Model integrisane forenzičke istrage poslovnih prevara
Integrated forensic investigation model of corporate fraud

Nataša Simeunović, Gojko Grubor, Nenad Ristić, Univerzitet Sinergija Bijeljina, BiH

***Apstrakt* – Isticanje novog polja forenzike, forenzičkog računovodstva, je prouzrokovano brzim promjena u elektronskom poslovnom okruženju te naglim porastom broja poslovnih prevara. Iako prevare možemo naći u mnogim oblicima, najčešće se svode na krađu sredstava i informacija ili zloupotrebu nečije imovine u obliku informacija. U današnjem svijetu, računovođe mogu najviše pomoći u istrazi korporativnih, ili bolje rečeno finansijskih prevara, koje danas preovladavaju u digitalnom okruženju. U ovom radu, autori su predložili model integrisane forenzičke istrage poslovnih prevara koji predstavlja spoj računovodstvenog, revizorskog i digitalnog istražnog postupka. No, prije nego što ovaj pristup može biti propisno verifikovan, potrebno je izvršiti dodatna ispitivanja.**

***Ključne riječi* – prevare, finansijske prevare, forenzičko računovodstvo, digitalna forenzička analiza**

***Abstract* – A new field of forensic accounting has emerged as current practices have been changed in electronic business environment and rapidly increasing fraudulent activities. Although fraud is taking many forms, it is usually found as theft of funds and information or misuse of someone's information assets. In today's world, accountants are the most helpful people to investigate corporate, or should we say financial frauds, which prevail in digital environment these days. In this paper, the authors proposed a model of integrated forensic investigation as a combination of accounting, auditing and digital forensic investigative process. Before this approach can be properly validated some future work needs to be done, too.**

***Keywords* – fraud, financial fraud, forensic accounting, digital forensic analysis**

I. UVOD

Savremeno doba digitalizacije podataka i modernizacija poslovnih procesa doveli su do stvaranja novih mogućnosti za počinioce finansijskih prevara, ali i za njihove istražitelje. Na mnogo načina se promijenio proces sprovođenja istrage, metode koje interni revizori koriste za planiranje i obavljanje posla, kao i pristupi koje koriste eksterni revizori da procijene rizik i izvrše reviziju. U isto vrijeme, javlja se i potreba za primjenom digitalnih forenzičkih alata u istrazi i obezbjeđivanju dokaza o kriminalnim radnjama u finansijskim izvještajima vršenih putem prikupljanja i obrade dokaza pohranjenih na računaru ili drugom nosiocu digitalnih podataka, a koje mogu biti vezan za određenu vrstu protivzakonitih aktivnosti.

Generalno posmatrano, prevare obuhvataju širok spektar ilegalnih aktivnosti jer se, za razliku od grešaka, sastoje u osmišljenom i namjernom pripremanju dokumenata, činjenica, informacija i situacija da bi se stvorili preduslovi da se neko na bazi pogrešnog predstavljanja činjenica u osmišljenim situacijama i okolnostima, podstakne da povjeruje u neistinu i u skladu sa njom da se ponaša i prema tome, trpi gubitak ili štetu [18]. Krađa sredstava ili informacija ili zloupotreba nečije imovine koja može dovesti do gubitka novca, povjerenja i/ili ugleda klijenta na tržištu su njeni najčešći oblici. Prevare se, najčešće, pojavljuju kao finansijske i prilično rijetko kao nefinansijske. Finansijska prevara je postala uobičajena pojava unutar mnogih preduzeća [6]. Većina slučajeva finansijskih prevara uklju čuje neku vrstu manipulacije prihodima, kao npr. precjenjivanje prihoda koje se obično javlja u poslovnim knjigama klijenta. Preduzeća jednostavno izmisle nastale prodaje, na odloženo ili plaćanjem u gotovom, čime nerealno i bez osnova unaprijed priznaju prihode, ili prikazuju fiktivne prihode, što direktno utiče na sastavljanje lažnih bilansa stanja i bilansa uspjeha [19].

