



UNIVERZITET SINGIDUNUM  
EPARTMAN ZA POSLEDIPLOMSKE STUDIJE

## MASTER RAD

---

# Otkrivanje prevara zaposlenih u IT sektoru

**Mentor:**

*Prof. dr Kosana Vićentijević*

**Kandidat:**

*Stanko Komarica*

Beograd, 2017. godina

## Sadržaj

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Uvod.....                                                                       | 4  |
| Predmet istraživanja.....                                                       | 5  |
| Cilj i značaj istraživanja.....                                                 | 5  |
| Hipoteze istraživanja.....                                                      | 6  |
| Metode istraživanja.....                                                        | 6  |
| Struktura istraživanja .....                                                    | 7  |
| 1    Prevare u internoj reviziji.....                                           | 8  |
| 1.1    Osnove interne revizije.....                                             | 8  |
| 1.1.1    Pojam interne revizora .....                                           | 8  |
| 1.1.2    Interni revizori .....                                                 | 9  |
| 1.2    Rizici od prevara .....                                                  | 9  |
| 1.3    Uloga interne revizije kod upravljanja rizikom.....                      | 12 |
| 1.4    Uloga internih revizora u otkrivanju prevara .....                       | 15 |
| 2    Prevare u IT sektoru.....                                                  | 17 |
| 2.1    Forenzičko računovodstvo u IT okruženju.....                             | 17 |
| 2.1.1    Pojam forenzičkog računovodstva .....                                  | 17 |
| 2.1.2    Cyber procedure za poslovno okruženje u Srbiji .....                   | 18 |
| 2.1.3    Primena forenzičkog računovodstva u IT sektoru .....                   | 23 |
| 2.2    Kompjuterski kriminal .....                                              | 25 |
| 2.2.1    Kritični nivoi računskih sistema .....                                 | 25 |
| 2.2.2    Cyber terorizam .....                                                  | 27 |
| 2.3    Primena Benfordovog zakona .....                                         | 29 |
| 3    Prevare u IT sektoru – istraživanje .....                                  | 32 |
| 3.1    Stavovi zaposlenih o prevarama u IT sektoru .....                        | 32 |
| 3.1.1    Rezultati istraživanja vezano za prevare zaposlenih u IT sektoru ..... | 32 |
| 3.1.2    Grafički i šematski prikaz rezultata .....                             | 35 |

|     |                                                                        |    |
|-----|------------------------------------------------------------------------|----|
| 3.2 | Mogućnost prevara u sklopu poslovno-računovodstvenog sistema IPIS..... | 43 |
|     | Zaključak.....                                                         | 51 |
|     | Literatura.....                                                        | 54 |
|     | Prilog – Anketa .....                                                  | 58 |

## Uvod

Da bi se obradile računovodstvene informacije u sistemu, potrebno je koristiti računar, a danas, skoro sve organizacije ga koriste. Postoji više aplikacije i sisteme koje organizacije koriste za vođenje računovodstva i revizije. Informacione tehnologije se, iz dana u dan, razvijaju što dovodi i do razvoja aplikacija i računovodstvenih programa. Što se informacione tehnologije razvijaju, to su veći i sistemski rizici, a upravljanje rizicima je jedno od važnih procesa u organizaciji.

Iako se organizacije i same žele boriti protiv prevara, sve je veći pritisak od strane nacionalnih i međunarodnih tela da se primenjuju strategije protiv rizika od prevara. Dobro mesto za početak razvijanja ove strategije je razmatranje ranijih slučajeva prevara, kako unutar organizacije, tako i van nje, a zatim da se sastavi lista elemenata koje bi trebalo ispraviti kako bi se sprečile prevare u organizacijama. Kako bi se upravljalo rizikom od prevara potrebno je da se identifikuje rizik, da se odradi tretman rizika od prevara, da se upravlja incidentima, da se meri rizik, i da se razvije organizaciona kultura. Sve ovo se odnosi na sprečavanje prevara u internoj reviziji.

Kod upravljanja rizicima u IT sektoru jako je bitna korporativna politika organizacije koju donose korporativna tela, koja istovremenu i nadziru kako se upravlja rizicima u organizaciji. Dobar plan upravljanja IT rizicima bi trebalo da sadrži niz koraka: identifikaciju rizika, procenu težine i frekvencije pojavljivanja IT rizika, utvrđivanje zaštitnih mera, dodeljivanje odgovornosti i domunetovanje IT kontrola, nadzor i reviziju plana upravljanja IT rizicima, kao i korporativni pristup IT rizicima i usklađivanje sa poslovnom strategijom.

## **Predmet istraživanja**

Predmet istraživanja u ovom radu se odnosi na prevare koje se dešavaju u organizacijama u sklopu interne revizije i IT sektora. Da bi se analizirali ovi pojmovi prvo se analizira interna revizija i rizici, jer bez upravljanja rizikom nije moguće ni sprečiti prevare niti ih identifikovati. Iz tog razloga se kroz čitav rad pominje upravljanje rizikom i u internoj reviziji i u IT sektoru. U radu ćemo istraživati kompjuterski kriminal i cyber terorizam koji je sve više pristupni iz razloga što se društvene mreže sve više razvijaju i daju mogućnost cyber teroristima da prenose propagandne poruke preko Facebook-a, Twitter-a, Instagrama ili YouTube-a. Forenzičko računovodstvo igra ulogu i u Cyber svetu. Uz pomoć forenzičkog računovodstva se mogu otkriti prevare u IT svetu, međutim, Cyber terorizam umnogome otežava da se ovaj proces odvija. Jedan od alata koji se koriste za otkrivanje anomalija digitalnim putem jeste Benfordov zakon. U radu ćemo se dotaći i primene ovog zakona.

Kako bismo došli do zaključka, obavili smo dve vrste istraživanja. Bavili smo se stavovima zaposlenih o prevarama u IT sektoru i došli smo do zaključka kako zaposleni, kao i eksterni korisnici mogu manipulirati u računovodstvenom programu IPIS, što predstavlja glavni predmet istraživanja u ovom radu, i na osnovu kojeg će se dokazati ili opovrgnuti postavljanje hipoteze.

## **Cilj i značaj istraživanja**

Cilj istraživanja je naći povezanost između prevara i rizika u internoj reviziji i IT sektoru. Značaj istraživanja je uvideti da se prevare mogu pojaviti u svim sektorima i da se rizici ne mogu otkloniti već samo minimizovati. Cilj rada je uvideti da u našoj zemlji postoje ljudi koji su čini prevare iz raznih razloga, kao i da se, u sklopu računovodstvenih programa, takođe mogu javiti razne manipulacije.

Cyber kriminal i Cyber terorizam su dva najveća problema današnjice, pogotovo iz razloga što se Internet i društvene mreže sve više razvijaju i daju velike prednosti Cyber teroristima da upravljaju našim svetom i da vrše kriminalne radnje i prevare i razne zlobne radnje. Značaj istraživanja leži u tome kako otkriti kriminalne radnje i prevare u IT sektoru, kako se odbraniti od Cyber kriminala i da li je uopšte moguće odbraniti se od Cyber kriminala.

## Hipoteze istraživanja

Glavna hipoteza: **IT sektor predstavlja sektor u kojem zaposleni mogu da vrše razne manipulacije i prevare, a alati za otkrivanje prevare nisu dovoljni da se prevare minimizuju ili zaustave.**

Sporedne hipoteze:

- 1. Interni i eksterni korisnici čine prevare u računovodstvenim programima na taj način što manipulišu podacima kako njima odgovara ili nekoj trećoj strani.*
- 2. Najveći broj prevara se vrši u IT sektoru, a razloga za to je mnogo: unapređenje na poslu, dobitak poslova u siromašnijim zemljama, spas organizacije u vreme krize, kako bi društvu bio odobren kredit i tako dalje.*
- 3. CAATT i Benfordov zakon su dva alata koja se koriste kako bi se društvo zaštitilo od prevara, međutim, tehnike i alati nisu dovoljni jer, sa druge strane, veliki broj faktora može da utiče na to da se prevara ne otkrije kao što su: zastarela tehnologija, zaposleni, nedovoljna interna kontrola, rizici i tako dalje.*
- 4. U IT sektoru postoji i veliki broj mogućnosti da se poćini prevara.*

## Metode istraživanja

U radu se koriste različite metode istraživanja: analiza, sinteza, dedukcija i indukcija. Metodom analize smo detaljno analizirali temu interne revizije i detekcije prevara u IT sektoru, Cyber kriminal i terorizam, i Benfordovu analizu. Prikupljanje podatka je bazirano na kabinetskom istraživanju (domaća, strana literatura, domaći i strani časopisi i podaci sa Interneta) i na primarnom istraživanju. Primarno istraživanje se odnosi na anketu koju je autor istražio u reviziji i računovodstvu i detekciji prevara u IT sistemu, kao i način na koji se vrši prevara u računovodstvenom sistemu IPIS.

## Struktura istraživanja

U uvodnom delu rada se govori o predmetu istraživanju, značaju i ciljevima istraživanja, hipotezama koje će se u radu opovrgnuti ili dokazati, metodama koje će se koristiti u istraživanju i strukturi drugog pristupnog rada.

Rad se sastoji iz tri celine koje bliže opisuju master rad:

1. Prevare u internoj reviziji predstavlja prvu celinu rada. U okviru ove celine daćemo glavne karakteristike interne revizije, povezanosti interne revizije sa internim kontrolama, rizike od prevara, kao i ulogu interne revizije u otkrivanju kriminalnih radnji i prevara.
2. Prevare u IT sektoru predstavlja drugu celinu rada. U okviru ove celine daćemo glavne karakteristike Internet forenzike, kompjuterske forenzike, kompjuterski kriminal i cyber terorizam koji je sve pristupni danas u svetu.
3. Prevare u IT sektoru-istraživanje predstavlja treću celinu rada. U okviru ove celine prikazano je studijsko istraživanje vezano za sprovedenu anketu u sektoru IT-a i računovodstvenom sistemu IPIS.

Nakon toga sledi zaključak u kojem se prikazuju dokazane ili opovrgnute hipoteze i literatura koja je korišćena u radu.

Nakon zaključka i literature, u prilogima, predstavljena su pitanja koja su postavljena u anketi.

## 1 Prevare u internoj reviziji

Prva glava rada se odnosi na prevare u internoj reviziji. Da bismo govorili o prevarama u oblasti informatike u internoj reviziji potrebno je da definišemo šta je to interna revizija i koja je uloga interne revizije u otkrivanju prevara. Interna revizija je povezana i sa upravljanjem rizicima i njihovim otkrivanjem, tako da ćemo se posvetiti i otkrivanju i upravljanju rizicima u internoj reviziji, što je povezano sa prevarama u organizaciji.

### 1.1 Osnove interne revizije

#### 1.1.1 Pojam interne revizora

Stanišić definiše internu reviziju kao proces u okviru organizacije koji se koristi kako bi se ispitala aktivnosti organizacije (*Stanišić, 2014, 154*). Interna revizija je nezavisna iz razloga što ne postoje obimi koje je ograničavaju ni restrikcije, a ona daje ocenu organizaciji o radu sistema i radnjama koje se dešavaju u samim sistemima. Interni revizori imaju ulogu da ispituju i ocenjuju sve radnje i aktivnosti kako bi se utvrdile određene činjenice, i na kraju ocenile, na osnovu donešenih zaključaka.

Interna revizija predstavlja nezavisnu organizacionu jedinicu u okviru organizacije koja ima za cilj da ispita i proceni delatnosti te organizacije, kao i njene poslove koje obavlja kao uslugu organizaciji. Interna revizija se uvodi u organizacije kako bi mogla njenim članovima da efikasno obavljaju sve aktivnosti u organizaciji. Samim tim, interna revizija se sastoji od analiza, procena, preporuka, saveta i informacije koje se, na osnovu delatnosti, donose i na osnovu kojih se vrši revizija. Interna revizija ispituje i procenjuje sistem internih kontrola što je povezano sa upravljanjem rizicima u organizaciji (*Stanišić, 2014, 163*).

### **1.1.2 Interni revizori**

Uloga internih revizora u organizaciji je takođe veoma bitna. Oni imaju ulogu da ispituju da li su finansijski i operativni podaci celoviti i da li su tačni, kao i da podatke identifikuju, izmere i klasifikuju, kako bi, na kraju podneli izveštaj menadžmentu (*Stanišić, 2014, 163*). Sem toga, interni revizori imaju zadatak da ispituju svaki sistem u okviru organizacije kako bi se poštovali sve politike, zakoni, postupci i planovi koji su značajni u organizaciji. Interni revizori imaju zadatak i da ispituju sve način za čuvanje sredstava, kao i da proveravaju da li ta sredstva postoje i da ocenje efikasnost i njihovu ekonomičnost. Još jedan od zadataka internih revizora je da ispituju poslove i računovodstvene programe kako bi videli da li su rezultati programa u skladu sa poslovima u okviru organizaciji i da li su ti programi sprovedeni na pravi način (*Stanišić, 2014, 163*).

Upravljanje rizikom je jedna od veoma važnih stavki koje vrše interni revizori u organizaciji. Oni imaju zadatak da ispituju i vrednuju adekvatnosti i efiksnosti internih kontrola, kao i da provere da li se sve dužnosti izvršavaju vezano za interne kontrole. Analiza i procena rizika je bitna kako bi se utvrdila pouzdanost poslovnih i finansijskih informacija kao i njihov integritet. Zaštita sredstava i pridržavanje svih regulativa, ugovora i politika u organizaciji je takođe povezana sa poslom internog revizora (*Stanišić, 2014, 164*).

## **1.2 Rizici od prevara**

Svet je prepun rizika. Pošto je rizik nešto od čega ne možemo da pobegnemo onda je najbolje da pokušamo da ga na najbolji način razumemo. Rizik se odnosi na potencijalne događaje koji mogu imati uticaj na postizanje ciljeva organizacije. Samim tim, upravljanje rizicima podrazumeva da se otkriva priroda nastanka rizičnih događaja, kao i da se pravi plan kako izbeći rizik. Prevara je rizik sa kojim se suočavaju sve organizacije, nezavisno od njihove veličine, sektora, poslovanja ili lokacije (*Samocui, Iyer, 2013, 15*).

Bankroti velikih organizacija, naslovi u novinama, kao i brojni izveštaji o poslovanju ukazuju da su prevare rasprostranjene svuda u svetu i da predstavljaju veliki problem za poslovanje organizacije. Brz razvoj informacionih i telekomunikacionih tehnologija, globalizacija, period teških ekonomskih krahova, sve ovo povećava rizik od prevara u svakom

segmentu ekonomije jedne zemlje i njenih organizacija. Prevare ugrožavaju poslovanje svake organizacija na mnoge načine i to ne samo da utiču da organizacije posluju lošije, nego to utiče na njihov ugled i moral zaposlenih. Prevara može da znači gubitak resursa i eroziju vrednosti organizacije.

Trend budućih kretanja u organizaciji, kao i analiza sadašnjeg i prethodnog stanja organizacije, kod utvrđivanja rizika u organizaciji je od velikog značaja. Ukoliko organizacija zna na koji način da upravlja rizicima onda će moći da na uspešan način realizuje sve ciljeve koje je postavila, čak i u promenjim uslovima, moći će da iskoristi sve šanse da ostvari dodatne vrednosti, kao i da izbegne sve rizike koje joj prete na tržištu u kojem organizacija posluje (*Vlaović-Begović, Ilić-Pupovac, 2012, 23*). Da bi menadžment donosio adekvatne odluke, interna revizija se mora fokusirati na proces upravljanja rizicima, jer je rizik potencijalna opasnost koja može da ugrozi da organizacija ne realizuje ciljeve na pravilan način. Organizacije mogu da prepoznaju rizik na vreme, međutim, rizik se ne može u potpunosti eliminisati, ali se može ublažiti (*Vlaović-Begović, Ilić-Pupovac, 2012, 23*).

Iako su organizacije upućene na to šta je rizik i kakve posledice može imati za organizaciju, ako se ne detektuje na vreme, organizacije i dalje nemaju sisteme i procedure da razumeju rizik, a uz to, ne znaju ni načine da otkriju rizik i da reaguju na njega. Principi upravljanja rizikom od prevare su u osnovi isti kao i principi za upravljanje bilo kojom vrstom rizika. Prvo, potencijalne posledice prevare unutar organizacije se moraju dobro razumeti. Rizik bi zatim trebalo biti smanjen razvojem i primenom strategija za upravljanje rizikom cele organizacije koja će obuhvatiti sve sektore u organizaciji (*Samocik, Iyer, 2013, 16*).

Rizik od prevare predstavlja mogućnost da zaposleni u organizaciji, menadžer ili bilo ko drugi počini prevaru koja će imati uticaj na organizaciju. Udar ili posledice prevare mogu imati pozitivni ili negativni uticaj na resurse organizacije. Ukoliko menadžeri rade u interesu organizacije onda mogu da izvrše prevaru kako bi izbegli da plaćaju poreze. Isto tako, trgovci na finansijskim tržištima mogu putem prevare oštetiti kupce kako bi poboljšali sopstveni rezultat i profit organizacije za koju rade. Finansijski ishod ovakvih prevara je privremeno pozitivan, ali uticaj na reputaciju organizacije i troškovi koji nastanu su negativni.

