ЖАКЛИНА СПАЛЕВИЋ*
КОСАНА ВИЋЕНТИЈЕВИЋ
Универзитет Сингидунум
Београд

УДК 336.6:343.3/.7(004.451.642)
Монографска студија
Примљен: 02.05.2017
Одобрен: 22.05.2017
Страна: 203-216

ФОРЕНЗИЧКО РАЧУНОВОДСТО И РЕВИЗИЈА У ДИГИТАЛНОМ ОКРУЖЕЊУ

Сажетак: Дигитална форензика у рачуноводству и ревизији односи се на способност прикупљања и коришћења података, који имају за циљ да спрече, открију, прате и истраже потенцијалне преваре, неправилности или неусклађености у пословању привредних субјеката. Начини нелегалних дигиталних активности постају све софистицираније. Форензичко рачуноводство и форензичка ревизија морају да прате и користе дигиталне алате у савременом пословном окружењу. Не постоје јединствени начини примене дигиталне форензике у форензичком рачуноводству и ревизији, јер се стално усавршавају и иду у корак или испред IT дигиталних достигнућа.

Кључне речи: дигитална форензика, правни аспекти дигиталне форензике, форензичко рачуноводство, форензичка ревизија, форензичка анализа података

Увод

Током последњих 25 година, cyber криминал еволуира од апстрактне идеје у опипљиве претње светском тржишту и сектору безбедности. У протеклих пет година пораст напада заснованих на Интернету довео је до тога да државе, привредни субјекти, медији и cyber стручњаци за безбедност отворено говоре о том проблему. *ISACA (Information Systems Audit and Control Association)*[1] је објавила истраживање на тему: *Cybercrime: Defending Your Enterprise How to Protect Your Organization From Emerging Cyberthreats* које пружа увид у нека изражена настојања cyber претњи и мере за заштиту привредног субјекта од ових претњи.[2] Дигитално кретање новца привлачи предузетничке криминалце, што доводи до веће криминалне активности широм света (McAfee Labs, 2015). Асоцијација сертификованих истражитеља превара - *ACFE (Association of Certified Fraud Examiner)*[3] је објавила извештај за 2016 годину. Резултати

* zspalevic@singidunum.ac.rs
[1] https://www.isaca.org/pages/default.aspx
[2] https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybercrime-Defending-Your-Enterprise.aspx.
[3] Association of certified Fraud Examiners, Retrived from: http://www.acfe.com/

истраживања обухватају обраду превара и злоупотреба кроз анализу 2410 случајева професионалних превара које су се догодиле у 114 земаља широм света.[4] Укупан губитак проузрокован преварама у наведеној студији премашује 6,3 милијарде УСА долара, са просечним губитком по случају од 2,7 милиона USA долара.

Детекциони метод	Евидентирани случајеви		
	2012. година	2014. година	2016. година
Дојаве	39,1%	42,2%	43,3%
Интерна ревизија	16,5%	14,1%	14,4%
Контрола менаџмента	13,4%	16,0%	14,6%
Случајно	5,6%	6,8%	7,0%
Усаглашавање рачуна	5,5%	6,6%	4,8%
Други методи	5,5%	0,5%	1,1%
Преглед документације	3,8%	4,2%	4,1%
Ревизија	3,8%	3,0%	3,3%
Законодавни органи	2,4%	2,2%	3,0%
Праћење / мониторинг	1,9%	2,6%	1,9%
IT контрола	1,3%	1,1%	1,1%
Признање	1,3%	0,8%	1,5%

Табела1: *Почетно откривање професионалних превара*

Табела 1. показује учесталост по критеријуму начина како су иницијално откривене преваре, укључујући поређење са истраживањем ове организације (*ACFE*) за 2012. и 2014. годину. Према анализи из 2016. године, на другом месту откривања превара је интерна ревизија (16,5%), а екстерна ревизија је на осмом месту (3,8%). На дигиталној технологији, као инфраструктури савременог пословања, је конципирана дигитална економија која се испољава кроз нове моделе пословања у области производње, услуга и других савремених сектора пословања. Истраживање које је 2016. године спровела консултантска фирма *Protiviti* у сарадњи са *North Carolina State University Enterprise Risk Management Initiative* обухватило је анкетирање 735 финансијских директора и извршних директора (407 из САД и 328 из других региона). Предмет истраживања је било 30 врста ризика са којима се суочавају њихове компаније. Према обрађеним анкетама *cyber* претње су на трећем месту глобалних ризика. Сваки од десет идентификованих топ ризика за 2017. годину је показао раст у односу на претходну годину.

