UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

ANALIZA POSLOVNE VREDNOSTI REVIZIJSKE SLEDI

Ljubljana, september 2016 MIRJANA JURJEVEC

IZJAVA O AVTORSTVU

Spodaj podpisana Mirjana Jurjevec, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Analiza poslovne vrednosti revizijske sledi, pripravljenega v sodelovanju s svetovalcem prof. dr. Alešem Groznikom

IZJAVLJAM

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študentke:_____

KAZALO

KAZALO TABEL

UVOD

Podjetja se soočajo z vedno težjo nalogo varovanja osebnih podatkov v svojih poslovno-informacijskih sistemih. Osebne podatke morajo ustrezno varovati pred notranjimi in zunanjimi nepooblaščenimi dostopi. Da bi zagotovila varnost osebnih podatkov, morajo v sistemih vzpostaviti sledljivost obdelave podatkov oziroma beležiti dostope do podatkov. To sledljivost dosežejo z vzpostavitvijo beleženja revizijskih sledi. Vodenje revizijske sledi izboljša učinkovitost varnosti informacijskega sistema, nadzira kršitve in jih tudi zmanjšuje.

Informacijskih pooblaščenec v svojih usmeritvah priporoča (Informacijski pooblaščenec, 2010), naj beleženje dostopov do osebnih podatkov omogoča poznejše preverjanje, kdo je, kdaj in do katerih osebnih podatkov dostopal. Pomembno je, da je identifikacija osebe, ki je stopila v stik s podatki, enolična.

Vodenje revizijskih sledi je z vidika zagotavljanja varstva osebnih podatkov oziroma zagotavljanja informacijske varnosti vedno pomembnejše. Za podjetje je pomembno ravnovesje med zagotavljanjem varnosti in pravicami pooblaščenih in nepooblaščenih uporabnikov, torej med varnostjo in uporabnostjo, kar je pri uporabi velike količine podatkov izjemno težko in vpliva na učinkovitost sistema. Hkrati so zahteve zakonodaje zapisane tako, da je zagotavljanje revizijskih sledi zelo zahtevno in drago. Podjetja imajo v svoje informacijske sisteme vpeljane različne programske rešitve za zagotavljanje revizijske sledi, ni pa na voljo splošne rešitve, primerne za večino.

Namen diplomskega dela je s teoretičnega in praktičnega vidika proučiti vodenje revizijskih sledi v podjetju. Vlogo in pomen revizijskih sledi bom preučila na podlagi strokovne literature, spletnih virov ter intervjuja s strokovnjakom, avtorjem programske rešitve za vodenje revizijskih sledi v podjetju Abakus plus, d. o. o., gospodom Borisom Oblakom. Odzivi uporabnikov o praktičnih rešitvah za zagotavljanje revizijskih sledi so slabi. Uspelo mi je pridobiti le intervju s strokovnjakom. Anketa med uporabniki mi je bila z vidika strokovnjaka zaradi nepriljubljenosti in občutljivosti tematike odsvetovana. Kljub temu sem želela vključiti praktične izkušnje vsaj enega od podjetij, vendar se to ni odzvalo.

Cilj diplomskega dela je ugotoviti, ali imajo revizijske sledi poslovno vrednost za podjetje, ki jih vodi. Podjetja so skladno z zakonodajo dolžna voditi revizijske sledi. Na podlagi ugotovitev iz preučevanja revizijskih sledi v podjetju želim dokazati, da pomen vodenja revizijskih sledi ni le poslovati skladno s predpisano zakonodajo, ampak ima tudi poslovno vrednost za podjetje. Za analizo poslovne vrednosti revizijskih sledi bom uporabila metodo stroškov in koristi.

Diplomsko delo se začne z uvodom. V naslednjih treh poglavjih je predstavljeno varovanje osebnih podatkov in pravne podlage za varovanje osebnih podatkov, revizijske sledi,

revizijske sledi v informacijskem sistemu ter programske rešitve za vodenje revizijske sledi. V petem poglavju je predstavljena praktična programska rešitev za vodenje revizijskih sledi Arbiter ter uvajanje in uporaba Arbitra v Aerodromu Ljubljana. Sledi opis vodenja revizijskih sledi v praksi v šestem poglavju ter proučitev poslovne vrednosti revizijske sledi na podlagi analize stroškov in koristi v sedmem poglavju. Diplomsko delo se konča s sklepom.