Jedan od osnovnih razloga nerazumevanja rizika od prevare je taj što se velika pažnja posvećuje metodama prevare a ne kako i zašto se dolazi do toga da se izvrši prevara. Do toga najčešće dolazi u organizacijama koje primenjuju okvire za upravljanje rizikom koji od menadžmenta zahteva procenu rizika od prevare zajedno sa drugim rizicima kojima je kompanija izložena i gde je fokus najvećim delom na kontroli rizika. Pošto su rizici od prevara povezani sa ljudima, ovaj rizik najviše možemo povezati sa operativnim rizikom.

Prevare, manipulacije i pronevere su nečasne radnje koje izvode svi zaposleni, počev od vrha do dna organizacione šeme poslovanja u svakoj organizaciji. Te radnje se mogu odnositi na fizičke krađe sredstva, utaju novca, primanje provizija od dobavljača, falsifikovanje, itd. Razlozi za prevare mogu biti razni, mada su to uglavnom lična materijalna korist, lični psihološki razlozi vezani za zadržavanje osećaja moći, politički uticaji, itd.

Smatra se da menadžeri i vlasnici organizacija retko kada čine prevare, ali postoje slučajevi da i oni mogu počiniti kriminalnu radnju u organizaciji. Ukoliko se otkrije da se desila prevara javnog privrednog društva u Republici Srbiji, to odmah znači da je društvo na meti medija i da cela država zna o kriminalnoj radnji koje je počinilo to društvo. U tom trenutku društvo gubi status kod investitora i ostalih stejkholdera, a njegov imidž na tržištu opada. U tabeli broj 1 se mogu videti sve vrste događaja koje mogu prouzrokovati operativne rizike.

**Tabela 1 – Vrste događaja koje mogu prouzrokovati operativne rizike**

| <b>Kategorija operativnih rizika</b>                | <b>Potkategorija</b>                               |
|-----------------------------------------------------|----------------------------------------------------|
| Interne prevare i aktivnosti                        | Neovlašćene aktivnosti                             |
|                                                     | Krađa i prevara                                    |
|                                                     | Unutrašnji sistem sigurnosti                       |
| Eksterne prevare i aktivnosti                       | Krađa i prevara                                    |
|                                                     | Spoljni sistem sigurnosti                          |
|                                                     | Druge namerne aktivnosti                           |
| Odnos prema zaposlenima i sigurnost na radnom mestu | Odnosi prema zaposlenima                           |
|                                                     | Sigurnost radnog okruženja                         |
|                                                     | Različitost i diskriminacija                       |
| Klijenti, proizvodi i poslovna praksa               | Prikladnost, transparentnost i poverljivost        |
|                                                     | Neodgovarajuća poslovna ili tržišna praksa         |
|                                                     | Greške u proizvodima i uslugama                    |
|                                                     | Selekcija, sponzorstvo i izloženost prema klijentu |
|                                                     | Savetodavne aktivnosti                             |
|                                                     | Nezgode i opšta sigurnost                          |
| Štete na fiksnoj imovini                            | Prirodne nepogode                                  |

|                                   |                                                                     |
|-----------------------------------|---------------------------------------------------------------------|
| Prekid u poslovanju i pad sistema | Katastrofe prouzrokovane ljudskim faktorom                          |
|                                   | Politički i zakonski rizik                                          |
|                                   | Neadekvatnost, neefikasnost, loše funkcionisanje ili pad IT sistema |
|                                   | Javne usluge/informacije, neraspoloživost dobavljača                |

Izvor: *Sopstvena izrada autora prema Adelsberger Z., et al., (2011), Operativni rizici kao teljem sistema upravljanja, Naučno-stručni skup „Sistem kvaliteta uslov za uspešno poslovanje i konkurentnost, Fakultet za industrijski menadžment, Unija poslodavaca Srbije Vrnjačka Banja, str. 4-5.*

Od kategorija iz tabele br. 1 za prevare zaposlenih u organizaciji se odnose interne i eksterne prevare i odnos prema zaposlenima i sigurnost na radnom mestu. Interne prevare i aktivnosti se odnose na gubitke usled namernih aktivnosti ili propusta koji uključuju najmanje jednu osobu koja radi za organizaciju ili radi u organizaciji. Eksterne prevare u organizaciji takođe predstavljaju gubitke usled namernih aktivnosti ili propusta ali od strane trećih lica. Kod eksterne prevare preovladava nameran čin. Odnos prema zaposlenima i sigurnost na radnom mestu se odnosi na gubitke usled ne primenjivanja zakona i drugih regulativa za rad, zapošljavanje, zdravstvenu i socijalnu zaštitu i sigurnost na radnom mestu.

### 1.3 Uloga interne revizije kod upravljanja rizikom

Osnovna uloga interne revizije prilikom upravljanja rizicima u organizaciji se odnosi na to da se pruže uverenja za proces upravljanja rizikom i uverenja o pravilnosti procene rizika. Jako je važno da se poznaje proces upravljanja rizicima i da se izveštava uprava o ključnim rizicima. Ako se desi da se rizik ne identifikuje onda interna revizija može da ima uloga savetodavaoca i da preporuči upravi kako da se poboljšaju procesi upravljanja rizikom i da predloži strategije bitne za proces upravljanja rizikom. Ni u kom slučaju interna revizija ne bi trebala samostalno da donosi odluke o upravljanju rizikom, niti da preuzima odgovornost za to. Uprava organizacije daje konačni sud o tome koju strategiju će organizacija koristiti da bi se odbranilo od potencijalnih rizika i za to uprava snosi odgovornost.

Kada govorimo o upravljanju rizicima u internoj reviziji tada je potrebno da znamo da postoji odeljenje interne revizije čiji je zadatak da pronade rizik, odnosno da se identifikuje i proceni rizik i koliko je organizacija podložna riziku. Zadatak odeljenja interne revizije jeste i da doprinese da se poboljša sistem kontrole. Praćenje i ocenjivanje rizika je jako važna za uspešnost poslovanja jedne organizacije. Odeljenje interne revizije treba da pronade rizike koji utiču na informacione sisteme, poslovanje i upravljanje organizacijom.

Interni revizori prvo prispituju tačnost poslovnih informacija i njihov integritet i posle procenjuju efikasnost i efektivnost poslova u okviru organizacije. To znači da interni revizori ispitivaju sve radnje koje se dešavaju u okviru organizacije i proveravaju sve programe koje organizacija koristi, na primer, da li je određeni program predstavio određene informacije tačnim i da li se svi poslovi sprovode onako kako je planiranu u organizaciji. Pored toga, revizori moraju i da budu upućeni u sisteme zaštite i programa i poslovnih radnji u organizaciji.

Interni revizori moraju da verifikuju postojanje sredstava i da ustanove, ukoliko dođe do zloupotrebe, šta je sve potrebno da se ispita i koje su se greške i nepravilnosti desile u procesima. Ovde je potrebno da interni revizori imaju određene veštine kako bi uopšte mogli da se bave ovim poslovom. Njihov zadatak je da ispituju zloupotrebu sredstava i da znaju da koriste program provere svih informacija u organizaciji. Na kraju, svi revizori moraju da se pridržavaju zakona, regulative i ugovora u okviru organizacije u kojima rade.

Izazov u internoj reviziji je potreba uprave da pomogne da se preveniraju gubici, ujedno i da se detektuju. Kako bi se ovo ostvarilo, mnogo vremena se mora odvojiti za ove, ni malo lake, aktivnosti, koje se ne mogu ni predvideti. Aktivnosti vezane za otkrivanje prevara su jedne od najvažnijih aktivnosti u organizaciji. Ukoliko sektor interne revizije radi zajedno sa drugim sektorima u detekciji i otklanjanju rizika onda se postižu ciljevi te organizacija i postiže se balan, što je bitno za organizaciju. Ne postoji organizacija koja nije izložena riziku i on zavisi od poslovnih procesa, efikasnosti internih kontrola, ako uopšte i postoje, a zavisi i od lica koja rade u organizaciji.

Najvažniji proces u otkrivanju prevara u reviziji jeste da se upotrebljavaju alati, tehnike i metode u otkrivanju, a to su fokus grupe, testiranja ili intervjui koji su vezani za oblast interne revizije. Interni revizori znaju koji su to motivi za prevare i mogućnosti i oni stalno moraju da prate procese u organizaciji, a ujedno i zaposlene, pošto su oni ti koji čine kriminalne radnje. Ukoliko interni revizore primete da se nešto čudno dešava ili u poslovnim procesima ili programima oni odmah obavljaju procenu rizika.

Upravljanje rizikom se vrši od top menadžmenta. Interni revizor je u obavezi da daje svoje mišljenje direktoru računovodstva svim aktivnostima i radnjama u okviru organizacije i o upravljanju rizikom i kontroli rizika u organizaciji. Uloga direktora je da bude odgovoran da se sistem interne kontrole održava i stalno unapređuje. Ukoliko postoji dobro okruženje u organizaciji, stalne provere internih kontrola i drugih procesa, onda se rizik može minimizirati, ali je jako teško da rizik ne postoji.

Jedan od najvećih problema jeste dovoljna neupućenost revizora u određene poslovne procese. U Republici Srbiji interna revizija nije dovoljno razvijena, a ukoliko interni revizor radi onda ima jako malo informacija o prevarama i rizicima, a danas postoji veliki broj prevara u organizaciji i van nje. Ocena rizika je jako bitna, a interni revizori su ti koji moraju imati znanja i veštine upravljanja i minimizovanja rizikom kroz proces ocene rizika i internih kontrola u organizaciji.

Slaba interna kontrola je jedan od najčešćih faktora povećanja rizika u organizacijama. U preduzećima u Srbiji postoji jako malo poverenje u zaposlene, a nema ni odgovarajućih procedura za ovlašćenje određenih lica, a i uspostavljanje podele dužnosti je jako slabo. Ovo dovodi da se počine prevare u preduzećima. Sem toga, veliki broj preduzeća u Srbiji nema etički kodeks poslovanja jer u organizaciji vlada loša korporativna kultura i etika. Sem toga, obuka je jako slaba i krizama se upravlja na nepravilan način. Postoji još mnogo razloga zašto se rizik od prevara povećava, a naši interni revizori moraju da se mnogo edkuju i da unapređuju veštine i znanja da bi mogli na pravi način da pristupe ovom „problemu“.

Pomenuli smo da je ocena rizika jako bitna. Odgovornost revizora je da identifikuje prevare, ali može biti teško locirati tragove i znati gde ih treba tražiti. Ocena rizika je sredstvo koje može da pomogne revizorima da otkriju prevare, a tri elementa procene rizika su (*Stanišić, 2014, 353-354*): identifikacija, merenje i određivanje prioriteta rizika.

*Identifikacija rizika* podrazumeva utvrđivanje rizika gde revizori traže procese koji su izloženi riziku, a jedan od načina identifikacije je upitnik interne kontrole za svaki poslovni proces.

*Merenje rizika* podrazumeva da se mernim sredstvima analizira prioridte rizika od prevare u područjima u kojima revizor posluje. Najteži deo kod procesa merenje rizika jeste ocenjivanje rizika, i ono se može meriti putem nekoliko metoda. Jedna od metoda merenja utvrđivanje zajedničkih faktora koji su uočljivi i merljivi. Svaki proces se zatim boduje prema snazi ili slabosti faktora korišćenjem skale od 1 do 9. Ti faktori, na primer, mogu biti odabrani prema vrednosti, uticaju na poslovanje ili prema kontrolnom okruženju.

*Određivanje prioriteta kod rizika* podrazumeva utvrđivanje odgovarajućih resursa za upravljanje tim rizikom. Menadžeri daju ocene određenim rizicima ako koriste metod utvrđivanja zajedničkih faktora. Na primer, na skali od 1 do 3 se smatra da je nizak rizik i to znači da postoji ali potencijal značajnog negativnog uticaja na prihode, kapital, stabilnost ili ugled. Na skali od 4 do 6 je umeren rizik i to znači umeren potencijal negativnog uticaja na prihode, kapital, stabilnost ili ugled. I na kraju, visok rizik podrazumeva ocene od 7 do 9 i to podrazumeva veliki potencijal za ozbiljan i znatan uticaj na prihode, kapital, stabilnost ili ugled organizacije.

#### **1.4 Uloga internih revizora u otkrivanju prevara**

Interni revizori mogu otkriti kriminalne radnje koje mogu uticati na kvalitet, integritet i pouzdanost finansijskih izveštaja. Interna revizija, ima prednost u sprečavanju i otkrivanju brojnih zloupotreba, u odnosu na nezavisnu reviziju. Iako je nezavisna revizija tradicionalno smatrana odgovornom za otkrivanje kriminalnih radnji, interni revizori su u najboljoj situaciji da obave tu ulogu. Oni se smatraju prvom linijom odbrane od nezakonitosti. Međutim, kriminalna radnja se često čini od višeg rukovodstva i u tim okolnostima interni revizori nailaze na prepreke u ispunjavanju svojih dužnosti i tada izbegavaju da se upuste u otkrivanje kriminalnih radnji (*Petković, 2010, 69*).

Da bi interni revizor bio uspešan u sprečavanju kriminalnih radnji onda on mora da pregleda svu dokumentaciju u organizaciji i da proveriti istinitost, tačnost i verodostojnost svih dokumenata, mora da zahteva sve izveštaje i objašnjenja od uprave, zaposlenih i da pregleda imovinu organizacije. Jedna od njihovih glavnih uloga jeste da pospeše interne kontrole i da organizacija napravi bolju poslovnu strategiju i da se napravi najbolja strategija upravljanja rizicima i internim kontrolama kako bi se smanjio rizik i smanjile prevare i mogućnosti za obavljanje kriminalne radnje u organizaciji.

Interni revizor mora da ima određeni nivo znanja kako bi identifikovao indikatore prevare, međutim, od internih revizora se može očekivati da budu stručni kao i forenzičke računovođe i forenzički revizori. Obaveze internog revizora u pogledu otkrivanja prevare uključuje odgovarajuća znanja, veštine i iskustvo u ovoj oblasti (*Stanišić, 2014, 356-357*).

Faktori koji doprinose prevari i dozvoljavaju prevaru se odnose na neefektivne interne kontrole, na dogovor zaposlenih koji podležu nedovoljnim kontrolama, kao i postojanje likvidnih sredstava u organizaciji (*Stanišić, 2014, 356-357*). Kada smo identifikovali koji su to faktori koji mogu doprineti da se dese prevare, sad ćemo identifikovati koji su to znaci koji upućuju na mogućnost prevara, navešćemo samo neke od njih (*Stanišić, 2014, 357*):

- Uzajmljivanje malih iznosa od kolega sa posla
- Unovčavanje ličnih čekova – nedatiranih ili postdatiranih
- Lični čekovi unovčeni ili vraćeno na nepropisan način
- Poverioci koji se pojavljuju na radnom mestu i preterana upotreba telefona da bi se poverioci izbegli
- Izraženo kritikovanje drugih kako bi se sumnja skrenula na njih
- Odgovaranje na pitanja nerazumnim objašnjenjima
- Igre na sreću u formi koja prevazilazi mogućnosti podnošenja gubitka
- Preterana sklonost piću, noćni život ili druženje sa sumnjivim ljudima, i tako dalje.

Interni revizori su odgovorni za otkrivanje prevara. Prvo, oni moraju da poseduju dovoljno znanja o prevarama, manipulacijama i kriminalnim radnjama. Oni moraju da poznaju sistem interne kontrole i ostalih kontrola i procesa u organizaciji. Oni takođe moraju da znaju da procene odgovarajuće pokazatelje koji pokazuju da je prevara mogla da bude počinjena i da odluče dalje procese i da li će se sprovesti istraga. Na kraju, njihova dužnost je da obaveste sve organe u organizaciji ukoliko dođe do istrage.

## 2 Prevare u IT sektoru

Prevare u IT sektoru predstavljaju drugu glavu rada. Ovaj deo rada objasniće ulogu forenzičkog računovodstva u sektoru informacionih tehnologija, kompjuterski kriminal i obradiće metodu i tehniku koja se bavi otkrivanjem prevara kao digitalni alat za otkrivanje prevara u finansijskim izveštajima – Benfordova analiza.

### 2.1 Forenzičko računovodstvo u IT okruženju

#### 2.1.1 Pojam forenzičkog računovodstva

Postupci, tehnike i metode koje se koriste kako bi se utvrdilo da li je došlo do prevara, malverzacija ili krađe u računovodstvenim postupcima i reviziji spada u forenzičko računovodstvo. Sem toga, forenzičko računovodstvo utvrđuje da li je došlo do pogrešnog prikazivanja ili promene u finansijskim izveštajima, da li je došlo do mita i korupcije u organizacijama ili u pojedinim sektorima u organizacijama, da li je došlo do kriminalnih radnji koje se tiču pranja novca, krađe, falsifikovanja finansijskih izveštaja, falsifikovanja hartija od vrednosti, da li je došlo do krivotvorenja, da li je došlo do iznuđivanja, i tako dalje (*Belak, 2001, 41-42*).

Prema autorima Hoopwood-u, Leiner-u i Young-u forenzičko računovodstvo predstavlja primenu istraživačkih i analitičkih veština sa ciljem rešavanja finansijskim pitanjima na način koji je u skladu sa standardima koje zahtevaju sudovi. Forenzičko računovodstvo se ne odnosi samo na finansijske istrage koje se sprovode u svrhu veštačenja u pravnim postupcima, već se odnose i na istrage za potrebe računovodstva, revizije, finansija i drugih delatnosti (*Hoopwood, et al., 2014, 4-5*).