Рб	Ризик	Рејтинг	
		2017. година	2016. година
1	Економски услови	6,61	5,83
2	Регулаторни оквир и надзор	6,51	6,06
3	*Cyber*-претње	5,91	5,80
…	…	….	….

Табела 2: *Топ глобални ризици за 2017.годину (Amato, N., 2016)*

[4] Report to the nations on occupational fraud and abuse 2016 global fraud study, Retrieved from: https://s3-us-west-2.amazonaws.com/acfepublic/2016-report-to-the-nations.pdf.

Европска асоцијација за управљање ризиком (*The Federation of European Risk Management Associations FERMA*)[5], као представник управљања ризиком привредних друштава на европском нивоу, сваке друге године објављује истраживање на тему топ десет ризика пословања у Европи. *FERMA* је u 2016. години објавила *European Risk and Insurance Report 2016* прикупљањем одговора преко 600 европских менаџера који управљају ризиком. Наведена истраживања су спроведена коришћењем *on line* анкета, што није случајно. Наиме, коришћење *on line* анкета добија на популарности због предности које даје овај модел; нека ранија истраживања су била углавном фокусирана на поређење између *on line* истраживања и других видова истраживања (*Gao, Z., House, L. A., Xie, J.*, 2015, 199-221). Пораст забринутости за континуитет пословања и cyber ризике указује на потребу привредних друштава да буду отпорнија на спољне претње у виду cyber напада.

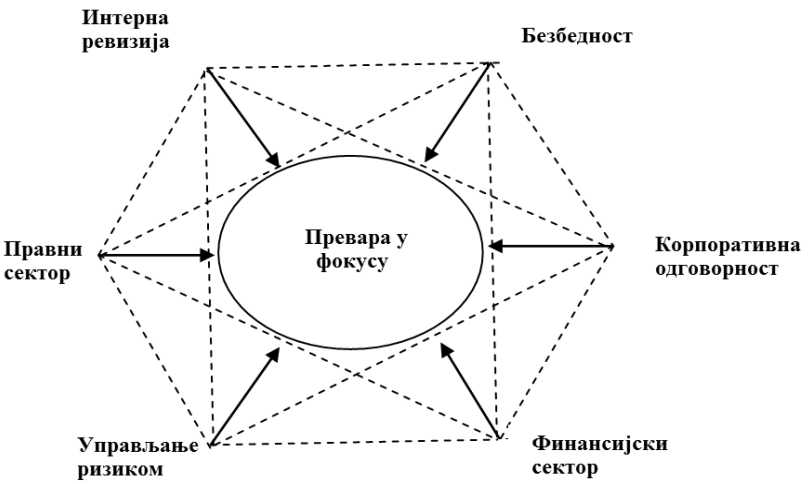
Првих десет ризика у 2016. години	Тренд у односу на 2014. год.	Вероватноћа	Ниво опадања	Ниво испуњености
Економски услови	раст	велика	*	*
Нарушавање континуитета пословања	ново	велика	**	**
Политичка, државна нестабилност	опадање	велика	*	*
Непоштовање прописа	опадање	велика	**	**
Конкуренција	опадање	велика	**	*
Репутација и бренд	опадање	средња	**	**
Cyber напад/приватност података	раст	велика	**	*
Маркетиншка стратегија	опадање	велика	**	*
ИТ системи у дата центрима	раст	средња	**	**
Каматна стопа и замена девиза	раст	средња	**	**
*** - Високи ** - Средњи * - Ниски				

Табела 3: *Топ 10 ризика у 2016. години (FERMA)*

Ризик *дигитална трансформација* није међу првих десет, упркос растућој забринутости за *cyber* нападе и приватност података. У зависности од типа привредног друштва, може се јавити потреба да се укључе представници људских ресурса, сектора набавке, IT сектора, комуникација и други који имају интерес да се на прави начин управља ризиком од преваре.

На Слици 1. (*Samociuk, S. M., Iyer, N.,* 2013: 44) приказани су организациони сектори компаније који се баве проценом могућих ризика од преваре. *Cyber* криминал је облик преваре. А превара је комплексан појам, како по садржини, тако и по обухвату поља на које се односи (Вукадиновић, 2016: 7). И најчешћа последица превара је неовлашћено отуђење или коришћење туђе имовине.

[5] http://www.ferma.eu/



Слика 1: *Стављање преваре у фокус*

Имовина је скуп свих субјективних имовинских права једног лица. Предмет имовине (Марковић, 2015: 170) су: стварна права, интелектуална имовинска права (ауторска права и права индустријске својине), права личности (ако су изражена у имовинском виду) и облигациона права (изузев оних која се не могу уопште новчано изразити).