Dakle, računovođa i revizor treba da traže ovakvu vrstu prevare u procesima interne kontrole i revizije. U kontekstu digitalnog okruženja, forenzičko računovodstvo igra važnu ulogu u otkrivanju ovakvih vrsta prevara koje računovodstvo i interna revizija nisu otkrili. Pa ipak, forenzičko računovodstvo je veliki izazov za redovne računovođe i računovodstvene revizore zbog nedostatka znanja i iskustva u digitalnoj forenzičkoj istrazi. Glavni cilj predloženog modela integrisanog procesa je promovisanje praktičnih potreba za zajedničkim, udruženim radom računovođa, revizora i digitalnih forenzičkih istražitelja u kompleksnom internet okruženju. Prema dostupnoj literaturi, trenutno je na tržištu prilično teško naći računovođu koji posjeduje znanje i iskustvo iz

 DOI: 10.7251/ZRSNG1501135S

olasti digitalne forenzičke istrage, kao i obratno. S aspekta forenzičkog računovodstva, ono se ponekad naziva i forenzičkom analitikom, što znači da se analiza digitalnih podataka vrši u cilju njihovog otkrivanja, oporavka i rekonstruisanja ili na drugi način u svrhu potvrđivanja ili pobijanja tvrdnje o nastaloj poslovnoj prevari [16]. Glavni koraci u forenzičkom računovodstvu su prikupljanje podataka, priprema, analiza i izvještavanje [16, 19]. Sa druge strane, digitalni istražni postupak može se definisati na više načina, u zavisnosti od svrhe primjene. Međutim, definicija forenzičke istrage koja preovladava u pravnom prometu uključuje sljedeće korake: forenzičko snimanje podataka, prikupljanje podataka (priprema i ekstarkcija), identifikacija i analiza podataka, izvještavanje, i analiza slučaja [15]. U ovom radu, autori predlažu model integrisane forenzičke istrage poslovnih prevara, koji se bazira na udruženom radu računovođa, revizora i digitalnih forenzičkih analitičara.

II. POSLOVNE PREVARE I FORENZIČKO RAČUNOVODSTVO

Uopšteno, taksonomija prevare može biti vrlo složena, jer se prevara može obaviti na više načina i pojaviti u mnogim oblicima kao što su zločin, korporativna prevara, menadžment i profesionalne prevare, nepoštenje, namjerna obmana, itd. Dakle, prevare, krađe, nepravilnosti, kriminal bijelog ovratnika i pronevjere su, takoreći, sinonimi. Glavni faktori koji mogu pokrenuti nekoga da počini prevaru uključuju mogućnost, racionalizaciju (ili lično opravdanje za činjenje/nečinjenje) i svaku vrstu finansijskog pritiska protiv nekoga. Ovi faktori su dobro poznati i objašnjeni u referenci [16]. *Finansijski pritisak* može biti značajan motiv prevarantima za krađu. *Racionalizacija* opisuje kako prevaranti pronalaze opravdanje za svoje kriminalne radnje? *Prilika* se može javiti kad je počinitelj na pouzdanom položaju koji prate slabosti, ili nedostatak internih kontrola koje pružaju okolnosti za prevaranta da počini zločin [16].

U redovnom procesu eksterne revizije, fokus je na uzorku transakcija, preciznosti i pouzdanosti finansijskih izvještaja, i napominjanju u izvještaju revizije u slučaju bilo kakvih odstupanja, grešaka, neuobičajenih pretjerivanja, itd [16]. Neki revizijski alati, kao što su revizijski alati podržani računarima - CAATs (*Computer Assisted Auditing Tools*) [9, 10], se trenutno koriste za rad sa velikim setovima finansijskih podataka, za procesuiranje složenih transakcija i kao pomoć revizorima u implementaciji postupaka revizije, poput sljedećih [9, 16]:

a) Testiranje transakcija i salda računa;
b) Identifikovanje nedosljednosti i oscilacija u transakcijama;
c) Programi za izdvajanje uzoraka podataka za revizijsko testiranje;
d) Ispitivanje opštih i aplikativnih kontrola računara; i
e) Ponovnim izračunavanjem pozicija koje je prethodno obavio računovodstveni sistemi.

Forenzički računovodstveni proces se razlikuje od redovne finansijske revizije, jer se bazira na potrazi samo za sumnjivim transakcijama, i koristi strogi digitalni forenzički proces [8, 12, 15]. Ovaj proces se sastoji od mnogih koraka kao što je prepoznavanje, snimanje, obračunavanje, vađenje, sortiranje i izuzeci u izvještavanju, neobičnosti, nepravilnosti i sumnjive transakcije, i potvrđivanje digitalnih finansijskih podataka i drugih računovodstvenih aktivnosti, sa ciljem izrade čvrstih dokaza za sudski proces [1]. Na žalost, ne postoji standardna procedura za otkrivanje svih vrsta prevara još uvijek, jer svaka prevara predstavlja specifičan slučaj.