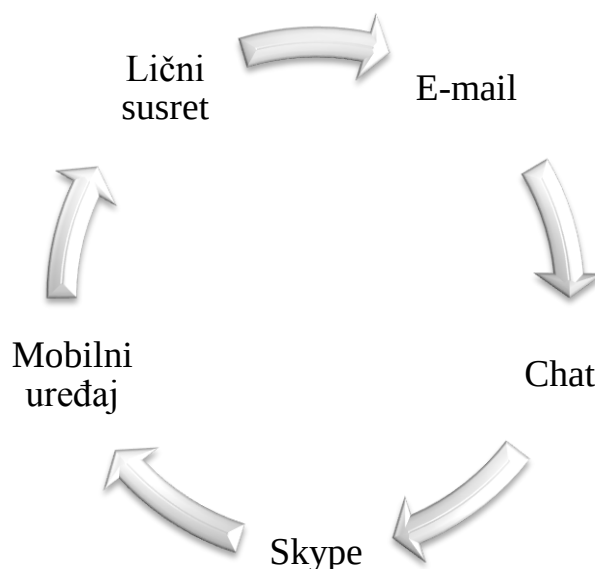
Takođe, važno je istaći da definicija forenzičkog računovodstva ne upućuje izričito na prevaru, iako istrage prevara čine deo forenzičkog računovodstva. Prevara je posledica obmane, namernog delovanja ili nedelovanja kako bi se ostvarila neka korist. Forenzičko računovodstvo obuhvata širi opseg od ispitivanja prevara; ono takođe uključuje usluge u vezi sa kupovinom preduzeća, procenom vrednosti imovine stečene u braku u slučaju razvoda, određivanjem vrednosti štete nanete poslovnoj imovini i izračunavanjem izgubljenog profita (Hoopwood, et al., 2014, 5).

Forenzičke računovođe predstavljaju lica koja poseduju profesionalna znanja iz oblasti kriminalnih radnji, što ukazuje na to da forenzičke računovođe moraju da poznaju znakove i simbole upozorenja, sve vrste šemi koje se pojavljuju u kriminalnom postupku, kao i druge naznake i „trendove“ koje se javljaju u vezi sa kriminalnim radnjama. Forenzičke računovođe moraju da prate i organizacije koje se bave otkrivanjem kriminalnih radnji, da poznaju druge forenzičke računovođe i prikupljaju dokaze, poseduju sertifikat iz oblasti računovodstva i revizije, ujedno i forenzike. Forenzičke računovođe moraju da poseduju i znanja iz drugih oblasti, kao što su statistika, matematika, ekonomije, finansije, informatika, istraživačke veštine i tako dalje. Oni se moraju konstantno unapređivati tako što posećuju seminare i konferencije na temu otkrivanja kriminalnih radnji i prevara kako u finansijskim izveštajima, tako i van profesije računovodstva i revizije.

### ***2.1.2 Cyber procedure za poslovno okruženje u Srbiji***

U preduzećima u Republici Srbiji cyber kriminal je veoma „popularan“. Zaposleni mogu da iznesu poverljive podatke iz preduzeća na nekoliko načina. Preduzeća nemaju bezbednosne provere i puštaju neautorizovane ljude u svoj sistem. Način da se podaci iznesu iz preduzeća su prikazani na dijagramu 1.

Dijagram 1 – Iznošenje poverljivih podataka iz preduzeća



*Izrada autora prema: Đekić M. D., (2016), Cyber procedure za poslovno okruženje u Srbiji, Tehnika, vol. 71, br. 3, str. 471.*

Načini da se podaci iznesu iz preduzeća su putem imejla tako što zaposleni, preko svoj ličnog imejla, primaju razne informacije koje mogu da budu štetne za vlasnika preduzeća. Da bi se vlasnik preduzeća zaštitio od ove vrste iznošenja podataka jeste da iznese svojim zaposlenima Kodeks ponašanja u cyber smislu i da se uvedu razne vrste kontrolnih testova i anketa kako bi se zaposleni proveravali.

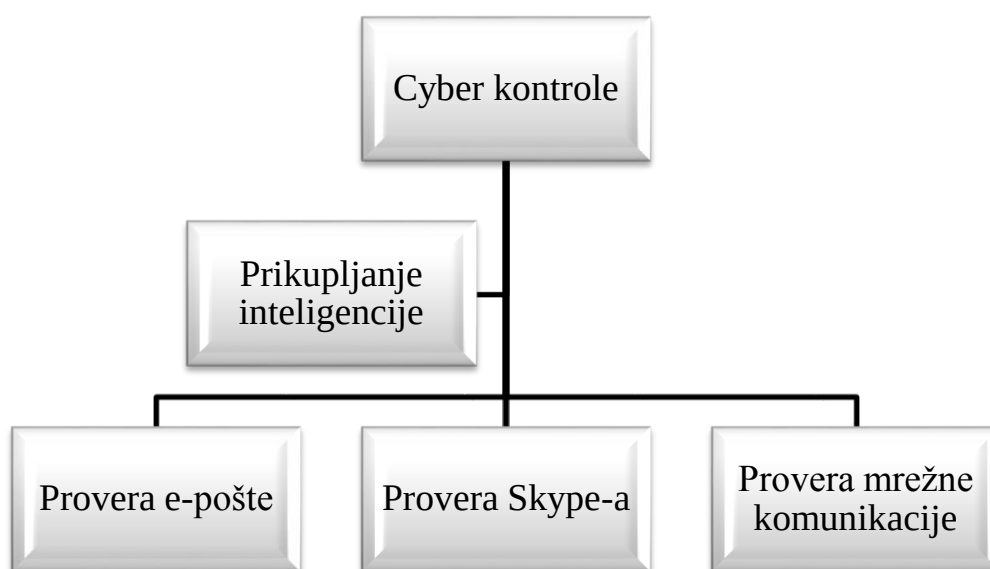
Putem chata na društvenim mrežama ili drugim portalima, zaposleni mogu da održavaju privatnu komunikaciju i da iznose poverljive informacije o vlasniku preduzeća, o trenutnoj situaciji o preduzeću i tako dalje. Vlasnici preduzeća ne mogu lako doći do otkrivanja ovakvih informacija, ali, mogu, kao i u prethodnom slučaju da iznesu svojim zaposlenima Kodeks ponašanja u cyber smislu i da se uvedu razne vrste kontrolnih testova i anketa kako bi se zaposleni proveravali.

Putem Skype-a, zaposleni takođe mogu da prenose informacije iz preduzeća, što može da bude rizično za vlasnika preduzeća. Mere prevencije u ovom slučaju su iste kao i kod prethodna dva slučaja. Zaposleni mogu putem mobilnih uređaja da prenose informacije iz preduzeća. Mere prevencije su veoma nezgodne u ovom slučaju, ali vlasnik može da odradi rutinske kontrole. Na kraju, zaposleni mogu da prenose poverljive informacije putem ličnih

susreta sa privatnim kontaktima iz svog života, tj. trećim licima. Ovo je najteži slučaj za proveru da li je došlo do iznošenja informacija iz preduzeća. Mere prevencije su iste kao i kod prethodnih načina iznošenja podataka iz preduzeća.

Da bi se vlasnici preduzeća zaštitili od ovakve vrste prenošenja informacija i podataka iz preduzeća, oni mogu organizovati cyber provere, tj. cyber kontrolu. Neke od cyber kontrola prikazaćemo u dijagramu 2.

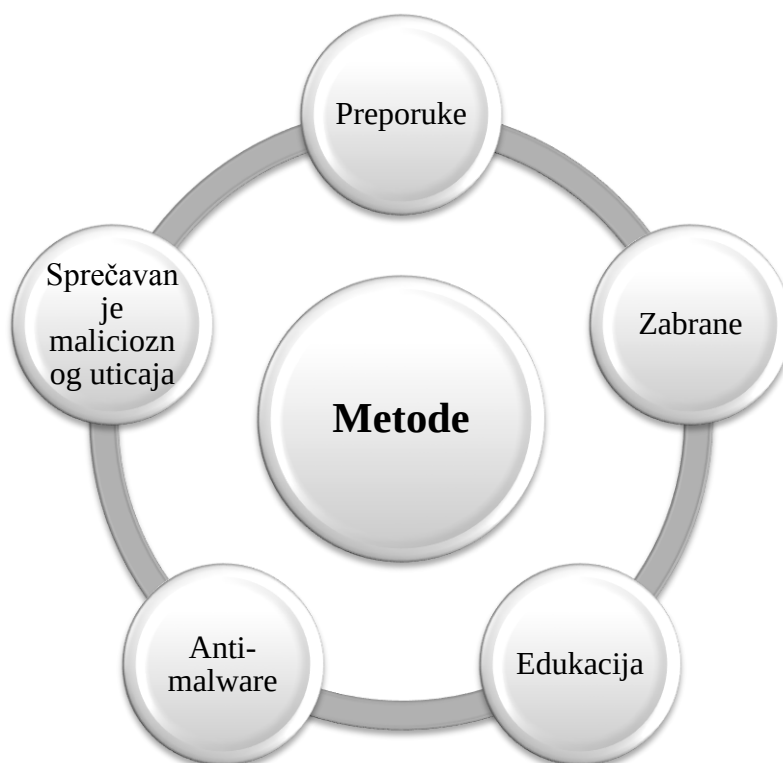
Dijagram 2 – Metode sprovođenja cyber kontrole u preduzeću



Izvor: Izrada autora prema: Đekić M. D., (2016), *Cyber procedure za poslovno okruženje u Srbiji*, Tehnika, vol. 71, br. 3, str. 472.

Cyber metode za kontrolu u preduzećima u Srbiji se sprovode proverom imejla, Skype-a i mrežnih komunikacija. Vlasnici preduzeća i menadžment moraju stalno da proveraju poslovne imejlove svojih zaposlenih kako bi mogli da otkriju da li zaposlene daju podatke o preduzećima trećim stranama, kao i da li se bave kriminalnim radnjama i prevarama. Sem toga, na taj način se proverava način na koji se komunicira interno u preduzeću i radna etika zaposlenih. Provera Skype-a podrazumeva uvođenje rutinskih kontrola Skype profila zaposlenih kako bi preduzeća bezbedno funkcionisala. Na kraju, vlasnici i menadžeri proveravaju i mrežne komunikacije, ukoliko dođe do određenih grešaka u mrežnom sistemu ili ukoliko dođe do namernih grešaka od strane zaposlenih. Kako bi se izbegle brige i cyber rizici, u preduzećima se vrši ispitavanje zaposlenih, sprovode se ankete, prave se kvizovi sa posebnim pitanjima kako bi se zaposleni kontrolisali.

Dijagram 3 – Metode preventivnog delovanja



Izvor: Izrada autora prema: Dekić M. D., (2016), *Cyber procedure za poslovno okruženje u Srbiji*, Tehnika, vol. 71, br. 3, str. 473.

Preporuke predstavljaju jednu od metoda od cyber zaštite. One podrazumevaju da vlasnici preduzeća izdaju i prate preporuke o tome kako treba bezbedno poslovati, kako upravljati rizikom i minimizovati rizike u preduzeću i na koji način sprečavati greške u poslovnom procesu. Preporuke se daju vezano za zaštitu i odabir lozinke. Lozinke koje sadrže mrežni sistemi ili bilo koji sistem u preduzeću, moraju biti veoma jake i moraju sadržati veliki broj različitih karaktera (kombinacija brojeva, znakova i velikih i malih slova) kako bi hakerima bilo što teže da upadnu u sistem. Preporuke se daju i u smislu da zaposleni ne stupaju u kontakt sa neovlašćenim licima, kao i da prijave svaku vrstu cyber incidenta, jer ukoliko ne prijave, zaposleni moraju preuzeti rizike na sebe i da „plate“ štetu.

Kada govorimo o zabrani, onda se odnosi na to da se zaposlenima zabranjuje da dele poverljive podatke o trećim licima vezano za bilo koje procese u preduzeću. Vlasnici i menadžeri stalno strahuju od toga da će zaposleni preneti važne informacije o preduzeću trećim licima koja mogu iskoristiti informacije protiv vlasnika i menadžmenta preduzeća. Vlasnici

preduzeća i menadžment mogu zabraniti zaposlenima da, tokom radnog dana, ne koriste mobilne telefone, komunikacione softvere, da ne dovode nezaposlena lica u preduzeća, i tako dalje.

Edukacija zaposlenih podrazumeva da zaposleni moraju imati osnovnu obuku vezano za cyber zaštitu kao i da idu na što više konferencija i seminara koji se tiču ove teme. Zaposleni moraju imati znanja o tome kako zaštititi program od neželjnih upada u sistem, kao i na koji način da kreiraju lozinku i da bezbedno koriste poslovni računar. Jedan od načina zaštite je korišćenje anti-malware zaštite.

Na kraju, zaposleni moraju da vode računa koga dovode u preduzeće, u smislu, ako se pojavila treća osoba koja želi da posluje sa preduzećem. Treća osoba može biti opasna za preduzeće, ukoliko se zaposleni dogovorio sa tom osobom da kompromituju preduzeće ili da maliciozni zaposleni sprečava vlasnika preduzeća ili menadžment da zaposle treće lica u preduzeće. Svi pomenuti vidovi su prisutni u Republici Srbiji.

Najveća pretnja sistemima jeste hakovanje. Kako u svetu, tako i u našoj zemlji postoje hakerske grupe koje, na ilegalan način, prodaju proizvode i usluge na „crnom“ tržištu, upadaju u tuđe računare, prave izmene, preuzimaju informacije i podatke iz računara i napuštaju isti sistem. U današnje vreme, hakovanje je podignuto na mnogo veći nivo, jer su hakeri inteligentno koordinisati i finansijski motivisani. Pomoću kriminalnih aktivnosti, putem online mreže, hakeri zarađuju novac. To nije samo čist upad u računar da pojedinca zbine i ukradu poneki podatak, Hakovanje je način zarađivanja. Hakerske grupe koriste određene komunikacione kanale kako bi međusobno kontaktirali i kako bi prodavali/kupovali proizvode i usluge, ili organizovali cyber akciju. Bezbednosim službama je veoma teško da otkriju hakere (Đekić, 2016, 762).

### 2.1.3 *Primena forenzičkog računovodstva u IT sektoru*

Pre nego što govorimo u značaju i primeni forenzičkog računovodstva u IT sektoru, potrebno je spomenuti Internet forenziku. Internet forenzika podrazumeva sve vrste pretraga i sakupljanja dokaza kako bi se istražile nezakonite ranje i aktivnosti od strane grupa ili pojedinaca, kao i da se osmisle sistemi zaštite na Internetu kako bi se smanjio kompjuterski kriminal. Kod Internet forenzike je veoma teško odrediti kad je ona nastala i u kojem mestu je nastala, ali se počeci Internet forenzike vezuju sa SAD-om. Internet forenzika predstavlja noviju disciplinu koja je počela da se razvija krajem osamdesetih godina prošlog veka, ali je ulaskom u novi milenijum, ova disciplina zaživela (*Antoliš, 2010, 122*).

S obzirom na snažno i komplementarno povezivanje računovodstva i informacionih tehnologija, kao i činjenicu da su informacioni sistemi postali paradigma funkcionisanja računovodstvenih procesa, posebno je važno prepoznati kompjutersku forenziku koja postaje predmet rada i interesovanja računovodstvene profesije u celini. Slede definicije najvažnijih pojmova u IT okruženju (*Mikerović, 2013, 193-194*):

- **Forenzika računanja** – *Computational Forensics* (CF) koja se odnosi na to da se vrše kompjuterske simulacije, analiziranja, prepoznavanja, kao i proučavanja i rešavanja situacija u raznim forenzičkim procesima. Forenzičari koji koriste ovu vrstu forenzike moraju da budu stručnjaci u IT sektoru i moraju poznavati forenzičku nauku.
- **Cyber forenzika** predstavlja analizu kompjuterskih medija kako bi se došlo do informacija i podataka, a da se pritom, pouzdanost podataka u kompjuterskim medijama ne naruši.

Kada govorimo o kompjuterskoj forenzici onda bi trebalo da analiziramo forenzički proces. On se sastoji od pripremanja, sakupljanja, ocenjivanja, analize i izveštavanja. Istraživač bi trebao da ima određena znanja i veštine kako bi mogao da vrši forenzičke procese u IT sektoru. Forenzičari u informatici bi trebalo da poznaju softverske alate koji služe kako bi se generisali izveštaji za sud. Ti alati se koriste u zavisnosti od slučaja do slučaja i ima veliki broj alata u istrazi. Ovo se odnosi na proces pripremanja.

Digitalna evidencija može da bude sakupljena iz različitih izvora kao što su digitalne kamere, telefoni, hard diskovi, računari, CD ROM, i tako dalje. Kada se rukuje digitalnim evidencijama forenzičari moraju biti veoma pažljivi pogotovo kada rukuju računarima. Mnoge

digitalne informacije su lake za menjanje, a čim se promene onda je jako teško da se detektuju. Ono što se radi u ovim slučajevima jeste kalkulacija kriptografskog *hash*-a, što znači transformaciju koja uzima jedan ulaz i vraća jedan *string* – niz fiksne veličine, koji se zove *hash* vrednost. To podrazumeva da se evidencija jednog fajla kalkuliše i nakon toga zapisuje u računarima istraživača i jedino tako se može evidencija uspostaviti.

