicije, u toku oporavka, izvlačenja i analize DD do izveštavanja i svedočenja/veštačenja na sudu. Funkcionalni model procesa pripreme IKT veštaka za svedočenje/veštačenje na sudu prikazan je na slici 1.



Slika 1. Model procesa pripreme IKT svedočenja/veštačenja ([4], prilagođeno od strane autora)

U skladu sa osnovnim principom DF istrage, DF istražitelj mora obezbediti autentičnost DP od trenutka fizičke akvizicije do završetka procesa svedočenja/veštačenja i arhiviranja DD. Ovaj dokaz se obezbeđuje uzimanjem elektronskog otiska (tzv. heš vrednosti) izvora DD. Ova se vrednost menja za svaku promenu sadržaja DP. Ako su heš vrednosti uzete u fazi logičke akvizicije i na kraju svedočenja/veštačenja iste, sud prihvata da je sačuvana autentičnost izvornih DP i DD. Ključne aktivnosti u procesu pripreme DF istražitelja za svedočenje/veštačenje na sudu opisane su u Tabeli 1.

Tabela 1. Ključne aktivnosti u pripremi za svedočenje/veštačenje digitalnog forenzičara

R.b.	Faza pripreme	Aktivnost	Kratak opis
1.	Fizička akvizicija	Nalog za pretragu	Pretraga i privremeno oduzimanje osumnjičenih uređaja (fizičkih izvora DD) za ispitivanje u forenzičkoj laboratoriji
2.	Fizička akvizicija	Uspostavljanje lanca čuvanja	Dokumentovanje dokaza o kontinuitetu čuvanja autentičnih izvor DP i DD od pristupa i fizičke akvizicije do arhiviranja procesa
3.	Logička akvizicija	Održavanje integriteta	Uzimanje e-otiska ili e-DNK, tzv. heš vrednosti imidža (bit po bit fizičke slike diska/medija) za dokazivanje integriteta DD
4.	Ispitivanje & Analiza DD	Validacija DD	Provera integriteta DD poređenjem heš vrednosti i dvostruka provera nekih DP, lokacija i značaja za kolaborativnu izgradnju čvrstog DD
5.	Izveštavanje	Razvoj formata izveštaja za ključne DD	Apstrakt nalaza, lista analiziranih DD, potpun opis fotografija, opis koraka za skupljanje i analizu tragova DD, kreiranje vremenske linije, odgovaranje na potencijalna pitanja (može se izbeći svedočenje)
6.	Svedočenje/veštačenje	Obezbediti pouzdanost DD i kredibilitet forenzičara	Validacija kompetencija forenzičara, relevantnosti DD, DF tehnika i alata za izgradnju čvrstih DD i ubedljivosti prezentacije DD kroz odgovore na verovatna pitanja: <i>Koji su DF alati korišćeni?; Ko je koristio DF alat/tehniku?; Gde su DP otkriveni?; Kako su DP vrednovani</i>

R.b.	Faza pripreme	Aktivnost	Kratak opis
			<i>(manuelno/drugim alatom)?; Šta su snaga i slabosti DD?; Postoji li alternativno objašnjenje?; Da li su tehnike akvizicije/analize pouzdano testirane?; Kojo su potencijalne/ poznate greške DF alata/tehnika?; Da li su DF alati/tehnike podvrgnute višestrukoj recenziji?; Da li su alati/tehnike opšte prihvaćeni u forenzičkoj zajednici? Koji standardi podržavaju DF istragu?</i>
7.	Svedočenje/ veštačenje	Način iznošenja i interpretacije	Interpretirati DD ne-tehničkom osoblju u sudu na jasan i koncizan način, koristeći ilustrativne forme i poznate metafore
8.	Svedočenje/ veštačenje	Vizuelizacija gde je moguće	Koristiti vizuelne forme za opisivanje konteksta i relevantnosti DD, sa različitim pomoćnim alatima za analizu i izveštavanje.

III. ZAKLJUČAK

Sa adekvatnim DF alatima i tehnikama DF analitičar može dobiti vredne i pouzdane DD koji mogu značajno uticati na istragu kompjuterskog kriminala ili parnice. Ključna faza dokazivanja kompjuterskog kriminala i prihvatljivosti DD na sudu je pouzdan oporavak tragova DD i primene metoda izveštavanja. Priprema svedoka/veštaka za prezentaciju DD na sudu treba da počne paralelno sa procesom DF istrage – od trenutka pretrage, pristupa i fizičke akvizicije osumnjičenog računara do analize DD i prezentacije na sudu. Za obezbeđivanje prihvatljivosti DD na sudu, u prvom koraku DF istrage treba uspostaviti lanac čuvanja i dokaz o autentičnosti DD. U svim fazama DF istrage primenjivati postojeće međunarodne standarde iz oblasti zaštite informacija i DF, bez obzora da li su isti usvojeni kao domaći standardi. Ovo je nužna pretpostavka zbog transnacionalnog karaktera kompjuterskog kriminala i potencijalne razmene DD između različitih država, zakonskih okvira i pravosudnih sistema. Veoma je značajno da digitalni forenzičar kao stručni svedok/veštak prenese sudu informacije o DD na jasan, koncizan i razumljiv način, bez upotrebe kompleksnih tehničkih termina i uobičajenog žargona tehnički obrazovanih lica. Treba, gde je god moguće, koristiti ilustracije i vizualizaciju za interpretaciju DD u činjenica prihvatljivih na sudu. Geolociranje DD i vremenska linija napada mogu pružiti validan i prihvatljiv uvid u relevantnost DF istrage. Za kreiranje stručnog izveštaja mogu se koristiti brojni pomoćni alati za izveštavanje i statističku obradu podataka.

LITERATURA

- [1] Brodsky, S. L., (2013), Testifying in Court: Guidelines and Maxims for the Expert Witness, Washington, DC, American Psychological Association, 2nd edition, ISBN: 978-1-4338-1212-5, 2013.
- [2] Fry test, (1993), USA 54 App DC 46, 293 F. 1013 (1923); Daubert test v. MERRELL Dow Pharmaceuticals, 509 US 579, http://en.wikipedia.org/wiki/Daubert_standard, (Pristupljeno: 11.09.2014).
- [3] Gonzales, A. R., Schofield, R. B. & Hagy, D. W., (2007), Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, National Institute of Justice (SAD) www.law.du.edu/images/uploads/library/evert/DigitalEvidenceinTheCourtroom.pdf, 2007, (Pristupljeno: 02.09.2014).
- [4] Magnet Forensics® & Internet Evidence Finder™ (2014), 8 Tips for Presenting Digital Evidence in Court, Magnet Forensics Inc., http://www.only-search.com/?q=magnet+forensics+incorporation&babsrc=HP_ss&s=web&rlz=0&sd=61&as=3&ac=0, (Pristupljeno: 29.09.2014).
- [5] Malone, D. M. & Zwier P. J. (2000), Effective Expert Testimony, <http://www.barnesandnoble.com/w/effectiveexpert-testimony-david-m-malone/1101750409?ean=9781556815645>, ISBN-13: 9781556815645, National Institute for Trial Advocacy, 2000.
- [6] National Institute of Justice (SAD), National center for Forensic Science (2003), Digital Evidence in the Courtroom: A guide for Preparing Digital Evidence for Courtroom Presentation, www.law.du.edu/images/uploads/library/evert/DigitalEvidenceinTheCourtroom.pdf, 2003.
- [7] Smith, F. C. & Bace, R.G., (2002), A Guide to Forensic Testimony – The art and Practice of Presenting Testimony as an Expert Technical Witness, Addison – Wesley, Boston SAD, 2002.
- [8] Vlatin program obuke za forenzičke eksperte, SAD (0201752794.pdf), <http://www.epbsi.com/government/forensic.html>, (Pristupljeno: 28.09.2014).

The Application of Information Analysis in Forensic Linguistics

Marijana Prodanović, Saša Adamović, Sinergija University, Bijeljina

Abstract- The main goal of this paper was to introduce the phenomenon of information analysis as a new method within the field of forensic linguistics, which can be used for the purposes of authorship attribution. The main characteristic of this method is that it does not need all the apparatus of the Internet locations in order to attribute authorship. Unlike other methods, usually used in the cases of plagiarism detection, which need all the accessible Internet locations, the method of information analysis uses textual materials, supposed to be one author, based on which it denotes similarities and/or differences among the language patterns used. Applying the mentioned method, on the textual sample we analysed for the purpose of this paper, we found a consistent usage of similar language patterns.

Keywords – information analysis; forensic linguistics; language patterns; plagiarism; authorship attribution

I. INTRODUCTION

A. Forensic Linguistics Paths

Questions of authorship have exercised minds since the Ancient times, when the writers of plays used to accuse each other of plagiarism. The issue of plagiarism detection and authorship identification is still an important one, especially in the field of writing for academic purposes.

In today's world, in which we are all interconnected by means of information technologies, scarcely does anything of what we say or write remains secret. As a consequence, people are nowadays more enabled not only to share knowledge among themselves, but also to retell or even copy someone's words than they have ever been before. Sharing knowledge and experience within a field of expertise is a valuable practice in scientific surrounding as well; then again, it appears that not everybody is willing to attribute certain lines to their original author. In cases when we face bad practices of borrowing, which lead to plagiarism, linguistic analysis is what is needed if we want to make sure that author attribution is performed in an accurate way. That kind of linguistic analysis belongs to the scopes of *Forensic Linguistics*.

The term of *Forensic Linguistics* had not been known and thus not used until 1968, when a linguistics professor Jan Svartvik mentioned the term in an analysis of statements, given to police officers at Notting Hill Police Station, in 1953. Namely, Timothy John Evans was accused of the murder of his wife and baby at Notting Hill, London, England (he was afterwards tried at the Central Criminal Court of England and Wales and eventually hanged at the Pentonville Prison). In the 1960's, the statements he had allegedly given to police following his arrest, troubled several people and Svartvik himself was asked to analyse the statements. At that time, he realised that the statements contained two completely different styles – a well-written style of an educated person and a spoken, rather formal style. That is why Svartvik could claim that the lines which had previously been attributed to Evans could have hardly been his own.

In the United States, the practice of forensic linguistic also started in a tight relation with the processes of interrogation. To be more precise, in 1963, Ernesto Miranda was convicted of armed robbery, but appealed on the grounds that he did not understand his right(-s) to remain silent or to have an attorney present. For this very reason, the Court of Appeal overturned his conviction three years later. Following this case, many legal cases in the USA have been named *Miranda* cases in the decades that followed.

Apart from police and courtroom-related issues, one of the main concerns of forensic linguistics is the detection of plagiarism and attribution of authorship to pieces of different types of written (or spoken and then transcribed) discourse. To be an author, in general, means to possess specific language patterns you tend to use on a regular basis, and after which you, i.e. your piece of writing, can be easily recognized among all the others (authors, i.e. pieces of writing). One of the first scientists who attempted to compare two texts using forensic linguistics methods was Augustus de Morgan, who used the "word length average as a marker" (Olsson, 2004:11). As for the sentence length average, it was some authors considered it to be a good enough marker for attributing authorship (Olsson, 2004). Anyhow, word/ sentence length average cannot be

considered the essential and only marker for attributing.

This is where the sub-branch of forensic linguistics takes the stage. Namely, there is the area belonging to *forensic stylistics*, which compares texts in terms of spelling, the design of the pages (formatting), the space between the words, handwriting, collocations, word frequency, capitalization, indentation, etc. (For further reading with regard to this topic, see: G.R. McMenamin, 2002). In his work, *Studies and Authorship Recognition: A Corpus-based Approach* (1998), Hänlein discusses the possibility of recognizing the stylistic profile of an individual (Olsson, 2004).

Be that as it may, a forensic linguist should take into account observations from research undertaken in fields as diverse as language and memory studies, *Conversation Analysis*, *Discourse Analysis*, *Theory of Grammar*, *Cognitive Linguistics*, *Speech Act Theory*, etc. The reason for this reliance on a broad spectrum of linguistic fields is understandable: the data a forensic linguist receives for analysis may require that something is said about how the average person remembers language, how conversations are constructed, the kinds of moves speakers or writers make in the course of a conversation or a written text, or they may need to explain to a court some aspects of phrase or sentence structure.

The implementation of forensic linguistics methods has mostly been prominent in the sphere of court processing, as described above. However, it is the phenomenon of authorship attribution with regard to scientific articles what we would like it to implement the methods in.

Speaking of an author's style (in writing), there are many criteria that can be applied in order to define one, but one should always bear in his/her mind that a thorough analysis is required in order to attribute certain language patterns to certain authors. For the purposes of this paper, we have made a clear-cut choice with reference to classification criteria. Namely, since we offer software which can easily follow any command an instructor issues to it, we have had to opt for some criteria in order to describe the software's functioning.

Apart from language length and the length of the text itself, which can be analysed with no difficulties in a relatively short span of time, numerous other factors can be measured, with almost the same convenience.

Style is the result of choices made by an author from a range of possibilities offered by the language system (Sanders: 1977).

What has also been examined by the authors (to name but a few of them: Mosteller & Wallace, 1963; Peng & Hengartner, 2002; Sichel, 1974; Smith, 1983,

etc.) from the field of linguistics are: distribution of function words, richness of vocabulary, parts of speech, negative particles, genitive, etc., in order to analyse linguistic similarity between the texts.

B. Perception of Information

The notions of information, as a phenomenon and communication, as a transmitter, play a crucial role in the field of information theory. We all do possess an intuitive image of what information represents; however, when it comes to scientific basis and interpretation of information had not been stated earlier than the middle of the past century, since that was the time when a rather new scientific discipline, the *Information Theory* came to life.

Information has become an important segment in all the scientific domains which deal with communication via symbols; consequently, not only does linguistics examine the phenomenon of information, but the mentioned phenomenon is being analyzed within the scopes of both social and technical sciences and even the arts.

This has led to the fact that nowadays, information is an interdisciplinary concept in its nature, for each of the scientific disciplines examining information is still making strenuous efforts in order to provide as many characteristics of the information's complexity as possible.

The term information traces its roots back to the Latin language (*informo*, -are, -avi, *atum*, 1.), when it was used for the process of making, shaping or putting something into action, i.e. effect. As the years were passing, the term started being used in different contexts, and thus its basic meaning started being changed. At the present moment, we can hardly say that there is a unique and widely accepted definition of information.

Shannon formulated the *theory of data compression*, as a part of one of his works. He came to the conclusion that there is a fundamental limit for data compression, without any loss (*lossless data compression*). This limit is called entropy rate and is being marked as *H*. Its exact value depends on the information source, i.e. of the source's statistical nature. Shannon claims that it is possible to compress data immediately at the source, with no loss, and with the compression level similar to *H*.

This concept has been widely used in information theory and communication theories, and Shannon himself used it to define the quantity of current pieces of information used in an English text. He defined the process in the following way: "The entropy is a statistical parameter which measures, in a certain sense, how much information is produced on the average for each letter of a text in a language. If the language is translated into binary digits (0 or 1),

in the most efficient way, the entropy H is the average number of binary digits required by letter of the original language.” (Shannon, 1951: 50).

II. METHODS

The observation of an random value or an event related to an occasional value represents a piece of information. Information quantity, provided by the occasional value observation or its event is measured on the basis of the resulting uncertainty change; as a result, we can conclude that entropy and information value are closely related concepts.

The leading idea has been the one related to the uncertainty change, and thus, information value has to be equal to the quantity of the uncertainty change. Our examination will start with the possibility system (S, P) , which is represented by a random variable X , which takes the value $x \in S$, with the possibility of $p_x(x)$. This random variable describes one experiment, in which the results are uncertain. The superiority measure, regarding this experiment, is provided within the entropy:

$$H(X) = -\sum_{x \in S} p_x(x) \log p_x(x) \quad (1)$$

When we have conducted the experiment, we start observing the specific value of $x \in S$. Afterwards, there is no uncertainty anymore, since the uncertainty which used to exist has been reduces to the posterior uncertainty of 0. The $H(X) - 0 = H(X)$ value is equal to the information quantity, which has been provided by the performance of this experiment. Thus, we can state that the entropy of one random value equals to the information quantity which has been provided by the observation of its one specific realization.

This idea evokes two major observations; namely, since information is equal to the entropy change, it is measured via the same units like the entropy itself, i.e. if the logarithm basis is in 2, the unit is one bit. The information quantity produced is the same for each and every possible realization of the random X value, no matter whether the possibility of realization is high or low.

This paper has conducted an information-theoretical text analysis, with the aim of an author's stylistic pattern characterization, where the text has presented the source of information. Starting from the given theoretical notions and Shannon's concept of information theory, we have designed the method for a rigorous analysis of the text which has previously been divided into fragments. The proposed theoretical-information text analysis would provide real solutions for the attribution of stylistic patterns to different authors, thanks to the textual content, as a

unique source of information. This would, undoubtedly, lead to a deep insight into the characteristics of a text as a unity, with specific reference to its originality and absolute authorship of the said author (-s).

In each and every fragment, we counted all the words used; afterwards, we defined their frequencies in fragments, respectively, as well as the quantity of information in each of the words, expressed in bits. The end result of the method is the mutual correlation of fragments in terms of frequency and quantity of information contained in each word. Apart from theoretical-textual analysis, we have also paid attention to keywords, related to topic of the text and their uniform distribution among the fragments.

The following information-related analyses have been conducted in this research:

- Information analysis of the whole text;
- Information analysis of the text divided into fragments;
- Comparative analysis of the correlation of fragments;
- Analysis of the uniform distribution of key words in the text.

For the purposes of this paper, we have developed a Java application, which enabled the realization of the analyses mentioned earlier. This application is a user-friendly one, since its users themselves define the method of its actual purpose for the very occasion.

III. RESULTS

The input parameters of the application represent the analysed text and the specified number of fragments that will be the observed parameters of the analysis of information.

This part of the paper will provide an insight into the data analysed, i.e. the parameters related to the text which is considered to be the work by a single author. The text has been analysed in terms of five fragments. The following example examines the following tokens: a, is, linguistics and metonymy.

Search "a" (5 hits in 5 files)			
new 1 (1 hit)			
Line 6: T: a	P: 16	IK: 4.370687406807218	
new 2 (1 hit)			
Line 3: T: a	P: 18	IK: 4.239465967068594	
new 3 (1 hit)			
Line 6: T: a	P: 15	IK: 4.52773768769889	
new 4 (1 hit)			
Line 5: T: a	P: 17	IK: 4.19330787579237	
new 5 (1 hit)			
Line 8: T: a	P: 13	IK: 4.584962500721157	

Fig. 1 The token “a”

Search "is" (5 hits in 5 files)	
new 1 (1 hit)	
Line 5: T: is P: 17 IK: 4.283224598810321	
new 2 (1 hit)	
Line 8: T: is P: 13 IK: 4.708951145156897	
new 3 (1 hit)	
Line 12: T: is P: 8 IK: 5.4346282276367255	
new 4 (1 hit)	
Line 7: T: is P: 14 IK: 4.473415918856853	
new 5 (1 hit)	
Line 11: T: is P: 10 IK: 4.9634740710571466	

Fig. 2 The token "is"

Search "linguistics" (3 hits in 3 files)	
new 1 (1 hit)	
Line 12: T: linguistics P: 9 IK: 5.20076228897785	
new 2 (1 hit)	
Line 87: T: linguistics P: 2 IK: 7.409390936137703	
new 5 (1 hit)	
Line 82: T: linguistics P: 2 IK: 7.285402218862249	

Fig. 3 The token "linguistics"

Search "metonymy" (3 hits in 3 files)	
new 1 (1 hit)	
Line 13: T: metonymy P: 9 IK: 5.20076228897785	
new 2 (1 hit)	
Line 99: T: metonymy P: 2 IK: 7.409390936137703	
new 5 (1 hit)	
Line 34: T: metonymy P: 4 IK: 6.285402218862249	

Fig. 4 The token "metonymy"

If we have a look at the data above, presenting the usage of the tokens of: a, is, linguistics and metonymy, we can see that there are, actually, no many differences when it comes to the frequency of their usage, both in terms of quantity and quality, i.e. the content of information placed within them. To be more precise, the a and is tokens show a rather superior level of uniform distribution among the fragments observed. Anyhow, on the other hand, the tokens of linguistics and metonymy appeared not to have distribution among the analysed fragments with values which are so similar as those regarding the abovementioned tokens of a and is. However, it is worth mentioning that differences in the latter tokens distribution among the observed parameters are not extreme.

IV. CONCLUSION

Starting from the assumption that the application of information analysis in forensic linguistics would provide significant results, with regard to the process of authorship attribution, we developed a Java application, which enabled a four-level analysis. This kind of analysis can, actually, give insight into details of language patterns used in the examined corpus and

thus provide a vivid description of the writing style applied, i.e. of its consistency throughout the text material. Given the fact that this is a user-friendly application, the researcher using it can manipulate its tasks and their complexity in the way he/she wants; namely, the analysis of a text can be done on various language levels, starting from the surface ones, by which we consider the text length or the length of sentences used in the text, till the more delicate levels, such as morphological analysis of the words used, the usage of active and/or passive voice, a consistency in the usage of definite and indefinite article, etc.

Anyhow, since our primary aim was to prove that information analysis is applicable as a method of forensic linguistics, particularly in the process of authorship attribution, we did not use all the possibilities of the developed application, but showed one of the directions in which the application can be used. Not only did this shed some light on the implementation on information analysis in the field of forensic linguistics, but it also raised some new research questions for us, which are to be examined in the future.

BIBLIOGRAPHY

- [1] Shannon, C. E. (1951). Predication and Entropy of Printed English. *Bell System Technical Journal*, 30, pp. 50-64.
- [2] Olsson, J. (2004). *Forensic Linguistics: An Introduction to Language, Crime, and the Law*. New York: Bloomsbury Publishing.
- [3] McMenamin, G. (2002). *Forensic Linguistics: Advances in Forensic Stylistics*. Boca Raton, London & New York: CRC Press.
- [4] Hanlein, H. (1998) *Studies in authorship recognition: a corpus-based approach*. Frankfurt: Peter Lang.
- [5] Mosteller, F. and Wallace, D. (1963). Inference in an Authorship Problem. *Journal of the American Statistical Association*, 58, pp. 275-309.
- [6] Peng, R. and Hengartner, H. (2002). Quantitative Analysis of Literary Styles. *The American Statistician*, 56, pp. 175-185.
- [7] Sichel, H. (1974). On a Distribution Representing Sentence-Length in Written Prose. *Journal of the Royal Statistical Society*, 137, pp. 25-34.
- [8] Smith, M. (1983). Recent Experience and New Developments of Methods for the Determination of Authorship. *Association for Literary and Linguistic Computing Bulletin*, 11, pp. 73-82.

The Implications of the Maturity Level of Strategic Alignment of ICT Systems Projects on Economic Criminality

Hajrudin Imamović, Comprehensive School "Ismet Mujezinović", Tuzla
 Gojko Grubor, Sinergija University, Bijeljina
 Dušan Regodić, Sinergija University, Bijeljina

Abstract – According to the Society for Information Management (SIM) research conducted from 2003 to 2013, the alignment of information communication technology systems (ICT systems) and business in the United States of America (USA) and the European Union (EU) represents one of the biggest problems of the modern business. If this problem is so pronounced in the developed economies, it can be assumed to be even more pronounced in those less developed. The outline of this problem lies in the strategic alignment of ICT systems Projects and business. This paper aims to show how the assessment maturity of strategic alignment factors (Communications, Metrics to assess the business value of ICT, ICT Governance, Partnership, Scope & Architecture and Human Resources skills) can identify the level of maturity of strategic alignment of ICT systems Projects and business and what connection it may have with economic criminality.

Key words – strategic alignment, ICT systems, ICT systems projects, organizations executives, supervisory and management boards, boards, economic crimes

Sažetak – Prema istraživanjima Society for Information Management (SIM) provedenim od 2003. do 2013. godine, usklađivanje informaciono komunikacionih tehnologija/informacionih sistema (ICT sistema) i poslovanja, u Sjedinjenim Američkim Državama (SAD) i Evropskoj Uniji (EU), predstavlja jedan od najvećih problema savremenog poslovanja. Ako je navedeni problem tako izražen u najrazvijenijim ekonomijama, može se pretpostaviti da je još veći u onim manje razvijenim. Okosnica ovog problema leži u strateškoj usklađenosti Projekata ICT sistema i poslovanja. Ovaj rad ima za cilj pokazati kako se procjenom zrelosti faktora strateškog usklađivanja (komunikacije, mjerenje ICT poslovne vrijednosti, ICT upravljanje, partnerstvo, obim i arhitektura i vještine ljudskih resursa) može identificirati nivo zrelosti strateške usklađenosti Projekata ICT sistema i poslovanja i kakvu vezu to može imati sa privrednim kriminalitetom.

Keywords – Strateško usklađivanje, ICT sistemi, Projekti ICT sistema, Rukovodioci organizacija, Nadzorni i upravni odbori, Odbori, Privredni kriminalitet.

I. INTRODUCTION

The problem of business criminality is evident in all countries in the world, especially in developing countries.

Particularly affected by this kind of crime, maybe even most of all, are investments in projects. Part of this are also ICT system projects, particularly outsourcing software projects, which, due to the peculiarities of an easy covering up of their shortcomings and the non-existence of regulatory demands for the control of the justification of investments, are an easy target for criminal activities.

In the organizations of the public sector where there is no strategic planning of the ICT system (and these are numerous, particularly in developing countries), and in the case of underdeveloped communications as well as poor understanding between the highest-ranking business managers and those responsible for the ICT systems, there is a realistic possibility of criminal activities. This is especially true when we add to this that there are no reliably gauged parameters of business needs, that no priorities in the area of investment in the ICT systems have been planned or established and where there is minimum partnership between organizations executives, supervisory and management boards, boards for ICT systems.

The biggest problem in such circumstances is how to identify the described situation? The audit that is under way cannot address this task properly for at least two reasons: first, the external audit as we know it, is not of a technological but rather financial nature and this in itself makes it impossible to identify the essence of the problem in such a way, which is reflected in the determination of priorities and the quality of ICT system projects, especially software projects. Secondly, an internal technological audit, even where there is one, is not independent enough to be able to have a critical attitude towards this kind of problem.

Keeping in mind all the above-mentioned, the area exposed to business criminality is obviously unprotected. Therefore, this paper aims to present a model which could help put the stated problem under control.

The following section of this paper presents an adapted strategic alignment maturity model – SAMM (Luftman, 2000) for the identification of economic criminality connected with ICT system projects.

The third section analyzes what implications the level of strategic alignment of ICT system projects and business operation can have for economic criminality.

The fourth section offers a conclusion with a suggestion for future research.

II. A MODE OF ECONOMIC CRIME IDENTIFICATION

In the late 1980s, business and IT system managers report the alignment problem (Lederer & Mendelow, 1989). From 1980 to 1994, this problem ranked among the top 10 issues of IT management according to the research conducted by the Society for Information Management – SIM, (Luftman and Kempaiah, 2007). Also, since 1994, the alignment problem has been ranked first or second among the top 10. According to the research conducted by SIM from 2003 to 2013 (Kappelman et al., 2013), alignment was qualified as the most important concern in such countries as the United States of America (USA) six times in the period of 10 years. A similar situation exists in the European Union (EU), where it was ranked number one concern of managers in the years 2013 and 2011, while in 2012 it was ranked second (Derksen and Luftman, 2014).

Such high importance is attached to the strategic alignment of business and ICT systems due to implications for an organization's performance, as many studies have indicated (Gupta, 1997; Tallon and Kraemer, 1999; Brynjolfsson and Hitt, 2000; Croteau and Bergeron, 2001; Kearns & Lederer, 2000; Cragg et al., 2002; Bergeron et al., 2004; Luftman and

Kempaiah, 2007). However, the authors of these studies intended to point out that this might have implications, not just for an organization's performance, but also economic criminality. To this effect, by delving into the relevant literature with the aim of finding instruments which could measure the level of strategic alignment between ICT systems and related projects with business operation, in which way the obtained parameters could be linked to the likelihood of business criminality, the authors adapted the SAM model (Luftman, 2000). This model rests upon the Strategic Alignment Model (SAM), (Henderson & Venkatraman, 1993), and it has become the most widely used model for the assessment of the maturity level of the strategic alignment between ICT systems and business operation in the last decade. It is made up of six criteria and the corresponding attributes for the assessment of five levels of the maturity of strategic alignment relying upon the metrics of the Capability Maturity Metric (CMM), Software Engineering Institute, Pittsburgh, SAD, (Humphrey, 1988). In this way, a model was devised with which it is possible to identify the causes and likelihood of economic criminality as shown in Figure 1.

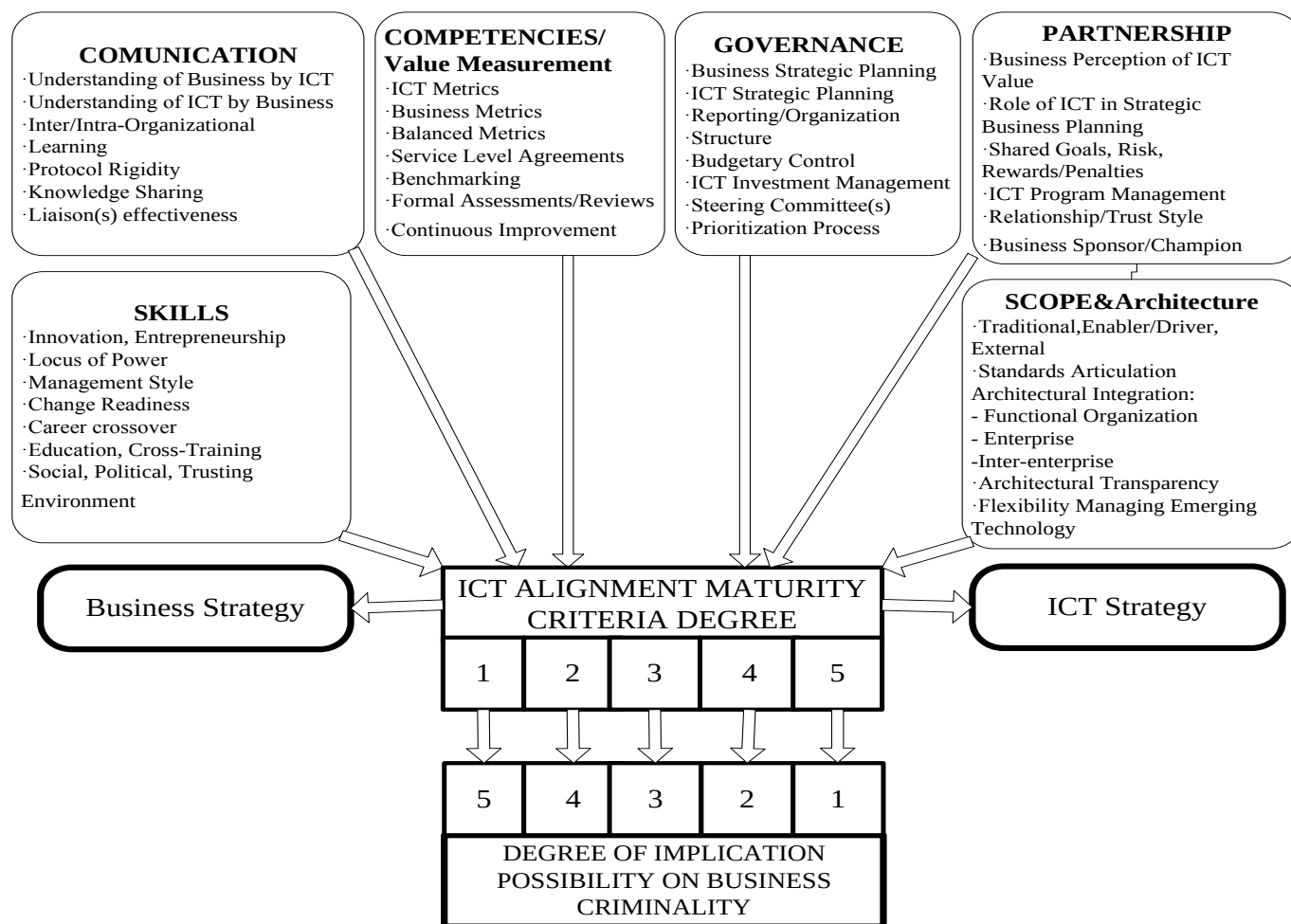


Figure 1 – Model for the Assessment of the Likelihood of Business Criminality (the adapted SAM model)

The six components for assessing alignment maturity are briefly explained below, (Luftman and Kempaiah, 2007). The specific criteria measured in each are listed in Figure 1.

Communications: Measures the effectiveness of the exchange of ideas, knowledge, and information between IT and business organizations, enabling both to clearly understand the company's strategies, plans, business and IT environments, risks, priorities, and how to achieve them.

Competency/Value Measurement: Uses balanced measurements¹ to demonstrate the contributions of information technology and the IT organization to the business in terms that both the business and IT understand and accept.

Governance: Defines who has the authority to make IT decisions and what processes IT and business managers use at strategic, tactical, and operational levels to set IT priorities to allocate IT resources.