V diplomskem delu je revizijska sled predstavljena z vidika poslovnega uporabnika kot del poslovno-informacijskega sistema. Zato bom v nalogi navajala poslovnega uporabnika kot podjetje (glede na vsebino občasno tudi kot naročnika oziroma uporabnika). Programske rešitve za zagotavljanje revizijskih sledi sem opisala do stopnje, za katero menim, da je potrebna za razumevanje tega diplomskega dela. Interpretacijo podatkov iz intervjuja z gospodom Oblakom bom navajala kot mnenje strokovnjaka (B. Oblak, osebna komunikacija, 16. junij 2016) občasno tudi kot avtorja programske rešitve.

Pri obravnavanju teme sem se osredinila na slovenski prostor. Po prebiranju tujih virov (O'Kelley, Ye, Jones, & Miller, 2015; Roratto & Dias, 2014) sem ugotovila, da uporaba in razvoj rešitev za zagotavljanje revizijskih sledi v tujini ne prednjači glede na trenutno situacijo v slovenskem prostoru. Iz literature je razbrati, da prav tako preverjajo stanje v praksi, ugotavljajo, da so uporabljene rešitve med uporabniki različne, ni se pa razvila splošna programska rešitev, primerna za večino, prav tako je slaba odzivnost uporabnikov glede izkušenj v praksi, zato priporočajo nadaljnje raziskave na področju zagotavljanja revizijskih sledi.

1 VARSTVO OSEBNIH PODATKOV

Varstvo osebnih podatkov se nanaša na podatke o posameznikih, fizičnih osebah. Podatki morajo biti obravnavani v skladu z določili Zakona o varstvu osebnih podatkov (Ur.l. RS, št. 86/2004, 113/2005 – ZInfP, 51/2007 – ZUstS-A, 67/2007, v nadaljevanju ZVOP-1), načini obdelave so različni, obdelujejo jih lahko upravljavci sami, pogodbeni upravljavci oziroma ustrezne službe v okviru svojih pristojnosti.

Osebne podatke je treba zavarovati ne le zato, ker tako zahteva zakonodaja, ampak ker se z njihovim (za)varovanjem zmanjša možnost zlorab osebnih podatkov. Če se kljub temu to zgodi in so osebni podatki ustrezno zavarovani, se odgovorna oseba lažje najde, s tem pa se poveča zaupanje v upravljavca osebnih podatkov oziroma v podjetje. Seveda obstajajo tudi razlogi proti varstvu osebnih podatkov, ker (za)varovanje osebnih podatkov pomeni veliko porabljenega časa, sredstev in energije (Slovenski odsek ISACA, 2016).

1.1 Pravni vidik varstva osebnih podatkov

V nadaljevanju bodo predstavljeni najpomembnejši predpisi in usmeritve s področja varstva osebnih podatkov.

1.1.1 Ustava Republike Slovenije

Ustava Republike Slovenije (Ur.l. RS, št. 33/1991, 42/1997-UZS68, 66/2000-UZ80, 24/2003-UZ3a, 47, 68, 69/2004-UZ14, 69/2004-UZ43, 69/2004-UZ50, 68/2006-UZ121, 140, 43, 47/2013, v nadaljevanju Ustava) kot najvišji pravni akt Republike Slovenije v 38. členu predpisuje **varstvo osebnih podatkov:**

- »Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.«
- »Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.«
- »Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.«

1.1.2 Zakon o varstvu osebnih podatkov

ZVOP-1 je pravi akt, ki natančno ureja varstvo osebnih podatkov, kot ga predpisuje Ustava. V nadaljevanju so navedena, za razumevanje tega diplomskega dela, bistvena določila ZVOP-1 po členih:

- 1. člen**: Vsebina zakona: »**S tem zakonom se določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov.«
- 2. člen: **Načelo zakonitosti in poštenosti: »**Osebni podatki se obdelujejo zakonito in pošteno.**«**
- 3. člen: **Načelo sorazmernosti: »**Osebni podatki, ki se obdelujejo, morajo biti ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo.«
- 6. člen 1: **»Osebni podatek** je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.«
- 6. člen 2: »**Posameznik** je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek.«
- 6. člen 3: »**Obdelava osebnih podatkov** - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, vpogled, uporaba,

razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev, povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).«