Neke od najvrednijih informacija dobijenih u toku forenzičke ocene mogu doći do korisnika računara. Intervju sa korisnicima može da donese korisne informacije oko konfiguracije sistema, aplikacija, ključeva enkripcije i metodologije. Forenzička analiza je mnogo lakša kada analitičar ima odobrene pristupe od korisnika enkriptovanih fajlova, sadržajima i mrežnim serverima.

Sve digitalne evidencije moraju biti analizirane radi utvrđivanja tipa informacija koje su memorisane. Za tu svrhu se koriste specijalizovani alati koji mogu da prikažu informacije u korisnom formatu za istraživače kao što su manuelno razmatranje, razmatranje materijala na medijumima, razmatranje *windows* registra za sumnjive informacije, otkrivanje i „razbijanje“ lozinki (Mikerović, 2013, 194). Kada se završi analiza onda se generiše forenzički izveštaj koji je uglavnom u pisanoj formi, mada može biti i u formi usmenog svedočenja, ili se može kombinovati i jedan i drugi pristup.

Kada smo odredili forenzički proces u IT okruženju potrebno je videti koliko je pouzdano koristiti računovodstvene podatke u IT sektoru. To podrazumeva da se zaštiti računarska oprema, programi i podaci od uništenja kao posledice hardverskih, softverskih i ljudskih grešaka, kao i zloupotrebe računara. Računarski sistemi su osetljivi na mogućnost neovlašćene upotrebe. Što je veća baza podataka veći je i rizik korišćenja informacija. Online sistemi imaju mnogo terminala i prenos podataka se vrši putem elektronske mreže. Povezani terminali su ranjiviji od samostalnih mikroračunara, jer je sistemu moguće pristupiti sa većeg broja lokacija. Neovlašćena osoba koja ima pristup udaljenom terminalu i koja poznaje lozinke, lako može pristupiti sistemu i izvršiti zloupotrebu. Stoga je revizora zainteresovan za razmatranje strukture i funkcionisanja sistema i ugrađenih kontrolnih mehanizama (Mikerović, 2013, 198).

## 2.2 Kompjuterski kriminal

Kako se razvijao Internet, a sa njim i telekomunikacione tehnologije, sve više je došlo do toga da se povećava broj korisnika na Internetu, kao i na društvenim mrežama. Povećanje broja korisnika je dovelo do povećanja kriminalnih radnji koje se učestalo dešavaju na elektronskoj mreži. Kompjuterski kriminal označava da neovlašćena osoba „upada“ u kompjuterski sistem drugog lica kako bi zloupotrebila podatke o transakcijama, interne podatke, i podatke sa kreditnih kartica ili iz računovodstvenih sistema kompanija koje se bave računovodstvo i revizijom (*Petrović, 2010, 245*).

Kompjuterski kriminal se značajno razlikuje od tradicionalnog obavljanja kriminalnih radnji. Pre svega, na Internetu, tj. na elektronskoj mreži, svako ko ima kompjuter i Internet može da se bavi kriminalnim radnjama, bilo da je ovlašćeni ili neovlašćeni korisnik. Kriminalna radnja na elektronskoj mreži se može izvršiti sa bilo kojeg mesta, u bilo koje vreme i sa bilo koje vrste kompjutera ili pametnog uređaja (pametni telefoni, tableti i slično). Elektronska mreža predstavlja automatizovani ambijent i brzina protoka informacija doprinosi da se kriminalne radnje dešavaju veoma brzo, a da je potrebno dosta vremena da se otkrije da je uopšte došlo do kriminalne radnje. Kada neautorizovana lica obavljaju kriminalnu radnju, ona ne ometaju rad kompjuterskog sistema, pa je rizik obavljanja kriminalne radnje na elektronskoj mreži sveden na minimum.

### 2.2.1 Kritični nivoi računskih sistema

U funkcionisanju računarskog sistema postoji pet osnovnih nivoa koji u stvari predstavljaju kritične tačke sa stanovišta zaštite od kompjuterskog kriminaliteta, jer je na svakom od tih nivoa računarski sistem podložan kriminalnim radnjama. Ti kritični nivoi su: ulaz, izlaz, programiranje, upotreba i prenos. S obzirom na ranjive tačke svakog kompjuterskog informacionog sistema (KIS), kompjuterskih kriminal se može pojaviti: u fazi ulaza, u fazi izlaza, u fazi programiranja, u fazi upotrebe i u fazi prenosa.

Faza ulaza podrazumeva da zaposleni unose podatke u kompjuter i prilikom ulaza oni mogu da ubacuju lažne slogove, da menjaju i brišu podatke, kao i da uklanjaju ključne ulazne dokumente. Zaposleni ovo rade kako bi generisali falsifikovani platni spisak ili kako bi povećali platu ili broj radnih časova i slično.

Faza izlazi podrazumeva da se kriminane radnje ispoljavaju u vidu krađe raznih vrsta podataka, planova, poslovnih tajni i slično i karakteristično za ovu fazu jeste da su tu upletena i treća lica koja nisu zaposlena u organizaciji. Faza programiranja kao treća faza podrazumeva da je greška svedena na minimum, a ako se desi da programeri pogreše onda se može automatski otkriti taa greška. Programeri mogu da zamene taj program ,da izbrišu značajne instrukcije, da ga modifikuju i slično. Jedna od najpoznatijih tehnika koja se ovde ističe je „trojanski konj“.

Faza upotrebe predstavlja sledeću fazu gde se upotrebljava matični računarski sistem od strane neovlašćenih osoba. Zaposleni u organizaciji mogu da koriste računar za obavljanje privatnih poslova a da troškove prebacuju na račun organizacije. Faza prenosa je peta faza u kojoj se mogu maskirati podaci, prikriti kanali prenosa i tako dalje.

Kao i kod interne revizije i kod kompjuterskog kriminala postoje rizici kojima je potrebno upravljati. Upravljanje rizikom u IT sektoru se vrši tako što se prvo identifikuju informaciona sredstva, zatim se vrši kvantitativno i kvalitativno izražavanje pretnji, nakon toga se procenjuje ranjivost sistema. Posle toga dolazi do otklanjanja nedostataka kontrole i na kraju se upravlja tekućim rizicima. Standardi koji regulišu upravljanje rizicima u IT sektoru su: CobiT, ITIL, ISDO 27001, Val IT, Basel II, SarbanesOxley i drugi zakonski okviri.

Kao i kod računovodstva, revizije i drugih delatnosti, kompjuterski kriminal se izvršava kada se spoje tri elementa i to приметni pritisak, приметna mogućnost i pravdajući stavovi. Примerni pritisak podrazumeva razlog zašto nastaje kompjuterski kriminal. Usled dramtičnog rasta potrebe za gotovim novcem, ukoliko organizacije žele da se spoje ili ukoliko jedna organizacije želi da preuzme drugu, i sličnih razloga dolazi do toga da se vrši kompjuterski kriminal. Kada se uvodi nova tehnologija, ako postoje složeni informacioni sistemi ili ukoliko se prenosi veliki broj podataka tada se stvaraju приметne mogućnosti da se vrši kompjuterski kriminal. I na kraju, ukoliko se приметi da postoje transakcije između nepoznatih subjekata ili ukoliko se приметi da postoji udaljenost između kupaca i dobavljača to može biti opravdajući stav zašto se vrši kompjuterski kriminal.

Na kraju, ono što nas najviše interesuje jeste kakve tehnike, metode i alati postoje da bi se sprečio kompjuterski kriminal. Interne kontrole u organizaciji se mogu koristiti kako bi se ublažio rizik ako govorimo o aktivnosti elektronskog plaćanja, na primer. Ako revizor uvede interne računovodstvene kontrole, kontrole pristupa kompjuterskom sistemu i ako se uvede zaštita od neovlašćenog pristupa i upada sa računarskih mreža, to su načini da se spreči kompjuterski kriminal.

Sem ovih načina, u praksi postoje dva alata i to CAATT i Benfordov zakon u forenzičkom računovodstvu. Prilikom izbora odgovarajućeg CAATT alata, računovođe i interni revizori bi trebalo da razmotre nekoliko osnovnih, još uvek aktivnih i bitnih karakteristika koje opredeljuju izbor CAATT alata. CAATT alati su laki za korišćenje, laki za ekstrakciju podataka, sposobni da pristupaju širokim varijantama baza podataka sa različitih platformi, sposobni da integrišu podatke sa različitim formatima, sposobni da definišu polja i selekcija iz standardnih formata, i tako dalje. U nastavku sledi detaljna analiza Benfordovog zakona.

### **2.2.2 Cyber terorizam**

Cyber terorizam je danas sve prisutniji, a države se nemoćno bore protiv ovog vida kriminala, iz razloga što je Internet postalo veoma moćno sredstvo i oružje. Internet i računare ekstremne organizacije koriste kako bi prisluškivale, ometale rad sistema, postavljali različite viruse, ugrožavale indentitet i poverljivost i dostupnost podataka na elektronskoj mreži. Cyber teroristi mogu da upadnu u računarsku mrežu i da naprave pravi kolaps u funkcionisanjih državnih institucija. Teroristi mogu da ugroze svet, ako se dobro edukuju i imaju adekvatnu IT obuku (Awan, 2014, 3, prema: Jonev, 2016, 212).

U fizičkom svetu, teroristi imaju za cilj da nanesu fizičke povrede i da izazovu smrt, dok cyber teoristi imaju za cilj da napadaju ekonomiju i privrednu jedne zemlje, tj. da ugroze njeno vitalno poslovanje i delovanje. Cyber teroristi, u cyber prostoru, mogu da plasiraju kompromitujuće fotografije, viode snimke, propagandni materijal, mogu da blokiraju sajtove državnih institucija, tj. mogu da urade sve on što bi zaplašilo jednu zemlju i ugrozilo njene stanovnike.

Cyber teroristi najviše koriste propagandu kao glavnu aktivnost cyber terorizma. Smatra se da postoji nekoliko hiljada terorističkih sajtova koji podržavaju Al Kaidu i islamski

terorizam. Uz pomoć Interneta i društvenih medija, islamske organizacije mogu da veoma lako stupe u kontakt sa svojim sledbenicima, i to mogu da rade uspešno upravo putem propagande. Cyber teroristi medijima šalju razne snimke medijima kako čine sva zlodela. Snimcima treba samo nekoliko minuta da obidu čitavu planetu. Islamska država koriste društvene medije kako bi napravila „revoluciju“. Najpoznatije društvene mreže koje koriste su Twitter, Facebook, YouTube i Instagram za širenje terorizma i video klipova sa uznemirujućim sadržajima (Jonev, 2016, 213).

Islamska država se obraća svetskoj publici, u odnosu na Al Kaidu koja prenosi poruke samo istomišljenicima. Islamska država koristi društvene mreže i Internet jer je svesna da su to dobri komunikacioni kanali distribucije za prenos uznemirujućih sadržaja koje će videti ceo svet. Grupa distribuira različite propagandne materijale na različitim jezicima i na različitim Internet portalima i društvenim mrežama kako bi povećala svoju grupu i imala „obožavatelje“. Putem Interneta, ova grupa regrutuje nove članove i širi se iz dana u dan. Islamska država koriste posebne kanale koji su zaštićeni i za koje su potrebne da se kriju IP adrese, lozinke, koriste šifrovane poruke i tako dalje.

**Tabela 2 – Prednosti cyber prostora za terorističke aktivnosti**

|                                                                                                                |                                                              |                                         |                                                             |
|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------|-------------------------------------------------------------|
| Nepostojanje fizičkih granica                                                                                  | Brzo i momentalno delovanje                                  | Niski troškovi                          | Nemogućnost utvrđivanja da li je napad nameran ili slučajan |
| Nemogućnost utvrđivanja da li je greška ili problem nastao u računarskom sistemu ili su ljudi napravili grešku | Cyber napad se ne može naslutiti, ne može se čuti ni osetiti | Nije jednostavno otkriti cyber napadača | Lokacija nepoznata                                          |
| Cyber oružje je jednostavno za korišćenje i svima dostupno, ekonomično i efikasno                              | Sposobnost da se reprodukuje i distribuira širom sveta       | Lak pristup elektronskoj mreži          | Sakrivanje IP adrese, šifrovani podaci                      |

Izvor: Izrada autora prema: Jonev K., (2016), *Sajber terorizam i upotreba sajber prostora u terorističke svrhe*, Bezbednost, vol. 58, br. 2, str. 206-222.

## 2.3 Primena Benfordovog zakona

Benfordov zakon jeste alat koji se primenjuje u otkrivanju prevara i lažiranih transakcija i njegova upotreba je doživela ekspanziju tek razvojem IT-a i koristi se digitalnom analizom za otkrivanje anomalija sa brojevima. Kako se pojavio problem ispravnosti finansijskih izveštaja tako se i dešavalo da nisu postojale određene regulative, sve dok se nisu pojavili Međunarodni računovodstveni i revizorski standardi, koje se Srbija obavezala još od 2004. godine da će ih primenjivati i od tad je Srbiji lakše da prazi poslovanje stranih kompanija i njihovih ćerki kompanija, međutim, sami standardi ne mogu da regulišu sve segmente računovodstva i revizije i napravio se prostor za pronevere i prevare i tu stupa Benfordov zakon u otkrivanju tih prevara.

Pre nego što su računari i kalkulatori bili popularni, naučnici su se oslanjali na logaritamske tablice i mogli su jednostavno i brzo da izračunaju određene pojave koje su bile važne u astronomiji, tako da je poznati američki astronom *Simon Newcomb* primetio da su početne stranice u logaritamskim tablicama istrošenije od ostalih stranica. Ono što je poznati astronom zaključio jeste da se prva cifra najviše ponavlja i to ga je dovelo da zaključka da je verovatnoća pojave cifre  $d$  kao prve cifre nekog podatka jednaka  $\log_{10}(1+d) - \log_{10}(d)$ , za sve  $d \in \{1,2,\dots,9\}$ . Ovaj isti fenomen je primetio i poznati fizičar *Frank Benford* koji je detaljnije istražio ovu pojavu na različitim skupovima kao što je površina reke, veličina stanovništva, itd., i po njemu Benfordov zakon dobija ime.

U praksi prikupljene numeričke podatke, danas se matematički modeliraju slučajnim varijablama. Ako se slučajna varijabla označim sa  $X$ , a njena prva značajna cifra sa  $D_1(X)$ , ove oznake se mogu iskoristiti da se iskaže Benfordov zakon. Benford je jednostavno pretpostavio da će verovatnoća pojavljivanja značajne cifre zadovoljavati iskaz  $P(D_1(X) = d) = \log_{10}(1 + 1/d)$ , za sve  $d \in \{1,2,\dots,9\}$  (*Basrak, et al., 2003, 1-6*).

Benfordov zakon je moguće primeniti na bilo kojoj prirodnoj populaciji, bilo da se radi o konvertibilnim markama, dolarima, jenima, kilogramima i slično. Benfordov zakon podrazumeva da brojevi pretpostavljaju relativnu veličinu sličnih objekata, kao što je neto prihod, obim trgovine, ili posmatranje neke gradske populacije.

Tabela 3 – **Prikaz frekvencije pojavljivanja prve cifre po Benfordovom zakonu**

| Prva cifra | Frenkfencija pojavljivanja |
|------------|----------------------------|
| 1          | <b>0,30103</b>             |
| 2          | 0,17609                    |
| 3          | 0,12494                    |
| 4          | 0,09691                    |
| 5          | 0,07918                    |
| 6          | 0,06695                    |
| 7          | 0,05799                    |
| 8          | 0,05115                    |
| 9          | <b>0,04576</b>             |

Izvor: *Mikerević D., et al., (2013), Forenzika poslovanja, Banja Luka, str. 220.*

Mikerović i njegovi saradnici su utvrdili da se kod Benfordove analize pojedine cifre ponavljaju u istim frekvencijama, kao i da se frekvencije smanjuju kako se povećava broj cifara. Ono, do čega su takođe došli ovi autori, to je da cifra koja počinje sa brojem 1, putem Benfordove analize, pokazuje verovatnoću ponavljanja od 30,1%; dok se ponavljanje cifre sa brojem 2 prikazuje sa verovatnoćom od 17,6%. To znači da 47,7% posmatranog skupa cifara imaju prve cifre koje su bile 1 ili 2 (*Mikerović, 2013, 220*).

Analize dobijene na osnovu Benfordovog zakona uključuju da, ako brojevi nisu pratili Benfordov zakon, tada je moguće uočiti abnormalnosti koje se događaju sa podacima, što može da bude osnovan razlog za uspostavljanje posebnog revizorskog procesa za detekciju tih abnormalnosti, odnosno mogućih prevara. Mogućnosti savremenih kompjutera čine da je primenu ovog zakona prilično lako sprovesti u različitim oblastima poslovanja.

Interni revizori i forenzičke računovođe koriste Benfordovu analizu kako bi se utvrdilo šta je dovelo do „praznina u podacima“ u finansijskim izveštajima. Interni revizori nemaju veštine otkrivanja prevara u finansijskim izveštajima, međutim, ukoliko uoče sumnjive transakcije ili sumnjive iznose na pozicijama u bilansima, mogu da menadžmentu prijave da sumnjaju u objektivnost finansijskih izveštaja. Programi koje koriste interni revizori za sprovođenje kontrola i utvrđivanje i kontrolisanja rizika u organizaciji nisu dovoljni za otkrivanje prevara kako u samoj organizaciji, tako i u finansijskim izveštajima. Benfordov zakon je upravo jedan od programa koji interni revizori mogu da koriste kako bi došli do odgovora da li je došlo do manipulacije sa transakcijama, kao i da se dođe do odgovora da li je došlo do slučajne greške u izveštajima.. Ono što je bitno prihvatiti kao objektivnu realnost je da se primenom Benfordovog zakona testira 100% transakcija jedne populacije, tako da se njegovom primenom, shodno revizorskim standardima i zahtevima, obezbeđuje pokrivenost,

analizu rizika, pristup uzrokovanju i ispunjenje zahteva protiv kriminalne radnje (*Mikerović, 2013, 221*).