Partnership: Gauges the relationship between a business and IT organization, including IT's role in defining the business's strategies, the degree of trust between the two organizations, and how each perceives the other's contribution.

Scope and Architecture: Measures IT's provision of a flexible infrastructure, its evaluation and application of

emerging technologies, its enabling or driving business process changes, and its delivery of valuable customized solutions to internal business units and external customers or partners.

Skills: Measures human resources practices, such as hiring, retention, training, performance feedback, encouraging innovation and career opportunities, and developing the skills of individuals. It also measures the organization's readiness for change, capability for learning, and ability to leverage new ideas.

For each of the six components five levels of maturity are established through an assessment in accordance with CMM, where level 5 is the highest level of maturity of strategic alignment. According to the presented model (Figure 1), the likelihood of economic criminality is inversely proportionate to the level of maturity. The main objective of this paper is to point to a possible link between the maturity level of the strategic alignment of ICT projects and business with economic criminality. That is to say, how one can detect economic criminality through the assessment of the maturity level of strategic alignment. The influence of the maturity level of the strategic alignment of ICT systems projects on the likelihood of economic criminality is shown in Table 1.

Table 1 – Strategic alignment maturity and level probability economic criminality

A – Level of maturity of strategic alignment of ICT systems Projects and business, Luftman (2000)	B – Level probability economic criminality
Level 1 – Initial/Ad-Hoc process •COMMUNICATIONS: Business/IT lack understanding •COMPETENCY/VALUE: Some technical measurements •GOVERNANCE: No formal process, cost center, reactive priorities •PARTNERSHIP: Conflict; IT a cost of doing business •SCOPE & ARCHITECTURE: Traditional (e.g., acctg, email) •SKILLS: IT takes risk, little reward; Technical training	Level 5 – Very high •poor communications •Not business oriented •Not priorities •Minimal partnership •There is no investment plan for ICT system projects •low wages
Level 2 – Committed process •COMMUNICATIONS: Limited business/IT understanding •COMPETENCY/VALUE: Functional cost efficiency •GOVERNANCE: Tactical at Functional level, occasional responsive •PARTNERSHIP: IT emerging as an asset; Process enabler •SCOPE & ARCHITECTURE: Transaction (e.g., ESS, DSS) •SKILLS: Differs across functional organizations	Level 4 – High •superficial •Not business-oriented •On lower levels •Minimal partnership •Business sponsorship of ICT systems projects is limited •Insufficient remunerations
Level 3 – Established focused process •COMMUNICATIONS: Good understanding; Emerging relaxed •COMPETENCY/VALUE: Some cost effectiveness; Dashboard established •GOVERNANCE: Relevant process across the organization •PARTNERSHIP: IT seen as an asset; Process driver •SCOPE & ARCHITECTURE: Integrated across the organization •SKILLS: Emerging value service provider	Level 3 – Median •business's understanding of IT is emerging •Some measurements established •Formal IT steering committees •Limited •ICT sistem suport •Development service provider
Level 4 – Improved/ managed process •COMMUNICATIONS: Bonding, unified •COMPETENCY/VALUE: Cost effective; Some partner value; Dashboard managed •GOVERNANCE: Managed across the organization •PARTNERSHIP: IT enables/drives business strategy •SCOPE & ARCHITECTURE: Integrated with partners •SKILLS: Shared risk & rewards	Level 2 – Small •Business-IT understanding high •Benchmarking is a routine practice •Very effective •ICT sistem offensive •Alignment with partners •Very important
Level 5 – Optimized process •COMMUNICATIONS: Informal, pervasive •COMPETENCY/VALUE: Extended to external partners •GOVERNANCE: Integrated across the org & partners •PARTNERSHIP: IT-business co-adaptive •SCOPE & ARCHITECTURE: Evolve with partners •SKILLS: Education/careers/rewards across the organization	Level 1 – Very small •Harmony •Benchmarking with partners •Alignment with partners •Business and IT are informal •Alignment business strategy •HR on a fairly high level

¹ A "balanced measurement" includes metrics for assessing both IT and the business. The metrics should be easy to understand, derived jointly by IT and business stakeholders, and prescribe a clear direction for improvement.

III. DISCUSSION

The model for the identification of a sample and likelihood of economic criminality as shown in Figure 1 and Table 1 suggests that fairly reliable indicators for the detection of economic criminality in an organization can be obtained through the assessment of the maturity of the six criteria of strategic alignment. This claim can be corroborated by an analysis of all the six criteria at each maturity level of strategic alignment. The maturity level 1 in column (A) is characterized by poor communications and partnership between business and ICT management in relation to ICT system projects which are not even planned nor is there a list of priorities. Such a situation is, in a word, non-transparent and presents, by definition, a very high level of probability of economic criminality as shown in column (B).

The maturity level 2 in column (A), although somewhat higher as compared to level 1, still implies a high level of probability of economic criminality, which has been substantiated by the description of all the six criteria of strategic alignment maturity in column (B).

The maturity level 3 in column (A) is the median level of strategic alignment maturity at which the maturity criteria for strategic alignment are comparatively well-balanced; corresponding to this is the level of probability of economic criminality as shown in column (B).

The maturity level 4 in column (A), where all the six criteria of strategic alignment maturity are at a fairly high level of maturity, does not leave much space for economic criminality in column (B), which means that the level of probability is small.

At the maturity level 5 in column (A), where all the six criteria of the maturity of strategic alignment between ICT systems and business operation are at the highest level and where they are aligned with the organization's partners, the level of probability of economic criminality is very small.

The success of software projects of ICT systems is corroborated by the findings of research conducted by *The Standish Group* (Clancy, 2014), according to which the rate of success was only 16.2%, whereas disputed projects made up 52.7% and 31.1% were cancelled altogether. According to the same source, there are four major reasons for the failure of ICT system projects, namely the absence of: (1) *the inclusion of beneficiaries*, (2) *support by executive management*, (3) *clear demands* and (4) *proper planning*.

In other words, the reason is the low level of strategic alignment between ICT system projects and business operation. How important strategic alignment is and who stands in its way is best proved by the following statements about the failure of software ICT projects, *The Standish Group*

(Clancy, 2014), John, Director of MIS at a government agency: "Probably 90% of application project failure is due to politics!" And Kathy, a programmer at a telecommunication company, offered an even more scathing comment on politics: "Sometimes you have to make a decision you don't like. Even

against your own nature. You say well, it's wrong, but you make that decision anyway. It's like taking a hammer to your toe. It hurts."

That is why it does not come as a surprise that the strategic alignment between ICT systems and businesses is problem number 1 in business operation.

From the model presented in this paper it is obvious that the level of strategic alignment of ICT systems and the level of probability of economic criminality are inversely proportionate. The lower the level of strategic alignment, the higher the level of probability of economic criminality. Still, there may be exceptions.

IV. CONCLUSION

Economic criminality in modern business operation is a ubiquitous problem in all countries, especially developing ones. However, while preparing this paper, the authors reviewed strategies of combating corruption, which is just one of the forms of combat against economic criminality in several relevant countries, and they were unable to find in those strategies any reliance on scientific and empirically proven models which might help in the identification of economic criminality. Due to the complexity of outsourcing software projects of ICT systems, an adequate approach and tools are needed for the detection of economic criminality.

An adequate approach could be the identification of the maturity level of strategic alignment, while an efficient tool could be the SAM model, which has already been empirically tested (Luftman, 2000). The model presented in this paper could be a good guideline and instrument for the detection of the level of probability of economic criminality.

The presented paper is of normative nature and its limitation is the fact that it has not been empirically tested yet, which is at the same time a recommendation for future research.

REFERENCES

- [1] Bergeron, F., Raymond, L. & Rivard, S. (2004), *Ideal Patterns of Strategic Alignment and Business Performance*, *Information & Management* 41(8): 1003–1020.
- [2] Brynjolfsson, E. & Hitt, L. (2000), *Beyond computation: information technology, organizational transformation and business performance*, *Journal of Economic Perspectives*, 14(4), pp. 23–48.
- [3] Clancy, T. (2014), *The Sum of All Fears*, The Standish Group Report Chaos – Project Smart, <http://www.projectsmart.co.uk/docs/chaos-report.pdf>.
- [4] Cragg, P., King, M. & Hussin, H. (2002), *IT alignment and firm performance in small manufacturing firms*, *Journal of Strategic Information Systems*, 11, pp. 109–132.
- [5] Croteau, A. & Bergeron, F. (2001). *An Information Technology trilogy: Business Strategy, Technological Deployment and Organizational Performance*, *Journal of Strategic Information Systems* 10(2): 77–99.
- [6] Derksen, B. & Luftman, J. (2014), *European key IT and Management Issues & Trends for 2014: Results of an International*

- Study, CIONET, http://blog.cionet.com/wp-content/uploads/2014/02/ITTTrends_2014print.pdf
- [7] Gupta, Y.P., Karimi, J. and Somers, T.M. (1997). *Alignment of a Firm's Competitive Engineering Management Sophistication: The missing link*, IEEE Transactions on Strategy and IT Management **44** (4): 399–413.
 - [8] Henderson, J.C. and Venkatraman, N. (1993). Strategic Alignment: Leveraging information technology for transforming organizations, IBM Systems Journal **32**(1): 4–16.
 - [9] Humphrey, W.S., "Characterizing the Software Process: A Maturity Framework," IEEE Software, 1988 Vol. 5, No. 2, pp. 73-79.
 - [10] Kappelman, L., Luftman, J. & McLean, E. (2013), *Research Team Presents. SIM IT TRENDS STUDY*, 34th Annual Society for Information Management's, SIMposium, Boston, http://c.ymcdn.com/sites/www.simnet.org/resource/collection/7A70D436-28BA-4E88-B958-C86941C704C3/2013_SIMposium.pdf, 11-November 2013.
 - [11] Kearns, G.S. & Lederer, A.L. (2000), *The Effect of Strategic Alignment on the use of IS-Based Resources for Competitive Advantage*, Journal of Strategic Information Systems, **9**(4): 265–293.
 - [12] Lederer, A.L. and Mendelow, A.L. (1989). Coordination of Information Systems Plans with Business Plans, Journal of Management Information Systems **6**(2): 5–19.
 - [13] Luftman, J. N. (2000), *Assessing business-IT alignment maturity*, Communications of the Association of Information Systems, **4**, 14, 1-50.
 - [14] Luftman, J. & Kempaiah, R. (2007), *An update on business-IT alignment: A line has been drawn*, MIS Quarterly Executive, Vol. **6** No. 3, pp. 165-177.
 - [15] Society of Information Management (SIM), www.simnet.org
 - [16] Tallon, P. and Kraemer, K. L. (1999), *A Process-oriented Assessment of the Alignment of Information Systems and Business Strategy: Implications for IT Business Value*, University of California, Irvine, Center for Research on IT and Organizations.

Penetraciono testiranje Android aplikacije

Penetration testing of Android application

Mladen Veinović, Univerzitet Singidunum, Miroslav Čajić

Sažetak—Pri kupovini mobilnog uređaja, bilo da je to telefon ili tablet računar, veliki broj korisnika se opredjeljuje za uređaje sa Android operativnim sistemom. Povećana upotreba ovog operativnog sistema, svakako, sa sobom donosi i niz bezbjednosnih problema koji utiču na stabilan i pouzdan rad određene korisničke aplikacije. U ovom radu biće analizirani uobičajni bezbjednosni propusti u kodu i dizajnu Android aplikacije koji utiču na stabilnost rada operativnog sistema. Provjeravanje nivoa pouzdanosti aplikacije biće utvrđeno na osnovu penetracionog testiranja. Metodološki utvrđenim penetracionim koracima i na osnovu već definisanih testova biće prezentovani određeni rezultati koji govore o bezbjednosnim propustima, a koji mogu biti prisutni u posmatranoj aplikaciji. U cilju izvršenja analize rada Android aplikacije biće upotrebljeni neki od penetracionih alata.

Ključne riječi – mobilni uređaj, Android, bezbjednost, aplikacija, penetracija

Abstract – When buying a mobile device, be it a phone or a tablet, a large number of users opt for devices with Android operating system. Increased use of the operating system, of course, brings with it a range of security issues affecting the stable and reliable operation of the specific user applications. In this paper we analyzed the usual security gaps in the code and design of Android applications that affect the stability of operation of the operating system. To check the reliability of the application will be determined based on penetration testing. Methodological determined penetration steps and on the basis of pre-defined tests will be presented some results that speak about security failures, and that may be present in the monitored application. In order to perform the analysis of labor Android applications will be used some of penetration tools.

Keywords – mobile device, Android, security, applications, penetration

I. UVOD

Penetracija predstavlja metod provjere nivoa bezbjednosti sistema. Zasniva se na simulaciji napada, odnosno, pokušaja uspostavljanja kontrole nad sistemom ili njegovim dijelom od strane neovlaštenog korisnika. Cilj ovakve vrste provjere jeste utvrđivanje granica bezbjednosnog okvira testiranog sistema. Samo testiranje se često izvršava neposredno prije nego što proizvod bude plasiran u prodaju. Na taj način se provjerava nivo bezbjednost uređaja koji je potrebno zadržati i poslije prestanka proizvodnje uređaja. U toku samog testiranja, posebno se testira i provjerava svaka linija otvorenog kôda.

Postupak penetracije možemo podijeliti u dvije kategorije, externu i internu. Podržana vrsta penetracije zavisi od vrste testova koji se koriste za simuliranje napada.

II. SPOLJNI PENETRACIONI TEST

Externa ili vanjska penetracija obavlja se od strane stručnih lica koji se lobiraju van sistema. Informacije koje posjeduju se veoma ograničene. U ovom slučaju cijeli sistem je obezbjeđen određenim brojem sigurnosnih prepreka koje održavaju nivo bezbjednosti. Ove bezbjednosne prepreke imaju zadatak da se sistemu ne može pristupiti s vani. Jedine informacije koje se daju testerima su URL i IP adresa uređaja. Većina alata koji se koriste od strane testera odnose se na prolazak kroz bezbjednosne prepreke kao i za skeniranje sistema. Na taj način je onemogućeno upoznavanje mogućih ranjivosti penetracionog sistema.

Na primjer, Android aplikacija koja ima root dozvole radi na portu 850. Sigurnosna prepreka, odnosno, firewall, je obično konfiguriran tako da ne dopušta skeniranje sistema kroz ovaj port. Na taj način štiti usluge koje rade preko ovog porta, što znači da u toku penetracije neće biti otkriven servis koji radi na tom portu. Međutim, ako Android aplikacija koja ima root dozvolu pokreće neki http server na portu 80, može doći do probijanja mrežne prepreke, jer je port 80 uvijek otvoren za komunikaciju, čime se smanjuje nivo bezbjednosti sistema.

III. UNUTRAŠNJI PENETRACIONI TEST

Interna penetracija ne uzima u testiranje sigurnosne prepreke osim u slučaju višeslojne arhitekture. U ovom testu se lakše mogu dobiti informacije na osnovu IP adrese i drugih podataka.

Na osnovu već pomenutog primjera, Android aplikacija sa root dozvolom koja komunicira preko porta 850, u internom testu, postoji velika mogućnost da će tester otkriti ovaj port preko kog se vrši usluga, kao što je i vjerovatno da neće biti blokiran nekom od sigurnosnih prepreka. U slučaju da usluga komunicira s drugim uređajima, to može biti lako otkriveno.

Pravilo je, da će interna ispitivanja penetracije pronaći više konfliktnih situacija u odnosu na vanjski penetracioni test. Vanjski testovi penetracije oslanjaju se na činjenicu da napadači ne mogu pristupiti uređaju preko mreže. Međutim, to ne znači da problemi koji se pronalaze u internim testovima penetracije su manje težine. Insajderi još uvijek mogu iskoristiti ove probleme. Osim toga, napadači izvana mogu iskoristiti ove probleme u slučaju određenog većeg napada, gdje u suštini mogu ući unutar mreže.

IV. METODOLOGIJA PENETRACIJE

U ovom dijelu opisana je metodologija penetracije metodom korak po korak. U suštini, ova metoda se bazira na ideji da se ne prati svaki korak po korak, ali su ovi koraci korisni kao smjernice, i mogu se mijenjati po potrebi u provođenju testa penetracije. Za većinu uređaja koji rade u Android okruženju, jedan od glavnih problema može biti taj koji prouzrokuje pokrenuta aplikacija sa root korisničkom dozvolom. Ovdje je stepen opasnosti povećan jer korisnik radi s višim nivoom privilegija. Ovu osobinu zlonamjerni korisnik može iskoristiti kako bi kompromitovao sam uređaj. Osim toga, korisno je i analizirati izvorni kod bezbjednosnih mehanizama u samom OS-u aplikacije.

Tipičan penetracioni test može biti podijeljen u četiri faze. To su:

1. *Planiranje* - odnosi se na prepoznavanje ključnih ciljeva posmatranog sistema.
2. *Istraživanje* - podrazumijeva prikupljanje informacija koje uključuju otkrivanje IP adresa, kontakta, sistemskih informacija, aplikacija, baza i sl.. U ovom slučaju potrebno je pokrenuti skeniranje i utvrditi koje usluge su dostupne na tim uređajima. Ako se uređaj smatra kompromitovanim, koristiti određene smjernice kako istražiti unutrašnjost uređaja, koji procesi su pokrenuti, itd
3. *Napad* - bazira se na na prethodnom istraživanju, ispitivanju sistema, aplikacija, baza koje su ranjive i mjerenjem nivoa ranjivosti. Ako je potrebno, moguće je ponavljati ovu fazu. Ako je uređaj sumnjiv, npr., uređaj sa root aplikacijom, uhvatiti i analizirati pakete pomoću aplikacije Wireshark. Izvršiti statičku analizu izvornog koda biblioteka i OS. Konkretno, pretraživati kod koji je namjenjen za konkretnog proizvođača mobilnih uređaja. U kodu treba analizirati sledeće vrste pitanja: curenja resursa, null pokazivač reference, pristup nezakonitim operacijama, pitanja kontrole protoka koji potencijalno mogu napraviti određene obilaznice oko bezbjednosnih mehanizama provjere i sl.. Pregledati konfiguracije datoteke, potražiti tekstove sa lozinkama, obične tekstove i druge podatke koji se skladište bez odgovarajuće bezbjednosne pažnje.
4. *Izveštavanje* - radi se o procjeni, klasifikaciji ranjivosti po različitim nivoima. Ti nivoi se mogu podijeliti na: kritične, manje kritične, umjerene i slabe. Izveštaj treba da sadrži i određenu analizu na osnovu datih preporuka i smjernica.

V. PENETRACIONO TESTIRANJE

Penetraciono testiranje Android aplikacija je kao i svako drugo testiranje za bilo koji drugi softver. Elemente koje treba uzeti u obzir, prilikom penetracije Android aplikacije koje uključuju napad su:

1. površina djelovanja.
2. interakcije s drugim komponentama (interno i eksterno),
3. komunikacija,
4. skladištenje podataka,
5. mogućnost primjene kriptologije,
6. protok informacija i

7. ostalo.

Površina napada: Svaki penetracioni test se fokusira na jezgro funkcionalnosti aplikacije. U zavisnosti od funkcije i značaja posmatrane aplikacije, tester se bazira na predmete koji su po njemu relevantni i kritični (npr., autentifikaciju, podatke, itd). Penetracioni testovi se obavljaju na osnovu relevantnih komponenti. Lokalne komponente koje ne sadrže kritične podatke treba drugačije testirati, odnosno, manje vremena treba trošiti na njih, u odnosu na komponente koje su u interakciji sa vanjskim aplikacijama Android sistema.

Interakcije sa drugim komponentama: U ovom slučaju aplikacija komunicira s drugim Android aplikacijama i izvan servera kroz različite **IPC** (InterProcess Communication) mehanizme. To uključuje socket-based komunikaciju, **RPC** (Remote Procedure Calls), emitovanje prolaznih i primljenih podataka, kao i druge Android-specifične IPC interakcije. Mnoge od tih veza moguće su kroz dozvole i na taj način najvažnije obratiti pažnju na dozvole i zahtjeve aplikacija kao i na funkcionalnost koja aplikacije izlaže drugim Android aplikacijama.

U slučaju Android-specifičnih komponenti, kao što je broadcastovanje, tester treba barem osigurati sledeće:

1. Osjetljive podatke ne treba propustati kroz IPC komunikaciju.
2. Određene specifične filtere ne treba koristiti u svrhu sigurnosti. Iako ti filteri mogu kontrolisati namjeru obrađivane aplikacije, koristiti je samo u implicitnim namjerama. Aplikacija uvijek može prisiliti obradu stvaranjem eksplicitne namjere.
3. Broadcastovanje ne koristiti kada se vrši prenos osjetljivih podataka, jer se u tom slučaju aplikacija ne može kontrolisati
4. Korisničke dozvole ne treba primjenjivati za aplikacije koje nemaju potrebu za više od jedne funkcije, to jest, primjenjivati princip najmanje privilegije.

Komunikacija: Važno je da se utvrdi da li aplikacija komunicira sa objektima izvan sistema, u slučaju kad server predstavlja bezbjedan kanal. Komunikacioni kanal u ovom slučaju treba biti šifrovan. Takođe, važno je da se razmotri na koji način se biraju sistemi za komunikaciju.

Skladištenje podataka: U suštini, svaka aplikacija vrši procjenu da li ti određeni podaci pripadaju aplikaciji. Tipična aplikacija može čitati i pisati podatke u obliku datoteka ili baza podataka. Oba ova zapisa mogu se čitati od strane određene aplikacije ili vanjskog korisnika. Tester treba razmotriti djeljnje aplikacija i kao i njihovu sklonosti ka dijeljenju u cilju provjere, kao i to da li postoje podaci koji su slučajno izloženi čitanju. Većina aplikacija komunicira s vanjskim okruženjem, kao što je Web, i puno podataka je pohranjeni na udaljenim serverima u određenim bazama podataka. Jedan od zadataka testera je i taj da treba pregledati podatke koji se prenose i arhiviraju na Offsite serverima. Još jedna stvar koja treba da se razmotri je i ta, kako se skladište

datoteke sa osjetljivim parametrima, kao što su akreditivi korisnika.

Mogućnost primjene kriptologije: Tester bi trebao pregledati standardne kriptološke načine šifrovanja aplikacija. Na primjer, da li je aplikacija vrši provjeru javnog ključa prije odobrenja ili tokom potvrde sertifikata? Kako aplikacije potvrđuje sertifikat? Da li aplikacija vrši stroge provjere sertifikata ili ne?

Protok informacija: Ovo se odnosi na protok informacija kada aplikacija izvršava određeni korisnički zahtjev preko polja za pretraživanje. Tester treba obratiti pažnju na to da li zahtjev otvara aplikaciju i ako je tako, kako prolaze potrebni parametri, preko GET ili POST zahtijeva?

Ostalo: Korisničke prijave se mogu pregledati za servise koje rade u pozadini u cilju uvida na njihov utjecaj na sistemske resurse. Postoji nekoliko dodatnih koraka koji su potrebni kao dio penetracije Android aplikacije. Pošto su Android aplikacije pisane u Java programskom jeziku, neophodno je da se preispita Java kod za tipične napade. Ako se aplikacija oslanja na osnovni izvorni kod ili biblioteke, bilo bi mudro da se provjeri ranjivosti izvornog kôda. Na kraju, važno je razmotriti kako se aplikacija vrši skladištenje podataka?

VI. ANALIZA PENETRACIONOG TESTA

Analiza penetracionog testa treba dati određene rezultate koji su se pokazali kao najbolji u praksi. Pri testiranju treba uzeti u obzir i neke određene postavke. Pregledom izvornog kôda Android aplikacije mogu se utvrditi određene anomalije koje se manifestuju u toku rada Android aplikacije. U toku analize identifikovana su sledeća pitanja koja narušavaju bezbjednosni okvira aplikacije:

Komanda ubacivanja: Napadač može uticati na komande koje se izvršavaju ili na okruženje u kome se izvršava, zaobilazeći bezbjednosne kontrole. Tipični primeri su parametri korisničkog ulaza koji se koristi u SQL upitu.

Curenje resursa: Aplikacija se ne odriče resursa nakon što se upotrebi. To može da dovede do problema sa performansama, ali takođe može biti dostupno za zlonamerne korisnike ili aplikacije.

Rukovanje greškama: U slučaju prijave greške, aplikacija ne uzima u obzir strukturu kôda i na taj način ne prikazuje sve kontrolne provjere potrebne ako određeni dio kôda nije izvršen.

Nebezbedni JNI Calls (Java Native Interface): Budući da Android aplikacija sadrži izvorni kôd napisan u C programskom jeziku, kroz JNL, u tom slučaju aplikacija se izlaže osnovnim pitanjima koja se vežu za bezbjednost izvornog kôda.

Na osnovu penetracione analize Android operativnog sistema sistema, došlo se do niza preporuka koje utiču na podizanje bezbjednosnog nivoa Android aplikacije. Ove preporuke je potrebno poštovati prilikom projektovanja aplikacija a neke od njih su:

1. Blagovremena doraditi biblioteke i aplikacije prije nego što je moguće identifikovati određene ranjivosti.
2. Osjetljive informacije (npr., SSN) ne treba slati preko URL-a. Za slanje osjetljivih informacija, uvijek treba koristiti HTTPS vezu.
3. Obratiti pažnju na to da brute force napadi nisu u velikoj mjeri mogući zbog ograničenog broja pokušaja za autentikaciju.
4. SSL (Secure Sockets Layer) je korišten za prodorno traženje resursa.
5. Identifikatore sesije ne treba slati u URL adresama.
6. Tokeni nisu uvijek lako dostupni.
7. Potrebno je sprovesti politiku složenih lozinki.
8. Log fajlovi ne sadrže osjetljive informacije i na odgovarajući način su zaštićeni.
9. Fajlovi je potrebno šifrovati na lokalnoj i spoljnoj memoriji.
10. Postupak pravilna validacije podataka potrebno je vršiti da bi se sprečila KSSS i SQL komandna ubacivanje, itd

VII. PENETRACIONE APLIKACIJE

Za pristupanje uređaju sa Android operativnim sistemom mogu se koristiti neke od alati koje su predviđene za fizički pristup, ili pristup preko mreže. U zavisnosti od namjere korisnika koriste se alatke namijenjen ciljnoj grupi. Neki od najčešće korišćenih su nabrojane u nastavku rada.

A. Nmap

Ako pretpostavimo da nemamo fizički pristup samom uređaju, ali imamo mogućnost pristupa Android uređaju preko mreže, u tom slučaju možemo koristiti Nmap, program za skeniranje posmatranog uređaja. U procesu skeniranja Nmap pokreće SYN (sinhronizaciju) skeniranja IP adresa, verzije OS-a, baze otisaka prstiju. Slike skeniranja sadrže listu otvorenih portova (usluga). U slučaju da prikupljanje slika snimljivih portova nije uspjelo, korisnik nema neke korisne informacije u vezi sa Android uređajem. Ukoliko je bilo koji od portova bio otvoren, imali bi mogućnost daljeg istraživanja.

B. BusyBox

BusyBox je Android aplikacija koja ima ulogu pružanja određenih standardnih Linux alata.² Zbog svoje veličine je idealan za uređaje sa ograničenom memorijom. Besplatan je, i potpuno je, kao open-source, dostupan pod GNU GPL licencom. Pošto pruža određeni broj novih komandi, prihvaćen je od strane developera kao nezaobilazni alat. Budući da je projektovan za Android, postoji mogućnost da ne radi na svim verzijama, kao što su one za desktop računare. Dakle, BusyBox predstavlja skup klasa i funkcija koje bilo koji program može da pozove, pa tako developer ne mora da ih

¹ [https://secwiki.org/w/Nmap/Android 22.02.2014](https://secwiki.org/w/Nmap/Android%2022.02.2014)

² <http://srbodroid.com/development/programiranje/sta-je-busybox/>

piše iz početka i da ih uključuje u svoju aplikaciju, što dosta smanjuje veličinu aplikacija.

C. Wireshark

Programski alat Wireshark koristi se za analizu mrežnih paketa. Namjenjen je za hvatanje podatka koji u paketima putuju mrežom i prikazivanje na najdetaljniji mogući način. Wireshark je tzv. „cross-platform“ mrežni alat, što znači da može raditi na različitim platformama. Podržan je i na različitim Unix operativnim sistemima među kojima su Linux, Mac OS X, BSD i Solaris. Wireshark je softverski alat koji „razumije“ strukturu različitih mrežnih protokola. Iz tog razloga, ima mogućnost prikaza podataka iz paketa koji su specifični za različite protokole. Wireshark koristi biblioteku Packet capture (PCaP) za hvatanje paketa, što znači da može hvatati samo pakete s mreža koje PCaP podržava, a to su Ethernet, IEEE 802.11, i sl. Podaci se mogu uhvatiti pravo s aktivne mrežne veze ili se mogu učitati iz datoteke u kojoj su sačuvani paketi. Sačuvani podaci mogu biti prikazani preko grafičkog korisničkog interfejsa, ili preko terminala pri upotrebi Tsharka alata. Wireshark sadrži i filter za prikazivanje podataka pomoću kojega se može prikazati i samo dio podataka. Budući da je Wireshark open source alat, na njemu je relativno jednostavno implementirati programske dodatke za nove protokole.

VIII. ZAKLJUČAK

Penetraciono testiranje daje rengensku sliku bezbjednosnog sistema testirane aplikacije. Testiranje se izvodi u svrhu pronalaženja slabih karika bezbjednosnog sistema testirane aplikacije. Vršiti se od strane ovlaštenih osoba koje posjeduju određeno znanje iz oblasti bezbjednosti softvera a koji nisu uključeni direktno u projektovanje testirane aplikacije. Penetraciono testiranje Android aplikacije je slično testiranju običnih Windows ili nekih drugih aplikacija, s tim razlikom da se u ovom slučaju u obzir moraju uzeti određene Android specifične okolnosti, koje ovaj operativni sistem, razlikuju od ostalih sistema.

Bezbjednosni propusti se identifikuju pri pokušaju neovlaštenog pristupa, odnosno, na osnovu maliciozne radnje koja može biti štetna po bezbjednosni sistem. Penetracija ima za cilj sprečavanje bezbjednosnih propusta na osnovu analize mogućih problema. Penetraciono testiranje je potrebno raditi za svaku aplikaciju prije nego što se ista pojavi na tržištu. Ranim otkrivanjem bezbjednosnih propusta, proizvođač doprinosi stabilnije i bezbjednijem radu aplikacije i periodu eksploatacije.

Prilikom penetracionog testiranja potrebno je voditi računa o sledećem:

- pronaći korisnika s najviše saobraćaja na mreži,
- identifikovati protokol i aplikaciju koje se trenutno koriste,

- -odrediti prosječni broj paketa u sekundi, prosječni broj bajtova u sekundi, ili ukupni promet na mreži,
- prikazati sve korisnike komunikacione mreže,
- -odrediti dužinu paketa kojeg koristi aplikacija za prenos podataka na mreži i sl;

Neki od bezbjednosnih problema koji utiču na bezbjednosne performanse sistema a koji su proizvod lošeg ili djelimično lošeg penetracionog testa su:

- spor odziv mreže, neprepoznavanja korisnika i sl,
- vremensko kašnjenja između korisničkog naloga za rad s mrežnim paketima i samog procesa rada s paketima,
- pogrešno konfigurisanje korisnika (npr. ponavljanje IP adrese u istoj mreži),
- asinhroni prenos podataka na mreži,
- identifikovanje neuobičajenog pregleda prometa na mreži,
- prisustvo **HTTP** (Hyper Text Transfer Protocol) grešaka,
- prisustvo aplikacija koje ne šifruju podatke koji se prenose,
- uočavanje neuobičajenih protokola,
- neprihvatljivog vrijeme odziva mrežnih servisa, **SRT** (Service Response Time);

Penetraciono testiranje je moguće uraditi sa određenim softverskim alatima. Ovi alati imaju mogućnost otkrivanja većine bezbjednosnih propusta i nepravilnosti u bezbjednosnom sistemu aplikacije. Neki od tih alata nabrojani su u radu. Za potrebe ovog rada korišten je alat Wireshark.

LITERATURA

- [1] Abhishek Dubey and Anmol Misra, “ android security, attacks and defenses”, CRC Press, 2013
- [2] Analiza alata Wireshark, NCERT-PUBDOC-2010-09-312
- [3] “Application Security Framework”, Open Mobile Terminal Platform (OMTP), 2008..June, 2008.
- [4] A. P. Felt, H. J.Wang, A. Moshchuk, S. Hanna, and E. Chin.Permission Re-Delegation, ” Attacks and Defenses”, In 20th USENIX Security Symposium, August 2011.
- [5] M. Hypponen, “State of Cell Phone Malware in 2007” 2007
- [6] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel, “ Semantically Rich Application-Centric Security in Android”, In 25th Annual Computer Security Applications Conference (ACSAC’09), December 2009.
- [7] Dan Morrill (Google),“ Inside the Android Application Framework“, 2008 Google I/O Session Videos and Slides
- [8] Enck, W., Ongtang, M., and McDaniel, P.,“ Understanding Android security“, *IEEE Security and Privacy*, vol. 7, no. 1,2010.
- [9] W. Enck, P. Gilbert, B. gon Chun, L. P. Cox, J. Jung, P. Mc-Daniel, and A. N. Sheth, “TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones”, In 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI’10), October 2010.
- [10] Shabtai, A., Fledel, Y., Elovici, Y., „Securing Android-Powered Mobile Devices Using SELinux“, to appear in *IEEE Security and Privacy*, 2010..
- [11] Ongtang, M., McLaughlin, S., Enck, W., and McDaniel, P. Semantically Rich, “Application-Centric Security in Android”, 2009.