Dakle, forenzički računovođa ili istražitelj prevara [1, 16, 19] se može definisati kao računovođa sa poznavanjem računovodstva, revizije i forenzičkih vještina koji istražuje slučaj finansijske prevare te može biti pozvan za vještaka u sudskom sporu [5, 16]. Međutim, ako „redovni“ računovođa ili revizor žele postati forenzičke računovođe, moraju proći različite kurseve iz finansijskog računovodstva, naprednog računovodstva prevara, revizije i kurs digitalne forenzičke istrage, kao što su [16, 19]:

- **Digitalna forenzička istraga**: primjena digitalnih forenzičkih načela, procedura, tehnika i alata.
- **Forenzičko računovodstvo**: primjena digitalne forenzičke istrage u računovodstvu.
- **Računari**: uključujući osnove hardvera i računovodstvene softvere (kao što su *Access, QuickBooks, SAP, Oracle* ...).
- **Pravo**: Osnove poslovanja, građanskog i krivičnog prava, kao i forenziku u sudskim sporovima.
- **Statistika**: Princip vjerovatnoće u testiranim transakcijama.
- **Ekonomija**: Bihejvioralnu ekonomiju za potrebe kvantifikacije štete u parnici.
- **Psihologija**: Kako se nositi s ljudim, kao savjetnik?
- **Etika**: Ako neko djeluje u granicama zakona, ali i dalje radi pogrešno.
- **Jezici**: Ako je počinioc govori drugi jezik.
- **Kriminologija**: Da bi shvatili kako prevaranti rade.

Forenzičke računovođe u svom radu mogu koristiti i neke matematičke modele, kao što su Benfordov zakon [3], faktor relativne veličine - *Relative Size Factor* (RSF), kao i *data mining* tehnike [6]. Benfordov zakon, se u reviziji i forenzici primjenjuje kao složeni oblik digitalne analize pomoću kojeg se gleda cijeli skup brojeva da bi se odredilo da li se svi brojevi uklapaju u očekivanu distribuciju [2, 3, 6], odnosno oni koji posjeduju drugačiji obrazac od uobičajenog predstavljali bi indikator prevare. Uprkos tome što posjeduje određene prednosti, Benfordov zakon sadrži i mnoga ograničenja. Detaljan opis je dat u članku pod referencom [3]. Pomoću RSF testiranja (*Relative Size Factor* - RSF) mogu se otkriti neobični podaci uzrokovani greškama ili prevarama [6].

DOI: 10.7251/ZRSNG1501135S

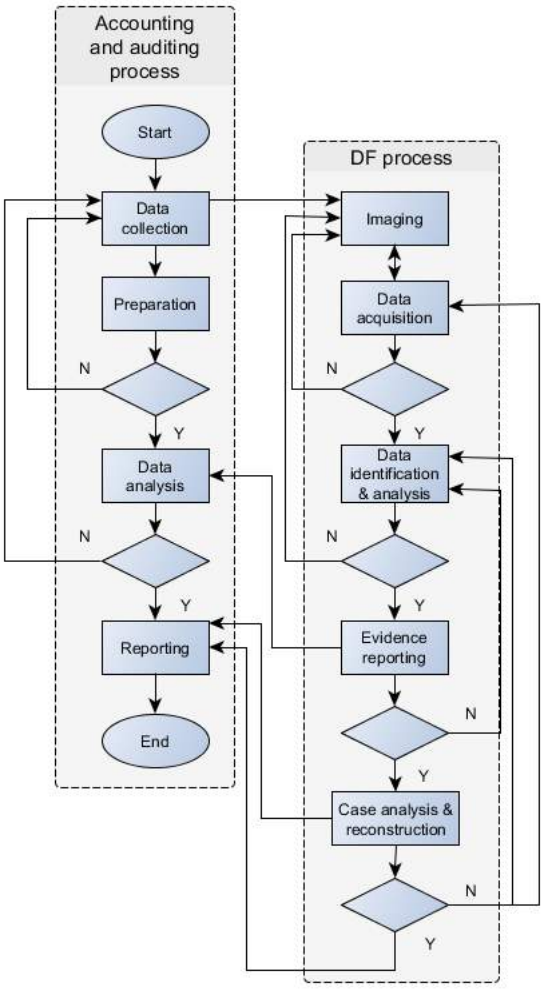
Eksponencijalni rast velikih skupova podataka (*Big data)* i informacionih tehnologija [11], kao i složene finansijske transakcije i pametniji prevaranti predstavljaju ogromne probleme tehnikama forenzičkog računovodstva. Međutim, neke napredne tehnike, kao što je *data mining* mogu pomoći forenzičkim računovođama u otkrivanju opštih karakteristika obrazaca lažnih podataka u transakcijama kao što su [6]:

a) neobične varijable ili unosi transakcija;
b) neuobičajeno visoka ili niska vrijednost varijable;
c) transakcije se u računovodstvu odražavaju u raznim datotekama; i
d) neobjašnjiva vrijednost dva ili više nepovezana zapisa.

III. MODEL INTEGRISANE FORENZIČKE ISTRAGE POSLOVNIH PREVARA

Pošto većina prevara uključuje finansijska pitanja, najlogičnije je da istrage o njima vrše računovođe. Međutim, prevara može biti vrlo složen a i digitalni forenzički analitičar (DFA) mora biti uključen u istražni postupak finansijskih prevara. Kako finansijske prevare uključuju namjerno precjenjivanje imovine, priho da i dobiti ili potcjenjivanje obaveza, troškova, i gubitaka [1], na takav način da to digitalni forenzički analitičari ne mogu samostalno shvatiti na pravi način, stručna procjena profesionalnih računovođa je neizbježna. U suprotnom, da bi se izbjeglo angažovanje usluga digitalnog forenzičkog analitičara, računovođe bi morale biti posebno obučene za sprovođenje digitalne forenzičke istrage i analize. Stoga, upošljavanje forenzičkih, računovodstvenih i revizijskih istražnih vještine u integrisani istražni model (slika 1) bi trebalo biti vrlo efikasno u praksi.

Ovaj model, u svojoj prirodi, predstavlja objedinjenost dva procesa u jedan. Oba, računovođa i digitalni forenzički analitičar (DFA) rade zajedno na istom predmetu finansijske prevare. Prvo, računovođa prikuplja sve raspoložive fizičke i elektronske podatake i informacije o istraživanom predmetu prevare i priprema sredstva za njihovu analizu. Na početku procesa digitalne forenzičke istrage, DFA sačinjava forenzičke slike (*image*) hard diskova računara osumnjičenih lica i/ili finansijskih aplikacija (npr. MS Excel datoteku namijenjenu finansijskom izvještavanju) i sve ostale forenzički relevantne informacije. Nakon toga, oni rade odvojeno, ali interaktivno, doslovno u svakom trenutku donošenja odluke. Dok forenzički računovođa analizira sve prikupljene pisane i pristupačne elektronske dokumente, podatke i informacije kao i druge materijalne dokaze, DFA izvlači relevantne forenzičke podatke iz slika u fazi akvizicije, identifikujući glavne podatke i analizirajući ih u narednom koraku istrage. Nakon izgradnje čvrstih digitalnih dokaza u vezi sa slučajem, DFA ih predaje forenzičkom računovođi prije faze konačnog izvještavanja.



Sl. 1. Model integrisane forenzičke istrage poslovnih prevara [7]

U stvari, oni zajedno vrše rekonstrukciju slučaja i sastavljaju završni izvještaj naručiocu istrage (npr. vlasnik, sudski organ ili bilo koja druga zainteresovana strana). Naime, prvi zadatak u integrisanom forenzičkog modelu predstavlja ispravna primjena računovodstenih, revizijskih i digitalnih forenzičkih procedura za prikupljanje, čuvanje, akviziciju, analizu i izvještavanje fizičkih i digitalnih dokaza na sudu [9, 15, 19]. Kada računovođa i DFA zajedno istražuju finansijske prevare, trebaju proučiti sve digitalne i druge materijalne dokaze u potrazi za tzv. crvenim zastavama, odnosno računovodstvenim znakovima upozorenja ili glavnim digitalnim forenzičkim podacima izvučenim iz svih izvora podataka, kao što su [11, 13]:

- priznavanje prihoda prije nego što je proizvod, roba ili usluga prodata;
- mnogo veći iznos prihoda od rashoda u izvještajima (bilansima);
- neusklađen rast vrijednosti zaliha i prodaje;
- kapitalizovani troškovi premašuju normu u grani djelatnosti;
- iskazani rast zarada koji ne prate novčani tokovi;

DOI: 10.7251/ZRSNG1501135S

- mnogo veći rast prihoda u odnosu na druge kompanije u grani;
- neuobičajena povećanja knjigovodstvene vrijednosti imovine;
- nemoguće je odrediti pravu prirodu transakcije;
- izmijenjene ili izbrisane fakture u finansijskim knjigama;
- otpisani krediti povezanim licima, itd.