Alati digitalne analize utemeljeni na Benfordovom zakonu u današnje vreme se uključuju u mnoge popularne softver pakete koji se reklamiraju, a forenzičar računovođa može i samostalno da oblikuje softver. Budući da je potencijalni trošak neotkrivene prevare visok, forenzičar računovođa koji koristi ovu tehniku mora voditi računa da ne preceni pozdanost takvih testova. Iako takvi testovi imaju puno prednosti, potrebno je istaknuti i određena ograničenja. To se posebno odnosi na (*Belak, 2011, 196*): statistički rezultati testa se moraju interpretirati veoma oprezno, Benfordova analiza treba biti primenjena samo na račune koji se podudaraju sa Benfordovom distribucijom i forenzičar računovođa mora biti svestan činjenice da izvesni tipovi prevara neće biti pronađeni ovom analizom.

Hipoteza koju bi ovde dokazali je: *Benfordova analiza predstavlja alat koji se koristi kako bi se detektovale prevare u različitim oblastima poslovanja koje ne zahtevaju specijalizovani i skup softver.*

### **3 Prevare u IT sektoru – istraživanje**

Prevare u IT sektoru predstavljaju studijsko-istraživačku glavu rada. U okviru ove glave rada odradićemo dva istraživanja. Prvo istraživanje će se odnositi na stavove zaposlenih o prevarama u IT sektoru, dok će se drugo istraživanje odnositi na otkrivanje prevara u računovodstvenom sistemu IPIS.

#### **3.1 Stavovi zaposlenih o prevarama u IT sektoru**

Metodom studije slučaja i ankete došlo se do toga da se odradi istraživanje vezano za prevare zaposlenih u IT sektoru u Republici Srbiji, gde su ispitanici morali da odgovore na određena pitanja vezano za prevare u IT sektoru. Ispitanici su zaposleni koji rade u različitim privrednim društvima u našoj zemlji čija je odluka bila da ne otkrivaju u kojim društvima rade, niti koje su njihove pozicije u tim društvima. Anketa je sprovedena u mesecu septembru 2016. i obuhvata 70 ispitanika, od kojih su 48 muškarci, a 22 žene. Ispitanicima je postavljeno 10 pitanja. Rezultati i zaključci istraživanja biće prikazani u nastavku rada. Anketa se nalazi u prilogu na kraju rada.

##### **3.1.1 Rezultati istraživanja vezano za prevare zaposlenih u IT sektoru**

*Pitanje br. 1: Pol: muški/ženski*

Rezultati odgovora na pitanje br 1.: 48 muškaraca, 22 žene.

*Pitanje br. 2: Da li se nekada počinili prevaru: Da/Ne*

Rezultati odgovora na pitanje br. 2: 56% odgovorilo da, 44% odgovorilo ne

*Pitanje br. 3: Ukoliko ste naveli na, navedite razloge zbog kojih je opravdano da organizacija ili pojedinac izvršiti kriminalnu radnju ili prevaru?*

Rezultati odgovora na pitanje br. 3:

- Ukoliko postoji pritisak treće strane od koje zavisi organizacija da se učini usluga od treće strane koje ima korist 30%
- Spas organizacije u vreme krize 25%
- Želja da se nađe posao u siromašnim zemljama 20%
- Kada organizacija želi da privuče investitore i akcionare i kako bi banke odobrile kredite 10%
- Želja za unapređenjem na poslu 15%

*Pitanje br. 4:* Ukoliko ste naveli Da, navedite razloge zbog kojih ste počinili prevaru?

Rezultati odgovora na pitanje br. 4:

- Želja za bogatstvom 30%
- Neadekvatna plata ili kašnjenje plate 25%
- Neplaćenje zaposlenima 25%
- Gubitak lične imovine 15%
- Mobing nad zaposlenima 5%

*Pitanje br. 5:* Koje od navedenih razloga smatrate da se najviše koriste kao podsticaj da se desi prevara: Neefektivna interna kontrola; Dogovor između zaposlenih koji podležu nedovoljnoj kontroli; ili Postojanje likvidnih sredstava, kao što je gotovina, hartije od vrednosti na donosioca ili lako utrživa roba?

Rezultati odgovora na pitanje br. 5:

- Neadekvatna interna kontrola 56%
- Dogovor između zaposlenih koji podležu nedovoljnoj kontroli 39%
- Postojanje likvidnih sredstava 5%

*Pitanje br. 6:* Ukoliko ste počinili prevaru, navedite u kojim sektorima ste to najviše činili?

Rezultati odgovora na pitanje br. 6:

- IT 42%
- Računovodstvo i revizija 25%
- Finansije 18%

- Marketing 15%

*Pitanje br. 7:* Obzirom na to da se sve više prevara dešava u IT sektoru, navedite mogućnosti zbog kojih mislite da se najveći broj prevara dešava u ovom sektoru?

Rezultati odgovora na pitanje br. 7:

- Informacije dostupne neovlašćenim korisnicima 3%
- Znatno proširen prostor kriminalnog delovanja 2%
- Skraćeno vreme kriminalnog delovanja, s obzirom na automatizovani ambijent, čija brzina sprečava nadzor i upravljanje 5%
- Postojanje veštih tehnika i metoda koje se izvršavaju istim mehanizmima, kao i zakonite, ne ostavljaju tragove, niti ometaju redovan rad sistema 25%
- Postojanje stabilnosti rizika, s obzirom da se jednom izgrađen modus može veoma dugo koristiti, sa potpuno istim, niskim, rizikom otkrivanja 25%
- Sve jednostavnije mogućnosti upotrebe kompjuterske tehnologije od strane sve većeg broja korisnika, kojima više nije nužno ni posebno tehničko obrazovanje 35%

*Pitanje br. 8:* Navedite koje tehnike koristi društvo u kojem ste zaposleni da bi se zaštitilo od prevara u IT sektoru?

Rezultati odgovora na pitanje br. 8:

- CAATT 78%
- Benfordov zakon 22%

*Pitanje br. 9:* Da li smatrate da su tehnike koje Vaše društvo koristi dovoljno tehnika i alat da se zaštite od prevara? Da/Ne

Rezultati odgovora na pitanje br. 9: Svi ispitanici odgovori NE.

*Pitanje br. 10:* Navedite razloge zašto ste dali odgovor Da/Ne?

Rezultati odgovora na pitanje br. 10:

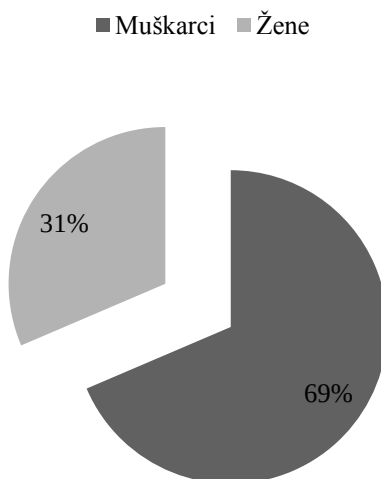
- Stari IT programi 25%

- Zaposleni ne vrše dovoljno kontrola 20%
- Zaposleni namerno govore da programe, koji rade, ne vrše dobro posao 30%
- Nedovoljan interna kontrole 27%
- Razne vrste rizika 8%

### 3.1.2 Grafički i šematski prikaz rezultata

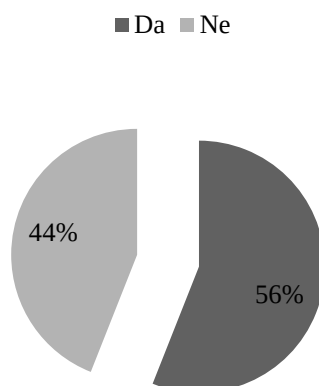
Prvo pitanje se odnosi na pol: ispitano je 48 muškaraca i 22 žene, što se u procentima vidi na dijagramu.

Dijagram 4 – Pol ispitanika



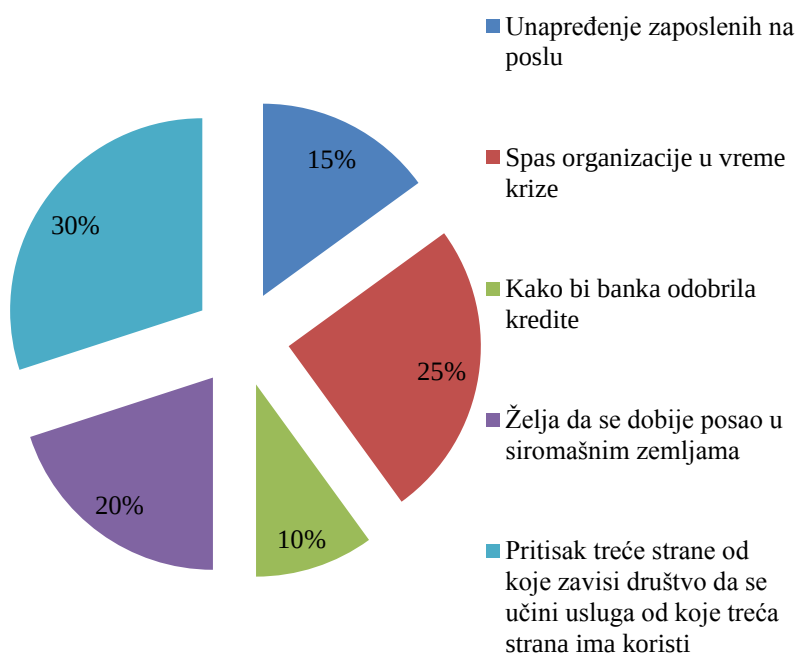
Izvor: Izrada autora

Drugo pitanje se odnosilo na to da li su zaposleni ikada počinili prevaru - 56% njih je odgovorilo da, a 44% odgovorilo ne. Odgovori se mogu videti na dijagramu 4.

Dijagram 5 – **Da li se ikada počinili prevaru?**

Izvor: *Izrada autora*

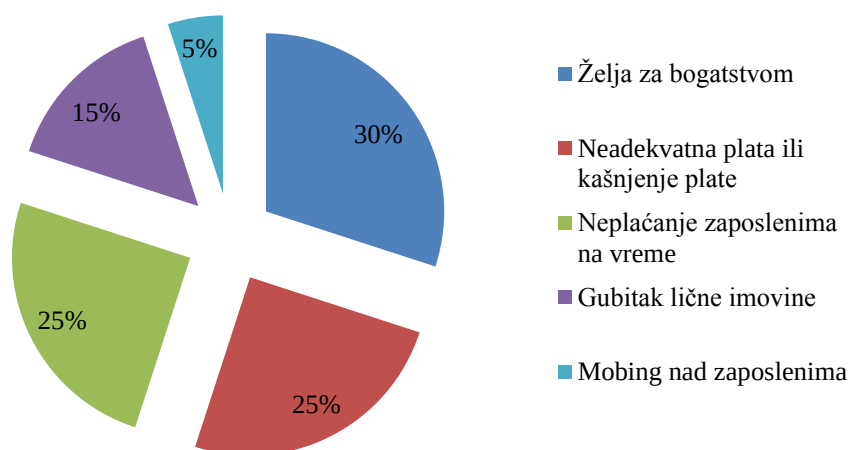
Treće pitanje se odnosilo na to da, zaposleni koji nisu počinili prevaru da navedu razloge, zbog kojih je, po njima, opravdano da organizacija ili pojedinac izvršiti kriminalnu radnju ili prevaru?

Dijagram 6 – **Razlozi za prevaru koju su naveli ispitanici koji nikada nisu počinili prevaru**

Izvor: *Izrada autora*

Ispitanici koji su odgovorili potvrdno na treće pitanje su, u četvrtom, naveli 5 glavnih razloga zbog čega su pribegavali kriminalnim radnjama, a to su: neplaćanje prekovremenog rada i neplaćanje rada uopšte, neadekvatna plata ili kašnjenje plate, gubitak lične imovine, želja za bogatstvom i mobing nad zaposlenima.

Dijagram 7 – **Odgovori ispitanika u %**

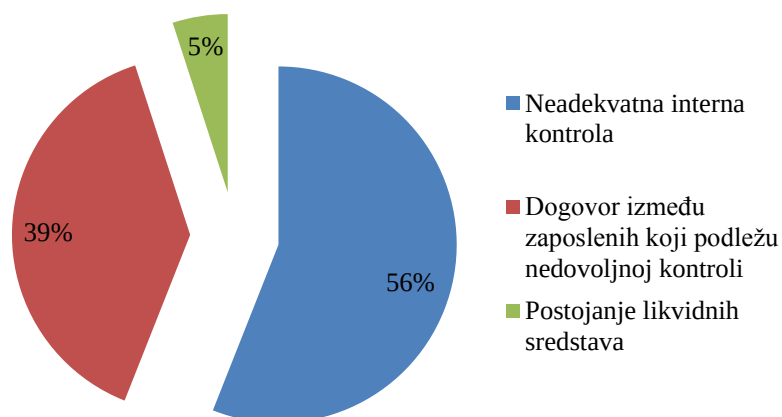


Izvor: *Izrada autora*

Ispitanicima je postavljeno pitanje da od ponuđenih odgovora odaberu jedan zbog kojih oni smatraju šta se najviše koristi kao podsticaj da se desi prevara u organizaciji. Pitanje koje je postavljeno i ponuđeni odgovori: Koje od navedenih razloga smatrate da se najviše koriste kao podsticaj da se desi prevara:

- Neefektivna interna kontrola
- Dogovor između zaposlenih koji podležu nedovoljnoj kontroli
- Postojanje likvidnih sredstava, kao što je gotovina, hartije od vrednosti na donosioca ili lako utrživa roba

Dijagram 8 – Razlozi zbog kojih ispitanici smatraju da se najviše koriste kao podsticaj da se desi prevara

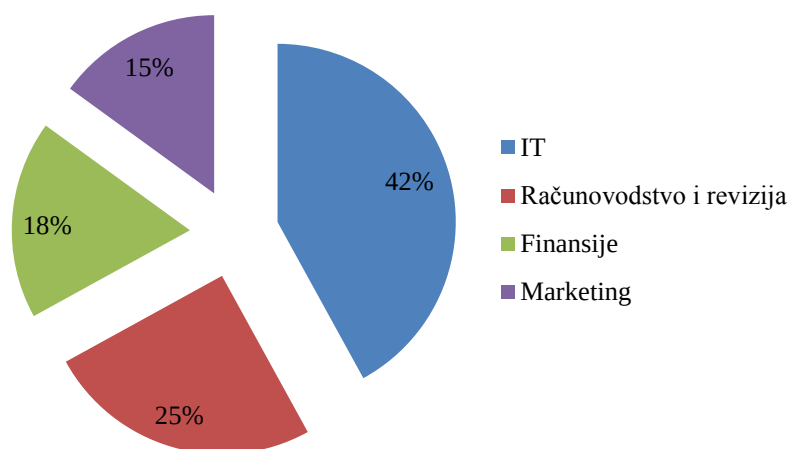


Izvor: Izrada autora

Najveći broj ispitanika je odgovorilo (56%) da je najčešći razlog zbog kojih ispitanici smatraju da se najviše koriste kao podsticaji da se desi prevara neadekvatna interna kontrola u organizacijama. Nakon toga 39% njih smatra da je jedan od podsticaja dogovor između zaposlenih, dok samo 5% njih smatra da je podsticaj za počinjenje prevare postojanje likvidnih sredstava, kao što je gotovina, hartije od vrednosti na donosioca ili lako utrživa roba.

Naredno pitanje koje smo postavili ispitanicima tiče se toga, da ukoliko su počinili prevaru, da navedu u kojim su to sektorima najviše činili. Na narednom dijagramu se vide rezultati.

Dijagram 9 – Sektori u kojima su ispitanici najviše izvršili prevara

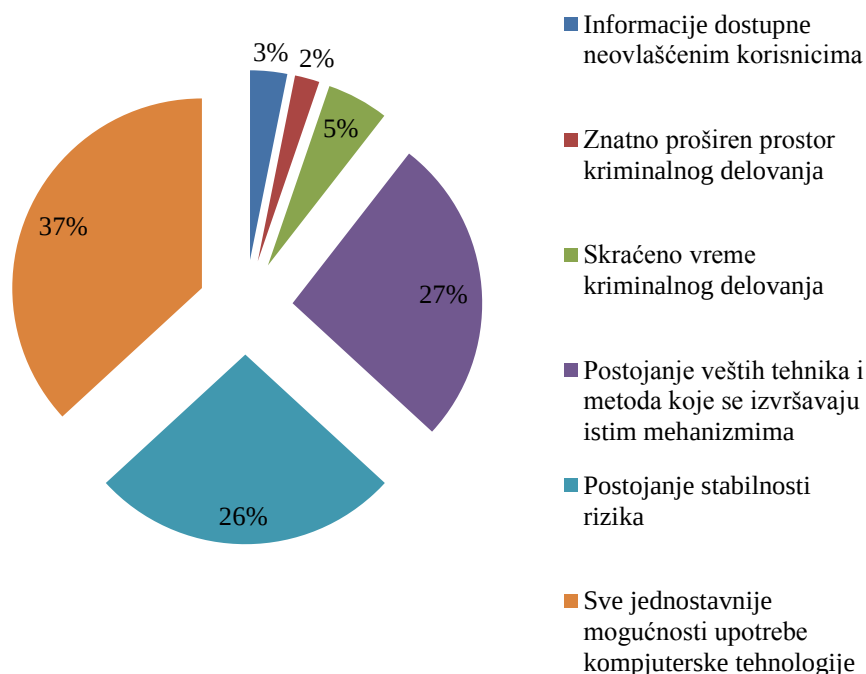


Izvor: Izrada autora

Najveći broj ispitanika (42%) je odgovorio da su najviše prevara počinili u IT sektoru, zatim u sektoru računovodstva i revizije (25%), zatim u sektoru finansija (18%) i najmanje u sektoru marketinga (15%).