Reto Meier, “Professional Android Application Development”, WROX, 2008.

Modelovanje tokova podataka u kazneno-popravnim institucijama Republike Srpske

Dataflow modeling in correctional institution in Republika Srpska

Bogdan Mirković, Slobomir P Univerzitet

Sažetak— Informacioni sistem se posmatra kao proces obrade koji na bazi ulaznih generiše izlazne podatke. Dovodenje ulaznih podataka i odvođenje izlaznih podataka iz sistema ostvaruje se korištenjem tokova podataka. Tok podataka predstavlja putanju kojom se kreću grupe podataka. U procesu modelovanja tokova podataka eliminišu se detalji te model tokova podataka treba shvatiti kao pojednostavljenu predstavu stvarnosti i predstavlja jedan od prvih koraka u razvoju informacionog sistema. Modelovanjem procesa tokova podataka u sistemu za izvršenje krivičnih sankcija dobija se uređena struktura sa jasno definisanim pravilima po kojima se ti procesi obavljaju. U radu su predstavljene osnovne karakteristike izvršenog procesa modelovanja informacionog sistema u sistemu za izvršenje krivičnih sankcija Republike Srpske uz poštovanje postojećih zakonski definisanih procedura i tokova informacija. Razvijeni model tokova podataka služi za razumijevanje načina funkcionisanja sistema i predstavlja osnovu za razvoj informacionog sistema u sistemu za izvršenje krivičnih sankcija.

Ključne riječi – tokovi podataka, modelovanje, informacioni sistem,

Abstract – The development of information and communication technologies, the advantages provided by speed and power of computer technology, databases, software applications, telecommunications systems and their applications in all areas of life and actions allow researches in the fields of criminology and penology, management and supervisor bodies whose scope of work is in these areas a wide range of options to integrate and analyze all relevant information in cases that information are integrated and the methodology, as well as user-friendly manner and adopted at all levels. In this paper is presented the application of hybrid architecture of the information system of correctional institutions in Republika Srpska developed by the authors of this paper and implemented in all organizational units of the system. Development information system of correctional institutions in Republika Srpska is a step in the framework of the professionalization and harmonization of correctional institutions within the prison reform project controlled by the RS Ministry of Justice. Presented solution defines symbiosis software solutions with hybrid architecture distributed throughout the Republika Srpska and implemented in all organizational units of the system for

enforcement of criminal sanctions, and other institutions that are associated with this system.

Keywords – dataflow, modeling, information system

I. UVOD

Za opis funkcionisanja realnih sistema veliki problem predstavlja nemogućnost korišćenja prirodnih jezika zbog njihove dvosmislenosti. S druge strane, precizan opis preko formalnih jezika je nerazumljiv za većinu ljudi.

Iz tih razloga, potrebno je koristiti takvu tehniku koja organizuje prirodne jezike na taj način da eliminiše dvosmislenost i omogućava efikasnu komunikaciju i međusobno razumevanje. Pokazalo se da je postupak modelovanja jedna od najefikasnijih tehnika za razumevanje i jednoznačnu komunikaciju.

U procesu modelovanja eliminišu se detalji, čime se umanjuje vidljiva kompleksnost sistema koji se proučava. U tom smislu model treba shvatiti kao pojednostavljenu predstavu stvarnosti. Preostali detalji se organizuju na takav način da bi eliminisali dvosmislenost i istakli bitne informacije. Koriste se grafičke prezentacije (uglavnom pravougaonici i linije) kako bi se obezbedilo da većina ljudi razmišlja o procesu modelovanja kao o slikovitoj prezentaciji (jedna slika zamenjuje i do 1000 reči). Pored grafičkog prikaza potrebno je dati i precizne definicije predmeta koji se pojavljuju u modelu, kao i priložni tekst, koji je kritičan prema modelu koji vrši svoju ulogu, kao sredstvo komunikacije.

U inženjerstvu model se konstruiše pre nego što se izgradi fizički sistem. Tako se, na primer, u automobilskoj industriji, izrađuju modeli koji su namenjeni ispitivanjima. Na taj način se obezbeđuje verovatnoća uspešnosti fizičkog proizvoda. U arhitekturi arhitekte izrađuju nacрте pre nego što pristupe izgradnji kuće. Nacrti predstavljanju logičku prezentaciju fizičke zgrade. Budući vlasnici kuće daju povratne informacije koje će biti prenesene na stvarni dizajn. Postupak modelovanja omogućava da sistem može biti svestrano analiziran, shvaćen i što je možda i najbitnije - saopšten drugima.

U radu su prikazane osnovne karakteristike razvijenog modela tokova podataka u sistemu za izvršenje krivičnih sankcija Republike Srpske u svim organizacionim jedinicama kao i u kompletnom sistemu. Razvijeni model koristi za razumijevanje sistema i načina njegovog funkcionisanja sa stanovišta tokova podataka u samom sistemu kao i podataka koje sistem dobija i prosledjuje drugim sistemima i predstavljao je osnovu za razvoj informacionog sistema kazneno-popravnih institucija Republike Srpske.

II. METODOLOGIJE MODELOVANJA PROCESA

Modelovanjem poslovnih procesa dobija se uređena struktura sa jasno definisanim pravilima po kojima se ti procesi odvijaju. Razlozi koji su motivisali nastanak modelovanja procesa su:

- da služe kao dokumentacija i uputstvo za opis kompleksnih poslovnih procesa. Jedno od osnovnih pravila je da što je dokumentacija veća - manje se čita. Dokument od jedne ili dve strane sa dijagramom, biće letimično pregledan i to onda kada se za to nađe vremena. Dokumentacija od 30 strana ima veliku šansu da mjesecima ne bude pročitana.
- da omoguće brze organizacione promjene, jer model procesa dokumentuje važne aktivnosti i omogućava uvid u kritične aktivnosti koje treba izvesti sa odgovarajućim resursima.

Najvažnija korist je prototipski pristup modelovanju, gdje se na brz i jednostavan način provjeravaju alternativne ideje. Mnogo je jednostavnije i jeftinije nacrtati model i provjeriti ga na "papiru", nego razviti novi informacioni sistem ili izvršiti reorganizaciju realnog sistema. Ovo je veoma bitna osobina jer brzi razvoj informacionih tehnologija i primena internet servisa, uslovljava potrebu za reinženjeringom koja zahtijeva radikalni redizajn poslovnih procesa koje je potrebno opisati i prije sprovođenja, prototipski provjeriti.

Primjena informacionih tehnologija u razvoju informacionih sistema je imala dvostruki uticaj na sistemsko i formalno utemeljenje modelovanja poslovnih procesa u organizacijama. Prvi uticaj se odnosio na zahtijevanje uvođenja dobro uređenih metoda odnosno metodologija, sa svrhom podrške u razvojnom procesu informacionih sistema odnosno u primjeni informacione tehnologije. S druge strane, došlo se do saznanja da primjena informacione tehnologije ne može biti efikasna ukoliko se i sam poslovni sistem odnosno organizacija u kojoj se primjenjuju nove tehnologije ne preoblikuje, kako bi se mogli iskoristiti potencijali sinergijske primjene informacionih tehnologija [1].

Danas se najčešće koriste tri integrisane metodologije modelovanja:

- IDEF skup integralnih metoda,
- UML – objektno usmjerena metodologija
- ARIS – integrisana metodologija

Sve tri su zasnovane na grafičkim jezicima i predviđene primarno za upotrebu kao softverski alati. Ručna upotreba nije isključena, ali je nepraktična kod imalo složenijih projekata, a naročito za duže vremenske intervale upotrebe.

ARIS se pojavljuje kao sveobuhvatni koncept i alat za arhitekturno modelovanje organizacija odnosno informacionih sistema. U teorijskom smislu je nastao 1990-tih godina i danas je relativno poprilično raširen u praksi.

UML (Unified Modeling Language) metodologija se bazira na konceptima objektno orijentacije u razvoju softvera. U teorijskom smislu koreni joj vuku iz 1980-tih godina, a kao metodologija se razvija posljednjih dvadesetak godina. U svojoj temeljnoj ideji, to je metodologija softverskog inženjerstva, ali sve više nastoji postati metodologija za modelovanje organizacija uz strogu objektnu orijentaciju.

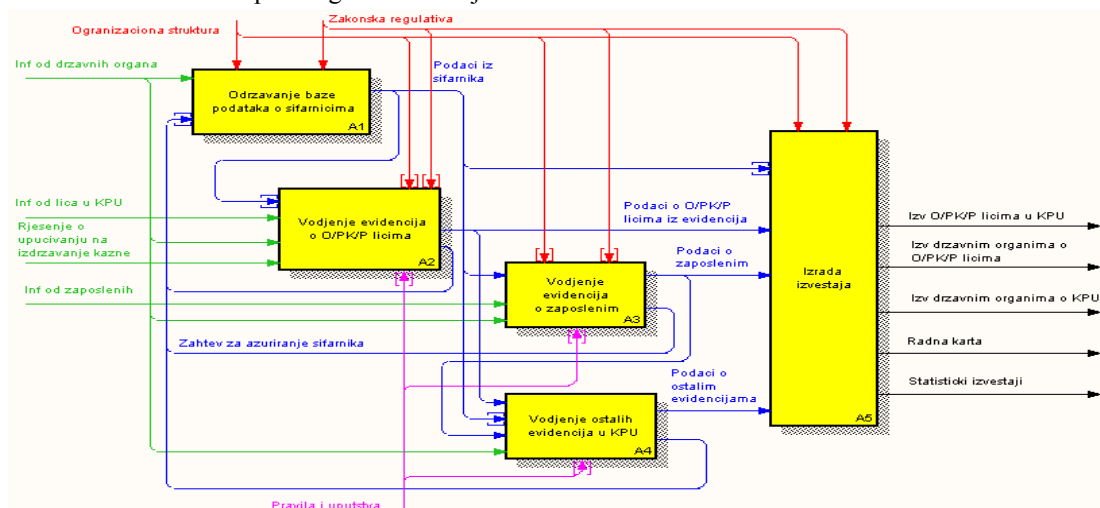
IDEF [2] metodologija obuhvata skup integrisanih modela, koji su definisani kao posebni standardi, a nastala je u okviru Agencije za obrambene informacione sisteme (DISA – Defense Information Systems Agency) ministarstva odbrane SAD (US DoD Department of Defense). IDEF metode su nastajale kroz niz godina, a dijelom su utemeljene na strukturnim metodama razvoja softvera odnosno informacionih sistema. IDEF (ICAMDEfinition) metodologiju razvila je US Air Force u okviru ICAM (Integrated Computer-Aided Manufacturing) programa tokom 1980-ih godina. IDEF metodologija u početku je obuhvaćala IDEF0 (standard USAF 1981a), IDEF1 (USAF 1981b), IDEF2 (USAF 1981c), i IDEF3 [3] metode namjenjene za modelovanje funkcija, informacija i procesa, respektivno. Postoje dvije verzije IDEF1: IDEF1 (1981) (USAF 1981b) i IDEF1x (1986) [4], [5]. IDEF1 se koristi za modelovanje informacija, dok se IDEF1x koristi za oblikovanje modela podataka u relacionim bazama podataka. Navedene metode su i najčešće korištene. Prvenstveno IDEF0, IDEF1X i IDEF3, te kasnije razvijena IDEF4. Daljnji razvoj nastavlja se 1990-tih kada su razvijene metode IDEF4 i IDEF5. IDEF4 je metoda za dizajn objektno orijentisanog softvera, koja integriše zahteve navedene u drugim metodama. IDEF4 omogućava upravljanje objektno orijentisanim načelima dizajna. IDEF5 je metoda za obuhvaćanje znanja s ciljem podrške ontologiji poslovne organizacije i u teoriji podržava metamodele. Idući korak u razvoju IDEF metodologije bio je razvoj IDEF6, IDEF8, IDEF9 i IDEF14 metoda. Namjena IDEF6 metode je logika dizajna, IDEF8 oblikovanje interfejsa čovjek-sistem. Metoda IDEF9 treba poslužiti za otkrivanje poslovnih ograničenja odnosno pravila, a IDEF14 za dizajniranje mrežnih sistema. Kasnije su razvijane i druge metode: IDEF7, IDEF10, IDEF11, IDEF12 i IDEF13 metode. IDEF7 za inspekciju informacionih sistema, IDEF10 za modelovanje informacionih činjenica, a IDEF12 za dizajniranje organizacije, IDEF11 za modelovanje implementacija, a IDEF13 za troslojnu shemu baze podataka.

III. DIJAGRAM AKTIVNOSTI I TOKOVA PODATAKA

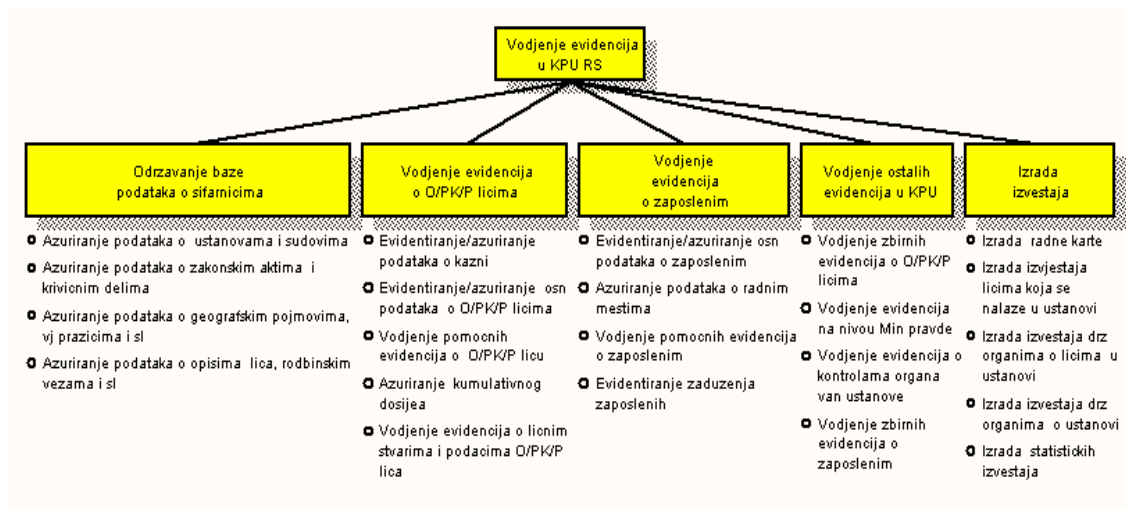
Funkcionalno modelovanje (IDEF0) omogućava sistematičnu analizu posla, tj. za svaku poslovnu funkciju se obezbjeđuje kontrola ispravnosti realizacije, planiraju se potrebni resursi da se funkcija realizuje, ulazi u poslovnu funkciju, kao i izlazi koji se na osnovu ulaza generišu. Dataflow (DFD) modelovanje, koje se koristi pri dizajniranju softvera, fokusira problem tokova podataka između procesa, kao i analizu skladišta podataka u cilju maksimalnog povećanja njihove raspoloživosti i smanjenja vremena

pretraživanja. Dijagram aktivnosti aplikativne podrške informacionom sistemu za vođenje evidencija u kazneno-popravnim ustanovama Republike Srpske na prvom nivou dat je na slici 1. Aktivnosti su smeštene u pravougaonice koji se

crtaju u dijagonalnom smeru od gornjeg levog ugla strane ka donjem desnom uglu. Svakoj aktivnosti mora se dodeliti naziv glagolske fraze te mora imati najmanje jednu kontrolnu i jednu izlaznu strelicu.



Slika 1: Dijagram aktivnosti za proces vođenja evidencija u KPU RS na prvom nivou



Slika 2. Stablo aktivnosti procesa vođenja evidencija u sistemu za izvršavanje krivičnih sankcija RS

Informacionim sistemom vođenja evidencija u sistemu za izvršenje krivičnih sankcija Republike Srpske uspostavlja se veza između sledećih potprocesa:

1. Održavanje baze podataka o šifarnicima;
2. Vođenje evidencija o osuđenim/prekršajno kažnjenim/pritvorenim licima;
3. Vođenje evidencija o zaposlenim;
4. Vođenje ostalih evidencija u KPU;
5. Izrada izveštaja.

Prijem lica u određenu ustanovu vrši se na osnovu Rješenja o upućivanju na izdržavanje kazne. U ovom Rješenju se nalaze svi potrebni podaci koji se odnose na vrstu kazne, dužinu kazne, krivična djela i zakonski akti na osnovu koje se vrši upućivanje na izdržavanje kazne i niz drugih podataka

koji zavise od vrste krivičnog djela. Pored ovog Rješenja, koje se dobija od nadležnog sudskog organa, postoji i dio podataka o licu koje se prima u ustanovu koji se dobijaju od lica koje je upućeno na izdržavanje kazne, a koji nisu sadržani u Rješenju. U toku izdržavanja kazne, lica koja se nalaze u ustanovi, zbog promjene određenih podataka, mogu iste dostaviti zaposlenim licima koji vode evidencije o licima u ustanovi. Drugu grupu podataka čine podaci dobijeni od lica koja su zaposlena u sistemu za izvršenje krivičnih sankcija Republike Srpske, a koji se prvenstveno tiču vođenja evidencija o zaposlenim licima. Posebnu grupu podataka na osnovu kojih se vode evidencije u ustanovama i Ministarstvu pravde čine informacija dobijene od državnih organa, a koje se tiču vođenja evidencija u ovom sistemu. Izlazni tok podataka iz procesa vođenja evidencija u sistemu za izvršenje krivičnih

sankcija Republike Srpske obuhvata skupove izvještaja: Izvještaji osuđenim/prekršajno kažnjelim/pritvorenim licima u KPU; Izvještaji državnim organima o osuđenim/prekršajno kažnjelim/pritvorenim licima; Izvještaji državnim organima o KPU; Radna karta; Statistički izvještaji.

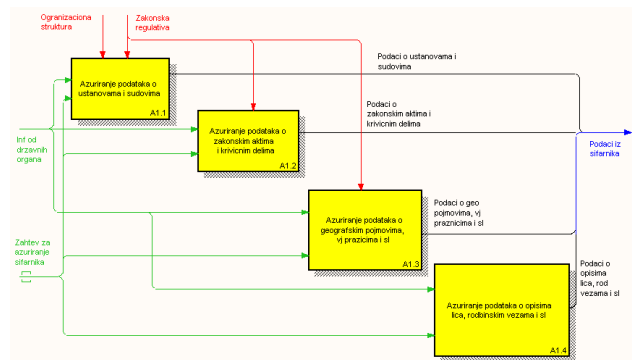
Stablo aktivnosti za informacijski sistem sistema za izvršavanje krivičnih sankcija Republike Srpske dato je na slici 2. Zbog preglednosti, ono je dato na 3 nivoa. Podređeni dijagram koji je nastao kao rezultat dekompozicije pokriva isti opseg kao i roditeljski dijagram.

Za proces A1 (Održavanje baze podataka o šifarnicima) ulazne tokove podataka čine:

- Zahtev za ažuriranje šifarnika koji može biti primljen od strane bilo kog korisnika sistema. U zavisnosti koje poslove vođenja evidencija vodi lice koje je uputilo zahtev za ažuriranje šifarnika, vrši se ažuriranje određene grupe podataka iz šifarnika.
- Informacije od državnih organa. Ove informacije mogu doći sa različitih nivoa državnih organa (organi Republike Srpske, Ministarstva pravde RS, Bosne i Hercegovine, Federacije Bosne i Hercegovine, Distrikta Brčko, kantona FBiH).

Izlazne tokove podataka sačinjavaju podaci o:

- Ustanovama i sudovima;
- Zakonskim aktima i krivičnim delima;
- Geografskim pojmovima, verskim praznicima i sl;
- Opisima lica, rodbinskim vezama i sl.

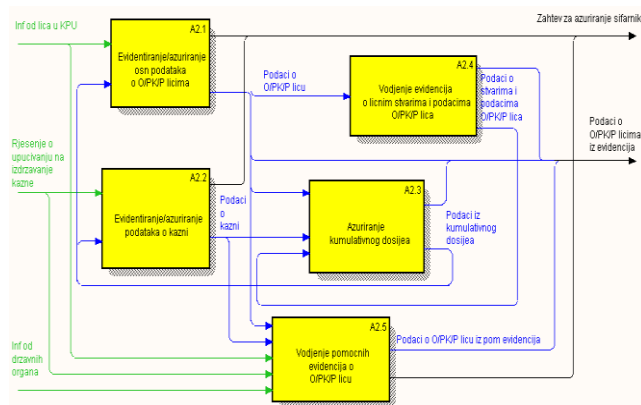


Slika 3. Dijagram tokova podataka za proces A1 (Održavanje baze podataka o šifarnicima)

U procesu A1 (Održavanje baze podataka o šifarnicima) vrši se ažuriranje dela baze podataka u kojoj se nalaze informacije potrebne za vođenje svih evidencija u sistemu za izvršavanje krivičnih sankcija. Održavanje ovog dela baze podataka vrši se na hijerarhijski višem nivou od ustanova (Ministarstvo pravde) i prosleđuje se svim ustanovama. Dijagram tokova podataka za ovaj proces dat je na slici 3.

U procesu A2 (Vođenje evidencija o osuđenim/prekršajno kažnjelim/pritvorenim licima) vrši se ažuriranje podataka u onom delu baze podataka u kojoj se nalaze podaci o pojedinim licima koja se nalaze na izdržavanju kazne u ustanovama. Dijagram tokova podataka za proces A2 (Vođenje evidencija o

osuđenim/prekršajno kažnjelim/pritvorenim licima) dat je na slici 4.



Slika 4. Dijagram tokova podataka za proces A2 (Vođenje evidencija o osuđenim/prekršajno kažnjelim/pritvorenim licima)

Proces A2 ima sledeće ulazne tokove podataka:

- Rješenje o upućivanju na izdržavanje kazne u kome se nalaze podaci vezani za vrstu, dužinu kazne, potrebnom tretmanu (ako je definisano) i ostali podaci bitni za početak izdržavanja kazne određenog lica.
- Informacije od lica u KPU koji predstavljaju podatke koji se dobijaju direktno od lica koja se nalaze na izdržavanju kazne i podatke koji se dobijaju iz ličnih dokumenata ovih lica.
- Informacije od državnih organa sa raznih nivoa (Republika Srpska, Bosna i Hercegovina, Federacija BiH, Distrikt Brčko i kantoni FBiH), a koji su važni za vođenje evidencija o licima koja se nalaze na izdržavanju kazne.

Proces ažuriranja podataka o osuđenim/prekršajno kažnjelim/pritvorenim licima ima sledeće potprocese:

- Proces A2.1. (Evidentiranje/ažuriranje osnovnih podataka o osuđenim/prekršajno kažnjelim/pritvorenim licima) je potrebno aktivirati u slučaju da se radi o unosu novog lica koje dolazi na izdržavanje kazne ili je došlo do promene osnovnih podataka o licima koja se već nalaze na izdržavanju kazne. Ulazne tokove podataka u ovaj proces čine informacije dobijene od lica koja dolaze na izdržavanje kazne ili se već nalaze na izdržavanju kazne (Inf od lica u KPU) i kao i Podaci iz kumulativnog dosijea lica koja se nalaze na izdržavanju kazne. Izlazne tokove podataka čine zahtevi za ažuriranje šifarnika (ukoliko je potrebno za neko lice proširi/ažurirati šifarnike), kao i podaci o osuđenom/prekršajno kažnjelom/pritvorenom licu.
- U Procesu A2.2. (Evidentiranje/ažuriranje podataka o kazni) se vrši unos (evidentiranje) podataka o kazni za lice koje je upućeno na izdržavanje kazne ili se vrši ažuriranje podataka o kazni za lice koje se već nalazi na izdržavanju kazne. Ulazne tokove podataka za ovaj proces čine podaci koji se nalaze u Rješenju o upućivanju na izdržavanje kazne za lica koja dolaze na

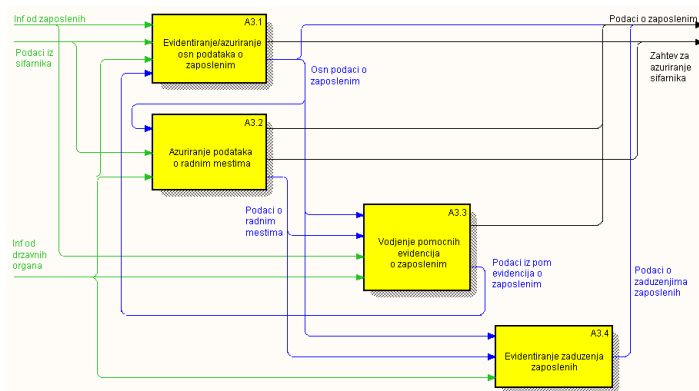
izdržavanje kazne, ali i Podaci iz kumulativnog dosijea lica koje se nalazi na izdržavanju kazne. Izlazni tok podataka iz ovog procesa čine zahtevi za ažuriranje šifarnika (ukoliko je potrebno ažuriranje šifarnika za neko lice) i Podaci o kazni.

- Proces A2.3 (Ažuriranje kumulativnog dosijea). U ovom procesu se vrši ažuriranje kumulativnog dosijea lica koje se nalazi u ustanovi. Kumulativni dosijea popunjava veći broj lica koja su zaposlena u ustanovama. Ovaj dosijea predstavlja najvažniji dio pomoćnih evidencija za lica koja se nalaze na izdržavanju kazne. Ulazne tokove podataka za ovaj proces čine osnovni podaci o licu i podaci o kazni za to lice. Izlazne tokove podataka iz ovog procesa čine Podaci iz kumulativnog dosijea. Ovi podaci predstavljaju dio izlaznih tokova podataka iz celokupnog procesa A2, ali i predstavljaju i povratne podatke u procese A2.2 i A2.3 čime utiču i na ove procese.
- Proces A2.4 (Vođenje evidencija o ličnim stvarima i podacima osuđenih/prekršajno kažnjenih/pritvorenih lica). Ovaj proces predstavlja vođenje velikog broja pomoćnih evidencija koje se tiču ličnih stvari koje se nalaze kod lica u ustanovi, zaduženja osuđeničkom opremom, finansijske podatke o licima. Ulazne tokove podataka u ovaj proces čine osnovni podaci o licima u ustanovama a izlazni tok podataka čine Podaci o ličnim stvarima i podacima osuđenog/prekršajno kažnjenog/pritvorenog lica.
- Proces A2.5 (Vođenje pomoćnih evidencija o osuđenim/prekršajno kažnjenim/pritvorenim licima). Ovaj proces predstavlja vođenje svih pomoćnih evidencija o licima u ustanovi koje ne obuhvataju procesi A2.3 i A2.4. Ulazne tokove podataka u ovaj proces predstavljaju podaci o licima u ustanovi (osnovni i podaci o kazni), Rješenje o upućivanju na izdržavanje kazne, Informacije od lica u KPU kao i Informacije od državnih organa (svih nivoa). Izlazne tokove podataka čine zahtevi za ažuriranje podataka o šifarnicima (ukoliko je potrebno) i podaci iz pomoćnih evidencija o osuđenim/prekršajno kažnjenim/pritvorenim licima.

U procesu A3 (Vođenje evidencija o zaposlenim) vrši se ažuriranje podataka u onom delu baze podataka u kojoj se nalaze podaci o licima koja su zaposlena u ustanovama. Dijagram tokova podataka za proces A3 (Vođenje evidencija o zaposlenim) dat je na slici 5. Proces A3 ima sledeće ulazne tokove podataka:

- Podaci iz šifarnika koji predstavljaju dio podataka iz šifarnika koji su bitni za vođenje evidencija o zaposlenim licima.
- Informacije od zaposlenih koji predstavljaju podatke koji se dobijaju direktno od lica koja se nalaze zaposlena u ustanovama i podatke koji se dobijaju iz ličnih dokumenata ovih lica.
- Informacije od državnih organa sa raznih nivoa (Republika Srpska, Bosna i Hercegovina, Federacija BiH, Distrikt Brčko i kantoni FBiH), a koji su važni za

vođenje evidencija o licima koja se nalaze zaposlena u ustanovama.



Slika 5. Dijagram tokova podataka za proces A3 (Vođenje evidencija o zaposlenim)

Proces ažuriranja podataka o zaposlenim licima ima sledeće procese:

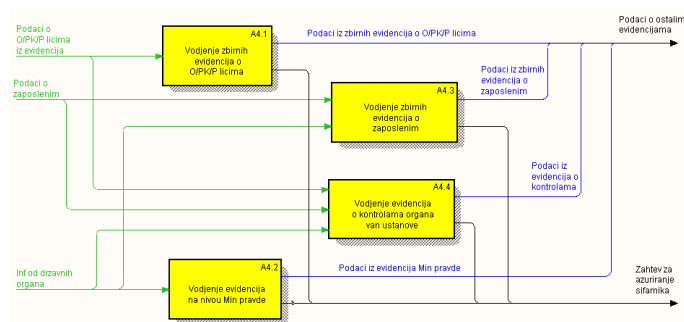
- Proces A3.1. (Evidentiranje/ažuriranje osnovnih podataka o zaposlenim). Ovaj proces je potrebno aktivirati u slučaju da se radi o unosu novog lica koje dolazi da radi u ustanovi ili je došlo do promene osnovnih podataka o licima koja se već zaposlena u ustanovi. Ulazne tokove podataka u ovaj proces čine informacije dobijene od lica koja dolaze da rade ili su već zaposleni u ustanovi, podaci iz šifarnika i informacije dobijene od državnih organa. Izlazne tokove podataka čine zahtevi za ažuriranje šifarnika (ukoliko je potrebno za neko lice proširi/ažurirati šifarnike), kao i podaci o zaposlenom licu.
- Proces A3.2. (Ažuriranje podataka o radnim mestima). U ovom procesu se vrši ažuriranje podataka o radnom mestu na koje je raspoređeno zaposleno lice (promena dotadašnjeg radnog mesta u slučaju da je lice zaposleno u ustanovi ili evidentiranje radnog mesta na koje je raspoređeno lice koje dolazi da radi u ustanovu). Ulazne tokove podataka za ovaj proces čine podaci koji se nalaze u šifarnicima, osnovni podaci o licima koja su zaposlena u ustanovi i informacije dobijene od državnih organa za to lice. Izlazni tok podataka iz ovog procesa čine zahtevi za ažuriranje šifarnika (ukoliko je potrebno ažuriranje šifarnika za neko lice) i Podaci o radnim mestima.
- Proces A3.3 (Vođenje pomoćnih evidencija o zaposlenim). Ovaj proces predstavlja vođenje svih pomoćnih evidencija o licima koja su zaposlena u ustanovi osim onih koje obuhvataju procesi A3.1 i A3.2. Ulazne tokove podataka u ovaj proces predstavljaju podaci o licima zaposlenim u ustanovi (osnovni i podaci o radnim mestima), Informacije od državnih organa (svih nivoa) i podaci koji se dobijaju od lica koja su zaposlena u ustanovi. Izlazne tokove podataka čine zahtevi za ažuriranje podataka o šifarnicima (ukoliko je potrebno) i podaci iz pomoćnih evidencija o zaposlenim.

- Proces A3.4 (Evidentiranje zaduženja zaposlenih). Ovaj proces predstavlja vođene određenog broja pomoćnih evidencija koje se tiču zaduženja zaposlenih lica u ustanovi (opremom, uniformom, radnim zadacima). Ulazne tokove podataka u ovaj proces čine podaci o licima zaposlenim u ustanovama (osnovni podaci i podaci o radnim mestima) i informacije dobijene od državnih organa. Izlazne tokove podataka čine zahtevi za ažuriranje podataka o šifarnicima (ukoliko je potrebno) i podaci o zaduženjima zaposlenih.

U procesu A4 (Vođenje ostalih evidencija u KPU) vrši se ažuriranje podataka u onom delu baze podataka u kojoj se nalaze podaci o ustanovama koje se tiču ustanove u celosti i vođenje evidencija na nivou Ministarstva pravde Republike Srpske. Dijagram tokova podataka za proces A4 (Vođenje ostalih evidencija u KPU) dat je na slici 6. Proces A4 ima sledeće ulazne tokove podataka:

- Podaci od osuđenim/prekršajno kažnjelim/pritvorenim licima koji predstavljaju podatke koji se dobijaju iz evidencija koje se vode o ovim kategorijama lica.
- Podaci od zaposlenim koji predstavljaju podatke koji se dobijaju iz evidencija koje se vode o zaposlenim licima.