U procesu digitalne forenzičke istrage, od presudnog značaja za uspješnu i efikasnu forenziku računara je sljedeći standardna procedura rada [8, 12, 14].

1. Zaštititi autentičnost izvora podataka u fazi snimanja;
2. Otkriti i oporaviti sve datoteke potrebne za istragu;
3. Identifikovati i analizirati najznačajnije prikupljene podatake i napraviti hronološki slijed događaja, i
4. Sumirati nalaze, napraviti evidenciju svih pribavljenih dokaza i sačuvati njihov integritet.

U tipičnom slučaju finansijske prevare, digitalni forenzički analitičar treba uzeti forenzičke slike hard diskova (HD) svih računara u računovodstvu, kreirati *hash* vrijednost svakog od njih, zadržati jednu kopiju kao referentnu i još jednu kao radnu kopiju [15, 19]. Dakle, DFA može raščlaniti informacije iz *Recent Docs Registry key* datoteke, ključ kojim su izlistane Excel-ove fajlove iz privremene Outlook datoteke (.pst) kao i druge lokacije npr. *file* serveri gdje bi korisnici mogli pohraniti podatke u redovnom procesu čuvanja sigurnosnih kopija podataka. U narednom koraku, on/ona može izdvojiti metapodatke i vidjeti datum kada su vršene skorašnje modifikacije, kao i ko je otvarao, uređivao ili štampao tabelu. Ovi metapodaci sadrže vremenske oznake koje su u korelaciji sa sistemskim fajlovima i vremenskim registrima (*Registry time stamps*) [14, 15]. Forenzički relevantni podaci dati u nastavku mogu se sačuvati kao skrivene informacije unutar metapodataka za MS Excel dokumente [4, 12]:

- Imena/inicijali korisnika, računar i kompanija;
- Naziv servera ili HD gdje je korisnik sačuvao podatke;
- Ostala svojstva datoteka i kratak pregled informacija;
- Nevidljivi dijelovi ugrađenih OLE (*Object Linking and Embedding*) objekata;
- Imena prethodnih autora i revizije dokumenata;
- Skriveni tekstovi i skrivene ćelije;
- Jedinstveni globalni identifikatori (GUIDs), itd.

Na žalost, prema *Microsoft Knowledge Base* [17] previše je teško (ako ne i nemoguće) dokazati kada je pojedina ćelija ili list/tabela modifikovana u MS Excel-ovoj datoteci, naročito ako opcija *Track Changes* nije prethodno omogućena. Pa ipak, forenzičkom računovođi ili digitalnom forenzičkom analitičaru se ponekad može dati Excel ili neka druga proračunska tabela ili fajl na ispitivanje. Dakle, analizom dokumenata se mora saznati koliko puta je datoteka "revidirana", kada je posljednji put uređivana, naziv korisničkog računa sa kojeg je izvršeno posljednje uređivanje, kao i kada je posljednji put štampana, itd. [13, 17].

IV. ZAKLJUČAK

Primjena modela integrisane forenzičke istrage poslovnih prevara, očito bi imala neke prednosti u praksi, uzimajući u obzir da forenzičke računovođe i revizori prevara veoma dobro poznaju načine nastanka poslovnih prevara i digitalnog forenzičkog analitičara koji je upoznat sa digitalnom forenzičkom naukom i posjeduje iskustvo u polju primjene različitih forenzičkih alata i tehnike. Oni bi trebali znati kako počinioci vrše prevare i glavne karakteristike raznih prevarnih šema. Ovakve informacije mogu im omogućiti efikasno obavljanje istrage finansijske prevare ili sprovođenje programa prevencije prevara. Poznavanje metoda činjenja prevara predstavlja glavni dio kritičkog znanja potrebnog računovođama, istražiteljima prevara i digitalnim forenzičkim analitičarima u efikasnom vršenju posla. Još jedan veliki dio čini razumijevanje crvenih zastava kao indikatora povezanih sa ovim prevarnim šemama, koji predstavljaju ključne podatke za forenzičku analizu. DFA mora izvršiti forenzičku istragu na način kao da će završiti pred sudom. U procesu forenzičkog računovodstva, najbolji način je proaktivno zaštititi računovodstvene datoteke ili *log*-ove držeći ih objedinjene i neizmijenjene, a naknadno ih samo revidirati. Oni mogu dokazati koji su korisnici pristupali, ili mijenjali, brisali ili kopirali neke datoteke. Integritet datoteka je najvažniji za svaku zakonsku regulaciju i dio je sigurnosne politike svakog društva ili digitalne forenzičke politike.