- 6. člen 4: »**Avtomatizirana obdelava** je obdelava osebnih podatkov s sredstvi informacijske tehnologije.«
- 6. člen 5: »Zbirka osebnih podatkov je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.«
- 6. člen 6: »**Upravljavec osebnih podatkov** je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov, oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.«
- 6. člen 7: »**Pogodbeni obdelovalec** je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov.«
- 6. člen 8: »**Uporabnik osebnih podatkov** je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki.«
- 16. člen: **Namen zbiranja in nadaljnja obdelava:** »Osebni podatki se lahko zbirajo le za določene in zakonite namene ter se ne smejo obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.«
- 21. člen: **Rok hrambe osebnih podatkov:** »**(**1) Osebni podatki se lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. (2) Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.«
- 22. člen: **Posredovanje osebnih podatkov:** »(3) Upravljavec osebnih podatkov mora za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče kasneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.«
- 24. člen: **Zavarovanje osebnih podatkov**
  - »(1) Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba
  - ter nepooblaščena obdelava teh podatkov tako, da se:
    - varujejo prostori, oprema in sistemska programska oprema vključno z vhodno-izhodnimi enotami;

- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

  - (2) V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativna programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov.
  - (3) Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.«

- 30. člen: **Pravica posameznika do seznanitve** »(1) Upravljavec osebnih podatkov mora posamezniku na njegovo zahtevo: 1. omogočiti vpogled v katalog zbirke osebnih podatkov; 2. potrditi, ali se podatki v zvezi z njim obdelujejo ali ne, in mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje: 3. posredovati izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj; 4. posredovati seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšne namen; 5. dati informacije o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave; 6. dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem; 7. pojasniti tehnične oziroma logično-tehnične postopke odločanja, če izvaja avtomatizirano odločanje o obdelavi osebnih podatkov posameznika.«

ZVOP-1 v 24. členu med drugim določa, da morajo biti osebni podatki zavarovani tako, da je mogoče poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov. Prav tako pa v 30. členu opredeljuje pravico posameznika do seznanitve, komu so bili njegovi osebni podatki posredovani, kdaj, na kateri podlagi in za kateri namen. Informacijsko sredstvo, ki omogoča ukrepanje na podlagi navedenih določil 24. in 30. člena ZVOP-1, je revizijska sled (Delak, 2014, str. 15).

ZVOP-1 postavlja določbe glede varstva osebnih podatkov. Ob kršitvah določb ZVOP-1 predpisuje globe. Ob kršitvah določb 24. in 30. člena ZVOP-1 so v 91. in 93. členu ZVOP-1 predpisane globe v višini:

- od 4.170 EUR do 12.510 EUR za en prekršek pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnosti,
- od 830 EUR do 1.250 EUR (24. člen) oziroma 2.080 EUR (30. člen) za en prekršek za odgovorno osebo pravne osebe, samostojnega podjetnika ali posameznik, ki opravlja dejavnost, državnega organa ali organa lokalne skupnosti,
- od 200 EUR do 830 EUR za en prekršek za posameznika, ki je storil prekršek.

1.1.3 Informacijski pooblaščenec

Inšpekcijski nadzor nad izvajanjem ZVOP-1 in drugih predpisov, ki urejajo varstvo in obdelavo osebnih podatkov, izvaja informacijski pooblaščenec. Informacijski pooblaščenec je samostojen in neodvisen državni organ. Njegova pooblastila in pristojnosti ureja Zakon o informacijskem pooblaščencu (Ur.l. RS, št. 113/2005, 51/2007 – ZUstS-A). Poleg področja varstva osebnih podatkov je informacijski pooblaščenec pristojen tudi za področje dostopa do informacij javnega značaja, ki ga ureja Zakon o dostopu do informacij javnega značaja (Ur.l. RS, št. 24/2003, 61/2005, 113/2005 – ZInfP, 109/2005 – ZDavP-1B, 28/2006, 117/2006 – ZDavP-2, 23/2014, 50/2014, 72/2014 – skl. US, 19/2015 – odl. US, 102/2015, 32/2016). Glavne naloge informacijskega pooblaščenca so: izvajanje inšpekcijskih postopkov in postopkov prekrškov, odločanje o pritožbah, priprava mnenj in smernic, domače in mednarodno sodelovanje (Slovenski odsek ISACA, 2016).