Финансијске и рачуноводствене преваре и злоупотребе

Финансијске преваре односно криминалне радње у финансијским извештајима представљају изазов на светском нивоу. Наиме, чак и најразвијеније тржишне економије са уређеним економско-правним системом нису у могућности да се изборе са проблемом финансијских превара.

Финансијске преваре су намерно, промишљено, нетачно тврђење или изостављање материјалних исказа или рачуноводствених података, који посматрано са осталим информацијама у целини, наводе на то да починилац промени или преуреди своју процену или одлуку (*Rezaee and Riley*, 2010, p. 5).Професионалне финансијске преваре према појавним облицима могу бити:

- против правно присвајање средстава или отуђење имовине,
- лажно финансијско извештавање и
- корупција.

Остали облици финансијских превара које ACFE није навео су: прање новца и компјутерски криминал.

Противправно присвајање средстава представља финансијску превару коју у највећем броју случајева врше запослени у организацији, самостално или у договору с трећим лицима. Запослени у овом случају користе своју позицију како би извршили злоупотребу ресурса организације, односно узимали, присвајали и користили за своје личне потребе материјална средства организа-

ције. Најчешћи облици проневере и злоупотребе имовине су: вишеструке исплате истом добављачу, неиздавање рачуна, плаћање фиктивних набавки, неевидентиране продаје, исплате зарада фиктивним радницима, лажне провизије и сл. Када се ради о појединим облицима противправног присвајања средстава, на светском нивоу у 2012. години највећи број случајева испољен је кроз неевидентиране продаје што износи 24,9% од укупног броја финансијских превара. Просечна штета по случају нанесена овом врстом преваре износи 100.000 УСА долара. Следећи најзаступљенији облик је противправно присвајање материјалне имовине који се односи на неодобрено коришћење машина, возила, компјутерске и друге опреме за приватне потребе. Овај тип злоупотребе имовине у 2012. години представља 17,2% од укупног броја превара.

Лажно финансијско извештавање је још један вид преваре и дефинише се као намеран акт издавања искривљених и обмањујућих финансијских извештаја у настојању да се избегне негативно мишљење о финансијској стабилности организације. Лажно финансијско извештавање се испољава у виду следећих пет повезаних облика: фиктивни приходи, лажна временска разграничења, прикривање обавеза и трошкова, неправилна обелодањивања, остале технике лажног финансијског извештавања (Петковић, 2011, 138).

Корупција представља злоупотребу јавних овлашћења за реализацију приватних користи. Како је она системска творевина, откривање корупције као сложене криминалне радње представља велики проблем због тога што обе стране које учествују у корупцији штите једна другу и обе имају користи од исте. Корупција наноси штету не само организацијама, него и економији земље јер разара поверење инвеститора, због чега опада ниво инвестиција, снижава се кредитни рејтинг земље, спречава раст и негативно утиче на развој. Према истраживању *ACFE* случајеви корупције заузимају средишње место у укупном броју финансијских превара, како по учесталости тако и по висини губитка, који просечно износи око 250.000 америчких долара.

Најчешћи облици превара у области рачуноводства (*Belak*, 2011: 42) су:

- непоштовање законске регулативе у циљу приказа жељених резултата,
- фалсификовање података и књиговодствених исправа,
- приказивање фиктивних догађаја,
- намерно искривљавање пословних догађаја и
- прикривање крађе новца и остале имовине.

Анализом рачуноводствених података проналазе се бројни облици превара. У основи се издвајају три карактеристична начина манипулисања подацима: злоупотреба правних прописа, манипулације у рачуноводственом евидентирању, непосредно кривотворење података у финансијским извештајима.

При злоупотреби правних прописа ради се о злоупотреби правних норми тако да се на изглед створи слика њиховог поштовања, а у ствари се унутар прописа траже путеви и странпутице, како би се постигли жељени пословни циљеви, а то је најчешће захтевани пословни исход. Да би се постигао тај циљ, бројним се манипулацијама стварају другачије вредности средстава, трошкова и одлива.

При манипулацијама у рачуноводственом евидентирању се ради о фиктивним или неправилним начинима рачуноводствене обраде података, с наменом да се прикрије права слика о стању средстава, извору средстава и пословном исходу. Овде се јављају погрешни и фиктивни рачуноводствени подаци, као нпр: подаци о фиктивној продаји и фиктивном приходу, манипулације приликом пописа средстава и обавеза, прецењивање и касније смањење вредности тих средстава организације, промене начина и метода вредновања, разбијање пословног догађаја и његове вредности на више саставних делова, прекњижавање са једнога конта на више конта и губитак прегледности пословног догадаја, намерно криво књижење стварних или привидних пословних догађаја на неправилна конта.