Informacije od državnih organa sa raznih nivoa (Republika Srpska, Bosna i Hercegovina, Federacija BiH, Distrikt Brčko i kantoni FBiH), a koji su važni za vođenje evidencija o ustanovama i Ministarstvu pravde Republike Srpske.



Slika 6. Dijagram tokova podataka za proces A4 (Vođenje ostalih evidencija u KPU)

Proces ažuriranja podataka o zaposlenim licima ima sledeće potprocese:

- Proces A4.1. (Vođenje zbirnih evidencija o osuđenim/prekršajno kažnjenim/pritvorenim licima). Ovaj proces je potrebno aktivirati u slučaju da se radi o vođenju evidencija u ustanovi koje nisu vezane za određeno lice nego za grupu lica iz ovih kategorija. Ulazne tokove podataka u ovaj proces čine podaci o ovim kategorijama lica. Izlazne tokove podataka čine zahtevi za ažuriranje šifarnika (ukoliko je potrebno za neku grupu lica proširi/ažurirati šifarnike), kao i podaci iz zbirnih evidencija o ovim kategorijama lica (brajna stanja pojedinih grupa, grupne aktivnosti (sportske, štrajkovi, pobune)).
- Proces A4.2. (Vođenje evidencija na nivou Ministarstva pravde). U ovom procesu se vrši ažuriranje evidencija

koje se isključivo na nivou Ministarstva pravde Republike Srpske. Ulazne tokove podataka za ovaj proces čine informacije dobijene od državnih organa. Izlazni tok podataka iz ovog procesa čine zahtevi za ažuriranje šifarnika (ukoliko je potrebno ažuriranje šifarnika za neku evidenciju) i Podaci iz evidencija Ministarstva pravde.

- Proces A4.3 (Vođenje zbirnih evidencija o zaposlenim). Ovaj proces predstavlja vođenje svih pomoćnih evidencija o licima koja su zaposlena u ustanovi a koja se tiču grupnih aktivnosti zaposlenih lica. Ulazne tokove podataka u ovaj proces predstavljaju podaci o licima zaposlenim u ustanovi, Informacije od državnih organa (svih nivoa) i podaci koji se dobijaju iz evidencija koja se vode za lica koja se u ustanovi nalaze na izdržavanju kazne. Izlazne tokove podataka čine zahtevi za ažuriranje podataka o šifarnicima (ukoliko je potrebno) i podaci iz zbirnih evidencija o zaposlenim.
- Proces A4.4 (Vođenje evidencija o kontrolama organa van ustanove). Ovaj proces predstavlja vođenje određenog broja pomoćnih evidencija koje se tiču kontrole rada ustanove od strane ovlašćenih lica (kontrole od strane lica koja rade u ustanovi i lica koja ne rade u ustanovi). Ulazne tokove podataka u ovaj proces predstavljaju podaci o licima zaposlenim u ustanovi, Informacije od državnih organa (svih nivoa) i podaci koji se dobijaju iz evidencija koja se vode za lica koja se u ustanovi nalaze na izdržavanju kazne. Izlazne tokove podataka čine zahtevi za ažuriranje podataka o šifarnicima (ukoliko je potrebno) i podaci iz evidencija o kontrolama.

IV. ZAKLJUČAK

U ovom radu su prikazane osnovne karakteristike modelovanja tokova podataka za informacioni sistem kazneno-popravnih institucija Republike Srpske. Primjenom IDEF metodologije uz podršku odgovarajućeg softverskog alata AllFusion Proces Modeler značajno je smanjeno vrijeme i trud za razvoj pomenutog informacionog sistema koji je implementiran u sve organizacione delove sistema. ZA modelovanje samoG sistema korišten je ograničeni broj oznaka što je omogućilo zainteresovanim osobama da vrlo brzo i lako mogu naučiti čitati IDEF dijagrame te uputiti odgovarajuće prijedbe razvojnom timu prije završetka procesa implementacije sistema u realnom okruženju.

LITERATURA

- [1] J. Bogati, D. Vuk, "IDEF metodologija modeliranja informacijskih sustava", Praktični menadžment, Vol III, br. 4, str. 93-99, 2012.
- [2] IDEF0 Standard, U.S. Government standards documents, 1993
- [3] Mayer R.J., Crump W.J., Fernandes R., Keen A., Painter M.K., "Information Integration for Concurrent engineering (IICE) compendium of methods report", Human resource directorate logistic research division, Wright-Patterson Air Force Base, Ohio, 1995.
- [4] Bruce, T., "Designing Quality Database with IDEF1x Information Models", New York: Dorset House Publishing, 1992.
- [5] Loomis, M.E.S., "Data Modeling - the IDEF1x Technique. Fifth Annual International Phoenix Conference on Computers and Communications", Scottsdale Arizona, IEEE, 1986.

Višekriterijumski pristup organizaciji rada računara u malim i srednjim preduzećima sa stanovišta zaštite i forenzike

A multicriteria approach to the organization of work of computers in small and medium-sized enterprises from the perspective of protection and forensics

Mališa Žižović, Univerzitet Singidunum, Nada Damljanović, Univerzitet u Kragujevcu, Kosana Vićentijević, Univerzitet Singidunum, Jelena Kaljević, Univerzitet Singidunum, Miodrag Žižović, Univerzitet Singidunum

Sažetak— Metode višekriterijumske analize se svakodnevno koriste pri donošenju odluka veće ili manje važnosti. Problem višekriterijumskog odlučivanja se svodi na zadatak poređenja alternativa ocenjenih prema većem broju različitih kriterijuma (najčešće različitog relevantnog značaja) primenom odgovarajućeg računa. Za dati skup alternativa i dati skup kriterijuma, prirodno se nameće pitanje koja alternativa je najbolja?

U ovom radu prikazano je kako se metode višekriterijumskog odlučivanja mogu primeniti na odabir adekvatnog pristupa organizaciji rada računara u malim i srednjim preduzećima sa stanovišta zaštite i forenzike. Poslovanje ovih preduzeća bitno je vezano za upotrebu računara pa se mora voditi i neprekidna briga o zaštiti od raznih neželjenih mogućnosti prestanka rada računara ili pogrešnog rada računara koje može biti izuzetno štetno po preduzeće.

Ključne reči – Računar; zaštita; alternativa; kriterijum; višekriterijumska analiza

Abstract – Multi-criteria analysis methods are used daily in decision-making of greater or lesser importance. The problem of multi-criteria decision comes down to the task of comparing alternatives valued by a number of different criteria (usually of different relevant importance) using the appropriate calculus. For a given set of alternatives, and provided set of criteria, a natural question arises which alternative is the best?

In this paper we show how multiple criteria methods can be applied to the selection of an adequate approach to the organization of work of computers in small and medium-sized enterprises from the perspective of protection and forensics. The business of these companies is significantly related to the use of computers, so it shall also be constant concern about the protection of various unwanted activities as the computer which not work or computers not work correctly, that can be extremely harmful to the company.

Keywords – Computer; protection; alternative; criterion; multicriteria analysis

I. UVOD

Prema nekim procenama (videti M. Žižović i saradnici, 2014), mala i srednja prduzeća su najbrojnija preduzeća u Evropi (oko 99%), a ona zapošljavaju oko 85% radne snage zaposlene u privredi Evrope. U današnje vreme, poslovanje ovih preduzeća je bitno vezano za računar. Na ovaj ili onaj način, računar se javlja u poslovanju ovih preduzeća. Pri tom, po pravilu, svi računari su su povezani sa drugim računarima, a samim tim su izloženi mogućnostima napada i neželjenih posledica tih napada kao što su gubici podataka, neželjene operacije, ili još gore, preuzimanje podataka, pa i imovine (novca) od strane onih koji su napade organizovali.

Jasno je da se izgrađuju i sistemi za odbranu od ovakvih napada, i pro tom su neki od ovih sistema "besplatni", a neki od ovih sistema se plaćaju. Potpunu, apsolutnu zaštitu ne pruža ni jedan od sisitema za zaštitu, ali neki su više, a neki manje efikasni.

Pored rada na svakodnevrim poslovima, u svakom od ovih preduzeća se mora voditi i neprekidna briga o zaštiti od raznih neželjenih mogućnosti prestanka rada računara ili pogrešnog rada računara koje može biti izuzetno štetno po preduzeće.

Ako postoji sumnja o privrednim prestupima u malim i srednjim preduzećima, onda je forenzika znatno komplikovanja ako je preduzeće imalo neku vrstu "napada" i potrebno je ustanoviti da li su štete nastale kao posledica napada ili kao posledica namernih pronevera.

Dakle, sa stanovišta vlasnika preduzeća (koji nisu obavezno i radnici preduzeća) je jako važno, i u cilju forenzike, da postoji dobra zaštita od napada (bilo da se on događa sa strane ili iz samog preduzeća kao posledica nesavesnog poslovanja - privrednog kriminala).

II. IZBOR NAČINA ZAŠTITE

U svakom preduzeću postoje razne mogućnosti za zaštitu od neželjenih posledica eventualnih napada.

Ovde ćemo posmatrati neke od mogućih alternativa koje su prikazane u Tabeli 1.

TABELA 1

Alternative	
A_1	Nabavka nekog od savremenih programa za zaštitu koji po proceni isporučio pružaju veliku zaštitu, i po pravilu, dosta koštaju.
A_2	Nabavka nekog od savremenih programa za zaštitu koji se mogu naći bez plaćanja, i koji, po proceni isporučio, pružaju dobru zaštitu.
A_3	Kombinovati prvu i drugu varijantu za razne računare u preduzeću (važnija mesta bolje zaštititi).
A_4	Najvažnija mesta u preduzeću u potpunosti izolovati od mreže, a ostala mesta zaštititi kao u alternativu A_1 .
A_5	Najvažnija mesta u preduzeću u potpunosti izolovati od mreže, a ostala mesta zaštititi kao u alternativu A_2 .
A_6	Najvažnija mesta u preduzeću u potpunosti izolovati od mreže, a ostala mesta podeliti u dve grupe i zaštititi kao u alternativu A_3 .

Dati skup alternativa ocenimo na osnovu četiri kriterijuma koji su prikazani u Tabeli 2.

TABELA 2

Kriterijumi	
C_1	Cena zaštite podataka preduzeća.
C_2	Sigurnost zaštite podataka preduzeća.
C_3	Sigurnost rada radnika u preduzeću.
C_4	Uticaj na organizacionu strukturu preduzeća.

Pretpostavka je da su svi kriterijumi maksimizirajućeg tipa (dovedeni su na tu varijantu), i da su ocene od 1 do 20 (sa tim što je 20 najbolje, a 1 najslabije).

Jasno je da je moguće postaviti i mnoge druge kriterijume kada je reč o izboru načina zaštite, ali smatramo da će i ovi kriterijumi zadovoljiti potrebe izbora u najvećem broju slučajeva.

TABELA 3

Ocene				
	C_1	C_2	C_3	C_4
A_1	7	15	17	18
A_2	20	14	15	18
A_3	12	15	16	17
A_4	8	20	17	16
A_5	18	20	15	16
A_6	13	20	16	15

Višekriterijumsko rangiranje predloženih alternativa po datim kriterijumima, biće izvršeno na osnovu Mrežnog metoda za višekriterijumsko ocenjivanje, M. Žižović i dr., 2011. Ovaj metod se bazira na računanju rastojanja date alternative A_i od hipotetički idealne- najbolje alternative A^* i hipotetički najgore alternative A_- . U račun se uključuje čitav niz parametara, počev od onih uobičajenih kojima se uzima u obzir značaj važnosti kriterijuma, do onih koji su za ovaj metod specifični kao što su funkcije kojima se opisuje značaj razlike između alternativa. Za jednu alternativu kažemo da je bolja od druge ako je bliža hipotetički najboljoj alternativu A^* i udaljenija od hipotetički najgore alternative A_- .

Kratak opis Mrežnog metoda biće dat u sledećem odeljku.

Ovde, u zavisnosti od težinskih koeficijenata za pojedine kriterijume, mogu se dobiti razni poređci alternativa. U principu, u svim varijantama je najbolja alternativa A_4 .

III. MREŽNA METODA VIŠEKRITERIJUMSKOG ODLUČIVANJA

Tokom poslednjih decenija razvijen je veliki broj metoda i tehnika višekriterijumske analize. U kombinaciji sa upotrebom modernih računara, većina ovih metoda ima dobru softversku podršku. Za pregled dostupnih metoda za rešavanje problema višekriterijumskog odlučivanja upućujemo na monografije I. Nikolić, S. Borović (1996), M. Radojičić, M. Žižović (1998), C. L. Hwang, K. Yoon (1981), E. Triantaphyllou (2000) i J. Figueira i dr. (2005).

U ovoj sekciji dati su osnovne pojmovi, oznake i rezultati u vezi sa Mrežnim metodom višekriterijumskog odlučivanja.

Neka je dat skup alternativa $A = \{a_1, a_2, \dots, a_m\}$ koje se ocenjuju prema skupu kriterijuma $C = \{c_1, c_2, \dots, c_n\}$. U opštem slučaju, različiti kriterijumi iz skupa C ne moraju imati isti značaj, pa ćemo podrazumevati da je svakom kriterijumu c_k , $k \in \{1, 2, \dots, n\}$ pridružen broj $z_k \in (0, 1)$ koji predstavlja

stepen važnosti tog kriterijuma pri ocenjivanju datog skupa alternativa.

Takođe, svakom kriterijumu pridružimo funkciju koja meri stepen značaja razlike među alternativama, tj. razmatraćemo funkcije $Z_k : A \times A \rightarrow [0, +\infty)$, za svaki kriterijum c_k , $k \in \{1, 2, \dots, n\}$, koja svakom paru alternativa $a_i, a_j \in A$ pridružuje nenegativan realan broj $Z_k(a_i, a_j)$.

Radi jednostavnijeg označavanja, pretpostavićemo da je za svaki $i \in \{1, 2, \dots, m\}$, alternativa a_i predstavljena kao uređena n -torka $a_i = (a_{i1}, a_{i2}, \dots, a_{in})$, ili ekvivalentno $a_i = (a_{ik})_{k=1}^n$, pri čemu svaka koordinata a_{ij} , kada $j \in \{1, 2, \dots, n\}$, jeste nenegativan realan broj koji predstavlja stepen zadovoljenja kriterijuma c_j .

Sada ćemo konstruisati dva nova skupa hipotetičkih alternativa. Ove alternative koristićemo pri računu koji ćemo nadalje prikazati. Dakle, za dati skup alternativa $A = \{a_1, a_2, \dots, a_m\}$, definišemo skupove $\bar{A}$ i $\underline{A}$ na sledeći način:

$$\bar{A} = \left\{ (\max_{i \in J} a_{ik})_{k=1}^n \mid J \in P(\{1, 2, \dots, m\}) \setminus \emptyset \right\},$$

$$\underline{A} = \left\{ (\min_{i \in J} a_{ik})_{k=1}^n \mid J \in P(\{1, 2, \dots, m\}) \setminus \emptyset \right\}.$$

Na osnovu definicije imamo da skup $\bar{A}$ sa prirodnim uređenjem $\leq_{\bar{A}}$ čini gornju polumrežu sa najvećim elementom $\max A$ koji ćemo označiti sa a^* i nazivati *najboljom alternativom*.

Dualno, imamo da skup $\underline{A}$ sa prirodnim uređenjem $\leq_{\underline{A}}$ čini donju polumrežu sa najmanjim elementom $\min A$ koji ćemo označiti sa a_* i nazivati *najgorom alternativom*.

Sada, u skupu $L = \bar{A} \cup \underline{A}$, možemo definisati parcijalno uređenje koje čuva uređenja u $\bar{A}$ i $\underline{A}$, tj. za sve $a, b \in L$, ako je $a \leq_{\bar{A}} b$ onda je $a \leq b$ i ako je $a \leq_{\underline{A}} b$ onda je $a \leq b$. U principu, $(L, \leq)$ je parcijalno uređen skup koji se može sagledati kao suma donje i gornje polumreže.

Neka su $a, b \in L$ takvi da je a pokriven sa b , tj. neka je $a < b$. Tada za svaki kriterijum c_k , $k \in \{1, 2, \dots, n\}$, definišemo *preferenciju alternative b nad alternativom a u odnosu na kriterijum c_k* na sledeći način

$$\delta_k(a, b) = Z_k(a, b) \cdot \frac{b_k - a_k}{a_k^* - a_{*k}}.$$

Neka su $a, b \in L$ dve priozvoljne alternative i neka je $P : a = p_1 < p_2 < \dots < p_j = b$ put u L od alternative a do

alternative b . Tada je *tekuća preferencija alternative b nad alternativom a u odnosu na kriterijum c_k duž puta P* definisana sa:

Ako je $\delta_k(p_i, p_{i+1}) = 0$, za sve $i \in \{1, \dots, j\}$, onda je $\delta_k^P(a, b) = 0$, a inače je

$$\delta_k^P(a, b) = \frac{1}{\sum_{i=1}^{j-1} Z_k(p_i, p_{i+1})} \sum_{i=1}^{j-1} \delta_k(p_i, p_{i+1}),$$

što je ekvivalentno sa

$$\delta_k^P(a, b) = \frac{1}{\sum_{i=1}^{j-1} Z_k(p_i, p_{i+1})} \sum_{i=1}^{j-1} Z_k(p_i, p_{i+1}) \frac{p_{k+1,i} - p_{ki}}{a_k^* - a_{*k}}.$$

Polazeći do alternative a , do alternative b se može stići preko više različitih puteva u L sa odgovarajućim tekućim preferencijama, pa ćemo *preferenciju alternative b nad alternativom a u odnosu na kriterijum c_k* definisati na sledeći način:

$$\pi_k(a, b) = \max \{ \delta_k^P(a, b) \mid P : a \rightarrow b \},$$

i zbog toga se *preferencija alternative b nad alternativom a* može sagledati kao n -torka:

$$\pi(a, b) = (\pi_k(a, b))_{k=1}^n.$$

Rastojanje alternative $a \in L$ od najbolje alternative a^* dato je sa

$$D_1(a) = \frac{1}{\sum_{k=1}^n Z_k} \sum_{k=1}^n Z_k \cdot \pi_k(a, a^*),$$

A rastojanje najgore alternative a_* od alternative a dato je sa

$$D_0(a) = \frac{1}{\sum_{k=1}^n Z_k} \sum_{k=1}^n Z_k \cdot \pi_k(a_*, a).$$

Sada, za dve alternative $a, b \in A$, kažemo da alternativa a *preferira* alternativu b ako je a bliža najboljoj alternativu i ako je najgora alternativa udaljenija od a . Takođe, kažemo da je alternativa a *indiferentna* sa b ako su podjednako udaljene od najbolje i najgore alternative. Inače kažemo da su alternative a i b *neuporedive*.

Ova relacija je parcijalno uređenje, a ako donosioci odluka žele da imaju totalno uređenje može se formirati sledeća relacija.

Za svaki $a \in A$, definišemo razliku

$$D(a) = D_0(a) - D_1(a).$$

Totalno uređenje definisano je sa:

za sve $a, b \in A$, a preferira b ako i samo ako je

$$D(a) > D(b),$$

i a je indiferentna sa b ako i samo ako je

$$D(a) = D(b).$$

Koristeći ovu metodu u našem primeru se dobija da je alternativa A_5 najbolja za skoro sve vrednosti težinskih koeficijenata, a pogotovu kada najveću vrednost težinskih koeficijenata dodelimo drugom i prvom kriterijumu.

IV. ZAKLJUČAK

Potpune zaštite umreženih računara nema. Isto tako i izolovani računari u koje se povremeno uključuju razni uređaji za prenos podataka, nisu nikada zaštićeni u potpunosti.

Postoji dosta veliki broj zaštita, od kojih su neke besplatne, a neke i veoma skupe. Na osnovu istraživanja raznih agencija za ocenu i testiranje zaštite, može se zaključiti da su skupe zaštite nešto malo bolje, ali ni one nisu potpuno sigurne.

Ovde je predložena kombinacija izolovanih računara za rad sa ključnim podacima za preduzeće (računovodstveni

podaci, finansijski podaci, ...), a ostali će biti zaštićeni na neki od mogućih načina. U tom slučaju je za ostale računare dovoljna i neka od besplatnih zaštita.

Ovako organizovanje rada računara u preduzeću omogućava i jednostavniju forenzičku analizu (u slučaju potrebe) i predstavlja i svojevrsan način zaštite od privrednog kriminaliteta.

LITERATURA

- [1] J. Cvijanović, *Organizazione promene*, Ekonomski institut, Beograd, 2004.
- [2] J. Figueira, S. Greco, M. Ehrgott, *Multiple Criteria Decision Analysis: State of the Art Surveys*, Springer Verlag, 2005.
- [3] C. L. Hwang, K. Yoon, *Multiple attribute decision making methods and applications*, Spriner-Verlag, 1981.
- [4] I. Nikolić, S. Borović, *Višekriterijumska optimizacija, metode, primena u logistici, softver*, Centar vojnih škola Vojske Jugoslavije, 1996.
- [5] M. Radojičić, M. Žižović, *Applications of methods of multicriteria analysis in bussines decision-making*, Technical faculty in Čačak, Serbia, 1998 (Monograph in Serbian).
- [6] M. Travar, J. Cvijanović, J. Lazić, *Kapacitet za mikroorganizacione promene*, Ekonomski institut, Beograd, 2009.
- [7] E. Triantaphyllou, *Multi-Criteria Decision Making Methods: A Comparative Study*, Kluwer Academic Publishers, Dordrecht, 2000.
- [8] M. Žižović, N. Damljanović, V. Lazarević, N. Deretić, *New method for multicriteria analysis*, U.P.B. Sci. Bull. Series A 73 (2) (2011) 13-22.
- [9] M. Žižović, N. Damljanović, K. Vićentijević, J. Kaljević, *Višekriterijumski izbor partnera za inovacioni projekat*, Međunarodna konferencija Inovacije u funkciji privrede, MEF Beograd, 2014.
- [10] M. Žižović, J. Kaljević, I. Pantelić, K. Vićentijević, *Multicriteria approach to organization of teaching Accounting*, International Scientific Conference, 2014, Gabrovo

Cyber kriminal i digitalna forenzika

Cyber Crime and Digital Forensics

Slađan Soldat, Gojko Grubor,
Univerzitet Sinergija

Apstrakt - Svjetska globalizacija i razvoj informacionih-komunikacionih tehnologija je rezultirao da u današnje vreme preko dve milijarde ljudi širom sveta aktivno na različite načine koristi Internet. Uslugama Interneta moguće je veoma uspešno unaprediti privredu i poslovanje, kao i mnoge druge oblasti i aspekte savremenog života. Istovremeno Cyber kriminal nanosi ozbiljne štete svjetskoj ekonomiji i nameće se kao novi vid kriminala. Ovaj rad ima za cilj da pruži cjelovit i adekvatan uvid u stanje Internet tj. Cyber kriminala sa akcentom na preventivnu i aktivnu zaštitu od Cyber kriminala, kao i ulogu digitalne forenzike za otkrivanje i dokazivanje Cyber kriminala.

Ključne reči: Cyber kriminal, Digitalna forenzika, Hacker, Internet, metode i alati.

Abstract - World globalization and development of information and communication technologies have as a result that nowadays over two billion people around the world actively in different ways using the Internet. The Internet services can successfully improve the economy and business, as well as many other areas and aspects of modern life. At the same time Cyber crime every day is harming the global economy and in different ways influences all areas of modern life. This paper has a goal to offer whole and adequate view inside Internet or Cyber crime state. Focus of the paper is on preventive and active protection from Cyber crime, including a role of digital forensic techniques and tools in detecting and proving crime.

Keywords: Cyber Crime, Digital Forensics, Hacker, Internet, methods and tools

I. UVOD

Na pojavu i nagli razvoj Cyber kriminala nije se mnogo čekalo. Cyber kriminal je u odnosu na klasični kriminal znatno kompleksniji i pruža neke nove mogućnosti za izvršioce kriminalnih djela i prognoze su da će u skorije vrijeme uzeti vodeću poziciju u odnosu na sve ostale vidove kriminala. U prilog tome su činjenice da se Informacione tehnologije (IT) veoma brzo razvijaju kao i Interneta koji je osnovno polje odvijanja Cyber kriminala.

Cyber kriminal sve više uzima udeo u odnosu na klasične vidove kriminala i nanose sve veću štetu. Ekonomije razvijenih država, već uveliko osećaju posledice Cyber kriminala. Krivična djela koja se izvrše pomoću Cyber kriminala su veoma različita i teško dokaziva pred sudovima zbog specifičnosti tehnika za izvođenje krivičnih dela i pojava oblika. Cyber kriminalci su u mogućnosti da djeluju

iz udaljenih lokacija i veoma često skriveni i anonimni što im omogućavaju moderne IT.

Na „udaru“ Cyber kriminala su uglavnom: finansijska sredstva, osjetljivi podaci pojedinaca, kompanija i država, osjetljivi biznis podaci, uključujući i manipulacije na berzama, trgovanja, razna intelektualna svojina, reputacija osoba i organizacija i sl. U zbiru, finansijska šteta izazvana Cyber kriminalom mjeri se u milionima pa čak i milijardama dolara. Zbog toga je veoma važno sprečiti ili držati pod kontrolom Cyber kriminal, što se najefikasnije postiže podizanjem svijesti o pretnjama Cyber kriminala i adekvatnim mjerama zaštite i prevencije. Takođe, veoma je bitno uspješno otkriti i dokazati Cyber kriminal pred sudom, što je zbog specifičnosti veoma teško dokazati. U otkrivanju i dokazivanju Cyber kriminala nezamenljiva je uloga digitalne forenzike, relativno mlade naučne discipline, definisane krajem 20. vjeka.

II. POJAVNI OBLICI CYBER KRIMINALA

Razvojem IT i masovnom upotrebom računara pojavljuju se i prve kompjuterske zloupotrebe i kriminal. Potrebno je razlikovati kompjuterski od cyber kriminala. Prvi se pojavljuje upotrebom računara, a cyber kriminal u mnogo širem kontekstu sa upotrebom računara i računarskih mreža, umreženih i neumreženih na Internet. Tačna definicija cyber kriminala ne postoji ali se može definisati kao „svaka kriminalna djelatnost koja se vrši upotrebom računara (hardvera i softvera), računarskih mreža i informacionih sistema“. Druga prihvatljiva definicija Cyber kriminala je: „kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemima i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža“, koja je data na Desetom kongresu Ujedinjenih Nacija posvećenog Prevenciji od kriminala i tretmanu počinioca, od aprila 2000. godine.

Pojavni oblici Cyber kriminala su raznovrsni: Cyber hakerstvo, Cyber sabotaze, Cyber špijunaža, Cyber krađe i prevare, Cyber piraterija ili pirastvo, Cyber terorizam, Cyber ratovanje itd. Cyber kriminal je sofisticirano sredstvo klasičnog kriminala, koje omogućava špijunažu, krađu i pranje novca, krađu intelektualne svojine, ratovanje itd. Njega je veoma teško definisati ili izvršiti preciznu podjelu, jer se neprekidno javljaju nove tehnike napada i novi pojava oblici kriminala.

III. CYBER HAKERSTVO

Cyber hakerstvo je jedan od najrasprostranjenijih vidova cyber kriminala. Hakerstvo ili hakovanje je postao problem krajem 20. veka i predstavlja neovlašćen pristup, ulaz, upad, delovanje u tuđu računarsku mrežu, računar, smart telefon ili neki drugi el. uređaj korisnika, upad u softver-aplikaciju, informacioni sistem i sl. U klasičnom smislu hakovanje predstavlja ekvivalent upadu u tuđu posede, a osnovne karakteristike su: neautorizovani i brižljivo planiran pristup i upad; nasilan pristup (probijanje zaštite napadnutog korisnika); napadač ili „haker“ je po pravilu na udaljenoj lokaciji od mesta napada; činjenem hakinga po pravilu haker čini niz prekršaja i krivičnih dela (špijunažu, prevaru, sabotažu, krađu, neovlašćeni pristupu, krađu autorskih prava, uznemiravanje privatnosti, širenje računarskih virusa i sl.). Hakerstvo je specifično po tome što ga izvode profesionalci i amateri. Krajem dvadesetog vjeka i početkom šire primjene računara, hakerstvo je uglavnom bilo „rezervisano“ za pojedince, manje hakerske grupe i uglavnom amatere. Razvojem IT, masovnom upotrebom računara i sličnih uređaja, te razvojem Interneta, hakerstvo počinje ozbiljno da se razvija i izvode ga različite „interesne“ grupe.

IV. TEHNIKE I ALATI HAKOVANJA

Hakerski alati zvanično nisu dozvoljeni, licencirani, testirani i slično, ali ogroman je problem što veoma često u zakonskim regulativama većine država nisu i eksplicitno zabranjeni. Jednostavnom pretragom Interneta nalazi se velika ponuda hakerski alata, uglavnom softverskih i sa neverovatnim mogućnostima. Hakerski alati su nastali nelegalno kao proizvod cyber kriminalaca i kao takvi potiču iz „podzemlja“, „crne ili sive zone“ i nisu testirani.

Exploit kits su paketi zlonamernih programa koji se uglavnom koriste za izvođenje napada sa ciljem širenja malicioznih programa. Prodaju se na crnom tržištu za nekoliko stotina do preko hiljadu dolara. Reč je, dakle, o konkurentnom tržištu sa mnogo igrača i mnogo autora. Kada se pojavio pre nekoliko godina, *MPack* je bio jedan od prvih primera ovakve vrste „alata“. Ubrzo su se pojavili *ICE-Pack*, *Fire-Pack* i mnogi drugi. Dobro poznati exploit kompleti su *Eleonore*, *YES Exploit Pack* i *Crimepack*. Napadom *sirove snage* uz pomoć hash algoritama krekuje lozinku od 16 pa i do 55 znakova). *Keylogger* alat služi za snimanje svega što je otkucano na tastaturi i slanje u poseban fajl u FTP server napadača.

Hakerski alati su često preuzeti i iz regularnih softvera koji prvenstveno služe za zaštitu ili istraživanje računarskih sistema, mreža i sl. Takvi primeri su softverski alati bazirani na Linux operativnom sistemu a to su: *Kali Linux* (naslednik *BackTrack 5, 2014*) za *testiranje sistema na proboj* (eng. penetration). Postoji ogroman broj alata koji su besplatno dostupni na Internetu i mogu se koristiti u hakerske svrhe i ako neki od njih služi samo za regularno skeniranje, kontrolisanje, mrežnog sadržaja ili paketa podataka, rada računara itd.

Hakeri često koriste i mogućnosti samog operativnog sistema (npr. *cmd - command prompt* i slično) za vršenje kriminala.

TOR browser, kreiran u američkoj mornarici kao treća generacija rutiranja tipa „crnog luka“, prvobitno je namenjen za zaštitu komunikacija vlade SAD na Internetu. Danas je dostupan softver, a otvorena računarska mreža koju veoma uspešno koriste hakerske grupe kriminalaca. *Tor browser* se na zvaničnoj stranici „Tor projekta“ objašnjava i opisuje kao „mreža virtualnih tunela“ koja omogućava korisnicima anonimnost na Internetu. Polovinom 2014. godine na internet portalima pojavila se vest da se sumnja, da su pojedine države uspjele da „provale“ anonimnost korisnika *Tor browsera* i samim tim dovodi se u pitanje njegova poverljivost.

Spam (neželjena pošta) je ogroman broj poruka nekorisne i neželjene e-pošte koju internet korisnici primaju. To su ponude za koje nikada nisu izrazili interesovanje, e-mail obavijesti o temama na koje se nisu pretplatili, lažne privatne poruke koje vode na web stranice za koje korisnik nije pre iskazivao interesovanje itd. Spam oduzima dragocjeno vrijeme žrtve i uznemirava, pogodan je i za širenje kompijuterskih virusa i drugih zlonamjernih programa.

Phising je oblik cyber kriminala koji je zasnovan na metodama društvenog inženjeringa. Naziv „phising“ je namerna greška i potiče od reči fishing (pecanje), a podrazumeva krađu i zloupotrebu podataka sa računara korisnika. Cyber kriminalac napravi „vernu“ kopiju sajtova finansijski institucija da privuku žrtve koje koriste te „kopije sajtova“ misleći da su na zvaničnim sajtovima finansijskih institucija i ostavljaju svoje podatke (brojeve bankovnih računa, pasworde, korisnička imena, brojeve naloga i sl.) dostupne cyber kriminalcu za krađu novca žrtve. Novi tip ili *phisinga* je „*tabnabbing*“. Dok se korisnik nalazi na Internet stranici na kojoj je spremljen „*tabnabbing*“, otvara se druga stranicu (*tab*), a postojeća stranica ili prva stranica mijenja oblik, npr. u login za e-mail i korisnik počinje da se loguje u e-mail, a ustvari kuca lozinku i korisničko ime u zlonamjernu stranicu.