Obzirom na to da se sve više prevara dešava u IT sektoru, zatražili smo od ispitanika da navedu mogućnosti zbog kojih misle da se najveći broj prevara dešava u ovom sektoru? Odgovori koji su naveli su sledeći, a na dijagramu se može videti kako su odgovori raspoređeni

- Informacije dostupne neovlašćenim korisnicima 3%
- Znatno proširen prostor kriminalnog delovanja 2%
- Skraćeno vreme kriminalnog delovanja, s obzirom na automatizovani ambijent, čija brzina sprečava nadzor i upravljanje 5%
- Postojanje veštih tehnika i metoda koje se izvršavaju istim mehanizmima, kao i zakonite, ne ostavljaju tragove, niti ometaju redovan rad sistema 25%
- Postojanje stabilnosti rizika, s obzirom da se jednom izgrađen modus može veoma dugo koristiti, sa potpuno istim, niskim, rizikom otkrivanja 25%
- Sve jednostavnije mogućnosti upotrebe kompjuterske tehnologije od strane sve većeg broja korisnika, kojima više nije nužno ni posebno tehničko obrazovanje 35%.

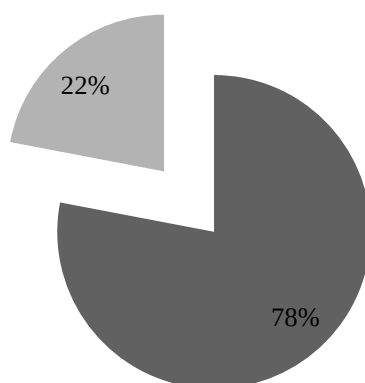
Dijagram 10 – **Mogućnosti zbog kojih dolazi do prevara u IT sektoru**Izvor: *Izrada autora*

Kao što možemo videti, 37% ispitanika smatra da je kompjuterska tehnologija sve jednostavnija za korišćenje i da i nestručna lica mogu da upravljaju tehnologijom, čime čine ilegalne radnje još jednostavnijim. Postojanje veštih tehnika i metoda koje se izvršavaju istim mehanizmima kao i zakonite se takođe posmatraju kao mogućnosti za počinjenje prevare u IT sektoru i to misli 27% ispitanika, 26% ispitanika misli da zbog postojanja stabilnosti rizika može doći do kompjuterske prevare. Mali procenat ispitanika misli da skraćeno vreme kriminalnog delovanja, informacije dostupne neovlašćenim korisnicima i znatno proširen prostor kriminalnog delovanja predstavljaju mogućnosti koje zaposleni mogu da iskoriste u kompjuterskom kriminalu.

Pitali smo ispitanike, koje od sve metode najčešće koriste u borbi protiv prevara. Njih 78% je odgovorilo da koristi CAATT alat, dok je njih 22% odgovorilo da koristi Benfordov zakon u otkrivanju kriminalnih radnji u IT sektoru, što se vidi na narednom dijagramu.

Dijagram 11 – **Koje metode koristite u borbi protiv prevare u IT sektoru**

■ CAATT alat   ■ Benfordov zakon

Izvor: *Izrada autora*

Na pitanje broj 9: Da li smatrate da su tehnike koje Vaše društvo koristi dovoljne da se zaštite od prevara? – svih 70 ispitanika odgovorilo ne. U narednom pitanju smo ih zamolili da nam napišu koji su to razlozi za njihov odgovor, a naredni dijagram prikazuje odgovore koje su ispitanici naveli.

Dijagram 12 – **Razlozi zbog kojih alati i tehnike nisu dovoljni da se društvo zaštiti od prevara u IT sektoru**

*Izvor: Izrada autora*

Ispitanici smatraju da većina društava koriste stare IT programe kako bi se zaštitili od prevara (25%). Oni takođe smatraju da zaposleni ne vrše dovoljno kontrola (10%), kao i da zaposleni namerno govore da programe, koji rade, ne vrše dobro posao, samo iz razloga kako se ne bi koristili da se otkrije prevara koju su zaposleni počinili (30%). Nedovoljna interna kontrola (27%) i razne vrste rizike (8%) takođe su razlozi koje su ispitanici naveli kao razloge zbog kojih alate, tehnike i metode nisu dovoljne da se otkriju prevare.

Ono što možemo zaključiti iz istraživanja je sledeće:

Najveći broj prevara se vrši u IT sektoru, a razloga za to je mnogo: unapređenje na poslu, dobitak poslova u siromašnijim zemljama, spas organizacije u vreme krize, kako bi društvu bio odobren kredit i tako dalje. CAATT i Benfordov zakon su dva alata koja se koriste kako bi se društvo zaštitilo od prevara, međutim, tehnike i alati nisu dovoljni jer, sa druge strane, veliki broj faktora može da utiče na to da se prevara ne otkrije kao što su: zastarela tehnologija, zaposleni, nedovoljna interna kontrola, rizici i tako dalje. U IT sektoru postoji i veliki broj mogućnosti da se počinu prevara, kao što su: visoka koncentracija na malom prostoru, prethodno proverenih i uređenih podataka, dostupnih kako ovlašćenim, tako i neovlašćenim korisnicima; znatno proširen prostor kriminalnog delovanja, koji za razliku od tradicionalnih vidova kriminaliteta, ne zahteva prisustvo izvršioca na mestu izvršenja kriviminalne radnje; skraćeno vreme kriminalnog delovanja, s obzirom na automatizovani ambijent, čija brzina sprečava nadzor i upravljanje; postojanje veštih tehnika i metoda koje se izvršavaju istim mehanizmima, kao i zakonite, ne ostavljaju tragove, niti ometaju redovan rad sistema, pa je samim tim, mogućnost otkrivanja svedena na najmanju meru, a u pojedinim slučajevima ograničena samo na otkrivanje u trenutku izvršenja kriminalne radnje; postojanje stabilnosti rizika, s obzirom da se jednom izgrađen modus može veoma dugo koristiti, sa potpuno istim, niskim, rizikom otkrivanja; sve jednostavnije mogućnosti upotrebe kompjuterske tehnologije od strane sve većeg broja korisnika, kojima više nije nužno ni posebno tehničko obrazovanje, proširuje krug mogućih izvršilaca kriminalnih radnji kompjuterskog kriminala, tako da je sve teže utvrditi njihovu tipologiju i karakteristike s obzirom na brzinu obrade podataka i raznovrsne mogućnosti njihovog ukrštanja i povezivanja.

### 3.2 Mogućnost prevara u sklopu poslovno-računovodstvenog sistema IPIS

IPIS predstavlja poslovno-računovodstveni sistem (ERP) koji mnoge kompanije, kako u Republici Srbiji, tako i u regionu koriste za robno i materijalno knjigovodstvo, finansijsko knjigovodstvo, POS, vrše obračun plata, formiraju putne naloge, vrši se blagajničko poslovanje i tako dalje. Prednosti sistema su sledeće (*dostupno na: <http://www.ipsoft-tg.com/ipis-poslovni-sustav>, preuzeto dana 15.10.2016.*):

- Stabilna i moćna platforma
- Funkcionalnosti preuzete iz Office paketa
- Copy/Paste stavka, polja
- Kloniranje svih obrazaca
- Automatski prenosi u finansijsko, KUF/KIF, platni promet, blagajnu, obračun plata, i tako dalje
- Uvoz/Izvor u Excel, Word, Pdf, i tako dalje, slanje mailom,
- Uvoz/Izvoz podataka u drugu bazu/aplikaciju
- Celokupan kod napisan od strane IPSof-a po trenutno važećim Zakonima i propisima
- Potpuno funkcionalna DEMO VERZIJA.

U nastavku slede slike koje prikazuju na koji način se može doći do prevara u okviru programa IPIS.

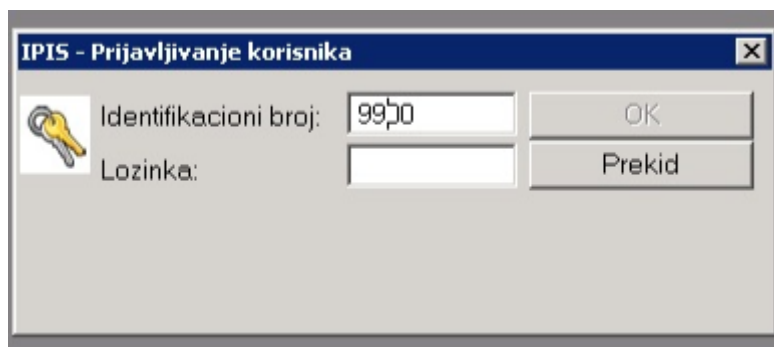
Slika 1 – **Integralni poslovni informacioni sistem**



Izvor: *Izrada autora*

IPIS je program koji obuhvata sve radne operacije jednog proizvodnog preduzeća ili preduzeća koje vrši usluge. Obuhvata računovodstvo, finansije, blagajnu i praktično sve što je vezano za procese. Program mogu koristiti svi tipovi preduzeća.

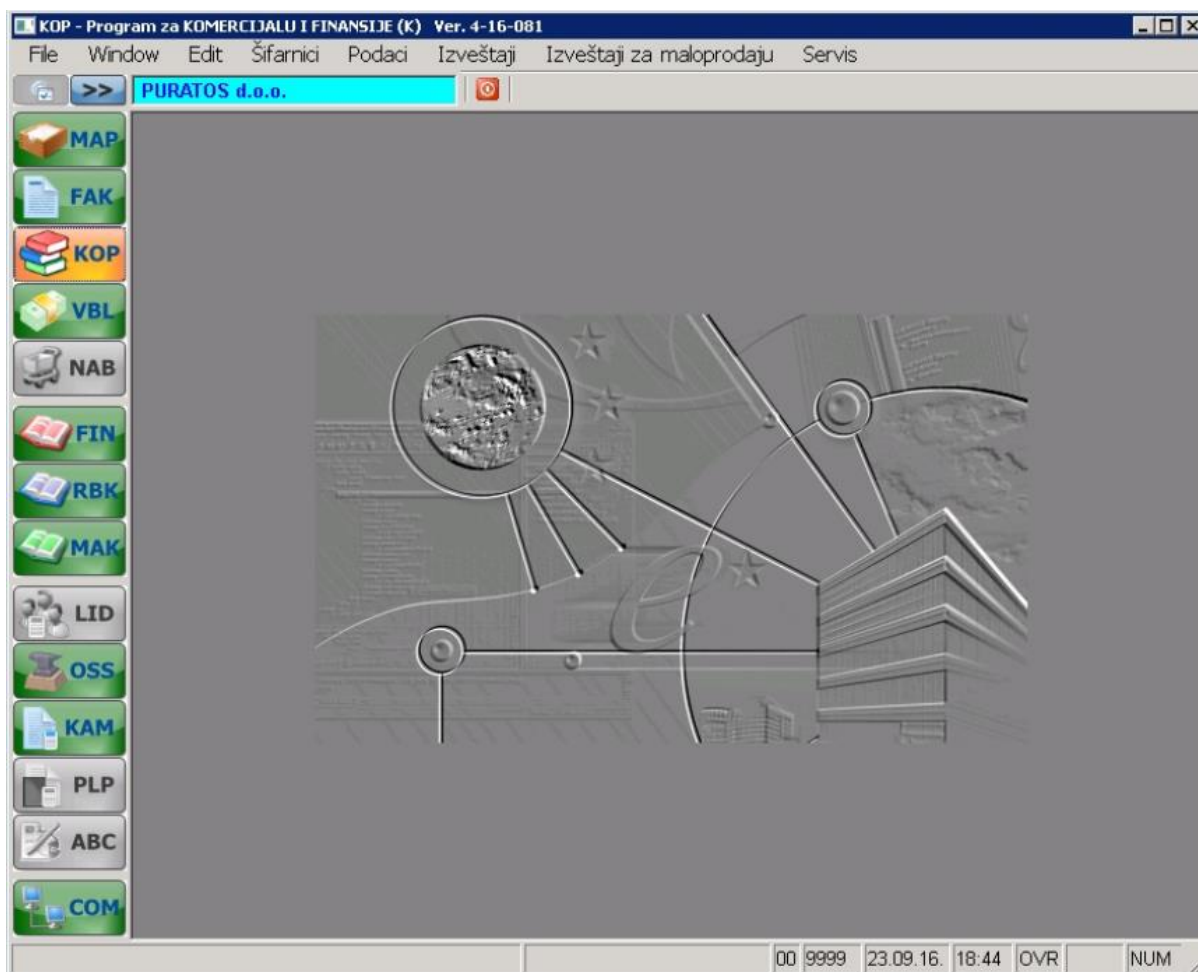
Slika 2 – **Prijavljivanje korisnika**



Izvor: *Izrada autora*

Slika 3 pokazuje način na koji se korisnici prijavljuju u program koristeći identifikacioni kod i lozinku. Već kod samog ulogovanja može doći do manipulacije od strane eksternih lica, tako što, ukoliko znaju identifikacione kodove, ili dobiju od strane nekog ko radi u kompaniji, mogu pristupiti u program i raditi šta god oni žele i menjati razne stavke u programu.

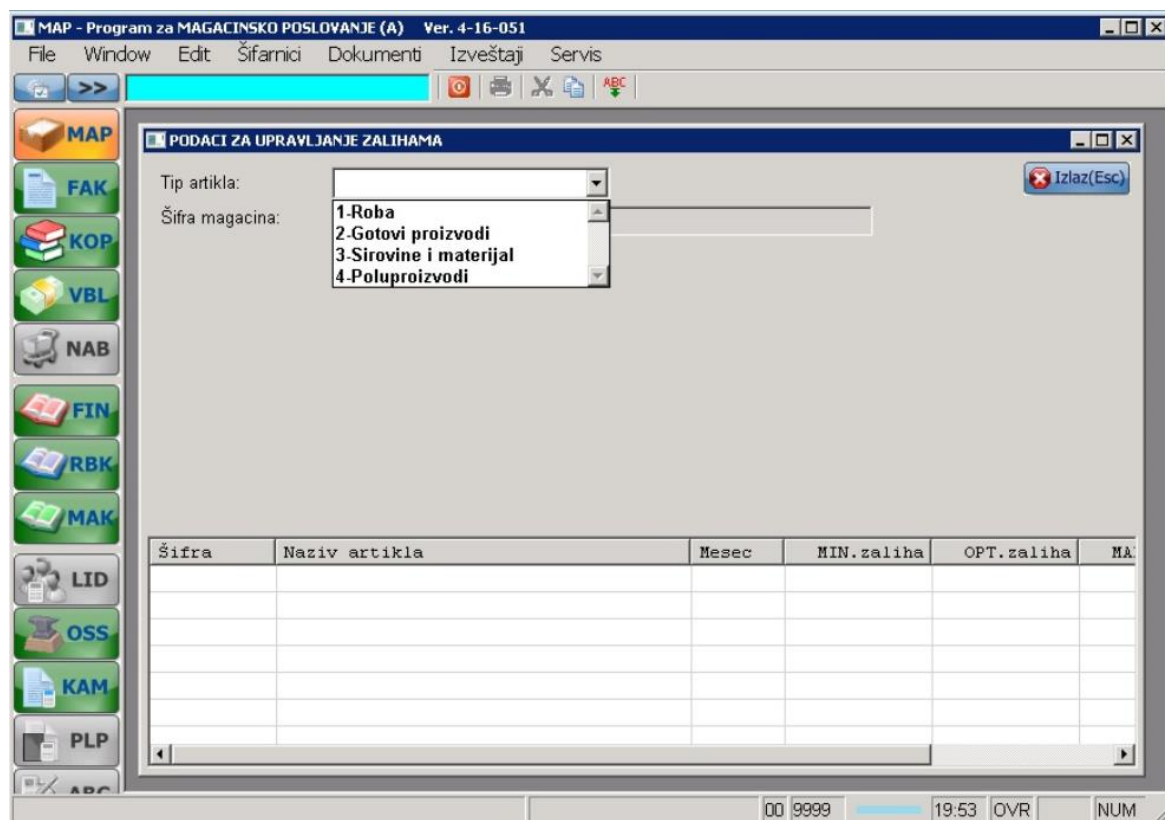
Slika 3 – Radno okruženje



Izvor: *Izrada autora*

Slika prikazuju radno okruženje samog programa. Tu su prikazani naredni programi: MAP program za magacinsko poslovanje, FAK program za fakturisanje, KOP program za komercijalno knjiženje i osnovni program za knjiženje ulaznih faktura, VBL program za vođenje blagajne, FIN program za finansijsko knjigovodstvo, MAP program za materijalno knjigovodstvo RBK program za robno knjigovodstvo, i lica koja žele da izvrše prevaru, kada se uloguju, u svaku od navedenih kartica mogu ući i menjati ono što njima najviše odgovora. I to ne samo eksterni korisnici, nego i interni korisnici mogu u bilo kojoj od pomenutih kartica menjati stavke i manipulirati.