Кривотворења података у рачуноводственим извештајима посебно у основним рачуноводственим извештајима долази у тренуцима када се починитељ тих дела не одлучи за манипулације у самом евидентирању, већ манипулише с подацима о билансу и, на пример, преноси их у посебне табеле и сврстава у неодговарајуће групе, или их рецимо не прикаже у стварној вредности, јер жели да прикаже циљну вредност економске категорије, да би задовољио очекивањима примаоца таквих извештаја.

Тип компаније	Процентуална заступљеност	Просечни губитак у *USD*
Приватне компаније	39,1%	278.000
Јавне компаније (компаније на берзи)	28,4%	142.000
Мале компаније (мање од 100 запослених)	38,2%	200.000
Средње компаније (101 до 999 запослених)	20,0%	176.000
Велике компаније (од 1000 до 9.999 запослених)	23,0%	116.00
Корпорације (преко 10.000 запослених)	18,9%	147.000

Табела 4: *Заступљеност превара према типу компаније*

Веома често оваква кривотворења починитељ ретроградно поправља, односно прилагођава податке у пословним књигама, а можда чак и у пословним листама. Величина финансијских превара такође у многоме зависи од типа компаније. Табела 4. приказује процентуалну заступљеност превара према типу компаније у САД, као и просечне месечне губитке (*Vonya*, 2009).

Дигитална форензика

Дигитална форензика обухвата употребу компјутерских и информационих система знања, заједно са правним знањима, у циљу анализирања и добијања правно прихватљивог дигиталног доказа, његове обраде и чувања на законски прихватљив начин. Она се примарно користи за истраге које су усмерене ка правним или законским питањима за спровођење које ће вероватно завршити на суду. Дакле нагласак је на правној прихватљивости прикупљених дигиталних доказа. Дигитални докази су изузетно нестабилни и могу се лако изгубити и бити искривљени. Постоји потреба да се они сачувају и да се њима рукује на начин који ће осигурати да нису, нити ће бити измењени или униш-

тени. Међутим проблем може настати због тога што дигитална форензика користи алате и технике који могу да се користе за опоравак изгубљених датотека и за унутрашњу управу (као што је праћење и проналажење злоупотреба).

У Великој Британији је у употреби процедура чувања "континуитета доказа", која обезбеђује сигурност да се дигитални докази прикупљају, обрађују, користе и чувају са дужном пажњом, тако да се не мењају или уништавају, или да не могу бити "закључани". Те процедуре укључују састављање документације о томе како се дигитални докази стичу, обрађују, користе, чувају, ко са њима рукује. Форензички дигитални докази који се користе на суду морају да буду прикупљени и документовани на правно прихватљив начин. Дигитална форензика се може користити за истраге ревизије и може бити веома корисна када се истражују преваре. Ревизори могу користити форензичке алате и технике, пратити, анализирати усклађеност са организационим политикама и регулативом.

Бављење дигиталном форензиком је делатност од које форензичари очекују за себе остварење одговарајуће зараде, те је битно да свој посао обаве што је могуће ефикасније. Та ефикасност се изражава кроз тзв. „форензичку спремност". *CESG Good Practice Guide No. 18, Forensic Readiness*,[6] дефинише форензичку спремност као: Постизање одговарајућег нивоа способности од стране организација како би биле у стању да наплате, очувају, заштите и анализирају дигитални доказ, тако да се ови докази могу ефикасно користити у свим правним стварима, у дисциплинским поступцима, или на суду.Није лако прогнозирати када може бити потребан неки дигитални доказ. Осим тога, употреба може бити за интерне потребе, или по основу регулаторних или законских захтева или других спољашњих разлога. Форензичка спремност помаже организацији да усмери своје активности, тако да проналажење дигиталних доказа постаје лако. Потребно је дигиталне доказе правилно приказати и чувати пре него што дође до инцидента. Дигитална форензика је делатност које се стално развија и од дигиталног форензичара се очекује да поседује и одговарајућа знања, али и вештине које мора стално унапређивати. Потребу сталног развоја дигиталне форезнике потврђују и резултати глобалног истраживања које су у новембру и децембру 2015. године спровели *ISACA i RSA Conference*[7].

Учесници анкете су потврдили да се методологије напада, повреда организација и података, убрзано и софистицирано развијају. Тренутно стање глобалног *cyber* обезбеђења је хаотично, и не очекује се да ће се напади успорити. Скоро 75% испитаника очекује да ће постати мета напада у 2016. години. *Cyber* криминалци су најзаступљенији криминалци.[8] Због природе истраживања, циљна популација се састојала од појединаца који имају *cybersecurity* посао. Наиме, од 842 људи који су учествовали у истраживању њих 461 има као примарни посао *cybersecurity* или безбедност информација.