Virus je računarski program koji se sam kopira u datotekama sa kojima dolazi u kontakt na računaru (uglavnom bez znanja vlasnika). Virus se razmnožava prenosom na drugi računar (prenosom zaraženih dokumenata, programa i slično). Prenosi se Internetom, računarskim mrežama, e-poštom, prenosnim medijima (USB memorija, CD-DVD itd) i slično. Uništava, briše i modifikuje fajlove na kompromitovanom računaru.

Crvi je računarski program sposoban da se automatski kopira sa jednog računara na drugi. Širenje je obično veoma brzo a najčešće se šire, e-mail (u prilogima, eng. attachment) ili računarskim mrežama, pre svega Internetom. Crvi ugrožavaju i računarske mreže i mogu da izazovu zagušenje mreže. Posедуje veliki asortiman malicioznih akcija.

Trojanac ili trojanski konj se u računar unosi „maskiran“ i „prikriven“ preko običnih programa koje korisnik preuzima sa Interneta (muzika, video, slike). Trojanci vrše zloćudne radnje na računaru unosom drugih malicioznih programa (crva) i to obično kroz skrivene procese u pozadini rada računara. Otkriva i prikuplja podatke (korisničke lozinke, bankovne račune, PIN brojeve bankovni kartica i slične podatke, prikupljanjem korisnikovih akcija na računaru (*kaylogger*) ili preusmeravanjem na zaražene web stranice (*downloader*) i sve to prenosi vlasniku „trojanca“.

DOS napadi ili napad odbijanjem usluge (eng. *Denial-of-Service attack*) predstavlja pokušaj da se neki računarski izvor učini nedostupnim korisnicima kojima je namenjen. Napad je sastavljen od sinhroniziranih i usklađenih pokušaja jedne ili više osoba da onemogući normalan rad i funkcionisanje ili da potpuno onespobu neku Internet stranicu ili servis. Ova vrsta napada se vrši „plavljenjem“ mreže informacijama ili zahtevima serveru za servise. Server može da primi ograničen broj zahteva, a slanjem velikog broja zahteva prema serveru može da uspori ili onespobi rad web servera, tako da ga korisnici ne mogu koristiti. **DDOS** napad je distribuirani DOS napad gde napadač kontroliše i sinhronizuje više izvora računara sa kojih šalje veliki broj zahteva ka serveru i tako ga „zagušuje“ ili onespobljava. Takav napad je moćniji jer napadač može da iskoristi veliki broj korumpiranih računara. Poznate su tzv. *botnet* mreže robotizovani računara za DDOS napade sa preko 1,200.000 korumpiranih računara.

Industrijska špijunaža odvija se u sferi industrijskih kompanija. U modernom društvu i 21. veku velike kompanije su često finansijski jače od omanjih država i zbog te svoje snage četo pribegavaju industrijskoj špijunaži. Kompanije koriste metode i alate koje obično koriste i Cyber kriminalci. Posedovanje prave informacije u pravo vreme o novim proizvodima i tehnologijama konkurencije velika je prednost kompanije. Cyber špijunaži pribegavaju po pravilu kompanije koje raspolazu ogromnim finansijskim sredstvima i sam tim su u mogućnosti da angažuju profesionalce hakere i nabave skupu tehnologiju i alate. Ulaganje u Cyber napad i špijunažu, ili sabotažu je do veličine koristi koju kompanija-napadač ima u tom slučaju.

Cyber terorizam je ređa pojava Cyber kriminala, ili možda manje medijski propraćena, a predstavlja cyber kriminal kada napadač želi da teroriše grupu, organizaciju, državu ili državne institucije. Ima iste ciljeve kao klasični terorizam samo što teroristi moraju da budu informatički pismeni, školovani, vješti u korišćenju računara itd. Ova vrsta terorizma je specifična i posebno zanimljiva teroristima jer omogućava da se izvrše napadi sa bezbedne daljine za teroristu i da se uz dobro poznavanje IT, trendova i inovacija, uspešno sakriva.

Cyber ratovanje se odvija kao i klasični rat, samo u Cyber prostoru, što ni u kojem slučaju ne umanjuje njegov značaj u odnosu na klasično ratovanje. Kao i u Cyber terorizmu, nastoji

se naneti šteta i ostvariti napad, samo što je u Cyber ratovanju sve mnogo organizovanije od Cyber terorizma i iza njega stoje države sa svom svojom tehnologijom, resursima, ljudstvom (profesionalcima), finansijama itd. O ozbiljnosti Cyber rata govori u prilog i to da su pojedine države oformile posebne jedinice vojske za Cyber ratovanje.

Piraterija softvera je korišćenje, umnožavanje, deljenje i distribucija tuđe svojine (softvera) bez dozvole vlasnika. Pojavom Interneta i razvojem modernih IT sve vrste piraterija su postale mnogo lakše za izvođenje. Piraterija softvera u cyber prostoru je veoma zanimljiva Cyber kriminalcima ali i običnim korisnicima koji se ne trude mnogo da izbegnu besplatne i lako dostupne piratske sadržaje i softvere. Korišćenjem piratskih softvera nanosi se šteta autoru i vlasniku softvera, ali i kompanijama, zapošljavanju, budžetu države itd. Sve se opet svodi na moralnu i društvenu odgovornost, a zakonska odgovornost zavisi od države u kojoj se desila piraterija softvera i kapaciteta države da adekvatno reaguje na to kriminalno djelo. Osim piraterije softvera, Cyber kriminalci kopiraju sve što donosi novac, a nekada samo da nanese štetu vlasniku.

Kolačići (engl. *cookies*) u računarstvu predstavljaju male tekstualne fajlove koji služe za identifikaciju korisnika prilikom posete nekoj web stranici. Funkcionišu tako da kada korisnik poseti i otvori neku web stranu, njegov internet pretraživač šalje zahtev HTTP (Hyper Text Transfer Protocol) serveru prema specifikaciji protokola. U odgovoru server vraća zahtevanu stranu, kojoj predhodi HTTP odziv. Ako server želi da snimi kolačić na korisnikov računar uslediće i takav zahtev, a server će ga snimiti na računar i koristiti pri sledećoj web poseti. Informacije koje sadrže cookies su različite i zavise od servera. Mogu da sadrže datume poseta i pristupne parametre korisnika. Ako nemaju datume poseta to su onda „session cookies“, što znači da traju samo dok se ne zatvori browser. Hakeri često koriste kolačiće da ukradu pristupne parametre web stranicama.

Rizici u Cloud Computing-u (CC) su nova pretnja koju hakeri mogu iskoristiti za napade na CC centre i servise korisnika. Ove pretnje nastaju zbog novih tipova ranjivosti virtuelizovanog CC okruženja, koju hakeri mogu da iskoriste, kao i nepoverenja korisnika CC servisa u bezbednost njihovih informacija u CC centrima. Korisnik koji pristupa cloud servisu može da se nađe u kompromitovanoj virtualnoj sredini koju hakeri i ostale zlonamerne osobe, grupe, kompanije, obavještajne službe i sl. mogu da zloupotrebe.

Rizici upotrebe pametnih telefona su isti kao za klasične računare, jer ti uređaji imaju u sebi integrisan računar. Korisnik pristupa Internetu najčešće preko wi-fi veze koja je veoma rizična u odnosu na kablovsku Internet vezu npr. ADSL. Takođe mogu pristupati Internetu i preko signala mobilnog operatera, tj. EDGE veze, 3G tj. UMTS, 4G itd. Korisnici ovih mobilnih uređaja često u svojim operativnim sistemima imaju uključenu opciju GPS i tako stalno ostavljaju fizičku

lokaciju dostupnu za sve pa i hakere. Osim fizičke lokacije mobilni uređaji su lakši i pogodniji da budu žrtve hakera i to zbog svoje specifičnosti i velikog broja ranjivosti u odnosu na klasične računare.

Rizici na društvenim mrežama na Internetu (facebook, twitter itd.) su evidentni i različiti po svom karakteru. Hackeri i Cyber kriminalci društvene mreže doživljavaju kao pogodno tlo za širenje zlonamernih programa i radnji, ali i kao izuzetnu mogućnost za manipulaciju koja im pomaže za izvršenje kriminalnih djela. Rizici i nedostaci društvenih mreža bi se mogli podeliti na dve osnovne grupe i to na rizike tehničke prirode i rizike društveno socijalne prirode. Rizici tehničke prirode na društvenim mrežama su: izloženost ličnih i drugi podataka koje korisnik ostavlja na društvenim mrežama. Pojedine društvene mreže često traže previše podatak pri registraciji, a sam tim ti podaci postaju dostupni zlonamernim hakerima. Sve su učestaliji incidenti na aplikacijama za društvene mreže, koji se se obično završe šturim saopštenjem i izvinjenem kompanije u čijem je vlasništvu aplikacija. Takođe je rizično i preterano djeljenje i nepravilno održavanje digitalnog profila, posebno sa aspekta zaštite privatnosti. Korisnici društvenih mreža veoma često nisu svesni da sve što postave, urade na društvenim mrežama je u vlasništvu kompanija koje su napravile te društvene mreže.

Rizici socijalnog karaktera na društvenim mrežama su: pretrpano dodavanje (virtualnih prijatelja, nesigurni kontakti i prijateljstva sa nepoznatim osobama, ostavljanje dosta podataka, kao što su fotografije, lični podaci, finansijski podaci i imovina itd.), nesvesno otkrivanje podataka o drugima prijateljima, deci itd. Neka istraživanja govore da 2/3 korisnika Interneta koristi i društvene mreže na Internetu. Ogroman broj korisnika u virtualnom okruženju je velika opasnost ili izazov, jer korisnik počinje da gubi percepciju klasičnog, fizičkog okruženja, i često zaboravlja gde se nalazi i kakvo mu je tačno okruženje.

Za vršenje finansijskih prevara, krađe i pranja novca veoma često se koriste usluge hakera, tehnike i alati cyber kriminalaca. Veliki je broj primjera cyber kriminala u vršenju finansijskog kriminala. Registrovanje firmi i pravnih subjekata, pranje novca kroz više bankovnih računa i više država postaje veoma brzo uz korišćenje cyber kriminala. Počinioci takvih djela računaju na anonimnost i lažno predstavljanje na Internetu. Ponekad u vršenju takvih djela nije potrebno neko naprednije ili kompleksnije hakovanje. Dovoljno je da se „presretnu“ npr. e-mail, bilo kakva komunikacija na Internetu, skajp, facebook i slično, i to od odgovarajuće osobe kao što je npr direktor kompanije ili službenik banke ili državni službenik i izvrši manja promene presretnutih podataka (kao što su brojevi bankarskih računa, JMBG brojevi, PIN brojevi, lozinke i sl.) i na taj način finansijska sredstva završe na računu kriminalca ili se kompromituju šifre, PIN-ovi i slično. Internet omogućava da kriminalac iz jedne države, otvori bankovni račun u drugoj državi, firmu u trećoj državi, drugu firmu u četvrtj državi itd.

Pa da pare „vrti“ i „pere“ kroz nekoliko država i to najčešće država sa različitim zakonima i na taj način zakomplikuje nadležnost krivičnog gonjenja u slučaju otkrivanja prevare. Intelakutalna svojina u cyber prostoru je gotovo nezaštićena jer brzo putuje kroz Internet mrežu i veoma je lako i pogodno izvršiti krađu. Kao i kod pranja novca tako i u slučaju krađe intelektualne svojine, kriminalac je u jednoj državi, npr. server sa ukradenim podacima u drugoj državi, distribucija ili prodaja ukradenog intelektualnog djela u trećoj ili više država. Sve to opet komplikuje nadležnost, otkrivanje i procesuiranje kriminalaca. Intelakutalna svojina na Internetu je raznovrsna, od knjiga, naučnih djela u elektronskom obliku, pa do programa i softwera. Šteta, materijalna i nematerijalna izazvana ovom vrstom kriminala je često nemerljiva.

V. METODE I ALATI ZA ZAŠTITU U CYBER PROSTORU

Tačno definisano pravilo mera za zaštitu u Cyber prostoru ne postoji iz jednostavnog razloga jer Cyber prostor i okruženje se svakodnevno mjenja. Takođe se menjaju i metode i tehnike Cyber kriminalaca, prema mestu gde se odvijaju i inovacijama u IT. Zato je i mere zaštite u cyber prostoru potrebno prilagoditi i razvijati u skladu sa aktuelnim bezbedbosnim rizicima u cyber prostoru. Bez obzira što se bezbednosne mere moraju razvijati u skladu sa bezbedbosnim rizicima u cyber prostoru, ipak postoje neke mere, tehnike pa i alati koji su neizostavni u zaštiti.

Osnovne mere zaštite u cyber prostoru uključuju sledeće:

- Provera indetiteta, profila, kompanije, osoba ili kompanija koje srećemo u Cyber prostoru.
- Obavezna informisanost o vrstama napada i tehnikama napada u Cyber prostoru, kao i informisanost koji proizvodi, softveri pa i kompanije su manje ili više bezbedni pri njihovom izboru u cyber prostoru.
- Proveriti hardwer i softwer, koji koristimo u cyber prostoru.
- Ne otvarati priloge uz e-mail (attachments) od nepoznatih pošiljalaca i ako ih ne očekujemo.
- Instalirati dobar firewall na svoj računar.
- Instalirati dobar antivirusni program na svoj računar
- Redovno ažuriranje antivirusnog programa
- Izvršiti bezbednosna podešavanja internet pretraživača
- Redovno skeniranje računara sa antivirusnim programom
- Koristiti ažuriranje operativnog sistema
- Izbor jake lozinke.
- Proveriti ekstenzije sumnjivog fajla
- Oprezno biranje cloude servisa
- Šifrovanje podataka
- Rezervne kopije podataka (eng. backup)
- Razvoj svesti da apsolutna sigurnost ne postoji

- Fizičko tehničke i normativne mjere zaštite
- Hardversko softverski alati za zaštitu u cyber prostoru

VI. OTKRIVANJE I DOKAZIVANJE CYBER KRIMINALA, DIGITALNA FORENZIKA

Digitalna forenzika je relativno mlada multidisciplinarna naučna disciplina koja uz strogu primenu naučnih metoda vrši identifikaciju, prikupljanje, obradu i prezentaciju digitalnih dokaza na sudu, uz očuvanje integriteta dokaza u lancu nadležnosti. Da bi dokazi bili prihvatljivi na sudu, u digitalnoj forenzici se koriste samo forenzički alati koji su naučno testirani i potvrđeni, uz primenu naučnih metoda i očuvanje integriteta dokaza. Digitalni forenzički alati se koriste i za oporavak obrisanih podataka, ali i za rekonstrukciju kompjuterskog incidenta ili kriminala u hardveru ili softveru.

Forenzičari digitalne forenzike su usko specijalizovani stručnjaci za različite oblasti računarskih sistema i mreža. Digitalnu forenziku možemo podeliti prema oblasti primene na: računarsku forenziku, forenziku mobilnih uređaja, mrežnu forenziku i forenziku baze podataka, Internet forenziku i cyber forenziku. Forenzičari moraju dobro poznavati i operativne sisteme (Windows, Linux, Mac OS, Android itd.) i usko se specijalizirati za neke od njih. Forenzičari kao i svi informatičari, moraju redovno pratiti razvoj informaciono komunikacionih tehnologija.

U procesu forenzičke istrage, digitalni forenzičar mora da sledeći strogo definisane principe i procedure digitalne forenzike, prikuplja izvore digitalnih dokaza, osigurava ih od bilo kakvih promena, vrše analizu digitalni dokaza, i rekonstrukciju događaja (često uz pomoć klasičnih nalaza istrage kriminalnog djela) i priprema razumljiv izveštaj, koji se najčešće koristi na sudu, a može i u internim istragama raznih organizacija.

U borbi protiv cyber kriminala, značaj digitalne forenzike je veoma velik jer ona otkriva, proaktivno sprečava razvoj cyber kriminala j predstavlja alat bez alternative za dokazivanje i sankcionisanje cyber kriminalaca.

Tipične forenzičke tehnike su: uzimanje forenzičke kopije (tzv. imidža) osumnjičenog medija, oporavak izmjenjenih i obrisanih podataka, čuvanje nepovredivosti digitalnih dokaza, dokumentovanje svake aktivnosti u procesu digitalne forenzičke istrage i rukovanja sa digitalnim dokazima, distribuirana i aktivna forenzička analiza digitalnih dokaza.

Proces digitalne forenzičke istrage najčešće se definiše kroz četiri faze:

1. Identifikacija/priprema
2. Forenzička akvizicija,
3. Forenzička analiza i
4. Prezentacija digitalnih dokaza.

Alati u digitalnoj forenzici mogu biti *hardverski* i *softverski*. Prvi su pouzdaniji, a drugi fleksibilniji i češće se koriste i tzv. korporativnoj forenzici.

Softverski alati sa otvorenim i zatvorenim kodom su ravnopravni i priznati u većini pravosudnih sistema u svetu. Postoje mnoge verzije i proizvođači alata koji se na neki način mogu upotrebiti u digitalnoj forenzičkoj istrazi. Neki su komercionalni a neki slobodni za preuzimanje i besplatni. Neki najznačajniji komercijalni alati koje koriste brojni zvanični organi istrage širom sveta su:

- **EnCase** (*Guidance Software*)
- **Forensic Toolkit –FTK** (*Access Data*)
- **P2** (*Paraben Corporation*)
- **ILook** (*Elliott Spencer & IRS*)
- **X-Ways Forensics** (*X-Ways Software*) itd.

Jedno od osnovnih pravila digitalne forenzike kaže da svaki softver koji uzima dobar imidž koji se može verifikovati i može pomoći pri ispitivanju računara može biti „forenzički softver“.

Hardverske forenzičke alate potrebno je menjati i obnavljati otprilike na svake dve godine, u skladu sa završetkom informacionih tehnologija (na 18 meseci). Generalno, forenzičke radne stanice se mogu podeliti na tri grupe:

- 1) Stacionarne radne stanice
- 2) Portabl radne stanice
- 3) Prenosna radna stanica
- 4) Blokatore upisivanje

Stacionarna radna stanica je računarski sistem sa nekoliko kućišta za eksterne hard diskove i mnogo perifernih uređaja visokih preformansi.

Portabl radna stanica je obično laptop računar sa skoro istim brojem perifernih uređaja kao i kod stacionarne radne stanice.

Prenosna radna stanica je obično laptop ugrađen u torbu sa manjim brojem manjih perifernih uređaja i kućišta.

Blokatori upisivanja su hardversko-softverski uređaji za sprečavanje upisivanja podataka u ispitivani disk.

Oni su neizostavni dio radnih stanica za digitalnu forenziku i sprečavaju i preventivno deluju na slučajni upisi podataka od strane digitalnog forenzičara .

VII. STUDIJE SLUČAJEVA

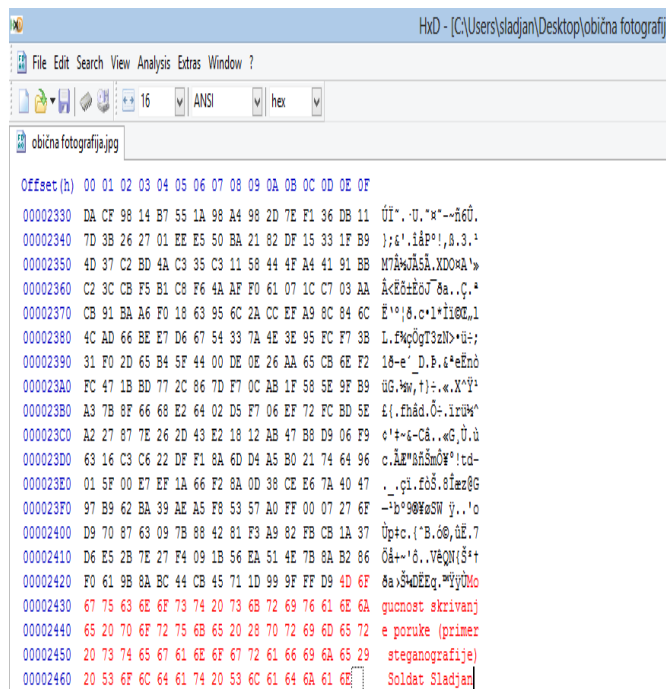
Mogućnost skrivanja podataka, poruka (kao što su: ključevi za enkripciju, passwordi/lozinke, brojevi bankovnih

računa, PIN kodovi, razne kriminalne poruke i instrukcije, jednostavno za tajnu komunikaciju kriminalaca) jednostavno je prikazan na primeru fotografije u .jpg formatu u koju je pomoću besplatnog heksadecimalnog editora H&D upisana poruka "Mogućnost skrivanja poruke-Steganografija- Soldat Sladjan" i to je primer steganografije.

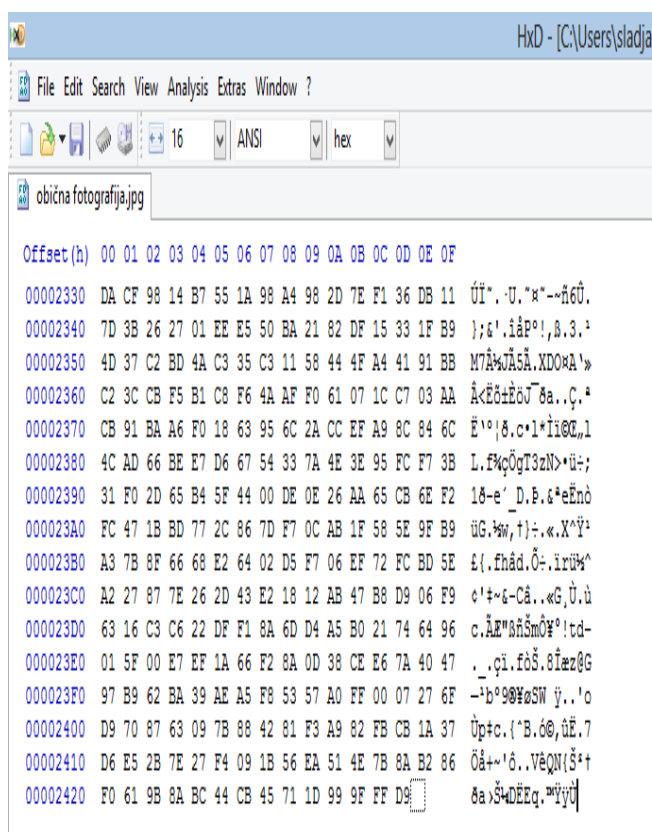
U prvom koraku biramo fotografiju na računaru (Slika 1.) i otvaramo fotografiju u H&D editoru (heksadecimalni editor na slici 2a) koja je u .jpg. formatu (naziv: *obična fotografija.jpg*).



Slika 1. Obična fotografija.jpg



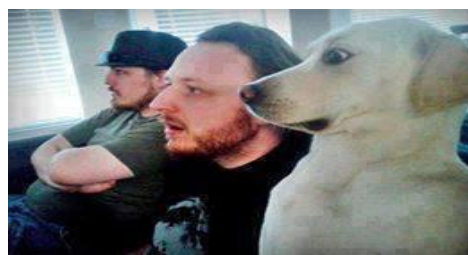
Slika 2b. Obična fotografija.jpg sa dodatom porukom



Slika 2a. Obična fotografija.jpg otvorena u H&D editoru

U drugom koraku na kraju heksadecimalnog koda fotografije ispisujemo poruku "Mogućnost skrivanja poruke-Steganografija- Soldat Sladjan" (Slika 2b)

U trećem koraku vršimo proveru da li je došlo do promene prvobitne fotografije (fotografija bez skrivene poruke) i vršimo poređenje vrednost obe fotografije (Slike 3a i 3b).



Slika 3a. Originalna fotografija, Obična fotografija.jpg (prvobitna fotografija bez ikakvih izmena)



Slika 3b. Izmenjena fotografija, Obična fotografija.jpg (sa izmenom pomoću H&D editora i skrivenom porukom)

Vizuelno nema razlike između prvobitne i izmenjene fotografije a jedina izmena je u veličini izmenjene fotografije. Originalna 9.262 bytes a izmenjena 9.326 bytes. Razlika 9.326-9.262= 62 . Razlika između originalne i izmenjene fotografije

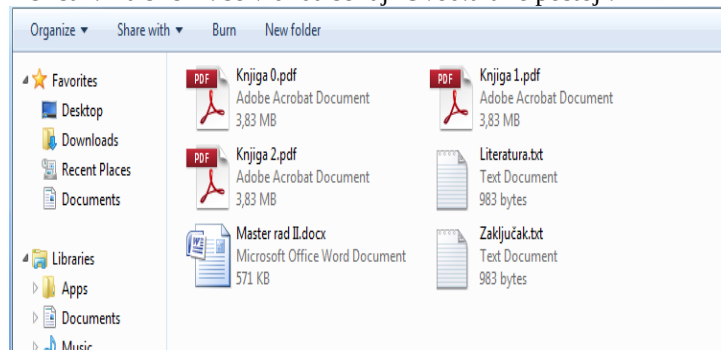
je 62bytes veća veličina izmenjene fotografije, ostalih promena nema (Tabela 1).

Tabela 1. Uporedna analiza originalne i steganografske fotografija

Detalji fotografije	ORIGINAL FOTOGRAFIJA	IZMENJENA FOTOGRAFIJA
Format	.jpg	.jpg
Veličina	9,04KB (9.262 bytes)	9,10KB (9.326 bytes)
Dimenzija	261x183	261x183
Rezolucija	96	96

Otkrivanje podataka

U ovom slučaju prikazana USB flash memoriju veličine 4.GB i forenzički alat EnCase, kako bi izveli eksperiment, radnje neopohodne za povrat namjerno izbrisano fajla sa USB flash memorije. Na USB flash memoriju je snimljeno 7. fajlova, jedan fajl pod nazivom "Uvod.txt" je namjerno izbrisan. Na slici 4. se vidi da se fajl Uvod.txt ne postoji.



Slika 4. sadržaja USB flash memoriji

Prvi korak je da utvrdimo o kakvoj se memoriji radi. Vizuelno uvidamo da se radi o USB memoriji, flash tipa, proizvođača takeMS. Drugi korak je da putem softvera saznamo detalje o USB memoriji. Neki detalji o memoriji se mogu počitati i sa čipa. Koristimo besplatni softverski alat USBDeview v2.30 i dobijamo slijedeće informacije (Slika 5):

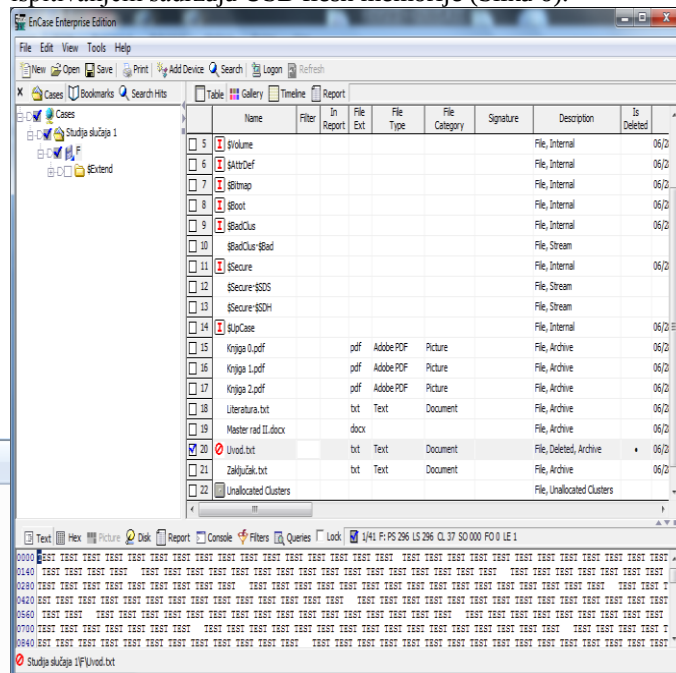
Device Name:	USB Colorline	Description:	takeMS USB Colorline USB Device
Device Type:	Mass Storage	Connected:	Yes
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	F:
Serial Number:	CCBB11012417423235673405	Created Date:	27.6.2014 2:23:25
Last Plug/Unplug Date:	28.6.2014 14:05:59	VendorID:	1c3d
ProductID:	2095	Firmware Revision:	1.00
USB Class:	08	USB SubClass:	06
USB Protocol:	50	Hub / Port:	
Computer Name:		Vendor Name:	
Product Name:		ParentID Prefix:	
Service Name:	USBSTOR	Service Description:	USB Mass Storage Driver
Driver Filename:	USBSTOR.SYS	Device Class:	USB
Device Mfg:	Compatible USB storage device	Power:	100 mA
USB Version:	2.00	Driver Description:	USB Mass Storage Device
Driver Version:	6.1.7601.17577	Instance ID:	USB\VID_1E3D&PID_2095\CCBB1101

Slika 5. slika sa info. USB flash memoriji

Treći korak je pokretanje programa EnCase, kreiranje novog slučaja "New" pod nazivom "Studija slučaja 1.", unosimo osnovne podatke o ispitivaču slučaja i određimoj lokaciji fajla. U ovom koraku još nismo pritupili USB flash memoriji.

Četvrti korak je pristupanje uređaju tj. USB flash memoriji i to vršimo putem komande "Add Device", i njegovom izborom. Nakon toga, softver učitava podatke sa USB fles memorije.

Nakon izvršenog trećeg i četvrtog koraka, možemo početi sa ispitivanjem sadržaja USB fles memorije (Slika 6).



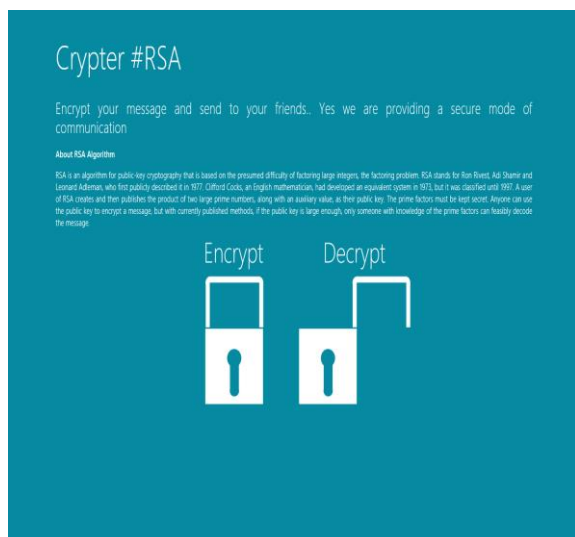
Slika 6. Ispitivanje sadržaja USB Flash memorije
Na slici 6. vidimo da se pod rednim brojem 20. nalazi fajl pod nazivom "Uvod.txt", koji je označen kao izbrisan (vidi se iz oznake u koloni "Is Deleted"). Sadržaj ovog fajla je vidljiv na donjem dijelu slike.

U petom koraku započinjemo sa oporavkom izbrisano fajla, tako što desnim klikom miša izaberemo komandu "Copy/UnErase", i označimo lokaciju za snimanje izbrisano fajla.

U ovom eksperimentu uspjeli smo uz pomoć forenzičkog programa EnCase da oporavimo namjerno izbrisani fajl.

Kriptozaštita podatka

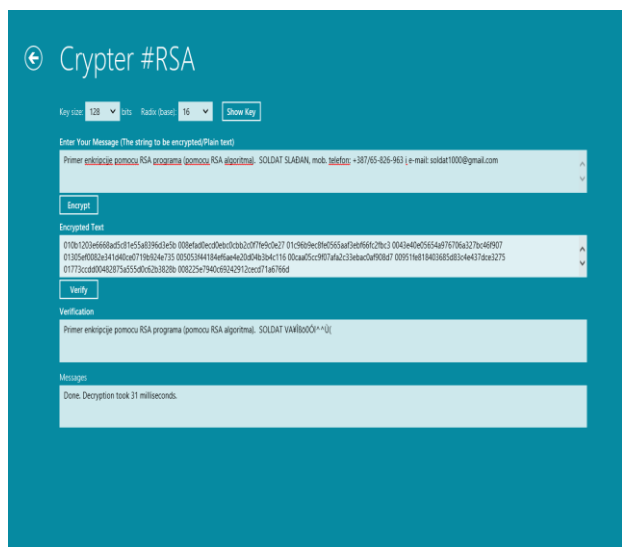
Pomoću programa Crypter # RSA koji koristi RSA algoritam za javni ključ enkriptovati ćemo poruku i tako ćemo postići bezbednost poruke, koju je moguće bezbedno poslati npr. putem e-mail-a jer ju je moguće kriptovati uz pomoć Crypter # RSA koji koristi RSA algoritam (Slika 7).