Slika 4 – Kartica za magacinsko poslovanje



Izvor: *Izrada autora*

U bilo koju karticu da uđemo, interni ili eksterni korisnici mogu da počine prevaru u svakom trenutku. Na primer u MAP kartici može doći do toga da magacioner ne zaduži stvarno određenu količinu robe, i slično. Razne vrste prevara se mogu vršiti u bilo koju karticu od ponuđenih sa slike da uđemo, jer interni ili eksterni korisnici mogu vrlo lako da manipulišu ovim karticama, i pišu ono što odgovara njima ili trećoj strani za koju rade. Prevare zaposlenih su najčešće kada se radi o računovodstvenim programima upravo iz ovih razloga što mogu da kontrolišu unos i brišu podatke kako im najviše odgovara.

Slika 5 – Primer lažnog fakturisanja

FAK - UNOS I ŠTAMPA DOKUMENATA

Datum dokumenta: 19.02.16 Šifra dokumenta: 21 RAČUN - OTPREMNICA

Šifra kupca: 003561 "DRAGOJEVIĆ" PEKARA - S.T.R. Iznos dokumenta: 31.354,80

Šifra magacina: 101 ZEMUN- MAGACIN ROBE

Način plaćanja: Ziravno (odloženo) Rok plaćanja: 30 Uplata na: 4) 275-10222109046-95 So: 4

Broj ugovora: Tovarni list: Lice:

Broj porudžbenice: Datum porudžb. 00.00.00

Broj otpremnice: 00000000 Datum prometa: 19.02.16

Tip artikla: 0-Roba i proizvodi

Artikal: Rabat: 0,00

PDV: 1-Na cenu

Tar. PDV: 00 Stopa PDV: 0,00

Količina: 0,00 0,00 Cena: 0,00 Iznos: 0,00

| R.Broj | Dat.fak. | R... | Artikal | Naziv artikla              | Količina | Cena   | Iznos     |
|--------|----------|------|---------|----------------------------|----------|--------|-----------|
| 00020  | 20.03.15 | 0001 | 5916    | Aloha Pastry 70% Plate HF- | 200,000  | 136,00 | 27.744,00 |
| 00021  | 20.03.15 | 0002 | 5931    | Aristo Primeur Crema HF    | 20,000   | 177,00 | 3.610,80  |
| 00022  | 20.03.15 |      |         |                            |          |        |           |
| 00023  | 20.03.15 |      |         |                            |          |        |           |
| 00024  | 20.03.15 |      |         |                            |          |        |           |
| 00025  | 20.03.15 |      |         |                            |          |        |           |
| 00026  | 20.03.15 |      |         |                            |          |        |           |
| 00027  | 03.08.15 |      |         |                            |          |        |           |
| 00028  | 17.09.15 |      |         |                            |          |        |           |

Izvor: Izrada autora

U FAK kartici gde se unose i štampaju dokumenta, interni ili eksterni korisnici mogu vrlo lako da brišu fakture ili da menjaju cene kako njima odgovara, i tako dalje. Lažno fakturisanje robe predstavlja jednu od metoda koja se koristi za pranje novca. Izdavanje faktura sa cenama nižim od onih na fer tržištu dovode izvoznika u takvu situacija da može da prebaci novac uvozniku, jer će isplata za dobra ili usluge biti niža od cene koju će uvoznik dobiti kada ih bude ponudio na otvorenom tržištu. Ako se desi da se izdaju fakture sa cenama višim od cena na fer tržištima, onda izvoznik ima takvu korist od uvoznika jer će mu isplata biti viša od vrednosti koju će dobiti uvoznik prodajom na otvorenom tržištu. Ako je razlika u ceni između fakturisane robe i isporučene mnogo veća onda se može ostvariti višak dobara što firme mogu iskoristiti za „crnu prodaju“, što takođe predstavlja prevaru, ako govorimo o promeni podataka u ovoj kartici.

Slika 6,7 – Ostale manipulacije

**KOP - KNJIŽENJE**

Datum knjiženja: 23.09.16 Šifra dokumenta: 14 ULAZNA FAKTURA-TROSAK

Podaci za dokument

Iznos dokumenta: 0,00

Broj fakture: Datum fakture: 00.00.00 Datum prometa: 00.00.00

Analitika dobavljača: 435300 DOBAVLJAC ZA TROSKOVE U ZEMLJ Rok plaćanja: 00.00.00

Šifra dobavljača: Način plaćanja:

Broj ugovora: Poziv na broj:

Upis(F12)

| R.Broj | Dat.knj  | Mag | Dokument                 | Br.dok.  | Partner | Iznos      | Iznos PDV | KUF       |
|--------|----------|-----|--------------------------|----------|---------|------------|-----------|-----------|
| 00034  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 5.400,00   | 900,00    | 18-403676 |
| 00035  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 511.137,00 | 0,00      | 15-403677 |
| 00036  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 5.400,00   | 900,00    | 12-403678 |
| 00037  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 460.283,00 | 0,00      | 09-403679 |
| 00038  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 7.200,00   | 1.200,00  | 06-403680 |
| 00039  | 23.09.16 |     | 74 ULAZNA FAKTURA TRO... | 1776-... | 010742  | 61.604,65  | 0,00      | 03-403681 |
| 00040  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 205.551,50 | 0,00      | 97-403682 |
| 00041  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 1.500,00   | 0,00      | 94-403683 |
| 00042  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 1.500,00   | 0,00      | 91-403684 |
| 00043  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 4.500,00   | 0,00      | 88-403685 |
| 00044  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 01/16... | 009808  | 4.500,00   | 0,00      | 85-403686 |
| 00045  | 21.09.16 | 309 | 09 ULAZNI RACUN -MATE... | IF16-... | 008814  | 541.344,80 | 49.213,16 | 30-200748 |
| 00046  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | IF16-... | 008814  | 7.543,92   | 1.257,32  | 82-403687 |
| 00047  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 90020... | 000132  | 153.646,05 | 25.607,68 | 24-403674 |
| 00048  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 90020... | 000132  | 137.735,35 | 22.955,91 | 79-403688 |
| 00049  | 23.09.16 |     | 14 ULAZNA FAKTURA-TROSAK | 16-36... | 010402  | 25.625,71  | 4.270,95  | 76-403689 |

**KOP - PRENOS U FINANSIJSKO KNJIGOVODSTVO**

Broj knjig. naloga: 170031 Datum knjiženja: 29.02.16

Šifra dokumenta: 09 ULAZNI RACUN -MATERIJAL

Upis(F12)

| R..  | Dat.knj  | Broj KUF  | Broj računa | Šifra i naziv dobavljača      | Mag. |
|------|----------|-----------|-------------|-------------------------------|------|
| 1.   | 14.09.16 | 200731 09 | 500004251   | 008790 DON DON D.O.O. BEOGRAD | 308  |
| 2.   | 14.09.16 | 200732 09 | R&C-S-10442 | 005577 INTERALLIS CHEMICALS D | 308  |
| 3.   | 14.09.16 | 200733 09 | 03062/16    | 010525 TIRA DOO               | 308  |
| 4.   | 14.09.16 | 200734 09 | RN-01197/16 | 000979 ARETOL DOO ZA PROIZVOD | 308  |
| 5.   | 15.09.16 | 200735 09 | 786-41      | 001508 LITOPAPIR AD-CACAK     | 308  |
| 6.   | 15.09.16 | 200736 09 | 2189/16     | 007231 "TIPOPLASTIKA" DOO     | 308  |
| 7.   | 15.09.16 | 200737 09 | 2209/16     | 007231 "TIPOPLASTIKA" DOO     | 308  |
| 8.   | 15.09.16 | 200738 09 | 2208/16     | 007231 "TIPOPLASTIKA" DOO     | 308  |
| 9.   | 15.09.16 | 200739 09 | 65-01563    | 009743 JOKER PLUS DOO         | 308  |
| 10.  | 15.09.16 | 200740 09 | 02188       | 004943 "MAT-PRODUKT" ZANATSKA | 308  |
| 11.  | 16.09.16 | 200741 09 | 474         | 002985 "ŠPRINT" D.O.O. PREDUZ | 308  |
| 12.  | 16.09.16 | 200742 09 | 1f-8719     | 005430 "KARLITO" D.O.O. PREDU | 308  |
| 13.  | 20.09.16 | 200743 09 | 9435        | 009208 BIOZRNCE DOO           | 308  |
| 14.  | 20.09.16 | 200744 09 | 2236/16     | 007231 "TIPOPLASTIKA" DOO     | 308  |
| 15.  | 20.09.16 | 200745 09 | 793-41      | 001508 LITOPAPIR AD-CACAK     | 308  |
| 16.  | 21.09.16 | 200746 09 | PO1-1-12... | 008609 LESKO EXPORT IMPORT D. | 308  |
| 17.  | 21.09.16 | 200747 09 | 30-01607    | 009743 JOKER PLUS DOO         | 308  |
| 18.  | 21.09.16 | 200748 09 | IF16-01241  | 008814 PFI D.O.O.             | 309  |
| ---- | ----     | ----      | ----        | -----                         | ---- |

Izvor: Izrada autora

I u kartici knjiženja može doći do manipulacija. Lažno finansijsko izveštavanje se može javiti u svakom domenu poslovanja u računovodstvu. Prikrivanje obaveza i troškova tj. izostavljanjem knjiženja obaveza pravnog lica, umanjeanjem troškova rezervisanja ili nepravilnom kapitalizacijom troškova tj. smanjenjem ili uvećanjem troškova pribavljanja koji se uključuju u nabavnu vrednost stalne imovine predstavlja jedan od oblika lažnog finansijskog izveštavanja koje se može ovde primeniti. Prenos podatka iz komercijalnog u finansijsko knjigovodstvo se takođe može zloupotrebiti.

Slika 8 – MAP manipulacije

| MAK- PREGLED UTROŠKA MATERIJALA |                                 |                |          |             |            |
|---------------------------------|---------------------------------|----------------|----------|-------------|------------|
| Za period: 01.09.16 - 30.09.16  |                                 | Izveštaj (F12) |          | Izlaz (Esc) |            |
| R.br                            | Šifra i naziv artikla           | J.m.           | Količina | Cena        | Iznos      |
| 1                               | 2087 Soft'r Silk                | Kg             | 20,60    | 229,88      | 4.735,53   |
| 2                               | 2112 Soft'r Cotton              | Kg             | 126,00   | 171,46      | 21.603,96  |
| 3                               | 2142 Quick Step Croissant       | Kg             | 84,00    | 167,92      | 14.105,28  |
| 4                               | 2155 Easy Satin Creme Cake 15%  | Kg             | 588,00   | 125,27      | 73.658,76  |
| 5                               | 2168 Quick Step Croissant A+    | Kg             | 220,00   | 187,19      | 41.181,80  |
| 6                               | 2169 Premix Easy Corn           | Kg             | 20,00    | 352,65      | 7.053,00   |
| 7                               | 2179 Soft R optimal             | kg             | 14,00    | 182,10      | 2.549,72   |
| 8                               | 2200 S500                       | Kg             | 7,00     | 199,97      | 1.399,79   |
| 9                               | 2206 Premix Easy rustik 43 %    | Kg             | 11,40    | 160,34      | 1.827,88   |
| 10                              | 2207 Premix Easy suvit          | kg             | 15,00    | 139,96      | 2.099,40   |
| 11                              | 2210 Premix Easy kopriva        | Kg             | 15,00    | 151,00      | 2.265,00   |
| 12                              | 2222 Premix Tegral Saher mix    | Kg             | 300,00   | 379,66      | 113.898,00 |
| 13                              | 2227 Premix Tegral raž specijal | Kg             | 300,00   | 122,72      | 36.816,00  |
| 14                              | 2229 Premix Tegral Ražina       | Kg             | 150,00   | 115,34      | 17.301,00  |
| 15                              | 2237 Premix Easy krofna         | Kg             | 30,00    | 292,65      | 8.779,50   |
| 16                              | 2240 Premix Puravita Powe       | kg             | 30,00    | 172,39      | 5.171,70   |
| ----                            | -----                           | ----           | -----    | -----       | -----      |
|                                 | UKUPNO                          |                |          |             | 354.446,32 |
| ----                            | -----                           | ----           | -----    | -----       | -----      |

Izvor: Izrada autora

Manipulacije se mogu dešavati i u kartici materijalnog knjigovodstva odnosno u utrošcima materijala u proizvodnji. Prikazivanje lažnih zaliha materijala je jedan od problema koji se ovde može javiti. Zalihe su često predmet lažnog izveštavanja, posebno u situacijama kada se radi o velikim količinama i vrednostima zaliha. Osim problema utvrđivanja količinske komponente zaliha, zbog neprisustvovanja revizora tokom popisa, problem predstavlja i cena po kojoj se vrši obračun tih zaliha. Prema *Međunarodnom računovodstvenom standardu 2 - Zalihe*, zalihe se obračunavaju po ceni koštanja ili neto prodajnoj ceni, zavisno od toga koja cena je niža. To podrazumeva obavezu revizora da se uveri u način utvrđivanja cena, kao i da izvrši računsku kontrolu obračuna vrednosti zaliha. Potvrda vrednosti zaliha se ne može izvršiti samo na osnovu pribavljene izjave menadžmenta. Ukoliko preduzeća obračunavaju zalihe samo po neto prodajnoj ceni, ili samo po prodajnoj ceni, tada postoji opasnost da se zalihe prikažu u većem iznosu, što se može direktno odraziti na povećanje dobiti. Većina preduzeća se ne odlučuje na varijantu obračunavanja zaliha po ceni koštanja zbog: - teškoća u obračunu cene koštanja, zbog specifičnosti delatnosti kojom se bavi preduzeće, - nestručnosti zaposlenog osoblja, - namernog neobračunavanja po ceni koštanja u slučajevima kada je ona niža od neto prodajne cene. Navedeni razlozi govore o prisutnim problemima potvrđivanja istinitosti tvrdnji menadžmenta o vrednosti zaliha.

Na osnovu svega rečenog vidimo da se čak ni kod računovodstvenih programa ne možemo zaštititi od rizika koji nam pretili od strane zaposlenih. Zaposleni su tu koji su najzaslužniji za prevare u računovodstvu kada se koriste računovodstveni programi jer oni mogu da menjaju i brišu dokumenta i razne druge informacije kako odgovara njima. Hipoteza koju smo dokazali ovim kratkim istraživanjem je sledeća:

*Interni i eksterni korisnici čine prevare u računovodstvenim programima na taj način što manipulišu podacima kako njima odgovara ili nekoj trećoj strani.*

## Zaključak

Osnovna uloga interne revizije prilikom upravljanja rizicima u organizaciji se odnosi na pružanje uverenja za proces upravljanja rizikom i uverenja o pravilnosti procene rizika. Jako je važno da se poznaje proces upravljanja rizicima i da se izveštaja uprava o ključnim rizicima. Ako se desi da se rizik ne identifikuje onda interna revizija može da ima uloga savetodavaca i da preporuci upravi kako da se poboljšaju procesi upravljanja rizikom i da predloži strategije bitne za proces upravljanja rizikom. Ni u kom slučaju interna revizija ne bi trebala samostalno donosi odluke o upravljanju rizikom, niti da preuzima odgovornost za to. Uprava organizacije daje konačni sud o tome koju strategiju će organizacija koristiti da bi se odbranilo od potencijalnih rizika i za to uprava snosi odgovornost.

Interni revizori igraju veliku ulogu u otkrivanju prevara primenjujući posebne veštine kako bi pribavili, analizirali i procenili dokazni materijal, i protumačili i saopštili nalaze. Jedna od analiza koju primenjuju jeste digitalni alat – Benfordova analiza koja je koristi kako bi se detektovale prevare u različitim oblicima poslovanja koje ne zahtevaju specijalizovani i skup softver. Benfordov zakon primenjuju razni analitičari, kao i forenzičke računovođe i revizori kako bi došli do zaključka da li je došlo do prevara u finansijskim izveštajima. Benfordov zakon se javio iz potrebe da se otkriju prevare u IT sektoru, a sve veći uticaj Interneta i telekomunikacionih tehnologija je doveo do toga da se veliki broj manipulacija i prevara dešava upravo putem pomenutih kanala. Što se povećava broj korisnika na Internetu, tako se povećavaju i „hakeri“, dolazi do veće upotrebe kompjuterskih virusa, a ujedno i kompanija koje se bave zaštitom računara. Benfordov zakon je jedan od alata koji koriste i informatičari u svom poslovanju i koriste određene programe za njegovo računanje.

**IT sektor predstavlja sektor u kojem zaposleni mogu da vrše razne manipulacije i prevare, a alati za otkrivanje preware nisu dovoljni da se prevare minimizuju ili zaustave** – predstavlja glavnu hipotezu rada koju smo dokazali u radu. Razvoje Interneta i društvenih mreža došlo je do sve većeg umrežavanja korisnika i sve veće zloupotrebe informacija i podataka iz preduzeća. Zaposleni vrše prevare i manipulacije u preduzećima, pogotovo u IT sektorima. U preduzećima u Republici Srbiji cyber kriminal je veoma „popularan“. Zaposleni mogu da iznesu poverljive podatke iz preduzeća na nekoliko načina (imejl, skajp, društvene mreže i tako dalje). Preduzeća nemaju bezbednosne provere i puštaju neautorizovane ljude u svoj sistem.