---

[6] *The National Archives, (2011):* Digital Continuity to Support Forensic Readiness, Retrieved from: http://www.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf

[7] https://www.rsaconference.com/

[8] https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

Дигитална форензика у рачуноводству

Форензичко рачуноводство интегрише рачуноводство, криминологију, компјутерску форензику (истраге), парнице, истражне услуге ревизије пословних проблема као што је приказано на *Слици 2.* према *Smith and Crumbley* (2009: 1- 24).

Слика 2: Вештине форензичког рачуновође (Smith, G., Crumble D.,2009: 68)

Област истраживања форензичког рачуноводства је широка и обухвата преваре, испитивање, *due diligence*, процену ризика, откривање лажираних финансијских извештаја, *cyber* криминала, илегални трансфер новца, модалитете ризика према *M. Wagner and P. Frank* (1986). Данас се у рачуноводственим евиденцијама информације обрађују и чувају у дигиталном облику. Тако да уколико дође до криминалне истраге неће бити могуће да се она спроведе без IT форензичког рачуновође. Мотивациони фактори криминалних радњи: могућност, притисак, рационализација, важе и за преваре у рачуноводству. Ови фактори креирају такозвани троугао незаконитих радњи. Могућност представља околност која је плодно тло за превару, јер лице просто има могућност да је изврши.

Рационализација је врста околности при вршењу превара где лице налази низ оправдања која његову намеру за вршење криминалне радње оправдавају. Притисак, чине околности које од лица која чине превару императивно, захтевају ликвидна средства која он на тај начин покушава да обезбеди.

Најчешћи облици кривичних дела са којима се сусреће форензички рачуновођа су: крађа, провална крађа, завера, проневера, превара, пљачка, изнуда, подметање пожара, подстицање, помагање и подржавање.

Дигитална форензика у ревизији

Дигитална форензичка ревизија је стручан истраживачки посао који ревизори обављају применом метода, техника истраживања, ослањајући се на рачуноводствена знања, знања интерне и екстерне ревизије и дигиталне технологије.

Ревизори морају да траже постојање материјално погрешних исказа у финансијским извештајима било услед грешака или преваре. *SAS* бр. 99, *Разматрање незаконитих радњи у ревизији финансијских извештаја*[9] и *briefing paper*, *Финансијска превара,*[10] коју је написала саветодавна група одбора *PCAOB* (*Public Company Accounting Oversight Board*), пружа ревизорима специфичне смернице о трагању за преваром (*William S. H., Jey J. L., George R. Y.,* 2014: 125).

Међународни стандард ревизије 240: Одговорност ревизора (током ревизије финансијских извештаја) за преваре усвојио је Одбор за међународне стандарде ревизије и уверавања (*International Auditing and Assurance Standards Board - IAASB*)[11] (*IAASB, 2015*). Интерни ревизори су упућени да у свом раду против превара у привредном субјекту примењују следеће Стандарде који су прописани у Међународном оквиру професионалне праксе од стране Института интерних ревизора (*IIA*[12]).

1. *IIA Стандард 1200: Стручност и дужна професионална пажња*
   1210 A2. - Интерни ревизор мора поседовати довољно знања да може да проучи ризик од преваре и начин на који организација њиме управља, али се од њега не очекује да поседује исти ниво стручног знања као особа чија је главна одговорност откривање и истраживање преваре (Међународни стандарди за професионалну праксу интерне ревизије (стандарди), 2016: 9).
2. *IIA Стандард 1220: Дужна професионална пажња*
   1220 A1. Интерни ревизори морају демонстрирати дужну пажњу, тако што ће узети у обзир вероватноћу појаве значајних грешака, превара или неусаглашености (Међународни стандарди за професионалну праксу интерне ревизије (стандарди), 2016: 10).
3. *IIA Стандард 2060: Извештавање вишег руководства и одбора*
   Извештавање, такође, мора обухватити и питања контроле и значајних изложености ризику, укључујући ризик преварних радње, питања, корпоративног управљања и остала питања која су неопходна или захтевана од стране одбора или вишег руководства.
4. *IIA Стандард 2120: Управљање ризиком*
   1220 A2. Активност интерне ревизије мора проценити могућност настанка преваре и начин на који се у организацији управља ризиком од преваре.
5. *IIA Стандард 2210: Циљеви ангажмана*
   2210 A2. Приликом утврђивања циљева ангажмана, интерни ревизори морају узети у обзир вероватноћу појављивања значајних грешака, преваре, неусаглашености и остале ризике.