Slika 7. Crypter # RSA

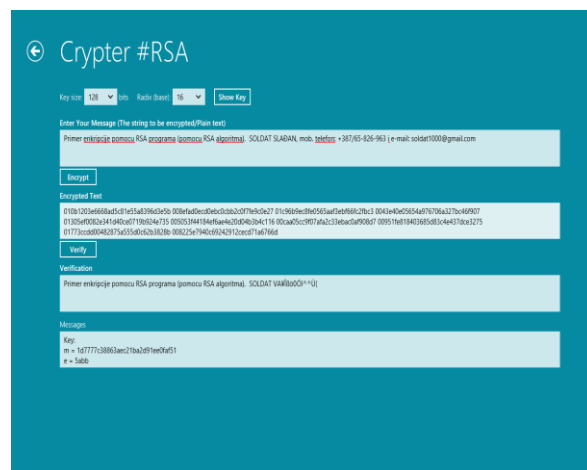
„RSA je oznaka za Ron Rivest, Adi Shanit i Leonard Adleman, koji su ga prvi javno objasnili 1997.god. Korisnik RSA generiše, a zatim objavljuje javni ključ na osnovu dva velika prosta broja, zajedno sa pomoćnim vrednostima., Tajni ključ mora da se drže u tajnosti.

- U prvom koraku uz pomoć Crypter # RSA koji koristi RSA algoritam, upisat ćemo podatak-tekst („Soldat Slađan, mob. telefon +387/65-826-963 i e-mail: soldat1000@gmail.com“) u polje za unos teksta.
- U drugom koraku pritiskamo-kliknemo taster za enkripciju i podatak tekst se kriptuje i prikazan je u polju ispod. Izabran je ključ veličine 128 bita(Slika 8).



Slika 8. Prikaz podatka i enkripcije podatka

U trećem koraku pritiskamo taster za pokazivanje ključa („Show Key“) i u krajnjem donjem polju prikazan je ključ i samim tim imamo sve potrebno za enkripciju i dekripciju podatka (Slika 9).



Slika 9. Prikazan ključ za dekripciju

VIII. ZAKLJUČAK

Razvojem IT sektora i Interneta došlo je do nezamislivog razvoja Cyber kriminala koji je po obimu i načinu izvršenja sigurno jedan od najvećih i najopasnijih vidova kriminala. Njegove posledice, razmjere i učinci su veoma teško za otkriti i neretko ostaju neotkriveni ili u sjeni drugih vidova kriminala.

Nikada nije bila značajnija potreba za jakom i razvijenom Digitalnom forenzikom jer jedino ona adekvatno, kvalitetno i sudski prihvatljivo precizno dokazuje kako je izvršen Cyber kriminal. Samim svojim djelovanjem Digitalna forenzika i preventivno djeluje jer Cyber kriminalci su svjesni da i u Cyber, Internet, virtualnom okruženju ima metoda i načina da budu efikasno otkriveni. Razvoj Interneta, informacionih tehnologija, masovnost njihove primjene svakako govori da će i Cyber kriminal sa svim svojim oblicima da zadaje ozbiljne kriminalne udarce svjetskoj ekonomiji i svjetskom društvu u svim segmentima. Podizanje svijesti o Cyber kriminalu kao rastućoj opasnosti koja i sad ima ogromnu veličinu po svim pokazateljima, kao i iznalaženju kvalitetnih načina za sprečavanje i otkrivanje je veoma poželjno kako bi se sprečio katastrofalan rezultat Cyber kriminala.

ZAHVALNOST

Veliku zahvalnost dugujem Prof. dr Gojku Gruboru koji predstavlja neiscrpan izvor ideja i inspiracija za naučnoistraživački rad. Kao i kolegi Adnanu Mujkanoviću, master inž IT-a, na tehničkoj pomoći pri izradi ovog rada.

LITERATURA

- [1] Grubor G., Milosavljević M.: *Digitalna forenzika računarskog sistema*; Beograd, 2009.god.
- [2] Grubor G., Milosavljević M. : *Istraga kompjuterskog kriminala*; Beograd, 2009.god..

- [3] Putnik N. i Miljković M.: Vojno delo (časopis): *Zloupotreba Kiber prostora kao sredstva masovne komunikacije*; Beograd 2012.god
- [4] Eoghan Casey, "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet", Academic Press, London, 2004.god.
- [5] Petrović R. Slobodan, Kompjuterski kriminal, Ministarstvo unutrašnjih poslova Republike Srbije – Beograd, 2001.
- [6] www.nmap.org
- [7] www.torproject.org
- [8] www.offensive-security.com
- [9] www.sectools.org
- [10] www.technotification.com
- [11] www.latesthackingnews.com
- [12] www.cybersecurityinstitute.biz
- [13] www.digital-evidence.org

Uticaj globalnih mreža i savremenih informacionih sistema na nastanak i razvoj forenzičkog računovodstva u Srbiji

The impact of global networks and modern information system on the occurrence and development of forensic accounting in Serbia

M. Milojević, Univerzitet Singidunum, P. Vukadinović, Univerzitet Singidunum, D. Miletić, Schneider Electric DMS NS

Sažetak— Poslednjih decenija naučna dostignuća dovela su do krupnih promena u načinu poslovanja i funkcionisanja jednog preduzeća. Razvoj računara i nastanak globalnih mreža omogućili su znatno brže i efikasnije odvijanja poslovnog ciklusa ali su otvorili i čitav niz problema vezanih za računovodstvenu kontrolu i sprečavanja zloupotreba u privrednim društvima. Uporedo sa primenom inovacija u poslovanju došlo je i do povećanja opasnosti od pojave kriminalnih radnji. Novine u poslovanju zahtevale su i promene tradicionalnog načina ispitivanja ispravnosti finansijskih izveštaja. Računovođe i revizori susreli su se sa brojnim prevarama u finansijskim izveštajima koje su uticale kako na njihovu reputaciju tako i na gubljenje poverenja u podatke koje oni pružaju korisnicima svojih usluga. Forenzičko računovodstvo nastaje kao posebna disciplina u okviru računovodstva i revizije kao odgovor na izazove koje savremene tehnologije pružaju i omogućuju u činjenju kriminalnih radnji. Cilj ovog rada je da ukaže na značaj, ulogu i neophodnost postojanja forenzičkog računovodstva prilikom sprečavanja i otkrivanja kriminalnih radnji u privrednim društvima, koja koriste savremene informacione sisteme, kao i da istakne neophodnost ulaganja u školovanje stručnih kadrova koji će se baviti ovim multidisciplinovanim zanimanjem.

Ključne riječi – *Informacioni sistemi, forenzičko računovodstvo, revizija, računovođa, finansijski izveštaji, prevare.*

Abstract – In recent decades, scientific achievements have led to substantial changes in the way of business and operations. The development of computers and the emergence of the worldwide networks have enabled faster and more efficient process of a business cycle but also opened the whole range of issues related to accounting control and prevention of abuse in companies. Along with the application of innovation in business, there was an increasing danger of criminal activity. The use of computers in business have required changes in the traditional way of testing the correctness of financial statements. Accountants and auditors have met with widespread fraud in the financial statements which contributed to their reputation and the loss of trust in the information that they provide to their customers. Forensic accounting occurs as a separate discipline within the accounting

and audit in response to the challenges that modern technologies offer and allow in the commission of criminal acts. The aim of this paper was to point to importance, role and necessity of the existence of forensic accounting in preventing and detecting criminal activities in the companies, which use modern information systems, and to emphasize the necessity of investing in the education of professional staff who will deal with this multidisciplinary interest.

Keywords – *Information Systems, forensic accounting, audit, accountant, financial statements, fraud*

I. POJAM I ULOGA FORENZIČKOG RAČUNOVODSTVA

Pronalazak računara i njihova upotreba u praćenju poslovanja kompanije značajno su uticali na postupak sprovođenja interne i eksterne kontrole. Dotadašnji način sprovođenja sistema kontrole morao je da pretrpi promene kako bi na adekvatan način mogao da odgovori zahtevima koji se pred ovaj sistem postavljaju. Ove promene ogledale su se u težnji da se upotreba računara stavi u direktnu funkciju sprovođenja kontrole. Brojne softverske kompanije se javljaju na tržištu sa svojim rešenjima i alatima kako bi kompanijama olakšale postupak kontrole finansijskih podataka..

Sa nastankom globalnih mreža počeo je i da se usložava proces odvijanja kontrole poslovanja. Poslovni ciklus se brže odvija, transakcije su upotrebom e-bankinga ubrzane a poslovanje jedne kompanije se često odvija u više država. Najveći uticaj na promenu dosadašnjeg načina poslovanja imao je nastanak interneta koji je komunikaciju i razmenu podataka o poslovanju kompanije između geografskih udaljenih tačaka sveo na uobičajnu i redovnu, kao da se poslovanje odvija gotovo na jednoj lokaciji. Sve ovo je uticalo da se na tržištu javi potreba za novim informatičkim alatima kako bi se na adekvatan način ispratilo poslovanje jedne kompanije.

U prilog nastanku specijalizovanih softverskih paketa za praćenje i kontrolu normalnog odvijanja poslovanja išao je i novi trend u poslovanju. Više ništa nije neobično kada jedna

kompanija posluje u više različitih zemalja, što podrazumeva jednu bitnu činjenicu, a to je da su vlasnici kompanije često udaljeni od zemlje u kojoj se odvija poslovanje kompanije. Samim tim otvara se mogućnost za brojne prevare i kriminalne radnje kako top menadžmenta preduzeća tako i od strane nižih hijerarhijskih struktura zaposlenih. Iz ovog razloga vlasnici kompanija se često ne oslanjaju isključivo na usluge revizora već angažuju stručnjake koji bi potvrdili kako sastavljane finansijske izveštaje kompanije tako i nalaze nezavisnih kontrola tj. eksternih revizora. Upravo odvojenost vlasništva i upravljanja ostavlja mogućnost da prevashodno menadžeri koji su udaljeni od matične kompanije ne rade u interesu vlasnika. Iz ovog razloga smatramo neophodno detaljno objasniti pojmove kriminalna radnja, forenzičko računovodstvo, finansijska revizija kao i objasniti međusobnu povezanost između ovih pojmova.

U rečnicima računovodstvenih termina ne postoji potpuno identična definicija kriminalnih radnji. U anglo saksonskom govornom području pod kriminalnom radnjom se podrazumeva razbojništvo – oduzimanje i prisvajanje tuđe imovine sa namerom njenog stalnog otuđenja od vlasnika¹. Evropsko ili kontinentalno govorno područje definiše kriminalnu radnju kao nezakonit čin (namerni prestup), prikrivanje ovog čina (često prikrivenog jednostavnim sredstvima), i sticanje koristi (pretvaranje prisvojenog u gotovinu). Zakonska definicija kriminalne radnje se odnosi na slučajeve kada osoba napravi izveštaj koji sadrži lažno predstavljanje materijalne činjenice i kada je svesna toga; kada se žrtva oslanja na izveštaj; i kada je posledica neistinitog izveštaja štetna žrtvi². Institut Američkih računovođa definisao je dve kategorije kriminalnih radnji:

- Namerno pogrešno prikazivanje finansijskih informacija
- Neopravdano prisvajanje tuđe imovine

Forenzičko računovodstvo (forensic accounting) se može definisati kao primena istražiteljskih i analitičkih veština sa ciljem otkrivanja manipulacija u finansijskim izveštajima koje odstupaju od računovodstvenih standarda, poreskih zakona i ostalih zakonskih odredbi³. Primer, ukoliko postoji sumnja da je došlo do manipulacije u finansijskim izveštajima jedne kompanije, tada to pripada u područje forenzičkog računovodstva. Računovođa forenzičar je iskusan, obučen i obrazovan za različite procese istraživanja kriminalne radnje: za efikasno obavljanje intervjua sa ljudima, za pripremu izveštaja za sud, za veštačenje na sudu i za funkcionisanje pravnog sistema.

Pod revizijom se podrazumeva proces objektivnog prikupljanja i procene dokaza vezanih za izjave uprave preduzeća o ekonomskim aktivnostima, kako bi se utvrdio stepen saglasnosti tih izjava sa utvrdjenim kriterijumima, a dobijeni rezultati preneli zainteresovanim korisnicima.

Revizija finansijskih izveštaja (FI) je ispitivanje FI radi davanja mišljenja o tome da li oni objektivno i istinito, po svim materijalno značajnim pitanjima, prikazuju stanje imovine, kapitala i obaveza, rezultate poslovanja, tokove gotovine i promene u sopstvenom kapitalu u skladu sa Međunarodnim računovodstvenim standardima IAS (International Accounting Standards) i Međunarodnim standardima finansijskog izveštavanja⁴. Sarbanes-Oxley akt iz 2002. godine opisuje detaljno postupke za sprečavanje i identifikovanje kriminalne radnje u toku revizije interne kontrole nad finansijskim izveštavanjem. Pažnja revizije je prevashodno usmerena na pružanje razumnog uveravanja da ne postoje materijalno značajne greške u finansijskim izveštajima. Na bazi iznetih definicija možemo definisati i različit opseg posla sledećih zanimanja: revizor kriminalnih radnji i računovođa-forenzičar.

Revizori kriminalnih radnji su uglavnom računovođe koji su po svojim stavovima, osobinama, veštinama znanju i iskustvu stručnjaci za sprečavanje i dokumentovano praćenje kriminalnih radnji u poslovnim knjigama.

Računovođenje-forenzičari dolaze na mesto zločina nešto kasnije u odnosu na revizore kriminalnih radnji, ali njihov glavni doprinos je u prevođenju složenih finansijskih transakcija i numeričkih podataka u pojmove koji su razumljivi običnom laiku.

Uzimajući u obzir navedene činjenice možemo doći i do cilja ovog rada a to je odgovor na dva pitanja:

1. da li su srpske kompanije i stručna javnost do detalja upoznati sa opsegom posla forenzičkog računovođe?
2. da li razumeju svrhu i upotrebu primene računara a naročito specijalizovanih programskih paketa u otkrivanju kriminalnih radnji?

Odgovori na postavljanja pitanja doneće nam saznanja o tome kako domaća stručna javnost vidi ulogu forenzičkog računovođe i da li pojedine kompanije poseduju alate za detekciju eventualnih nepravilnosti u finansijskim izveštajima.

II. METODI

U svrhu ispunjenja teorijskih i empirijskih ciljeva rada koriste se metode prikupljanja i klasifikovanja relevantnih podataka prikupljenih iz sekundarnih izvora kao što su knjige, stručni časopisi i publikacije, statistički bilteni i izveštaji te ostali javno dostupni izvori podataka. Od metoda naučnog istraživanja korišćena je analiza, sinteza, indukcija i dedukcija. Cilj primene metoda naučnih istraživanja jeste da se ponikne u srž i kompleksnost problema vezanog za manipulaciju finansijskim izveštajima i uloge koje imaju forenzički revizori.

III. KRIMINALNE RADNJE I SOFTVERI

Sa stanovišta našeg zakonodavstva kriminalna radnja može da bude:

¹ Singleton, Tommie; Singleton, Aaron; Bologna, Jack and Lindquist, Robert (2006): *Fraud Auditing and Forensic Accounting*: New York: John Wiley&Sons, p. 13.

² Coderre, David (2009): *Computer-Aided Fraud Prevention and Detection*: New York: John Wiley&Sons, p.3.

³ Belak, Vinko (2011): *Poslovna forenzika i forenzičko računovodstvo*, Zagreb: Belak Excellens doo, p.2.

⁴ Stanišić, Milovan (2006): *Beograd: Revizija i primena računara*: Univerzitet Singidunum, p. 17.

- Krivična radnja – zahteva dokaz o namernom obmanjivanju.
- Građanski prekršaj – zahteva da žrtva pretrpi određenu štetu.
- Osnov za raskidanje ugovora – proglašava se nevažećim⁵.

Kroz istoriju računovode su se borile protiv kriminalnih radnji tako što su insistirale na razdvajanju dužnosti između lica koja su radila sa gotovinom ili drugom imovinom i onima koji su obavljali knjiženje u poslovnim knjigama. Zahtevana je stroga podjela između dostupnosti određenog sredstva i odgovornosti koja se tiče evidentiranja transakcija. Ovakav način se zasnivao na zaključku da je mogućnost da dođe do krađe smanjena jer je sada potrebno da najmanje dve osobe stupe u dogovor i izvrše krađu. Uz to insistirano je da svaku poslovnu odluku u vezi sa imovinom prati određena vrsta pisano dokumenta.

Pojavom računara nastao je i novi oblik skladištenja podataka tj. nastale su baze podataka. Prva kompanija koja je primenila računare u svom poslovanju bila je kompanija General Electronic. Do 1958. godine nije postojalo sistematsko praćenje krivičnih dela povezanih sa računarima, ali od ove godine Stanford Research International (SRI) je počeo da prati zloupotrebe počinjene putem računara.

TABELA 1: Pregled prijavljenih kriminalnih radnji povezanih sa računarom

Godina	Broj prijavljenih zloupotreba
1958	3
1968	13
1977	31
1978	Ukida se praćenje

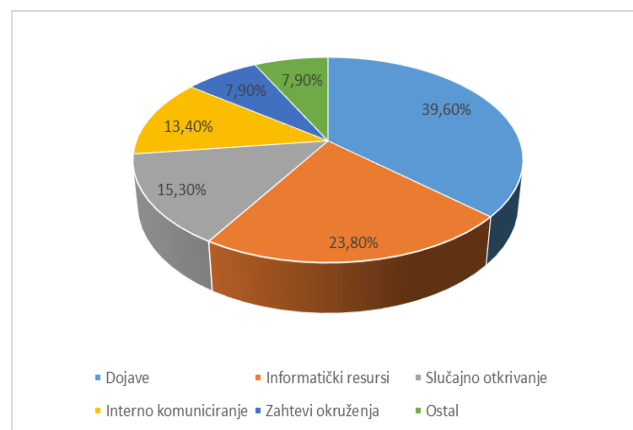
Izvor: Stanford Research International

Nakon 1978. godine SRI je prekinuo sa evidencijom iz razloga jer se smatralo da broj prijavljenih i ostvarenih kriminalnih radnji u vezi sa primenom računara se drastično razlikuje.

Stručna javnost, ali i vlasnici kompanija često su se pitali iz kog razloga finansijski revizori ne otkrivaju veći broj kriminalnih radnji? Rasprostranjeno je mišljenje da finansijski revizor je dužan da otkrije kriminalnu radnju ukoliko je ona bila izvršena u vreme obavljanja revizije od strane finansijskog revizora. Ipak većina autora se slaže da su postupci revizora osmišljeni tako da razotkrivaju materijalne greške a ne nematerijalne kriminalne radnje⁶. Razlozi iz kojih revizori ne mogu da razotkriju kriminalne radnje je i zavisnost finansijskih revizora od uzorka i na oslanjanje na ispitivanje revizorskog traga. Po najnovijem istraživanju koje je sprovedla revizorska kompanija KPMG metodi u istraživanju

kriminalnih radnji su dojave (39,60%) i informatički resursi (23,80%).

Grafik 1: Razlozi otkrivanja kriminalnih radnji



Izvor: KPMG

Na bazi sprovedenog istraživanja možemo zaključiti da najveći broj kriminalnih radnji se u današnjem vremenu otkriva putem dojava zaposlenih iz preduzeća. Ovo je i u vezi sa istraživanjem Alberta i ostalih⁷ koji su izveli zaključak da 90% prevara u vezi sa kriminalnim radnjama u jednoj kompaniji potiče pre svega od zaposlenih.

Poslednjih decenija borba protiv tehnološkog kriminala zahtevala je permanentno usklađivanje i unapređenje postojećih zakonskih rešenja. U tabeli broj 2 prikazan je spisak standarda kojim se reguliše borba protiv kriminalnih radnji počinjene putem računara.

TABELA 2: Standardi kojim se reguliše borba protiv tehnološkog kriminala.

Redni broj	Standard
1	Sarbanex-Oxley act 2002
2	Coso – The Committee of Sponsoring Organizations of the Treadway Commission
3	COBIT-Control Objectives for information and related Technology
4	SAS 94-Statment of Auditing Standards, pruža revizorima smernice o uicaju Informacionih tehnologija na unutrašnje kontrole
5	SAS 99- razmatranje prevara i revizorskog izveštaja
6	ISO 9000-Standard za kvalitet
7	ISO 27001-precizira spisak bezbednosnih kontrola (11 oblasti)

Izvor: <http://www.uirs.rs> (Stansilav Polić)

Najpoznatija softverska rešenja kojim se olakšava rad revizorima i forenzičkim računovodama su IDEA (Interactive Data Extraction and Analysis), ACL (Audit Comand Language), SESAM (ESKORT Computer Audit), TopCAATs i Analyzer. Oni služe za utvrđivanje pojedinosti kao što su prosečna vrednost, apsolutna vrednost, najviša i najniža vrednost, broj negativnih, nultih i pozitivnih vrednosti i sl. Na ovaj način brzo se može identifikovati da li postoji potreba za dubljom analizom tj. da li je potencijalno izvršena kriminalna

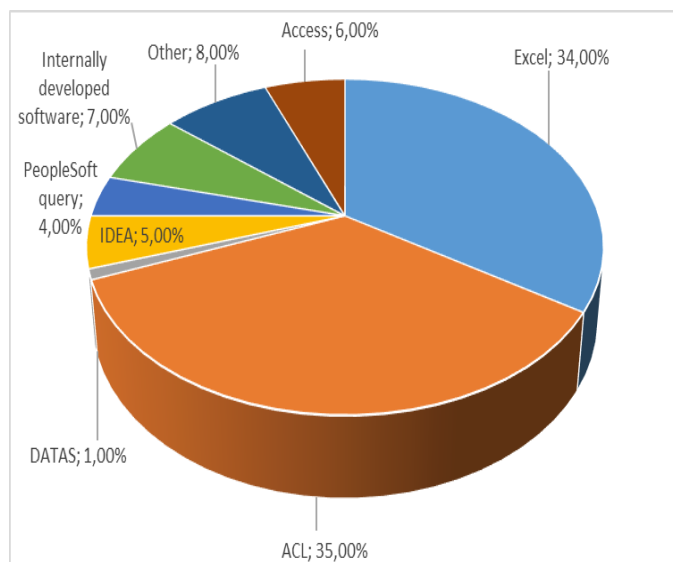
⁵ Polić, Stanislav (2014): Treća konferencija internih revizora: Beograd, Udruženje internih revizora.

⁶ AICPA, (2006) Consideration of Fraud in a Financial StatemeExaminers, ACFE (2006) Report to the Nation on Occupational Fraud and Abuse, <http://www.acfe.com/resources/publications.asp?copy=rttn>

⁷ C. Albert, W.S. Albert and J.G. Dunn (2001): Can Auditor Detect Fraud: A review of the Research Evidence, Journal of Forensic Accounting Vol.2 (1). pp. 1-12.

radnja. Bez postojanja ovih softvera i novih inteligentnih informacionih sistema jako teško je u praksi bilo odrediti koji podaci zahtevaju dodatne analize a koji ne⁸. Računovodama, revizorima i finansijskim analitičarima primena ovih programskih paketa je znatno olakšala obavljanje osnovnog posla i unapredila kvalitet izraženog mišljenja o podacima⁹. Dva najpoznatija softvera za primenu u praksi prilikom obavljanja revizije i kontrole finansijskih izveštaja su IDEA i ACL. Oba ova programa su deklarirana kao SRS Specijalizovani revizijski softveri. U odnosu na Excel oba programa su naprednija zbog njihove brzine, tačnosti i „inteligencije“ u odnosu na popularne Microsoft platforme.

GRAFIK 2: Primena softvera u detekciji kriminalnih radnji.



Izvor: ACL&KPMG

Na bazi sprovedenog istraživanja renomirane revizorske kompanije KPMG koje je sprovedeno uz pomoć ACL možemo zaključiti da najveći broj kompanija u borbi protiv kriminalnih radnji koristi ACL. Ove podatke smatramo izuzetno korisnim iz razloga da se domaća javnost upozna sa značajem ovog veoma moćnog programa i njegovom primenljivošću u praksi. Ovaj program u sebi sadrži integrisane automatske alate za prepoznavanje duplih faktura i anomalija u pojavljivanju brojeva kao i mogućnost za sprovođenje paralelne simulacije i digitalne analize.

Iz ovog razloga interesantni su rezultati ankete revizorske kompanije Price Water Coopers (PWL). Ova revizorska kuća je ispitala odgovor na dva pitanja:

1. U koje svrhe se koriste podaci dobijeni data analytics tehnikama?
2. Da li u Vašoj kompaniji primenjujete data analytics tehnike?

⁸ D. Coderre, "Primena kompjutera u sprečavanju i otkrivanju kriminalnih radnji," John Wiley&Sons, Hoboken, New Jersey 2009, pp 197-203.

⁹ M. Milojević, I. Terzić, V. Marjanović, (2014): Application of Benford Analysis in detecting anomalies in the financial statements – case of Serbian large companies, Belgrade: Conference Sinteza Apr, 2014.

Tabela 3: Primena savremenih informacionih (računovodsvenih) sistema u najvećim kompanijama.

Procenat	Način na koji ispitanici vide upotrebu softvera
85%	Podaci dobijeni upotrebom softvera važni su za potvrdu revizorskog izveštaja.
81%	Podaci dobijeni upotrebom softvera važni su za poboljšanje kvantifikovanog određivanja problema.
74%	Podaci dobijeni upotrebom softvera važni su za bolju procenu rizika
71%	Ispitanika planira da primeni data analytics tehnologije, ali nema plan kada i kako će ih primeniti. (shvata njihovu bitnost)
31%	Ispitanika koristi data analytics tehnologije.

Izvor: PWC (2013)

Sprovedeno istraživanje PWC pokazuje da većina menadžera najuspešnijih kompanija je upoznata sa benefitom korišćenja data analytics tehnologija, ali ipak istraživanje ukazuje da samo 31% njih ove tehnologije koristi u sopstvenom poslovanju. Iz ovog razloga smatra se da će upotreba ovih data analytics tehnologija u narednim godinama drastično porasti.

IV. ZAKLJUČAK

Nastankom globalizma i proces kontrole poprima drugačije oblike. Kao jedan nov vid zaštite ispravnosti i valjanosti finansijskih podataka javlja se forenzičko računovodstvo. Njegova uloga postaje sve značajnija sa usložavanjem poslovnih kombinacija. Da bi forenzičko računovodstvo moglo da odgovori zahtevima koji se pred njega postavljaju pored zakonske regulative neophodno je da postoji primena savremenih informacionih sistema i SRS. Najnovija istraživanja, renomiranih revizorskih kompanija, iz ove oblasti ukazuju da relativno mali broj menadžera u kompanijama koristi u praksi ove data analytics tehnologije, iako je većina njih upoznata sa benefitom njihovog korišćenja. Smatramo da će se narednih godina u Srbiji upotreba savremenih računovodsvenih informacionih sistema i SRS naglo povećati i da će biti potrebno edukovati nove kadrove kako bi se odgovorilo izazovu koje zanimanje forenzičko računovodstvo nosi. Do sada u praksi nije bilo značajnijih slučajeva manipulacije sa finansijskim izveštajima zabeleženih u Republici Srbiji, ali primenom pomenutih softverskih paketa i uzimajući u obzir međunarodnu praksu, za očekivati je da se u narednim godinama otvori pitanje verodostojnosti finansijskih izveštaja pojedinih kompanija.

LITERATURA

- [1] Singleton, Tommie; Singleton, Aaron; Bologna, Jack and Lindquist, Robert (2006): Fraud Auditing and Forensic Accounting: New York: John Wiley&Sons, p. 13.
- [2] Coderre, David (2009): Computer-Aided Fraud Prevention and Detection: New York: John Wiley&Sons, p.3.
- [3] Belak, Vinko (2011): Poslovna forenzika i forenzičko računovodstvo, Zagreb: Belak Excellens doo, p.2.
- [4] Stanišić, Milovan (2006): Beograd: Revizija i primena računara: Univerzitet Singidunum, p. 17.
- [5] Polić, Stanislav (2014): Treća konferencija internih revizora: Beograd, Udruženje internih revizora.

- [6] AICPA, (2006) Consideration of Fraud in a Financial State Examiners, ACFE (2006) Report to the Nation on Occupational Fraud and Abuse,
<http://www.acfe.com/resources/publications.asp?copy=rttn>
- [7] C. Albert, W.S. Albert and J.G. Dunn (2001): Can Auditor Detect Fraud: A review of the Research Evidence, Journal of Forensic Accounting Vol.2 (1). pp. 1-12.
- [8] D. Coderre, "Primena kompjutera u sprečavanju i otkrivanju kriminalnih radnji," John Wiley&Sons, Hoboken, New Jersey 2009, pp 197-203.
- [9] M. Milojević, I. Terzić, V. Marjanović, (2014): Application of Benford Analysis in detecting anomalies in the financial statements – case of Serbian large companies, Belgrade: Conference Sinteza Apr, 2014.

Tehnike otkrivanja privrednog kriminaliteta

Discovery techniques in economic crimes

Munir Hadrović, Univerzitet „Mediterran“, Podgorica, Slavica Pantović, „Univerzitet „Mediterran“, Podgorica

Sažetak - Privredni kriminalitet je izuzetno izražena društveno negativna pojava manifestovana kroz privredna poslovanja koja omogućavaju pojedincima i društvenim grupama da njegovim kršenjem steknu imovinsku korist. Pored zakonodavnih okvira i rješenja, za detekciju ove vrste kriminaliteta izuzetno važnu, čak i odlučujuću ulogu ima kompjuterska ili računarska forenzika. Kompjuterska ili računarska forenzika je proces skupljanja, analize i izvještavanja o digitalnim podacima na način koji je prihvatljiv za zakonsko procesuiranje. Može se koristiti za detekciju i prevenciju kriminalne radnje u slučajevima gdje su dokazi sačuvani u digitalnoj formi. Slično drugim formama u pravnim forenzikama, procesi u kompjuterskoj forenzici zahtijevaju veoma dobro poznavanje računarskog hardvera, softvera, kao i sofisticiranih tehnika za sprečavanje kompromitovanja i uništavanja dokaza. Prevenstveno se suočava sa popravkom i analizom latentnih podataka i dokaza koji mogu postojati u različitim formama, od analize otiska prsta i DNK analize uzete iz krvi, sve do fajlova na hard disku. Zbog toga što je ovo nova disciplina, još uvijek je standardizacija i konzistencija u sudovima i industriji malo zastupljena. Kao rezultat toga, nije priznata kao zvanična naučna disciplina. Pored navedene definicije, može se kazati i da je to disciplina koja kombinuje elemente zakona i računarske nauke u cilju skupljanja i analize podataka iz računarskih sistema, mreža, bežičnih komunikacija i uređaja za skladištenje podataka, u formi koja je prihvatljiva za zvanični sudski slučaj.

Ključne riječi – *privredni kriminalitet, privredno poslovanje, zakonodavni okvir, kompjuterska forenzika, dokazi*

Abstract - Economic crimes have become an extraordinarily negative social pathology committed through business and trade communications which makes it possible for individuals and groups in a society to violate a law and benefit from it. Besides the legitimate frames and solutions in detecting these crimes, a decisive role has been assigned to the cyber and computer forensics. Computer and cyber forensics is a

process of gathering, analyzing and reporting on digital data in a way adequate for legitimate processing. It might be used in detecting and preventing crime in the cases where an evidence has been saved in the digital form. Like other forms in legal forensic proceedings, the proceedings in computer forensics require a very good knowledge of computer hardware, software as well as sophisticated techniques in preventing distortion and destruction of all the evidence. It predominantly deals with the correction and analysis of latent data and evidence that might exist in different forms, starting from DNA analysis of blood samples to the hard disc files. Due to the fact that it is a new discipline, both standardization and consistency in courts have not yet been represented. Besides the quoted definition, it seems worthwhile saying that this is a discipline encompassing the elements of law and computer science in order to obtain and analyze data from the computer systems, networks, wireless communication and appliances for data storage in a form acceptable for a legal court procedure.

Key words: *economic crimes, business and trade, legal frame, computer forensics, evidence*

I. UVOD

Danas je nezamislivo pričati o privredi ili poslovanjima koji nijesu u potpunosti bazirani na računarskom sistemu. Za to je odgovorna informatička revolucija. Rapidan razvoj tehnologije i tehnoloških rješenja nesporno je doveo do određenih posledica negativnog karaktera. Glavna problematika u ovom dobu jeste pojava kompjuterskog kriminaliteta¹ koji se intezivno prepliće sa privrednim kriminalitetom. Ova pojava se razvija veoma brzo sa, veoma često, katastrofalnim posledicama po privredne subjekte. Danas je moguće iz parka u našem komšiluku, primjenom mobilnog uređaja, izvršiti pljačku neke finansijske ustanove na drugom kontinentu za veoma mali vremenski period. Ako

¹Sajber (Cyber) kriminalitet – Kriminalna aktivnost izvršena pomoću računara ili Interneta – Oxford Dictionary

bismo uz ovo naveli da ovu radnju može izvršiti maloljetnik, dobar poznavalac računarskih sistema, postaje jasno koliko je ova pojava opasna.

U ovom radu razmotrićemo međunarodno-pravne okvire, konvencije i direktive Evropske Unije za borbu protiv kompjuterskog kriminaliteta, kao i par procesuiranih primjera iz okruženja koji su zaokupili veliku pažnju javnosti.