Cyber terorizam je danas sve prisutniji, a države se nemoćno bore protiv ovog vida kriminala, iz razloga što je Internet postalo veoma moćno sredstvo i oružje. Internet i računare ekstremne organizacije koriste kako bi prisluškivale, ometale rad sistema, postavljali različite viruse, ugrožavale indentitet i poverljivost i dostupnost podataka na elektronskoj mreži. Cyber teroristi mogu da upadnu u računarsku mrežu i da naprave pravi kolaps u funkcionisanjih državnih institucija. Teroristi mogu da ugroze svet, ako se dobro edukuju i imaju adekvatnu IT obuku.

Cyber teroristi najviše koriste propagandu kao glavnu aktivnost cyber terorizma. Smatra se da postoji nekoliko hiljada terorističkih sajtova koji podržavaju Al Kaidu i islamski terorizam. Uz pomoć Interneta i društvenih medija, islamske organizacije mogu da veoma lako stupe u kontakt sa svojim sledbenicima, i to mogu da rade uspešno upravo putem propagande. Cyber teroristi medijima šalju razne snimke medijima kako čine sva zlodela. Snimcima treba samo nekoliko minuta da obidu čitavu planetu. Islamska država koriste društvene medije kako bi napravila „revoluciju“. Najpoznatije društvene mreže koje koriste su Twitter, Facebook, YouTube i Instagram za širenje terorizma i video klipova sa uznemirujućim sadržajima.

U radu, u studijsko-istraživačkom delu rada, sprovedeno je istraživanje putem ankete u IT sektoru. Istraživanjem smo došli do dokazanih sporednih hipoteza u master radu:

1. Najveći broj prevara se vrši u IT sektoru, a razloga za to je mnogo: unapređenje na poslu, dobitak poslova u siromašnijim zemljama, spas organizacije u vreme krize, kako bi društvu bio odobren kredit i tako dalje.
2. CAATT i Benfordov zakon su dva alata koja se koriste kako bi se društvo zaštitilo od prevara, međutim, tehnike i alati nisu dovoljni jer, sa druge strane, veliki broj faktora može da utiče na to da se prevara ne otkrije kao što su: zastarela tehnologija, zaposleni, nedovoljna interna kontrola, rizici i tako dalje.
3. U IT sektoru postoji i veliki broj mogućnosti da se poćini prevara, kao što su: visoka koncentracija na malom prostoru, prethodno proverenih i uređenih podataka, dostupnih kako ovlašćenim, tako i neovlašćenim korisnicima; znatno proširen prostor kriminalnog delovanja, koji za razliku od tradicionalnih vidova kriminaliteta, ne zahteva prisustvo izvršioca na mestu izvršenja kriviminalne radnje; skraćeno vreme kriminalnog delovanja, s obzirom na automatizovani ambijent, čija brzina sprečava nadzor i upravljanje; i tako dalje.

Osim prvog istraživanja, u radu smo sproveli još jedno istraživanje vezano za manipulacije i prevare u računovodstvenom programu IPIS. Kod računovodstvenih programa se ne možemo zaštititi od rizika koji nam pretili od strane zaposlenih. Zaposleni su tu koji su najzaslužniji za prevare u računovodstvu kada se koriste računovodstveni programi jer oni mogu da menjaju i brišu dokumenta i razne druge informacije kako odgovara njima.

Kompjuterski kriminal označava da neovlašćena osoba „upada“ u kompjuterski sistem drugog lica kako bi zloupotrebila podatke o transakcijama, interne podatke, i podatke sa kreditnih kartica ili iz računovodstvenih sistema kompanija koje se bave računovodstvo i revizijom. Veoma je važno napraviti alate, tehnike i metode kako bi se zaposleni sprečili u obavljanju ovakvih radnji, pogotovo kada su u pitanju računovodstveni sistemi, kao što je IPIS.

## Literatura

- 1) Alvin A., et al., Auditing and Assurance Services An Integrated Approach, 14 edition, ACL, 2012.
- 2) Barjaktarović, L., Jović, Z., Milojević, M., Poslovne finansije (2nd ed.). Univerzitet Singidunum Beograd, 2015.
- 3) Belak V., Poslovna forenzika i forenzično računovodstvo, borba protiv prijevare, Belak Excellenx d.o.o., Zagreb, 2011.
- 4) Bošković M., Kriminalistika – metodika, Policijska akademija, Beograd, 2005.
- 5) Hoopwood W.S., et al., Forenzičko računovodstvo, Univerzitet Singidunum, Beograd, 2014.
- 6) Knežević G., Ekonomsko-finansijska analiza, Univerzitet Singidunum, Beograd, 2007.
- 7) Koletnik F, Kolar I., Forenzičko računovodstvo, Zveza računovodij, finansičnikov in revizorjev Slovenija, Ljubljana, 2008.
- 8) Mikerević D., et al., Forenzika poslovanja, Banja Luka, 2013.
- 9) Petković A., Forenzička revizija, Kriminalne radnje u finansijskim izveštajima, Proleter A.D. Bečej, Novi Sad, 2010.
- 10) Savez računovođa i revizora Srbije, Revizija kriminalne radnje i forenzičko računovodstvo, Beograd, 2010.
- 11) Savez računovođa i revizora Srbije, Revizija kriminalne radnje i forenzičko računovodstvo, Beograd, 2006.
- 12) Stanišić M., Revizija, Univerzitet Singidunum, Beograd, 2009.
- 13) Stanišić M., Interna kontrola i revizija, Univerzitet Singidunum, Beograd, 2014.

### *Časopisi i stručni članci:*

- 1) Aleksić M., et al., Uloga i značaj forenzičkog računovodstva u otkrivanju finansijskih prevara, EMC Review- Časopis za ekonomiju i tržišne komunikacije. Vol. 10., Br. 2. 2015., str. 229-236., dostupno na: <http://doisrpska.nub.rs/index.php/economyandmarket/article/view/2024/1948>
- 2) Antoliš K., (2010), Internetska forenzika i cyber terorizam, Recenzija, Policija i sigurnost, Vol.19 No.1 Ožujak 2010., str. 121-128. dostupno na: <http://hrcak.srce.hr/79411>

- 3) Arežina N., et al., Forenzički računovođa: Urođena osobina ili veština koja se stiče?, Međunarodna naučna konferencija Univerziteta Singidunum, Finiz, 2014-Fonrezika, Univerzitet Singidunum, Beograd, 2014.
- 4) Barjaktarović, L., Milojević, M., Terzić, I., Results of applience of Benfors's law on Serbian companies, XIV International Symposium SymOrg, Zlatibor, 2014., dostupno na:  
[https://www.researchgate.net/profile/Ivica\\_Terzic/publication/271834628\\_RESULTS\\_OF\\_APPLIENCE\\_OF\\_BENFORD'S\\_LAW\\_ON\\_SERBIAN\\_COMPANIES/links/54d345360cf2b0c6146d3eb5.pdf#page=131](https://www.researchgate.net/profile/Ivica_Terzic/publication/271834628_RESULTS_OF_APPLIENCE_OF_BENFORD'S_LAW_ON_SERBIAN_COMPANIES/links/54d345360cf2b0c6146d3eb5.pdf#page=131)
- 5) Basrak, B., et al., Benfordov zakon, Math. e, Vol. 23., No. 1. 2003., dostupno na:  
[http://hrcak.srce.hr/index.php?show=clanak&id\\_clanak\\_jezik=175512](http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=175512)
- 6) Bešlić D., Bešlić I., Stečaj privrednog društva kao posledica manipulativnog finansijskog izveštavanja, Škola biznisa, Br. 3-4., 2013., dostupno na:  
<http://www.vps.ns.ac.rs/SB/2013/3.9.pdf>
- 7) Budimir N., Forenzičko računovodstvo, Anali poslovne ekonomije, godina V, sveska 1, broj 8., 2013.
- 8) Dimitrijević D.S., Forenzičko računovodstvo – sredstvo zaštite kvaliteta finansijskog izveštavanja, doktorka disertacija, Univerzitet u Kragujevcu, Ekonomski fakultet, Kragujevac, 2013., dostupno na: <http://nardus.mpn.gov.rs/handle/123456789/3530>
- 9) Dragović NJ., Etika u poslovanju. Teme, Vol. 35., Br. 4., 2011., dostupno na:  
<http://teme2.junis.ni.ac.rs/public/journals/1/previousissues/teme4-2011/teme%204-2011-36.pdf>
- 10) Durtschi C., et al., The effective use of Benford's law to assist in detecting fraud in accounting data, Journal of Forensic Accounting, Vol5/1524-5586, 2004., dostupno na:  
[https://www.researchgate.net/profile/Cindy\\_Durtschi/publication/241401706\\_The\\_Effective\\_Use\\_of\\_Benford's\\_Law\\_to\\_Assist\\_in\\_Detecting\\_Fraud\\_in\\_Accounting\\_Data/links/54982f4a0cf2c5a7e342a59e.pdf](https://www.researchgate.net/profile/Cindy_Durtschi/publication/241401706_The_Effective_Use_of_Benford's_Law_to_Assist_in_Detecting_Fraud_in_Accounting_Data/links/54982f4a0cf2c5a7e342a59e.pdf)
- 11) Đekić M. D., (2016), Cyber procedure za poslovno okruženje u Srbiji, Tehnika, vol. 71, br. 3, str. 471-474., dostupno na: <http://scindeks.ceon.rs/article.aspx?artid=0040-21761603471D>
- 12) Đekić M. D., (2016), Pametno konfigurisanje računara kao prevencija od hakovanja i cyber špijuniranja, Tehnika, vol. 71, br. 5, str. 761-764., dostupno na:  
<http://scindeks.ceon.rs/article.aspx?artid=0040-21761605761D>.

- 13) Đorđević D., Vukasović B., Ekonomsko-finansijsko veštačenje u sudskim sporovima-teorija i praksa, Ekonomika, Vol. 57., Br. 1., 2011., dostupno na: <http://scindeks.ceon.rs/article.aspx?artid=0350-137X1101080D>
- 14) Jeremić, Z., Milojević, M., Terzić, I., Business performance of the largest exporters in Serbia during the period 2008-2014, Ekonomika preduzeća, Vol. LXIII, No. 5-6, pp. 293-305, 2015., <http://scindeks.ceon.rs/article.aspx?artid=0353-443X1506293J>
- 15) Jeremić, Z., Milojević, M., Terzić, I., Uticaj likvidnosti na poslovanje preduzeća koja su u skladu sa zakonom o računovodstvu Republike Srbije razvrstana kao velika pravna lica. Paper presented at Synthesis 2015 - International Scientific Conference of IT and Business-Related Research, dostupno na: [https://www.researchgate.net/profile/Ivica\\_Terzic/publication/300485726\\_Uticaj\\_likvidnosti\\_na\\_poslovanje\\_preduzeca\\_koja\\_su\\_u\\_skladu\\_sa\\_zakonom\\_o\\_racunovodstvu\\_Republike\\_Srbije\\_razvrstana\\_kao\\_velika\\_pravna\\_lica/links/57236a6108ae586b21d885ab.pdf](https://www.researchgate.net/profile/Ivica_Terzic/publication/300485726_Uticaj_likvidnosti_na_poslovanje_preduzeca_koja_su_u_skladu_sa_zakonom_o_racunovodstvu_Republike_Srbije_razvrstana_kao_velika_pravna_lica/links/57236a6108ae586b21d885ab.pdf)
- 16) Jeremić, Z., Milojević, M., Terzić, I., Business performance of 15 largest exporters in food-processing industry in the period 2008-2014, Ekonomika Poljoprivrede, Vol. LXIII, No 3 (741-1112), pp.943-958, 2016., dostupno na: <http://www.ea.bg.ac.rs/images/Arhiva/2016/Broj%203/14%20EP%203%202016lq.pdf>
- 17) Jonev K., (2016), Sajber terorizam i upotreba sajber prostora u terorističke svrhe, Bezbednost, vol. 58, br. 2, str. 206-222., dostupno na: <http://scindeks.ceon.rs/article.aspx?artid=0409-29531602206J>
- 18) Jukić O., Muhurdarević N. (2003), Benfordov zakon, Naučno – stručni skup sa međunarodnim učešćem KVALITET Zenica, Bosna i Hercegovina
- 19) Koletnik F., Koletnik-Korošec M., Forenzičko računovodstvo u funkciji sprečavanja i otkrivanja gospodarskoga kriminala, Zbornik radova: Ekonomske reforme u BiH i Evrope integracije, XI Međunarodni simpozij, Neum, 2008.
- 20) Milojević, M., Terzić, I., Marjanović, V., Application of Branford Analysis in detecting anomalies in the financial statements – case of Serbian large companies. Paper presented at Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide. doi:10.15308/sinteza-2014-564-570, 2014., dostupno na: <http://portal.sinteza.singidunum.ac.rs/paper/111>
- 21) Milojević, M., Terzić, I., Miletić, D., Stamenković, S., The Role of ERP Solutions in Managing Corporations From the Accounting Perspective. Paper presented at Sinteza

- 2016 - International Scientific Conference on ICT and E-Business Related Research. doi:10.15308/Sinteza-2016-352-358, 2016.
- 22) Mitrić M., et al., Forenzičko računovodstvo – karika koja nedostaje u obrazovanju i praksi, Časopis za teoriju i praksu menadžmenta, Management, 2012/65, Fakultet organizacionih nauka, Beograd, 2012.
- 23) Mrvić-Petrović, N., et al., Medicinska veštačenja u krivičnom i parničnom postupku. Vojnosanitetski pregled, Vol. 72., Br. 8., 2013., dostupno na: <http://www.doiserbia.nb.rs/img/doi/0042-8450/2015/0042-84501300054M.pdf>
- 24) Petković A., Šta je zaista forenzičko računovodstvo. U: VI Kongres računovođa i revizora Crne Gore – Finansijsko izveštavanje u funkciji unapređenja poslovnog ambijenta u Crnoj Gori, Bečići: ISRCG, 2011.
- 25) Spahić N., Otkrivanje prevara i pronevera u finansijskim izveštajima, In International Scientific Conference of IT and Business-Related Research-SINTEZA, 2014., dostupno na: <http://portal.sinteza.singidunum.ac.rs/paper/16>
- 26) Spahić N., Primjer otkrivanja manipulisanja bazom podataka jedne vrste računovodstvenog softvera uz pomoć alata digitalne forenzike, In International Scientific Conference of IT and Business-Related Research-SINTEZA, 2014., dostupno na: <http://portal.sinteza.singidunum.ac.rs/paper/214>
- 27) Stančić, P., et al., Forenzičko računovodstvo-odgovor profesije na prevare u finansijskim izveštajima, Teme-Časopis za Društvene Nauke, 2013., Br. 4., dostupno na: <https://www.cceol.com/search/article-detail?id=216036>
- 28) Stanišić M., Uloga interne revizije u otkrivanju i sprečavanju prevara u bankama, Bankarstvo, Vol. 36., Br. 1-2., 2007., dostupno na: <http://scindeks.ceon.rs/article.aspx?artid=1451-43540702020S>
- 29) Tica J., Kriminalne radnje i greške, Industrija, Vol.31., Br.1-2., 2003., dostupno na: <http://scindeks.ceon.rs/article.aspx?artid=0350-03730302093T>
- 30) Vukoja B., Značaj forenzičkog računovodstva i revizije za pouzdanost finansijskih izveštaja u BiH, Financing – Naučni časopis za ekonomiju, Br. 2. 2012.
- 31) Vukoja B., Unković I., Primjena metoda interne revizije i kontrole kao instrument za otkrivanje kriminalnih radnji i prevara, Zbornik radova 6, VII Godišnja konferencija, Društvena odgovornost interne revizije, Sarajevo: Udruženje internih revizora u BiH, 2013.

## **Prilog – Anketa**

*Pitanje br. 1:* Pol: muški/ženski

*Pitanje br. 2:* Da li se nekada počinili prevaru: Da/Ne

*Pitanje br. 3:* Ukoliko ste naveli na, navedite razloge zbog kojih je opravdano da organizacija ili pojedinac izvršiti kriminalnu radnju ili prevaru?

*Pitanje br. 4:* Ukoliko ste naveli Da, navedite razloge zbog kojih ste počinili prevaru?

*Pitanje br. 5:* Koje od navedenih razloga smatrate da se najviše koriste kao podsticaj da se desi prevara: Neefektivna interna kontrola; Dogovor između zaposlenih koji podležu nedovoljnoj kontroli; ili Postojanje likvidnih sredstava, kao što je gotovina, hartije od vrednosti na donosioca ili lako utrživa roba?

*Pitanje br. 6:* Ukoliko ste počinili prevaru, navedite u kojim sektorima ste to najviše činili?

*Pitanje br. 7:* Obzirom na to da se sve više prevara dešava u IT sektoru, navedite mogućnosti zbog kojih mislite da se najveći broj prevara dešava u ovom sektoru?

*Pitanje br. 8:* Navedite koje tehnike koristi društvo u kojem ste zaposleni da bi se zaštitilo od prevara u IT sektoru?

*Pitanje br. 9:* Da li smatrate da su tehnike koje Vaše društvo koristi dovoljno tehnika i alat da se zaštite od prevara? Da/Ne

*Pitanje br. 10:* Navedite razloge zašto ste dali odgovor Da/Ne?