---

[9] Consideration of Fraud in a Financial Statement Audit, Retrieved from: http://www.aicpa.org/research/standards/auditattest/downloadabledocuments/au-00316.pdf

[10] Consideration of Fraud in a Financial Statement Audit, Retrieved from: https://pcaobus.org/Standards/Auditing/pages/au316.aspx

[11] https://www.iaasb.org/

[12] https://na.theiia.org/Pages/IIAHome.aspx

Неке ревизорске куће имају одељења која се баве форензиком. Одељење форензичке ревизије у оквиру ревизорске куће обухвата следеће послове: саветодавну подршку судским споровима, сведочење на суду, истрагу преваре (*Rezaee*, 2002: 227).

Правци унапређења дигиталне форензике

Два су правца унапређења ефикасности дигиталне форензике у рачуноводству и ревизији:

Развој и примена алата за дигиталну форензику у рачуноводству и ревзији

Форензичка анализа података у рачуноводству и ревизији подразумева прикупљање и обраду података, који треба да спрече, открију, прате или истраже потенцијалне преваре, неправилности или неусклађености у пословању привредних субјеката. Ревизорска кућа *Ernst&Young*[13] у сарадњи са компанијом *Longitude Research*[14] спровела је глобално истраживање о коришћењу форензичке анализе података. Истраживање је обухватило 665 руководилаца у привредним субјектима који активно користе форензичку анализу података (FDA – eng. *forensic data analytics*).

По претходном истраживању из 2014. године[15], 64% испитаника је сматрало да је ниво инвестиција у алате за форензичку анализу података задовољавајући. Према резултатима истраживања из 2016. године тај проценат износи само 55%. У наредне две године, троје од петоро испитаника планира додатна улагања у форензичку анализу података. Као главне разлоге, за та улагања, испитаници наводе виши ризик од cyber криминала (53%) и надзор од стране регулаторних органа (43%).

Мултинационалне компаније све више користе напредну дигиталну форензичку анализу података, да би се супротставиле повећаним ризицима пословања са којима се суочавају. Нове технологије и технике праћења и надзора им помажу при управљању ризицима везаним за преваре и cyber нападе. Коришћење података је све софистицираније, те 75% испитаника тврди да рутински анализира велику количину података, што им омогућава бољи увид у потенцијалне ризике у оквиру њиховог окружењу.

Привредна друштва традиционално користе форензичке анализе података током истрага превара. Коришћењем *FDA* алатки за превенцију и детекцију

[13] Global Forensic Data Analytics Survey 2016, Retrieved from: http://www.ey.com/Publication/vwLUAssets/ey-forensic-data-analytics-survey-2016/$FILE/ey-forensic-data-analytics-survey-2016.pdf

[14] Global Forensic Data Analytics Survey 2016, Retrieved from: http://www.longituderesearch.com/work/global-forensic-data-analytics-survey-2016/

[15] Global Forensic Data Analytics Survey 2014: Retrieved from: http://www.ey.com/Publication/vwLUAssets/EY-Global-Forensic-Data-Analytics-Survey-2014/$FILE/EY-Global-Forensic-Data-Analytics-Survey-2014.pdf

потенцијалних превара може се избећи да до њих (а самим тим и пословних губитака) уопште и дође. Другим речима, уместо да се алатке форензичке анализе података користе искључиво у реактивне сврхе (тј. истраге), њихово коришћење у превентивне и детективне сврхе може бити од велике користи за компаније. На основу спроведеног истраживања следи да компаније које су имале позитивно искуство са коришћењем *FDA*, су потрошиле 1/3 својих буџета намењених за превенцију превара и усклађеност пословања, управо на унапређење *FDA*.

Правни оквир за унапређење дигиталне форензике у рачуноводству и ревизији

Форензички рачуновођа ради у области права и зато је битно да познаје кривичне и грађанске поступке и врсте кривичних дела која постоје. Од форензичког рачуноће се захтева сарадња са стручњацима из правних и дигиталних наука у правцу разрешења форензичког проблема.

Број и назив главе у Кривичном Законику	Назив кривичног дела	Члан
Глава двадесет прва Кривична дела против имовине	Утаја	207
	Превара	208
	Неосновано добијање и коришћење кредита и других погодности	209
Глава двадесет друга	Пореска утаја	229
	Прање новца	231
Кривична дела против привреде	Несавестан рад у привредном пословању	234
	Проузроковање стечаја	235
	Проузроковање лажног стечаја	236
	Злоупотреба овлашћења у привреди	238
Глава тридесет друга Кривична дела против правног саобраћаја	Фалсификовање исправе	355
	Посебни случајеви фалсификовања исправе	356
	Фалсификовање службене исправе	357
	Навођење на оверавање неистинитог саобраћаја	358

Табела 5: *Криминалне радње према кривичном законодавству Републике Србије*

Криминалне радње према одредбама кривичног законодавства Републике Србије са којима форензички рачуновођа треба да буде упознат су приказане у наредној табели 5. У области форензичког рачуноводства посебан акценат на директну примену и примену методе индукционог закључивања дат је кроз:

- Закон о рачуноводству, "Службени гласник РС", број 62/2013;
- Закон о ревизији, "Службени гласник РС", број 62/2013;
- Закон о спречавању прања новца и финансирања тероризма, "Службени гласник РС", бр. 20/2009, 72/2009, 91/2010 и 139/2014;
- Закон о привредним друштвима,"Службени гласник РС", бр. 36/2011, 99/2011, 83/2014 - др. закон и 5/2015;
- Закон о кривичном поступку Републике Србије ("Сл. гласник РС", бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014);

- Кривични законик ("Сл. гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014);
- Закон о агенцији за борбу против корупције ("Сл. гласник РС", бр. 97/2008, 53/2010, 66/2011 - одлука УС, 67/2013 - одлука УС, 112/2013 - аутентично тумачење и 8/2015 - одлука УС).
- Закон о одговорности правних лица за кривична дела, "Службени гласник РС", бр. бр. 97/2008;
- Закон о привредним преступима, "Сл. лист СФРЈ", бр. 4/77, 36/77 - испр., 14/85, 10/86 (пречишћен текст), 74/87, 57/89 и 3/90 и "Сл. лист СРЈ", бр. 27/92, 16/93, 31/93, 41/93, 50/93, 24/94, 28/96 и 64/2001 и "Сл. гласник РС", бр. 101/2005 - др. закон;
- Закон о прекршајима, "Службени гласник РС", бр. бр. 65/2013, 13/2016 и 98/2016 - одлука УС;

Закључак

Послови дигиталне форензике ће у будућем периоду бити све актуелнији. Неопходно је стално проширивати и усавршавати листу форензичких алата и правну регулативу. То ће допринети да методе за спречавање и откривање превара у рачуноводству и ревизији постану адекватне све софистицираним методама сумњивих трансакција. Примена дигиталне форензике у рачуноводству и ревизији подразумева знања из: информационих технологија, права, криминологије, националне и међународне регулативе из области рачуноводства, интерене и екстерене ревизије, етике за професионалне рачуновође. Пословно окружење у Републици Србији захтева да се дигитална форензика у рачуноводству и ревизији што пре укључи у законску регулативу и да се што пре крене са применом у текућем и наредним пословним периодима. Повећана употреба и зависност од информационих технологија за вођење привредног субјекта довели су до доступности дигиталних података који могу да се користе да се у случају нежељених пословних догађаја открије: шта, где, како и зашто се десило. Дигитални докази могу да доведу до оптужнице или правдања појединца или привредног субјекта. Дигитални докази треба да се третирају са дужном пажњом.

Привредни субјекти морају бити свесни важности форензичког планирања и форензичке спремности, јер је то услов континуитета и напретка њиховог пословања. Неки докази могу бити измењени или изгубљени, па се у том случају проблем преваре не може решити на прихватљив начин. Форензичка спремност у великој мери смањује ове проблеме, посебно зато што велики део доказа потребних је доступан пре инцидента, током инцидента и када истрага почне. Форензичка спремност помаже у обезбеђивању поступања запослених са политиком организације или регулативама због сталног праћења и преиспитивања. Правац унапређења дигиталне форензике треба да буде у томе да се алатке форензичке анализе података не користе искључиво у реактивне сврхе (тј. истраге), већ и у превентивне и детективне сврхе.

Литература:

1. Amata, N. (2016): The top global risks for 2017, Retrieved from: http://www.cgma.org/MAGAZINE/NEWS/PAGES/2017-TOP-GLOBAL RISKS-201615723.ASPX
2. Amato, N., (2016): The global risks for 2017, Retrieved from: http://www.cgma.org/magazine/news/pages/2017-top-global-risks-201615723.aspx
3. Association of certified Fraud Examiners, Retrived from: http://www.acfe.com/
4. Belak, V. (2011): *Poslovna forenzika i forenzičko računovodstvo Borba protiv prevare*, Belak Excellens d.o.o. Zagreb.
5. Consideration of Fraud in a Financial Statement Audit, Retrieved from: http://www.aicpa.org/research/standards/auditattest/downloadabledocuments/au-00316.pdf
6. Consideration of Fraud in a Financial Statement Audit, Retrieved from: https://pcaobus.org/Standards/Auditing/pages/au316.aspx
7. Ferma (2016): European risk and Insurance report, Retrieved from: http:// ferma.eu/app/uploads/2016/09/FERMA-ERIR-2016_VF_26_10_2016.pdf.
8. Gao, Z., House, A. L., Xie. J. (2015): *Online Survey Data Quality and Its Implication for Willingness-to-Pay: A Cross- Country Comparison*, Canadian Journal of Agricultural Economics, 2015, John Wiley and Sons.
9. Global Forensic Data Analytics Survey 2016, Retrieved from:
10. http://www.ey.com/Publication/vwLUAssets/ey-forensic-data-analytics-survey-2016/$FILE/ey-forensic-data-analytics-survey-2016.pdf
11. Global Forensic Data Analytics Survey 2016, Retrieved from:
12. http://www.longituderesearch.com/work/global-forensic-data-analytics-survey-2016/
13. Global Forensic Data Analytics Survey 2014: Retrieved from:
14. http://www.ey.com/Publication/vwLUAssets/EY-Global-Forensic-Data-Analytics-Survey-2014/$FILE/EY-Global-Forensic-Data-Analytics-Survey-2014.pdf
15. Hopwood, W., Leiner, J. J., Young, R. G. (2014): Forenzičko računovodstvo, Izdavač: Univerzitet Singidunum, Beograd.
16. Marković, V. (2015): *Imovina i odgovornost za obaveze preduzetnika*, FINIZ Međunarodna naučna konferencija Univerziteta Singidunum, Beograd
17. Međunarodni standardi za profesionalnu praksu interne revizije (standardi), Preuzeto sa: https://na.theiia.org/translations/Public Documents/IPPF-Standards-2017-Serbian.pdf
18. McAfee Labs, (2015) : „Threats Report“, Retrieved from: https://www.mcafee.com/hk/resources/reports/rp-quarterly-threats-aug-2015.pdf.
19. Petković A.(2011). Tehnike sačinjavanja lažnih finansijskih izvještaja. Podgorica: Računovodstvo i revizija, Institut sertifikovanih računovođa Crne Gore.
20. Report to the nations on occupational fraud and abuse 2016 global fraud study, Retrieved from: https://s3-us-west-2.amazonaws.com/acfepublic/ 2016-report-to-the-nations.pdf.
21. Rezaee, Z.; Riley, R. (2010). *Financial statement fraud - Prevention and detection*. New Jersey: John Wiley and Sons
22. Rezaee, Z., (2002), Financial Statement Fraud: Prevention and Detection, New York: Wiley.
23. Samociuk, S. M., Iyer. N. (2013): Kratak Vodič kroz RIZIK OD PREVARE, Otkrivanje prevare i stvaranje otpornosti, Naslov originala A Short Guide to Fraud Risk, NORIPS, Profiprint Beograd.

24. Smith, G. S., Crumbley, D. L. (2009): How Divergent are Pedagogical Views Toward the Fraud/Forensic Accounting Curriculum? Global Perspectives in Accounting Education Vol. 6.
25. Smith, G. S., Crumbley D. L. (2009): *Defining a Forensic Audit*, Journal of Digital Forensics, Security and Law, Vol. 4(1), pp. 61-80.
26. *The National Archives, (2011):* Digital Continuity to Support Forensic Readiness, Retrieved from: http://www.nationalarchives.gov.uk/documents/ information-management/forensic-readiness.pdf
27. Vukadinović, P. (2016): *Forenzička revizija: teorijske refleksije i empirijske šeme prevara,* Revizor Vol.. XIX, No. 74, 2016, Beograd.
28. Vonya Global. (2009): Executive Survey – Strategic Plan for the Prevention and detection of fraud, Final report., pp. 4.
29. Wagner, M., Frank, P. (1986): Management Advisory Services Technical Consulting Practice Aid 7: Litigation Services, New York: AICPA.
30. William S. H., Jey J. L., George R. Y. (2014): Forenzičko računovodstvo, Izdavač: Univerzitet Singidunum, Beograd.
31. https://www.iaasb.org/
32. http://www.ferma.eu/
33. https://www.isaca.org/pages/default.aspx.
34. https://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Cybercrime-Defending-Your-Enterprise.aspx.
35. https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf
36. https://na.theiia.org/Pages/IIAHome.aspx
37. https://www.rsaconference.com/

DIGITAL FORENSICS IN ACCOUNTING AND AUDITING

Summary: Digital Forensics in terms of Accounting and Auditing refers to the ability to collect and use the data, aiming to prevent, detect, monitor and investigate potential fraud, irregularities or inconsistencies in the operation of business enterprises. Illegal digital activities are becoming more sophisticated. Forensic accounting and forensic audits must follow and use digital tools in contemporary business environment. There are no standard modes of application of digital forensics in forensic accounting and auditing areas, but they are constantly improved and stay abreast or ahead of the digital achievements in IT field.

Key words: Digital forensics, legal aspects of digital forensics, forensic accounting, forensic auditing, forensic data analysis