II. PRAVNI OKVIRI

Ne može se govoriti o tehnikama otkrivanja bilo kog kriminaliteta ukoliko za to ne postoji jaka, kako domaća tako i međunarodna, pravna osnova i pravni okvir. Domaći zakonodavni okvir je generalno ograničen. Iz tih razloga, problemi u ovoj oblasti su morali da budu riješeni na međunarodnom nivou kroz međunarodni pravni okvir, koji je prouzrokovao usvajanje adekvatnih međunarodno pravnih instrumenata. Prvi međunarodni sporazum koji reguliše materijalno pravni, procesno pravni, organizacioni i međunarodni okvir krivičnih djela koja su izvršena putem računara, interneta i drugih računarskih mreža jeste Konvencija o Sajber kriminalu Savjeta Evrope (CETS br. 185).² Ova Konvencija trenutno predstavlja jedini međunarodno pravno priznat i kontinentalno rašireni pravni instrument u oblasti visokotehnološkog kriminaliteta.

Drugi pravni okvir je Direktiva 2013/40/EU³. Donijeta je od strane Evropskog parlamenta 20. avgusta 2013. godine i odnosi se na napade usmjerene protiv informacionih sistema. Cilj Direktive je da približi krivičnim zakonodavstvima zemalja članica Unije oblast napada protiv informacionih sistema uspostavljanjem minimalnih pravila koji se odnose na definiciju krivičnih djela i odgovarajućih krivično pravnih sankcija.

III. PRIMJER – OTKRIVANJE I GONJENJE

Zloupotreba brojeva bankovnih platnih kartica, kako na Internetu tako i na ATM/POS terminalima,

najzastupljenija je u Crnoj Gori. Izvršioci ovih djela imaju direktnu novčanu korist koju stiču podizanjem novca na ATM terminalima, ili materijalnu korist kupovinom posredstvom POS terminala.

Trenutno, najaktuelniji način prikupljanja brojeva bankovnih kartica obavlja se uz pomoć metode Fišing (*Fishing – prim.prev.pecanje*), a sastoji se u tome da se od lakovjernih korisnika Interneta prikupe brojevi bankovnih kartica. Kriminalac najprije kreira kompletan lažni web sajt sa elektronskom prodavnicom gdje će nuditi svoje proizvode, tražeći da se u odgovarajuća polja za unos podataka unesu podaci o bankovnom računu kako bi se transakcija izvršila, a jedan od tih podataka je i broj platne bankovne kartice. Kada kriminalac dobije tražene podatke, može izvršiti neograničen broj zloupotreba, tačnije, sve zloupotrebe koje donosi elektronsko poslovanje i elektronska trgovina.

Drugi način prikupljanja digitalnog zapisa bankovnih kartica vrši se direktno na ATM bankomatima i POS terminalima, gdje kriminalac fizički postavlja elektronski uređaj *Skimmer* na mjestu gdje se ubacuje bankovna kartica, a sa ciljem da očita digitalni zapis sa magnetne trake na kartici i istovremeno ga memoriše. Kasnije, prikupljeni memorisani podaci se pomoću posebnog uređaja narezuju na bijelu plastiku, odnosno na blanko karticu. Važno je pomenuti da su kriminalci iz okruženja izuzetno aktivni u Sjedinjenim Američkim Državama, a u skladu sa zvaničnim podacima FBI (Američkog federalnog istraživačkog biroa)⁴.

Na primjer, U Majamiju – Florida, četiri Rumunska državljana su optužena i proglašena krivim što su proizveli i postavili Skimming uređaje širom Floride. U trajanju od jedne godine, podizali su sa bankomata \$1000 ili više dnevno. Uhapšeni su 17. aprila 2009. godine. Dvojici je ponuđena kaucija od \$250.000 a drugoj dvojici je određen pritvor do okončanja postupka. Zapriječena kazna je do 15 godina zatvora.

Dalje, u Čikagu je 17. Juna 2010. godine uhapšen Srpski državljani Ljubiša Sokolović (59 godina) koji je pokušao da kupi Skimming uređaj. Uhapsili su ga

² CETS No. 185 - Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Budapest, 23.XI.2001.

³ DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

⁴ FBI – Federal Bureau of Investigation – www.fbi.gov

ICE⁵, kao i pripadnici IRS⁶. Protiv njega je podignuta optužnica za pokušaj prevare i prijetu mu kazna od 10 godina zatvora. Važno je napomenuti da kriminalac Sokolović nikada nije uspio da kupi uređaj već da je samo pregovarao sa nekim čovjekom o kupovini. Kupio je par djelova, ali čovjek sa kojim je pregovarao je bio u stvari FBI specijalni agent.

U New York-u je, na 21 mjesec zatvora, osuđen bugarski državljani zbog učešća u timu koji je koristio sofisticirane skimming uređaje na ATM bankomatima. Time je uspio da ukrade oko \$1,8 miliona sa oko 1400 korisničkih bankovnih računa u New York okruženju. Optužen je da je u periodu od 2007. do 2009. godine postavljao Skimming uređaje na ATM bankomatima, kao i male kamere koje su bilježile PIN kodove koji bi korisnici bankomata unosili. Uz zatvorsku kaznu, određeno mu je vraćanje \$1,838,001. Ovaj kriminalac je još u bjekstvu.

Kako se zaštititi od ovakvih, vrlo opasnih, pojava? U većini pomenutih slučajeva, banke su bile te koje su u znatnoj mjeri pomogle da se ovakve stvari otkriju i procesuiraju. Znamo da su ATM bankomati u vlasništvu banaka i da su banke te koje imaju uvid u njihov rad. One svakodnevno unapređuju bezbjednosne sisteme, posebno one koje se odnose na ATM bankomate i na elektronsko bankarstvo. Sljedeći primjer iz Crne Gore će nam dati jasnu sliku o tome kako su banke inkorporirane u cijeli proces, od prikupljanja dokaza do konačne sudske odluke. Radi se o jednom licu koje je sa lažnim karticama podigao 11.000€ sa četiri bankomata u Crnoj Gori.

Naime, crnogorska policija je podnijela krivičnu prijavu protiv M.Ž. (27), iz Podgorice jer se sumnja da je falsifikovao i zloupotrebio kartice i kartice za bezgotovinsko plaćanje na štetu Prve Banke Crne Gore i NLB Montenegro banke filijala u Baru.⁷ M.Ž. je uhapšen 28. oktobra 2011. godine u Baru ispred ATM-bankomata Prve banke Crne Gore, a nakon nekoliko prethodno uspješno izvršenih transakcija podizanja novca. Pregledom su u njegovom novčaniku pronađene četiri lažne kartice, koji je odgovarao opisu jednog od dva nepoznata lica za

kojim je prethodno bila raspisana lokalna potjernica jer su neovlašćeno pribavili lažne kartice i iste upotrebljavali kao prave podižući novac na bankomatima. Prva Banka Crne Gore i NLB Montenegro banka su 14. oktobra 2011. godine Upravi policije - Područnoj jedinici u Baru podnijele krivičnu prijavu protiv NN lica koja su počev od 21. septembra 2011 godine do 13. oktobra 2011 god korišćenjem falsifikovanih platnih kartica zadužili terminale ovih banaka i time uspjeli da isplatom gotovine ostvare protivpravnu imovinsku korist u iznosu od 10.000 €, kod Prve Banke CG i 1.000 € kod NLB Montenegro Banke. Time je načinjena i materijalna šteta samim izdavaocima ovih kartica, bankama koje najvjerovatnije potiču sa prostora Velike Britanije. Osmatranjem četiri bankomata i vršenjem zasjeda u kritično vrijeme, uhapšen je M.Ž. Postoje osnovi sumnje da je imenovani na području Crne Gore i u drugim primorskim opštinama vršio ova krivična djela, u društvu sa još za sada neidentifikovanim licem, kojom prilikom su uspjeli podići veće novčane iznose.

Navedeni primjeri su samo jedan mali dio mogućnosti zloupotreba računarskih sistema koji su direktno povezani sa privrednim i računarskim kriminalitetom. Danas smo svjedoci svakodnevnih „hakerskih napada“ koji imaju različite motive i razloge sa uglavnom katastrofalnim poslasticama. Jedan od aktuelnih primjera ovih dana svakako jeste Američki hakerski napad na 80% kineskih sajtova. Rezultat je porazan, samim tim što je u cijeli slučaj morao da se uključi američki državni sekretar Džon Keri koji je saopštio da će pregovori između Amerike i Kine u oblasti kibernetičke bezbjednosti biti izuzetno teški. Saradnja Kine i SAD izgubila je na intenzitetu ranije ove godine, pošto je američko ministarstvo pravde optužilo pet pripadnika kineske vojske za „hakovanje“ američkih kompanija radi krađe komercijalnih tajni. Kineski zvaničnici uzvratili su protivoptužbama na račun američke vlade za hakovanje, nakon što je saradnik Agencije za nacionalnu bezbednost (NSA) Edvard Snouden izneo tvrdnje da su SAD upadale u mreže i servere u Kini i Hongkongu. Načelnik državnog biroa za internet Lu Vej je danas branio kinesku odluku o zabrani stranih internet servisa, kao što je „Fejsbuk“, rekavši da je to učinjeno zbog zaštite nacionalnih interesa. Prema njegovim riječima, Kina je uvek vrlo gostoljubiva ali

⁵ ICE - Department of Homeland Security's Immigration and Customs Enforcement Bureau

⁶ IRS - Criminal Investigations Division of the Internal Revenue Service

⁷ www.vijesti.me – 1.11.2011.

može da bira “koga će pustiti u kuću”. Iz ovoga se može zaključiti da je kompjuterski kriminalitet itekako povezan sa privrednim kriminalitetom i da tehnike za detekciju i prevenciju važe za oba tipa kriminaliteta. Ako se ne pronađu prave tehnike i metode u borbi protiv kompjuterskog kriminaliteta, privreda postaje izuzetno osjetljiva na neprijateljske napade koji se stalno dešavaju, a da, na žalost, vlasnici privrednih subjekata često poslednji za to saznaju.

Sljedeći primjer pokazuje kakve je posledice na privredu, tačnije na jednu od najvećih američkih banaka, ostavio hakerski napad u kome je pokradeno 83 miliona klijenata. U tom napadu kontakti, elektronske adrese, brojevi telefona i adrese vlasnika računa su dospjeli su u ruke hakera, dok su lozinke, brojevi za socijalno osiguranje i datumi rođenja ipak sačuvani. Napadnuti su računi 76 miliona malih domaćinstava i 7 miliona malih preduzeća. Ovaj napad se smatra najvećim hakerskim napadom u istoriji. Napad je izvršen u junu, ali je otkriven u julu 2014. godine. Čitav slučaj, istorijskih razmera, objelodanjen je tek u avgustu. Iz banke tvrde da finansijske informacije klijenata nisu kompromitovane, što znači da nije bilo krađe lozinki, datuma rođenja i brojeva za socijalno osiguranje. Od otkrivanja hakerskog napada, kompanija nije registrovala nikakvene uobičajene prevare klijenata povezane sa ovim. Ukoliko odmah upozore banku na neovlašćene transakcije na njihovim računima, klijenti se neće smatrati odgovornim za iste. Najveća banka u SAD po obimu kreditnog novca i novčanih aktiva, sarađuje sada sa FBI-om i američkom tajnom službom kako bi se razriješio ovaj napad.

IV. ZAKLJUČAK

Borba između izvršioca krivičnih djela privrednog i kompjuterskog kriminaliteta i institucija za borbu protiv istih je u poslednje vrijeme dobila vrlo izražene primjese tehnološke revolucije. Toliko je važno ozbiljno shvatiti pravu primjenu računara da je nezamislivo bez toga ući u ovu borbu. Kriminalci svakodnevno rade na razvoju sofisticirane opreme i metoda za izvršenje ovih krivičnih djela, a da im fizičke granice između država apsolutno ne predstavljaju nikakvu smetnju. U skladu sa tim, institucije moraju da imaju veoma intezivne i agresivne metode u borbi protiv ove pojave.

U suštini, tehnike za otkrivanje privrednog kriminaliteta su bazirane na primjeni tehnologije i da se i kod nas polako ali sigurno formiraju svi pravni okviri i mehanizmi koji će goniocima protiv ovih tipova kriminalaca dati vjetar u leđa. Standardizacije su u toku, a pored domaćih pravnih okvira primjenjuju se i međunarodni. Navedeni primjeri iz prakse su zaista zastrašujući, ali je ipak veliko ohrabrenje kako su se institucije i privredni subjekti nosili sa tim i kako su ih riješili.

LITERATURA

- [1] K. D. Mitnick, W. L. Simon, “The Art of Intrusion: The Real Stories Behind the Exploits of Hackers”, Intruders and Deceivers, Wiley Publishing, December 27, 2005.
- [2] J. Luttgens, M. Pepe, K. Mandia, “Incident Response & Computer Forensics”, Third Edition, Mc Graw Hill, August 8, 2014
- [3] M. T. Britz, “Computer Forensics and Cyber Crime: An Introduction (3rd Edition)”, Prentice Hall; 3 edition (May 26, 2013).
- [4] S. Levy, “Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition”, O'Reilly Media; 1 edition (May 30, 2010).
- [5] C. Easttom, J. Taylor, “Computer Crime, Investigation, and the Law”, Cengage Learning PTR; 1 edition (April 9, 2010).
- [6] B. Stamenković, A. Balota, “Visokotehnološki kriminal – praktični vodič kroz savremeno krivično pravo i primjere iz prakse”, OEBS misija u Crnoj Gori (Mart, 2014).

Dijeljenje i integracija informacija u kazneno-popravnim institucijama Republike Srpske

Sharing and information integration in correctional institution in Republika Srpska

Bogdan Mirković, Slobomir P Univerzitet, Nenad Mirkonj, Ministarstvo pravde Republike Srpske

Sažetak— Razvoj informaciono-komunikacionih tehnologija, prednosti koje pružaju brzina i snaga računarske tehnike, baze podataka, programske aplikacije, telekomunikacioni sistemi i njihova primjena u svim oblastima života i djelovanja omogućavaju naučnim radnicima iz oblasti kriminologije i penologije, upravnim i nadzornim organima čiji je djelokrug rada u ovim oblastima, širok spektar mogućnosti za objedinjavanje i analiziranje svih relevantnih informacija u slučajevima da su informacije integrisane na metodološki, kao i prihvaćen i razumljiv način na svim nivoima. U ovom radu predstavljena je primjena hibridne arhitekture informacionog sistema kazneno popravnih institucija Republike Srpske razvijena od strane autora ovog rada i implementirana u svim organizacionim dijelovima sistema. Razvoj informacionog sistema kazneno popravnih institucija Republike Srpske predstavlja stepenik u okviru rada na profesionalizaciji i harmonizaciji cjelokupnog sistema u okviru Projekta reforme zatvora kontrolisanom od strane Ministarstva pravde RS. Predstavljeno rješenje definiše simbiozu programskog rješenja sa hibridnom arhitekturom distribuiranom na cijelom području Republike Srpske i implementiranu u svim organizacionim jedinicama sistema za izvršenje krivičnih sankcija, kao i drugim institucijama koje su povezane sa ovim sistemom.

Ključne riječi – dijeljenje informacija, integracija informacija, informacioni sistem, hibridna arhitektura

Abstract – The development of information and communication technologies, the advantages provided by speed and power of computer technology, databases, software applications, telecommunications systems and their applications in all areas of life and actions allow researches in the fields of criminology and penology, management and supervisor bodies whose scope of work is in these areas a wide range of options to integrate and analyze all relevant information in cases that information are integrated and the methodology, as well as user-friendly manner and adopted at all levels. In this paper is presented the application of hybrid architecture of the information system of correctional institutions in Republika Srpska developed by the authors of this paper and implemented in all organizational units of the system. Development information system of correctional institutions in Republika Srpska is a step in the framework of the professionalization and harmonization of correctional institutions within the prison reform project controlled by the RS Ministry of Justice.

Presented solution defines symbiosis software solutions with hybrid architecture distributed throughout the Republika Srpska and implemented in all organizational units of the system for enforcement of criminal sanctions, and other institutions that are associated with this system.

Keywords – information sharing, information integration, information system, hybrid architecture

I. UVOD

Svaki organizacioni sistem, pa tako i sistem za izvršavanje krivičnih sankcija zahtijeva određene informacije na osnovu kojih se vrši upravljanje, odnosno rukovođenje. Rastom organizacije i rukovodnog nivoa, povećava se količina podataka na osnovu kojih se vrši rukovođenje, pa u jednom trenutku individualne mogućnosti čovjeka (iskustvo, intuicija i logička analiza) postaju nedovoljne za efikasno rukovođenje, a samim tim i ograničavajući činilac njegovog unapređenja. Uvođenjem informacionih tehnologija u funkcije upravljanja sve više do izražaja dolazi kvantitativna analiza zasnovana na automatizaciji informacionih procesa, a uloga čovjeka se pomjera u pravcu kreativnih funkcija [1].

Arhitektura informacionog sistema zasniva se, prije svega, na primjeni određene infrastrukture informacionih tehnologija kako bi se ostvarili prethodno definisani i usvojeni poslovni ciljevi organizacije. U zavisnosti od ciljeva i načina poslovanja organizacije, moguće su različite arhitekture informacionih sistema. Arhitektura informacionog sistema predstavlja mapu na najvišem nivou ili plan raspoređivanja informacija u organizaciji, uključujući i razmještaj računarske i telekomunikacione opreme. Kreiranje poslovne arhitekture je cikličan proces koji se opisuje u planovima organizacije, vizije organizacije, ciljeva i problema, kao i informacija koje su potrebne za podršku poslovanju. Slično poslovnoj arhitekturi, i arhitektura informacionog sistema podložna je promjenama, uslovljena prije svega, razvojem novih informacionih tehnologija.

Za proces definisanja arhitekture informacionog sistema, potrebno je imati u vidu specifičnosti svake od poslovnih organizacija u kojima se određeni oblici informacionih sistema uvode. Za uvođenje informacionih sistema u poslovne procese

organizacije potrebno je razlikovati sljedeće komponente infrastrukture:

- materijalno-tehnička komponenta (hardware: uređaji, sredstva namijenjena obradi podataka odnosno informacija)
- nematerijalna komponenta (software: ljudsko znanje ugrađeno u računare, uređaje i opremu koja je predmet obrade ili određuje način obrade podataka u sistemu)
- ljudska komponenta (lifeware: svi ljudi u bilo kojoj funkciji i s bilo kakvom namjenom koji učestvuju u radu sistema i koriste rezultate obrade podataka odnosno informacija)
- organizaciona komponenta (ogrware: sve mjere, metode i propisi kojima se koordinira rad prethodno navedene četiri komponenta kako bi one činile djelotvornu cjelinu)
- prenosna (mrežna) komponenta (netware: sredstva i veze za prenos podataka na daljinu, odnosno telekomunikaciona sredstva i veze u sistemu)
- sredstva obezbjeđenja i objekti u kojima se vrši implementacija informacionog sistema.[2]

Sve navedene komponente aktivno i trajno djeluju jedna na drugu kao uzrok i istovremeno kao posljedica, što se zove interakcijom ili međudjelovanjem.

Potreba za automatizacijom poslovnih procesa u sistemu za izvršavanje krivičnih sankcija uočene su još osamdesetih godina dvadesetog vijeka kada je počela masovnija primjena računarske tehnologije u svim segmentima života. Sistemi razvijeni u sistemu za izvršenje krivičnih sankcija na prostoru SFRJ su zastarjeli i nisu više u upotrebi. U više navrata su dograđivanja i razvijana programska rješenja za potrebe platformi računara tipa Honeywell i HP, u kom obliku danas više ne egzistiraju. U današnje vrijeme brzog razvoja personalnih računara i masovnog opremanja svih organa i kazneno popravni institucija istim, primjena jedinstvenog informacionog sistema ima značajne prednosti koje se ogledaju u stalnom praćenju i ažuriranju relevantnih podataka posmatrane ustanove (institucije), kao i svih ustanova (institucija) Republike Srpske i Ministarstva pravde, povećavaju tačnost podataka, iznalaženju varijantnih rješenja za realizaciju podataka, smanjenju potrebnog ljudstva, značajnom ubrzanju proračuna, a time i procesa odlučivanja i rukovođenja u pojedinim ustanovama (institucijama) kao i sistema za izvršavanje krivičnih sankcija u cjelosti.

Realizacija informacionog sistema u sistemu za izvršavanje krivičnih sankcija, kao i razvoj potrebne arhitekture koju informacioni sistem podržava, predstavlja izazov sa stanovišta upotrebe relativno jeftinih informacionih tehnologija pokrivajući sve elemente sistema u domenu vođenja evidencija o osuđenim, prekršajno kažnjenim i pritvorenim licima, kao i vođenje evidencija o licima zaposlenim u sistemu. Simbioza koju je potrebno napraviti u finansijski teškoj situaciji zahtijeva poseban pristup u razvoju sistema u cjelini ne narušavajući osnovne karakteristike

sistema za izvršavanje krivičnih sankcija u pogledu dostupnosti podataka.

II. ARHITEKTURA INFORMACIONOG SISTEMA

Postoje različiti oblici arhitekture informacionih sistema:

- veliki ili mainframe računar sa mrežom inteligentnih terminala ili PC računara,
- PC arhitektura, samostalno ili u mreži i to PC-Lan ili bežični LAN,
- distribuirana arhitektura gdje se obrada dijeli na više računara korišćenjem mreže. Razvojem interneta ona postaje dominantna u većini organizacija. Varijanta ovog tipa je i kooperativna arhitektura (engl. cooperative processing) koja se sastoji od geografski razdvojenih računara koji zajednički rade na izvršavanju specifičnih zadataka. Takođe, podvarijanta ove arhitekture je client/server arhitektura gdje su zadaci obrade i korišćenja razdvojeni od servera i klijenta.
- nasleđeni sistemi (engl. legacy systems) su stariji informacioni sistemi koji postoje za određene namjene (obračun plata, magacinsko poslovanje...),
- arhitektura svako sa svakim (engl. peer-to-peer ili P2P) je podvarijanta mrežne arhitekture koja se ne ostvaruje preko centralnog servera. Njena prednost je u mogućnosti širenja i rad u virtuelnom okruženju.

Prema definiciji Instituta za softverski inženjering [3], softverska arhitektura predstavlja: strukturu komponenti programa/sistema, njenih unutrašnjih relacija i principa i direktiva koje određuju dizajn i evoluciju tokom vremena. OSCI (Object Oriented Client/Server Internet) aplikacije su veoma složene aplikacije tako da njihova arhitektura i inženjering zahtijevaju analizu mnogobrojnih faktora, kao što su: postojeća arhitektura podataka, zahtjevi (po pitanju funkcionalnosti, operativnosti, organizacije, zaštite podataka), postojeće aplikacije koje moraju biti povezane sa novom aplikacijom, infrastruktura i standardi [3].

Definisanje arhitekture informacionog sistema [4] kazneno popravni institucija Republike Srpske je realizovano u nekoliko koraka:

- Razvijen je objektni model tako da je dobijena predstava apstraktnih komponenti aplikacija i apstraktnih poruka za izmjenu objekata. Veličina objekta (mali objekat koji predstavlja programsku rutinu i veliki (poslovni) objekat koji predstavlja programske entitete (programske aplikacije)) su bitni atributi za definisanje softverske arhitekture. U ovom koraku su korištene objektno orjentisane tehnike analize i dizajna.
- Dijeljenje, koncentracija i grupisanje objekata tako da su dobijena tri logička sloja: sloj prezentacije, sloj logike aplikacije i sloj podataka. Dijeljenjem u ova tri sloja omogućena je veća fleksibilnost softvera i njegovo korištenje.

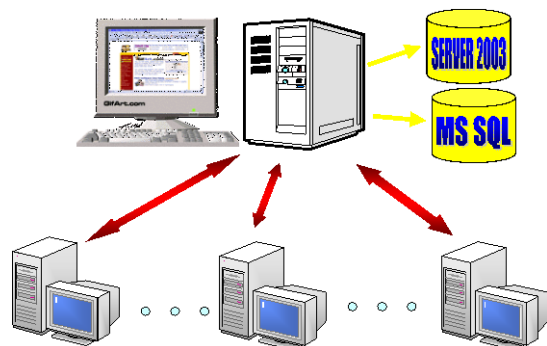
- Podijeljena je logička arhitektura na klijent i server dio čime su definisani fizički slojevi aplikacija.
- Izvršena je procjena i biranje odgovarajuće infrastrukture potrebne za podršku aplikacijama. Ovaj korak je podrazumijevao razmatranje velikog broja pitanja, kao što su: protokoli za razmjenu, mrežni servisi itd.
- Analizirane performanse i alocirane glavne razmjene podataka. Važan faktor je i sigurnost, administrativna podrška, dostupnost i drugo. Glavno pitanje je bilo definisanje najboljih mjesta za alociranje podataka (kako u okviru pojedine ustanova (institucije) tako i sa stanovišta cjelokupnog sistema), procesa i korisničkog interfejsa.

Pored navedenih koraka u definisanju arhitekture informacionog sistema, bitno je i vršiti definisanje mogućnosti organizacije sa stanovišta finansijskih pokazatelja poslovanja što je u ovom slučaju predstavljalo ograničavajući faktor.

III. IMPLEMENTACIJA HIBRIDNE ARHITEKTURE

Informacioni sistem koji je razvijen za sistem izvršavanja krivičnih sankcija Republike Srpske namijenjen je svim organima u pojedinim ustanovama, kao i zaposlenima u Ministarstvu pravde Republike Srpske čiji djelokrug djelovanja i rada podrazumijeva rad sa osuđenim, prekršajno kažnjenim, pritvorenim licima, ali i licima koji su zaposleni u navedenom sistemu.

Različit obim, kao i struktura i opis poslova koje je potrebno obaviti, uslovljavaju i različit pristup. U sistemu kao što je ovaj sistem, poslovi su podijeljeni po funkcionalnim cjelinama pa im je tako i u slučaju identifikacije i rješavanja problema i pristupano. Pojedine informacije su potrebne odmah nakon prijema u određenu ustanovu, a pojedine nisu neophodne odmah nakon prijema osobe u sistem. Zbog ovakve situacije u rješavanju određenih problema, bilo je potrebno odmah prići sa tog stanovišta i rješavati iste.



Slika 1: Organizacija sistema unutar ustanove

Zbog haotičnog i raznolikog stanja u načinu rješavanja potreba zaposlenih za primjenom informacionih tehnologija za obavljanje poslova vezanih za evidentiranje i izvještavanje o osuđenim, prekršajno kažnjenim i pritvorenim licima, kao i podataka o licima zaposlenim u sistemu za izvršavanje

krivičnih sankcija Republike Srpske, razvijen je jedinstveni informacioni sistem za praćenje promjena koje se dešavaju u ustanovama i Ministarstvu pravde RS kao hijerarhijski višoj instanci. Ovakav informacioni sistem je sveobuhvatan i jedinstven za sve organizacione dijelove kako cjelokupnog sistema, tako i za sve segmente pojedinih organizacionih jedinica.

Finansijske mogućnosti Ministarstva pravde RS i ustanova koje se nalaze u njenom sastavu uslovilo je da se fizička implementacija uradi u sistemu za upravljanje bazom podataka MS SQL Server [5] i programskom jeziku VBA [6].

Cjelokupan informacioni sistem je realizovan u četiri aplikacije: Administracija, Prijavnica, Zaposleni, Ustanova. Aplikacije su instalirane na centralnom računaru koji se nalazi u svakoj od kazneno-popravnih institucija kao i u Ministarstvu pravde RS. Arhitektura sistema prikazan je na slici 1.

Aplikacije su izgrađene preko niza formi, složenih objekata, preko kojih je omogućen rad sa bazom (editovanje, prikazivanje,...) čime je korišćenje aplikacija vrlo lako.

Čuvanje podataka je omogućeno redovnim backup-om podataka i njihovim smještanjem na magnetnim i optičkim medijima. Zaštita podataka je realizovana kombinacijom fizičke zaštite (pristupa centralnom računaru u ustanovi), kao i definisanjem prava pristupa na nivou korisnika:

- unos i pregled podataka na nivou ustanove,
- samo pregled podataka na nivou ustanove,
- rad sa šifarnicima na nivou Ministarstva pravde,
- pregled i izvještavanje na nivou Ministarstva pravde.

U zavisnosti od potrebe korisnika u ustanovi za ažuriranjem i pregledom određenih podataka, a u skladu sa opisom poslova koje zaposleni obavlja u ustanovi, mogu se definisati prava pristupa za svakog pojedinog korisnika. U ustanovi, pored ovoga, postoje i poslovi koje podrazumijevaju pristup podacima određene kategorije tako da su definisana prava pristupa:

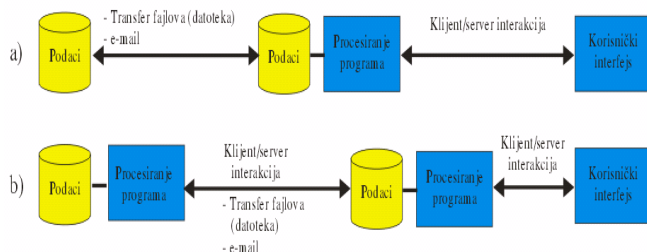
- administrator (mogućnost ažuriranja i pregleda svih podataka),
- upravnik (mogućnost pregleda svih podataka),
- zdravstvena služba (ažuriranje podataka vezanih za zdravstvenu službu i pregled određenog dijela podataka o osuđenim licima),
- prijavnica (mogućnost ažuriranja podataka vezanih za rad Službe obezbjeđenja),
- prevaspitna služba (mogućnost pregleda svih podataka i ažuriranja podataka vezanih za rad Prevaspitne službe),
- pravna služba (mogućnost ažuriranja i pregleda podataka o zaposlenim licima),
- matična služba (mogućnost ažuriranja i pregleda svih podataka vezanih za rad matične službe i referenata za izvršenje krivičnih sankcija),
- zaposleni (mogućnost ažuriranja i pregleda podataka o zaposlenim licima u ustanovi).

Na nivou Ministarstva pravde Republike Srpske, licima kojima je dozvoljen pristup podacima, omogućen je pregled svih podataka koji se odnose na ustanove, ali bez mogućnosti ažuriranja podataka. Ažuriranje podataka omogućeno je samo

u onom segmentu koji se odnosi na ažuriranje podataka koji se tiču Ministarstva pravde (podaci o zaposlenim i podaci o šifarnicima koji su jedinstveni za cijeli sistem).

Stanje komunikacione opreme u ustanovama (institucijama) sistema za izvršavanje krivičnih sankcija u Republici Srpskoj ogleda se u nepostojanju dovoljnog broja direktnih telefonskih linija, kao i nemogućnosti povezivanja na globalnu svjetsku mrežu (internet) sa dovoljnom brzinom protoka podataka. U skladu sa stanjem komunikacione opreme, odlučeno je da se razmjena podataka između ustanova i organa Ministarstva pravde Republike Srpske omogući putem elektronske pošte (u obliku dokumenata) preko telefonske mreže, kao i preko magnetnih i optičkih medija. Dodatno pitanje koje je trebalo riješiti je mogućnost razmjene podataka sa drugim institucijama koje u obasti svoga djelovanja rade sa podacima dobijenim iz ustanova (institucija) Ministarstva pravde Republike Srpske. Ovakva situacija je prouzrokovala da se prilikom izbora arhitekture informacionog sistema donese odluka da se primijeni hibridna (mješovita) arhitektura sa odlikama troslojne klijent/server arhitekture kao zasebne arhitekture u svakoj organizacionoj jedinici sistema za izvršavanje krivičnih sankcija. Troslojnu klijent/server arhitekturu odlikuju skalabilnost, tehnološka fleksibilnost, dugoročna isplativost, bolji odgovor sistema na poslovne potrebe, poboljšan korisnički interfejs kao i veoma bitna redukcija rizika.

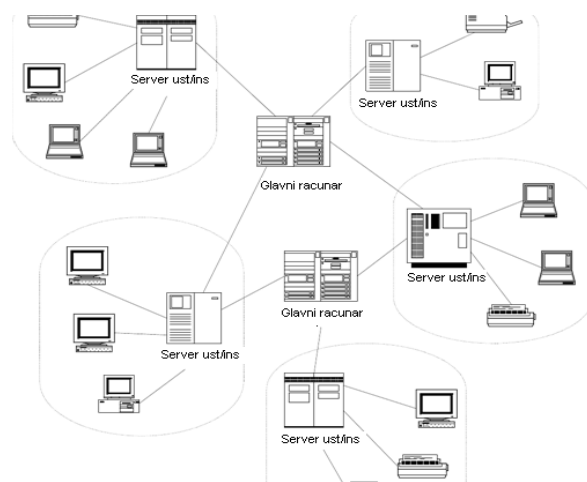
Hibridna arhitektura nastaje u slučajevima spajanja i kombinovanja različitih klasa arhitektura. Danas se pod pojmom hibridne arhitekture smatraju sistemi nastali kombinovanjem različitih klasa konvencionalnih sistema sa pojedinim tehnikama [7]. U slučaju informacionog sistema kazneno popravnih institucija Republike Srpske, klijent/server arhitektura je primijenjena izmenu drugog i trećeg sloja, dok se sa prvog i drugog sloja obavlja razmjena fajlova. Ovo se koristi kada u okviru jednog LAN-a PC računari pristupaju SQL serveru koji se periodično dopunjava podacima sa glavnog servera baze ili se dopunjavanje vrši i na glavni server baze (slika 2a). Kada se vrši popunjavanje glavnog servera baze podataka u određenim vremenskim razmacima, kada se popunjavanje podataka vrši iz glavnog servera baze podataka ili kombinacija ova dva popunjavanja baza podataka onda se primjenjuje klijent/server interakcija između prvog i drugog sloja, ali i između drugog i trećeg sloja troslojne arhitekture informacionog sistema (slika 2b).