Da bi se potvrdile prednosti primjene modela integrisane forenzičke istrage, potrebno je, u budućnosti, istražiti i analizirati još mnogo slučajeva finansijskih prevara. Prema mišljenju autora, i digitalna forenzička analiza kao i finansijsko računovodstvo u digitalnom okruženju su prilično kompleksni da bi mogli biti istraženi od strane samo jedne osobe. Vjerovatno, vrlo mali broj ljudi bi mogao u potpunosti samostalno izvršiti istragu bilo koje tipične finansijske prevare u digitalnom okruženju ispravno čime se, možemo reći, opravdava primjena opisanog modela.

LITERATURA

[1.] B. K B Kwok, *Forensic Accountancy*, 2nd editions, LexisNexis, 2008.

[2.] Belak V., *Poslovna forenzika i forenzično računovodstvo*, Belak Excellens d.o.o., Zagreb, 2011.

[3.] *Benford's Law Excel 2007/2010 software*, Forenzika%20Excela/Benford's%20Law%20Software,%20Excel%20data%20analysis,%20Excel%20forensics.html, (preuzeto 10.06.2015).

[4.] D. Kernan, *Hidden Data in Electronic Documents*, GIAC GSEC Practical (v.1.4b, Option 1), SANS Institute InfoSec Reading Room, 2004.

[5.] D. Winch, *Finding and using a forensic accountant*, http://www.accountingevidence.

DOI: 10.7251/ZRSNG1501135S

com/documents/articles/Forensic%20accountant1.pdf, October 2007

[6.] Dr. P.K. Panigrahi, *Discovering Fraud in Forensic Accounting Using Data Mining Techniques*, 1426 the Chartered Accountant, April 2006.

[7.] Grubor G., Ristić N., Simeunović N, Integrated Forensic Accounting Investigative Process Model in Digital Environment, IJSRP, ISSN 2250-3153, Volume 3, Issue 12, December 2013

[8.] H. Carvey, *Windows Forensic Analysis DVD Toolkit*, Ch. 8, pg. 411, Syngress Publishing. Inc. ISBN 13: 978-1-597-422—9, 2009.

[9.] http://www.fbi.gov/news/stories/2012/march/forensic-accountants_030912/forensic-accountants_030912, *FBI Forensic Accountants*, (preuzeto 10.06.2015.).

[10.] http://www.isaca.org/Journal/Past-Issues/2003/Volume-1/Pages/Using-CAATS-to-Support-IS-Audit.aspx, *Using CAATs to Support IS Audit* (preuzeto 20.07.2015).

[11.] IBM, *Big data at the speed of business*, http://www-01.ibm.com/software/data/bigdata, (preuzeto 21.05.2015).

[12.] J. J. K., Bejtlich, R. Rose, W. C., *Real Digital Forensics - Computer security and incident response*, Addison-Wesley, 2008.

[13.] J. R. King, *Document Production in Litigation: Use an Excel-Based Control Sheet*, National Association of Valuation Analysts, Mar 4, 2009.

[14.] M. Milosavljević, G. Grubor, *Computer Crime Investigation*, ISBN: 978-86-7912-171-4, University Singidunum, www.singidunum.ac.rs, 2010.

[15.] M. Milosavljević, G. Grubor, *Computer System Digital Forensic*, ISBN: 978-86-7912-175-2, University Singidunum, www.singidunum.ac.rs, 2009.

[16.] M. Nigrini, *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations*, ISBN: 978-0-470-89046-2, Wiley and Sons, 2011.

[17.] Microsoft Knowledge Base, *How to minimize metadata in Microsoft Excel workbooks*, Article ID: 223789, Revision: 5.1, 2007.

[18.] Stanišić M., Revizija, Univerzitet Singidunum, Beograd, 2009.

[19.] T. W. Singleton, A. J. Singleton, *Fraud Auditing and Forensic Accounting*, Fourth Edition, John Wiley & Sons, Inc., 2010.

DOI: 10.7251/ZRSNG1501135S