Slika 2: Hibridna arhitektura informacionog sistema

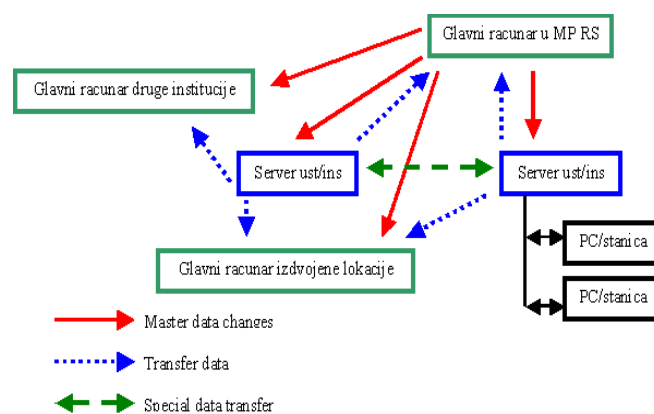
Hibridna arhitektura nastaje u složenim poslovnim sistemima gdje povezuje dva ili više zvjezdastih mreža u jedan

sistem.[2] U takvim sistemima postoje jedan ili više glavnih računara, a računari koji se mogu dodavati u sistem mogu bilo na bilo kom mjestu raspoređeni (slika 3).



Slika 3: Shematski prikaz hibridne arhitekture

Razmjena podataka i komunikacija između pojedinih organizacionih jedinica sistema je omogućena preko globalne svjetske mreže (internet) korištenjem servisa elektronske pošte instaliranim na pojedinim računarima unutar svake od organizacionih jedinica. Razmjena podataka od hijerarhijski nižih ka višim instancama se obavlja po propisanoj proceduri u određenim vremenskim intervalima. Po potrebi, razmjena podataka se može obaviti i u drugim terminima na osnovu zahtjeva. Elektronska razmjena podataka između institucija sistema se takođe mogu razmjenjivati putem ovog sistema pri čemu se moraju definisati dodatni uslovi korištenja ovog modula propisani internim pravilima sistema za izvršavanje krivičnih sankcija u Republici Srpskoj. Razmjena grafičkih elemenata (fotografije) obavlja se istovremeno u obliku posebnih formiranih cjelina. Shema razmjene podataka u sistemu za izvršavanje krivičnih sankcija u Republici Srpskoj je prikazana na slici 4.



Slika 4: Shema razmjene podataka

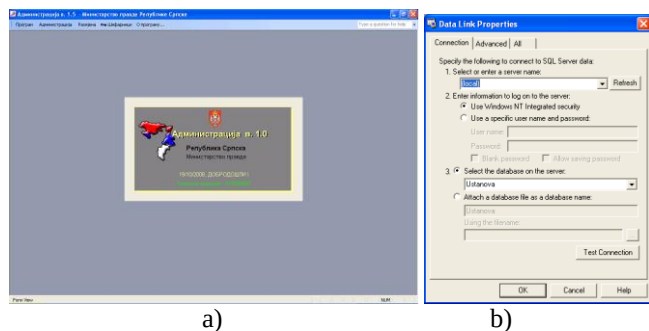
Razmjena podataka obavlja se na više različitih načina što je uslovljeno zakonskom regulativom i internim aktima. Odgovorna lica u pojedinim ustanovama (institucijama) podatke iz svoje ustanove (institucije) dostavljaju

elektronskim putem na glavni računar Ministarstva pravde Republike Srpske (Transfer data). Razmjena podataka između ustanova (institucija) koje predstavljaju instance na istom hierarhijskom nivou obavlja se na osnovu posebnog zahtjeva (Special data transfer). U hijerarhijski najvišoj instanci (Ministarstvo pravde Republike Srpske) vrši se ažuriranje posebnih šifarnika koji su jedinstveni na nivou cijele Republike Srpske, a čiji sadržaj proizilazi iz zakonske regulative ili potreba pojedinih ustanova (institucija). Razmjena takvih podataka se vrši u određenim vremenskim intervalima od strane Ministarstva pravde Republike Srpske prema svim drugim organizacionim jedinicama uključenim u sistem (Master data changes).

Definisanje podataka koji se razmjenjuju sa drugim institucijama koje ne predstavljaju organizacione jedinice sistema za izvršenje krivičnih sankcija (Ministarstvo unutrašnjih poslova, pravosuđe) vrši se po posebnoj proceduri u zavisnosti od potreba tih institucija i zakonske regulative osim u slučaju razmjene podataka iz Ministarstva pravde (Master data changes) koji se vrši redovno i u potpunosti kao i sa drugim organizacijama.

IV. APLIKATIVNA PODRŠKA RAZMJENI PODATAKA

Aplikacija Administracija (slika 5a) je namijenjena za rad prevashodno licima koja rade na održavanju informacionog sistema u ustanovama i Ministarstvu pravde RS i koja rade na razmjeni podataka unutar sistema za izdržavanje krivičnih sankcija kao i licima u drugim institucijama koja rade na prihvatanju i obradi dobijenih podataka. Aplikacija je realizovana preko menija (meni Program: Povezivanje, Izlaz, meni Administracija: Praćenje aktivnosti, Parametri, meni Razmjena: Šifarnici, Podaci – izdvajanje, Podaci – preuzimanje, Šifarnici, meni O programu). Izborom opcije Program - Povezivanje omogućava da se izvrši ažuriranje i uspostavljanje veze aplikacije sa bazom podataka preko standardne forme (slika 5b).

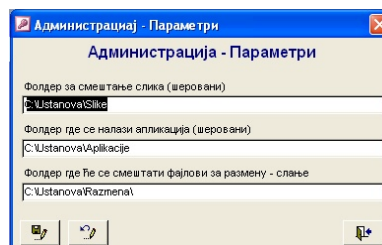


Slika 5: Izgled main forme aplikacije (a), forma uspostavljanja veze sa bazom podataka (b)

Izbor menija Administracija omogućava, preko svojih opcija, praćenje aktivnosti koje su vezane za rad sa informacionim sistemom kao i podešavanje parametara za rad ove, ali i ostalih aplikacija. Izgled forme nakon pokretanja opcije Parametri dat je na slici 6. Na ovoj formi se vrši ažuriranje podataka o direktorijumima za čuvanje fotografija osuđenih lica, direktorijuma na kome se nalaze izvršne

datoteke aplikacija, kao i direktorijum u kome se vrši čuvanje dokumenata za razmjenu podataka sa drugim institucijama sistema za izvršavanje krivičnih sankcija.

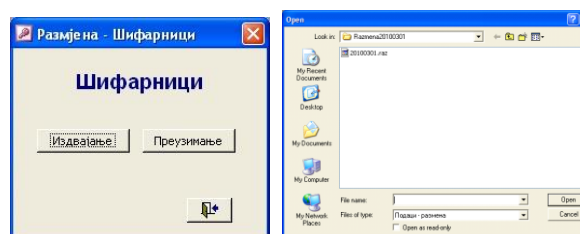
Izborom opcija iz menija Razmjena omogućava korisniku programa da izvrši operacije izdvajanja ili preuzimanja podataka ka ili od drugih korisnika koji se ne nalaze u istoj kazneno popravnoj ustanovi. Izdvajanje/preuzimanje podataka o šifarnicima koji se nalaze u okviru baze podataka vrši se pokretanjem opcije Šifarnici (slika 7a). Šifarnici se ažuriraju na centralnom računaru u Ministarstvu pravde RS a preuzimanje je omogućeno na centralnim računarima u ostalim organizacionim jedinicama Ministarstva pravde RS i kazneno popravnim ustanovama kao i drugim institucijama uključenim u sistem.

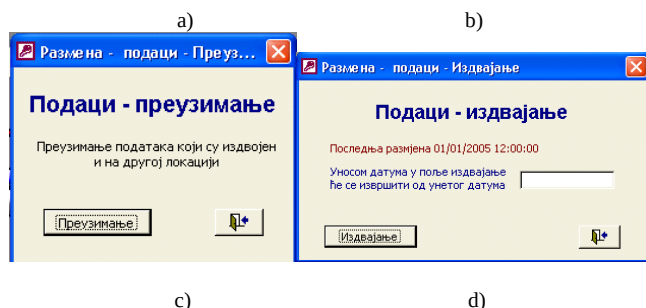


Slika 6: Izgled forme za definisanje osnovnih parametara

Izdvajanje/preuzimanje podataka iz baze podataka vrši pokretanjem opcija Podaci – izdvajanje i Podaci - preuzimanje. Izdvajanje je moguće izvršiti na centralnim računarima u kazneno popravnim ustanovama, dok je preuzimanje moguće izvršiti na računarima u Ministarstvu pravde RS. Datoteka sa izdvojenim podacima se automatski snima na direktorijum koji je određen definisanjem parametara sistema, dok se izbor podataka (dokumenta) koji su dostavljeni i koje treba ažurirati u bazu podataka sistema vrši uz pomoć standardne forme Windows operativnog sistema za izbor dokumenta (slika 7b) dok se preuzimanje datoteka vrši pomoću posebne forme (slika 7c).

Izdvajanje podataka je omogućeno izvršiti na dva načina u zavisnosti od potrebe. Prvi način je automatski gdje se za razmjenu/slanje podataka pripremaju (izdvajaju) podaci koji su ažurirani od trenutka poslednjeg izdvajanja podataka. Drugi način je da se odredi datum od kada se žele pripremiti podaci za slanje (razmjenu). U ovom slučaju za razmjenu (slanje) biće pripremljeni svi podaci koji su ažurirani od datuma koji je unesen (slika 7d).





Slika 7: Izgled formi za pripremu i preuzimanje dokumenata za razmjenu (a-izdvajanje/preuzimanje, b-forma za definisanje šifamika datoteke, c – pokretanje preuzimanja podataka, d- definisanje datuma za izdvajanje podataka

V. ZAKLJUČAK

Realizacijom hibridne (mješovite) arhitekture u razvoju informacionog sistema u kazneno popravnim institucijama Republike Srpske napravljen je korak prema implementaciji i daljem razvoju informacionih tehnologija u ovaj segment državne uprave. Simbiozom razvijenog softverskog rješenja i arhitekture, u skladu sa stanjem telekomunikacione opreme u kompletnom sistemu, dobijeno je rješenje koje omogućava krajnjim korisnicima da povećaju kvalitet svoga rada, skrate vrijeme vođenja evidencija u ustanovama i Ministarstvu

pravde Republike Srpske, ali i da dobiju kvalitetne izvještaje u što kraćem vremenskom roku. Time je postignuta jednoobraznost prikupljanja, evidentiranja i izvještavanja o stanju u sistemu za izvršenje krivičnih sankcija na teritoriji cijele Republike Srpske. Sličan sistem, uz prilagođavanje zakonskim regulativama vezanim za pojedine zemlje, može se koristiti i u Republici Crnoj Gori i Republici Srbiji. Prednosti ovakvog sistema ogledaju se u činjenici da su korištene relativno jeftine informacione tehnologije čije prilagođavanje postojećim sistemima ne predstavlja velike finansijske troškove.

LITERATURA

- [1] S. Vujović, "Informacioni sistemi u poslovanju i menadžmentu", Slobomir P Univerzitet, Slobomir, 2005.
- [2] K.Klastic, „Uvod u uredsko poslovanje“, Tehničko veleučilište u Zagrebu, Zagreb 2004,
- [3] www.sei.cmu.edu
- [4] A.Umar, „Application (Re)Engineering: Building Web-Based Application and Dealing with Legacies“, PrenticeHall 1997.
- [5] M. Gunderloy, J.Jordan, „SQL Server 2000“, Mikro knjiga, Beograd, 2001.
- [6] „Microsoft Office 2000“, Mikro knjiga; Beograd, 2001
- [7] W.Blackard, „Managing Peer-to-Peer Traffic in Network Environments“, TippingPoint, 2005.

Održavanje flote: Upotreba data mining-a i statistike u prevenciji zloupotreba

Fleet Maintenance: Use of Data Mining and Statistics in Fraud Prevention

Miloš Dobrojević, www.magma.rs, Belgrade, Serbia

Sažetak— U oblasti upravljanja i održavanja flote, pronevere, prevare ili krađe predstavljaju veliki problem, bilo da je reč o gorivu, mazivima, delovima ili zloupotrebi flotnih jedinica. ERP sistemi i integrisani sistemi za praćenje vozila, hardver i softver, su postali previše kompleksni i generišu ogromne količine podataka, dok je ekstrakcija i razumevanje dobijenih informacija prevazišla ljudske mogućnosti. Sa druge strane, ne postoji univerzalna procedura koja bi bila pouzdana, jednostavna, precizna i primenjiva u različitim kompanijama ili sastavima flote. Sve to otežava otkrivanje i prevenciju privrednog kriminala, i zahteva primenu inteligentnih metoda za ekstrakciju podataka i statističku analizu u softveru za menadžment i održavanje flote.

Ključne riječi – softver za upravljanje voznim parkom; data mining; data driven management; statistička analiza; prevencija kriminala

Abstract – In fleet management and maintenance domain, embezzlement, fraud or theft, whether involving fuel, lubricants, parts or units misuse, are significant problems. ERP systems and embedded vehicle tracking systems, hardware and software, which are getting very complex and in some cases over engineered, generate tremendous quantities of data, well beyond human ability to extract or understand given information. On the other hand, there is no universal procedure which would be reliable, simple and precise, yet applicable to every company and fleet structure. All this makes difficult to detect and prevent fleet related white-collar crime, and calls for use of intelligent data extraction and statistical analysis methods in fleet management and maintenance software.

Keywords – fleet management software; data mining; data driven management; statistical analysis; crime prevention

I. UVOD

Kompanije koje u svom sastavu poseduju flotu vozila se svakodnevno suočavaju sa nizom izazova vezanih za eksploataciju i održavanje voznog parka. To su kompleksni sistemi sa velikim brojem mašina i zaposlenih, razgranatom organizacionom strukturom i visokim operativnim troškovima.

U današnjoj globalnoj ekonomiji, jedan od imperativa je smanjenje operativnih troškova, što se između ostalog odnosi i na troškove posedovanja, održavanja i eksploatacije voznog parka. U praksi, to se može postići podizanjem efikasnosti

funkcionisanja sistema kao celine, a jedan od preduslova je efikasno prikupljanje podataka u realnom vremenu.

A. Preopterećenost informacijama

U protekloj deceniji, na tržištu se pojavio veliki broj softverskih i hardverskih rešenja za praćenje različitih segmenata poslovanja flote mašina. Međutim, takvi sistemi su u međuvremenu postali izuzetno složeni, sa velikim brojem parametara koji se prate, a količina podataka prikupljenih na dnevnoj osnovi je odavno prevazišla ljudsku sposobnost ekstrakcije i razumevanja dobijenih informacija. Kao primer, u tabeli 1 je dat raspon broja prikupljenih logova rada mašine dnevno i na mesečnom nivou za samo jedan parametar.

TABELA 1 - PRIKUPLJANJE INFORMACIJA
BROJ LOGOVA ZA 1 PARAMETAR NA OSNOVU BROJA MAŠINA U FLOTI
I IZABRANOG VREMENSKOG INTERVALA

Broj vozila	Interval [s]	Broj logova [10^6]	
		Dnevno ¹	Mesečno ¹
1	1	0.029	0.861
500		14.400	432.000
1000		28.800	864.000
1	30	0.001	0.029
500		0.480	14.400
1000		0.960	28.800
1	300	0.000	0.002
500		0.048	1.440
1000		0.096	2.880

B. Operativni problemi

Flota u čijem se sastavu nalaze mašine različitih proizvođača, tipova i namene, kao i razgranata organizaciona struktura kompanije sa organizacionim jedinicama na različitim geografskim lokacijama, često podrazumeva saradnju sa različitim dobavljačima goriva, maziva i rezervnih delova. Pri tome je velika verovatnoća da svaka od tih kompanija koristi različite informacione sisteme, a podatke o obavljenim transakcijama dostavlja u nestandardizovanom formatu.

C. Ljudski faktor

Iz perspektive menadžmenta, donošenje poslovnih odluka na osnovu prikupljenih podataka je očigledna prednost.

¹ Osmočasovno radno vreme, 21 radni dan u mesecu

Međutim, to ne znači da će svi zaposleni sa odobravanjem prihvatiti uvođenje informacionog sistema u svakodnevni rad, dok se u pojedinim grupama može očekivati i opstrukcija, slika 1^[1].



Slika 1 - Spremnost zaposlenih da prihvate uvođenje informacionog sistema na osnovnu priznatog i stvarnog učinka

D. Stanje u Republici Srbiji

U Republici Srbiji ne postoje javno dostupni statistički podaci o eksploataciji vozila i mašina koje su u vlasništvu budžetskih korisnika, niti je ta oblast zakonski regulisana^[2]. Državna revizorska institucija (www.dri.rs) je 2014. godine objavila izveštaj o reviziji svrsishodnosti poslovanja "Upravljanje službenim vozilima direktnih korisnika budžeta Republike Srbije" u kome su prikupljeni podaci za 2012. godinu^[2]:

- Ukupno 26,966 službenih vozila
- 6,244 vozila opšte namene, 25% od ukupnog broja, 30% u ukupnim izdacima.
- Detaljnom analizom obuhvaćeno 15 od 126 direktnih budžetskih korisnika, 88% od ukupnog broja vozila, 84% ukupnih rashoda.
- 12,000km godišnje po vozilu
- Prosečna starost 9.5 godina
- Prosečna potrošnja 9.8 litara / 100km
- 1,9 milijardi dinara troškovi održavanja vozila opšte namene (~3,000€ po vozilu)
- Troškovi goriva - 60% ukupnih troškova
- Tekuće popravke i održavanje - 20% ukupnih troškova
- 1 krivična prijava zbog zloupotreba

Neefikasnost upravljanja je obrazložena nedostatkom zakonske regulative, kao i da evidencije direktnih budžetskih korisnika ne obezbeđuju tekuće i sveobuhvatne podatke o broju vozila, njihovoj iskorišćenosti i rashodima. Postupak revizije svrsishodnosti trajao je oko godinu dana^[3].

TABELA 2 - ODRŽAVANJE FLOTE MAŠINA
MESEČNI UTROŠAK RADNOG VREMENA ZA REDOVNO ODRŽAVANJE

Broj vozila	Intervencija mesečno	Nalozi za nabavku	Utrošak vremena	
			Časova ¹	Rad. dana ²
1	1	1	0.5	0
10		10	5	1
100		100	50	6
500		500	250	31
1000		1000	500	63
1	4	4	2	0
10		40	20	3
100		400	200	25
500		2000	1000	125 (6) ³
1000		4000	2000	250 (12) ⁴

II. PRIMENA STATISTIKE I DATA MINING-A

Ako se uzmu u obzir složena organizaciona struktura, broj instanci u lancima odlučivanja i nabavke, tehnička priroda održavanja i upravljanja flotom mašina i najvažnije - ljudski faktor, dobija se okruženje pogodno za obavljanje kriminalnih radnji koje je teško otkriti i preduprediti, a manifestuju se u vidu krađe, pronevere ili prevare prilikom redovnog održavanja i remonta mašina, ili zloupotrebe flotnih jedinica prilikom eksploatacije.

U procesu upravljanja flotom mašina, sledeće stavke se mogu identifikovati kao osetljive tačke podložne kriminalnim radnjama:

1. Eksploatacija
 - Gorivo
 - Angažovanje flotnih jedinica
2. Održavanje
 - Rezervni delovi
 - Potrošni materijal (maziva, akumulatori, gume)
 - Kontrola kvaliteta
 - Stanje i ispravnost mašine
3. Lanac nabavke
 - Nalozi za nabavku, tabela 2
 - Proces nabavke
 - Kontrola kvaliteta

Prevare su suptilne, i zahtevaju sofisticiranu analizu setova podataka da bi bile otkrivene i predupređene. Adekvatne alate za takvu analizu pružaju statistika, data mining i mašinsko učenje.

A. Statistika

Formiranje odgovarajućeg statističkog modela u funkciji zadatog cilja je od suštinske važnosti za efikasno praćenje dešavanja u sistemu. Od pravilnog izbora parametara zavisi veličina dobijenih setova podataka, koliko će oni biti pogodni

² Polučasovna intervencija

³ Osmočasovno radno vreme

⁴ Potreban broj zaposlenih neposredno na održavanju, 21 radni dan u mesecu

za analizu, kolika će biti brzina analize i kakav će biti kvalitet dobijenih rezultata.

Moderni sistemi za praćenje vozila kombinuju GPS, GPRS i web tehnologije da bi obezbedili konstantan protok podataka o vozilu/mašini prikupljenih pomoću digitalnih i analognih inputa^{[4][5]}. Neke od informacija koje se prikupljaju su:

- GPS koordinate
- Brzina kretanja
- Odstupanje od zadate rute
- Odstupanje od saobraćajnih pravila
- Vreme starta i gašenja motora
- Broj obrtaja
- ECU podaci
- Nivo goriva u rezervoaru
- Pozicija i nagib vozila / mašine itd.

B. Data mining

Podaci o pređenoj kilometraži, utrošku goriva, istoriji servisa i održavanja mašina mogu se beležiti pomoću namenski kreiranog softvera, mogu se unositi u običnu Excel tabelu, ili, kako je to najčešće slučaj u našoj zemlji, mogu se čuvati u papirnim dokumentima. Međutim, ukoliko kompanija ne raspolaže alatima za analizu sačuvanih podataka, ne može steći uvid u ostvareno poslovanje. Time se onemogućavaju analiza, smanjenje troškova i predviđanje, a odluke se donose na osnovu pretpostavki umesto na osnovu činjenica^[6].

Data mining se koristi za otkrivanje obrazaca u setovima podataka u cilju povećanja efikasnosti radnih operacija. Izvučene informacije se mogu kombinovati na različite načine u funkciji automatizacije procesa ili pripreme informacija za dalju obradu. U oblasti održavanja mašina, to se pre svega odnosi na

- Redovno održavanje (ulja, filteri)
- Preventivno održavanje
- Investiciono održavanje
- Potrošnju goriva i maziva
- Potrošni materijal (gume, akumulatori, kočione obloge, remeni, ...)
- Praćenje radnih parametara

Ekstrakcija i analiza podataka se mogu vršiti u realnom vremenu ili u zadatim intervalima (dnevno, nedeljno, mesečno), uz pravovremenu automatizovanu distribuciju informacija. U slučaju detekcije nepravilnosti ili odstupanja od očekivanih vrednosti, informacije o tome mogu biti iskorišćene za detaljniju analizu da bi se utvrdilo da li je u pitanju tehnički ili organizacioni problem, ili se pak radi o potencijalnoj prevari. Obaveštenja i/ili upozorenja mogu biti ugrađeni u standardne izveštaje koji se automatski distribuiraju.

C. Mašinsko učenje

Mašinsko učenje predstavlja tehniku izrade modela formiranih na osnovu prikupljenih informacija. Takvi modeli se potom mogu koristiti umesto propisanih parametara za predviđanje ili donošenje odluka prilikom održavanja mašina.

Softverska rešenja bazirana na ovoj tehnici mogu da se koriste za praćenje željenog parametra tokom vremena, a kada se vrednosti parametra približe projektovanim granicama, softver može da inicira korektivnu meru. Primena ovakvih softverskih alata omogućava kompanijama implementaciju strategije za održavanje zasnovanu na pouzdanosti mašina^[7].

D. Primena softverskog alata za praćenje operativnih parametara flote vozila i otkrivanje pokušaja prevare

Cilj istraživanja je bio da se ispita sposobnost softverskog rešenja da primenom pomenutih metoda prikaže potencijalne nepravilnosti prilikom održavanja flote mašina i stepen uticaja ljudskog faktora na kvalitet rezultata. Korišćen je softver Magma Fleet ManagerTM^[8] sa sledećim instaliranim modulima^[9]:

- Vozni park, putnička vozila
- Raspored mašina
- Status mašina
- Servis
- Gorivo
- Angažovanje mašina

Baza podataka je popunjena slučajno generisanim podacima o kilometraži, potrošnji goriva i održavanju flote vozila koju čine putnički automobili i nekoliko vrsta teretnih vozila. Modelovanje je izvršeno na osnovu uzorka sa podacima o delu voznog parka jedne velike građevinske kompanije, granice varijacije osnovnih vrednosti su usklađene sa preporučenim parametrima održavanja, pri čemu su u obzir uzeti starost vozila, način održavanja i vrsta eksploatacije.

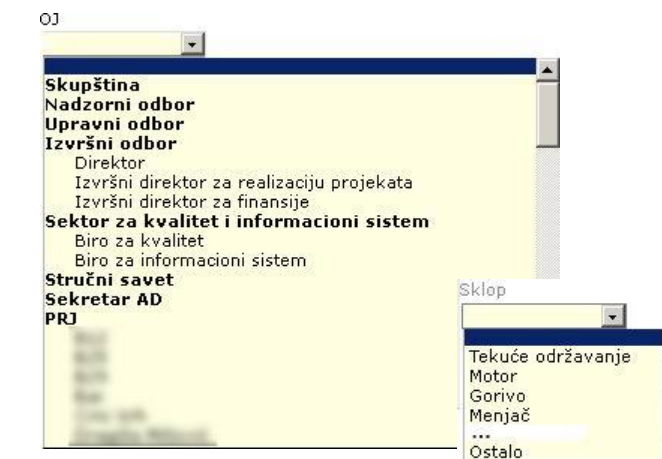
- Gradska vožnja
- Međumesna vožnja
- Rad na gradilištu
- Prosečna starost putničkih vozila 10 godina
- Prosečna starost teretnih vozila 15 godina
- Ugovorno održavanje
- Samostalno održavanje

III. REZULTATI

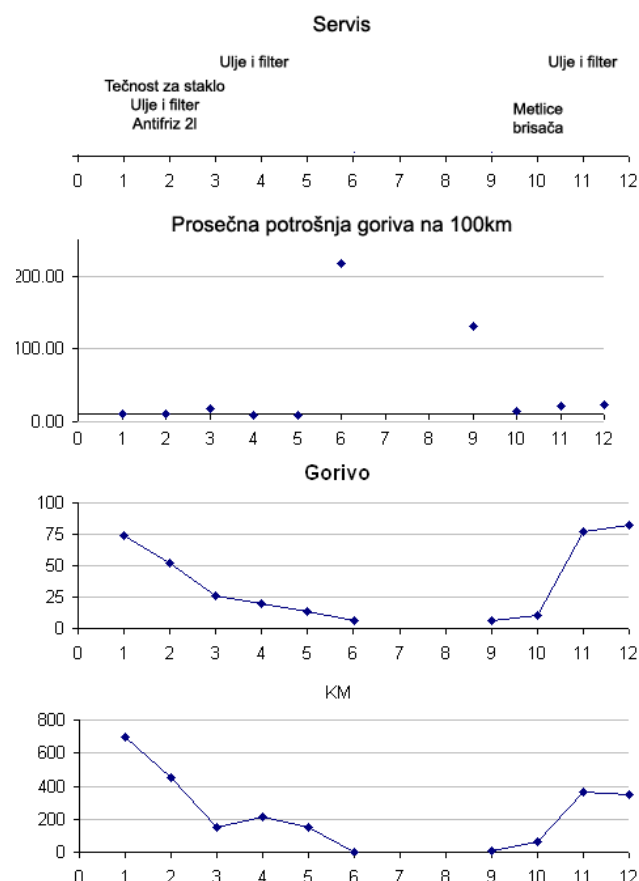
Sledeće osobine upotrebljenog softvera su se pokazale ključnim:

- Grupisanje mašina prema pripadnosti organizacionim jedinicama, slika 2.
- Dostupnost podataka u realnom vremenu.
- Praćenje potrošnje goriva.
- Praćenje servisa, popravki i drugih intervencija po karakterističnim sklopovima, slika 2.
- Distribucija ovlašćenja za pristup
- Filtriranje podataka prema različitim kriterijumima.

Na slici 3 je prikazan presek podataka za određeno vozilo u izabranom vremenskom intervalu, u ovom primeru to je jedna kalendarska godina. Na slici su uporedo prikazani servisni podaci, podaci o prosečnoj potrošnji goriva, nabavci goriva i pređenoj kilometraži.



Slika 2 - Simulacija organizacione strukture kompanije (levo) i klasifikacija intervencija na mašinama po karakterističnim sklopovima (desno)



Slika 3 - Uporedni grafički prikaz podataka za putničko vozilo u izabranom vremenskom periodu

Na dijagramima su lako uočljiva odstupanja od prosečnih vrednosti. Ukoliko nije u pitanju statistička greška, odstupanja mogu da ukažu na:

- probleme sa tehničkom ispravnošću mašine
- loš, neredovan ili zlonameran unos podataka
- kvalitet goriva, maziva, potrošnog materijala
- zloupotrebe u eksploataciji ili prilikom održavanja mašine

Daljom proverom podataka u odgovarajućem modulu softvera za flotni menadžment i unakrsnom proverom sa podacima u kompanijskom ERP softveru može se steći detaljniji uvid u srž problema.

IV. ZAKLJUČAK

Statistika, data mining i mašinsko učenje su tehnologije koje omogućavaju analizu i pronalaženje skrivenih obrazaca u velikim količinama podataka. Međutim, da bi se dobili kvalitetni rezultati, potrebno je pažljivo odabrati optimalan skup parametara koji se prate i analiziraju.

Akvizicija podataka se može obavljati u realnom vremenu, manuelno ili automatski pomoću GPS/GPRS tehnologije, web servisa i softvera za upravljanje flotom mašina zasnovanog na web tehnologiji.

Rezistentnost sistema na ljudski faktor se može povećati povezivanjem softvera za upravljanje flotom sa drugim aplikacijama u okviru kompanijskog informacionog sistema.

Uvid u rezultate poslovanja, a time i u potencijalne zloupotrebe, je moguć u realnom vremenu na svakoj organizacionoj instanci u okviru kompanije, u skladu sa realnim ovlašćenjima.

Ukoliko su ispunjeni ovi preduslovi, softver za flotni menadžment može da, pored svoje osnovne namene, posluži i kao efikasno sredstvo za otkrivanje nepravilnosti i eventualnih zloupotreba prilikom eksploatacije i održavanja flote mašina.

LITERATURA

- [1] J. Bladt and B. Filbin, Harvard Business Review (2014), "Who's Afraid of Data-Driven Management?", pristup 20.11.2014, dostupno na <https://hbr.org/2014/05/whos-afraid-of-data-driven-management/>
- [2] Državna revizorska institucija (2014), "Upravljanje službenim vozilima direktnih korisnika budžeta Republike Srbije", pristup 30.08.2014, dostupno na <http://www.dri.rs/lat/mediji/saopštenja-za-javnost/160--27-2014-.html>
- [3] "Radoslav Sretenović: Postoje zloupotrebe sa službenim vozilima", pristup 20.09.2014, dostupno na <http://www.blic.rs/Vesti/Politika/496469/Sretenovic-Postoje-zloupotrebe-sa-sluzbenim-vozilima>
- [4] G. Ivanović, D. Stošić, D. Jovanović (2013) "GPS/GPRS tehnologije u upravljanju pomoćnom mehanizacijom na površinskom kopu uglja", XI međunarodna konferencija "Održavanje i proizvodni inženjering", Budva, Crna Gora.
- [5] Chang-Yi Chen et al, "Using Data Mining Techniques on Fleet Management System", pristup 07.10.2014, dostupno na <http://proceedings.esri.com/library/userconf/proc04/docs/pap1801.pdf>
- [6] D. A. Kolman (2013), "Data mining for improved maintenance management", pristup 14.11.2014, dostupno na <http://www.vehicleservicepros.com/article/10886642/data-mining-for-improved-maintenance-management>
- [7] Skytree (2014), "Improve Operational Readiness with Machine Learning Based Prescriptive Maintenance", pristup 14.11.2014, dostupno na http://www.skytree.net/wp-content/uploads/2014/10/PMSolution_Sheet.pdf, solution sheet
- [8] M. Dobrojević (2013), "Magma Fleet Manager v2.0", XIV Međunarodni naučni skup Sinergija, p263-267, ISBN 978-99955-26-32-0
- [9] "Modules - Magma Fleet Management", pristup 30.06.2014, dostupno na <http://en.magmafleetmanagement.com/features/modules-d139>