Informacijski pooblaščenec v svojih usmeritvah (Informacijski pooblaščenec, 2010), za katerih izdajo določa pravno podlago 49. člen ZVOP-1, poudarja proaktivno naravnan »koncept vgrajene zasebnosti«, kar pomeni, da bi varstvo osebnih podatkov, zasebnosti morali načrtovati pri vzpostavitvi sistemov med njihovim nastajanjem, saj kasnejše prilagajanje in zniževanje tveganj zlorabe lahko vzame veliko časa, stroškov in celo ugleda. Upravljavcem osebnih podatkov informacijski pooblaščenec svetuje uporabo mednarodno uveljavljenih standardov varovanja informacij, periodično preverjanje prisotnih, znanih ranljivosti, transparentnost uporabljenih rešitev za varovanje osebnih podatkov, spoštovanje posameznika tako, da se mu omogoči ustrezna informiranost glede obdelave njegovih osebnih podatkov (kateri podatki se bodo obdelovali, kdo bo njegove podatke obdeloval in za kateri namen bodo njegovi podatki posredovani tretjim osebam in katerim, kako in koliko časa se bodo njegovi podatki hranili, se lahko njegove podatke iz baz izbriše, uniči). Informacijski pooblaščenec v svojih smernicah posebej poudarja pomembnost beleženja dostopa do podatkov oziroma sledljivost dostopa do podatkov v okviru »obdelave osebnih podatkov«, kot jo določa ZVOP-1. »Z drugimi besedami to pomeni, da je glede na tveganje in naravo podatkov, ki se bodo obdelovali, treba zagotoviti popolno revizijsko sled, torej beleženje vsakega dostopa do podatkov. Odstopanje od tega načela je možno le na podlagi ustrezne analize in obravnave tveganj« (Informacijski pooblaščenec, 2010, str. 11).

1.1.4 Druge pravne podlage in usmeritve

Zgoraj navedeni predpisi so osnovni pravni temelji (za)varovanja osebnih podatkov. Poleg navedenih zagotavljanje sledljivosti podatkov oziroma vodenje revizijskih sledi posredno določajo in priporočajo tudi drugi predpisi in usmeritve. Nekateri so splošni, veljajo ne glede na vrsto dejavnosti, nekateri se uporabljajo glede na vrsto dejavnosti, ki jo opravlja podjetje, nekateri veljajo le za proračunske uporabnike. V nadaljevanju navajam nekatere izmed njih:

- Zakon o javnih financah (Ur.l. RS, št. 79/1999, 124/2000, 79/2001, 30/2002, 110/2002 – ZDT-B, 56/2002 – ZJU, 127/2006 – ZJZP, 14/2007 – ZSPDPO, 109/2008, 49/2009, 38/2010 – ZUKN, 107/2010, 110/2011 – ZDIU12, 46/2013 – ZIPRS1314-A, 101/2013, 101/2013 – ZIPRS1415, 38/2014 – ZIPRS1415-A, 14/2015 – ZIPRS1415-D, 55/2015 – ZFisP, 96/2015, v nadaljevanju ZJF). ZJF v členih 99 in 100 opredeljuje notranjih nadzor javnih financ pri proračunskih uporabnikih.
- Usmeritve za notranje kontrole (2004) Ministrstva za finance Republike Slovenije, Urada Republike Slovenije za nadzor proračuna. Gradivo navaja, da mora biti sled zagotovljena ne glede na to, ali se vodi ročno ali elektronsko. Proračunski uporabnik mora delo organizirati tako, da je dokumentiran celoten postopek poslovanja skupaj s transakcijo.
- Zakon o bančništvu (Ur.l. RS, št. 25/2015, 44/2016 – ZRPPB, v nadaljevanju ZBan-2). ZBan-2 v členih 125–127 predpisuje zaupne podatke ter dolžnost varovanja in uporabo zaupnih podatkov.
- Zakon o elektronskih komunikacijah (Ur.l. RS, št. 109/2012, 110/2013, 40/2014 – ZIN-B, 54/2014 – odl. US, 81/2015, v nadaljevanju ZEKom-1). ZEKom-1 v 31. točki 3. člena opredeljuje »kršitev varstva osebnih podatkov«, ki ga v nadaljevanju navaja v okviru določb posameznih členov.
- Zakon o davčnem postopku (Ur.l. RS, št. 117/2006, 24/2008 – ZDDKIS, 125/2008, 85/2009, 110/2009, 1/2010 – popr., 43/2010, 97/2010, 24/2012 – ZDDPO-2G, 24/2012 – ZDoh-2I, 32/2012, 94/2012, 101/2013 – ZDavNepr, 111/2013, 22/2014 – odl. US, 40/2014 – ZIN-B, 25/2014 – ZFU, 90/2014, 95/2014 – ZUJF-C, 23/2015 – ZDoh-2O, 23/2015 – ZDDPO-2L, 91/2015, v nadaljevanju ZDavP-2). ZDavP-2 v 38. členu določa »elektronsko obdelavo podatkov«, v okviru katere je v 8. in 9. točki člena predpisano, da mora zavezanec za davek uporabljati tako računalniško opremo in elektronske naprave, ki omogočajo izpis izvornih podatkov in sprememb izvornih podatkov. To mu morajo zagotoviti tudi prodajalci oziroma dobavitelji programske opreme v programskih rešitvah.
- Pravilnik o zahtevah za računalniške programe in elektronske naprave, upravljanje in delovanje informacijskega sistema ter o vsebini, obliki, načinu in rokih za predložitev podatkov (Ur.l. RS, št. 35/2013, 42/2013 – popr., 57/2013, 18/2016) je pravilnik, ki natančno opredeljuje 8. in 9. točko 38. člena ZDavP-2.
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Ur. l. RS, št.

30/2006, 24/2014 – odl. US, 51/2014, v nadaljevanju ZVDAGA). ZVDAGA ureja varstvo dokumentarnega in arhivskega gradiva in je z vidika varovanja podatkov pomemben glede časa hrambe podatkov, če so roki določeni drugače, kot to določa 2004-1.

- Zakon o gospodarskih družbah (Ur.l. RS, št. 42/2006, 60/2006 – popr., 26/2007 – ZSDU-B, 33/2007 – ZSReg-B, 67/2007 – ZTFI, 10/2008, 68/2008, 42/2009, 33/2011, 91/2011, 100/2011 – skl. US, 32/2012, 57/2012, 44/2013 – odl. US, 82/2013, 55/2015, v nadaljevanju ZGD-1). 39. člen ZGD-J določa pojem poslovne skrivnosti, ki med drugim vključuje tudi podatke, zaradi katerih bi nastala škoda, če bi zanje izvedela nepooblaščena oseba.

Uratnik (2011, str. 160–161) navaja, da zakoni in predpisi zahtevajo in priporočajo uporabo revizijske sledi v informacijskih sistemih. Vendar ne navajajo neposredno, kako jo v sistem vgraditi in uporabljati. Pri določanju, kakšna mora biti revizijska sled in kako jo uporabljati, so natančnejši standardi in dobre prakse na področju informacijske tehnologije, saj imajo revizijsko sled za pomemben člen zagotavljanja varnosti informacijskih sistemov.

Zato je pri zagotavljanju revizijskih sledi poleg upoštevanja veljavnih pravnih aktov priporočeno tudi upoštevanje smernic mednarodno uveljavljenih standardov, priporočil varovanja informacij v informacijskih sistemih. Nekateri izmed njih so omenjeni v nadaljevanju (poglavje 3.2).

2 REVIZIJSKA SLED

Podjetja se dnevno srečujejo z veliko količino podatkov, ki jih morajo varovati kot poslovno skrivnost. Te podatke je treba ustrezno hraniti in hkrati zagotoviti njihove revizijske sledi. **Revizijska sled je informacija o tem, kateri podatek je bil predmet obdelave, kdo ga je obdeloval, komu je bil posredovan in na kateri pravni osnovi** (Merc & Šavnik, 2015, str. 9).

Informacijski pooblaščenec (2010) izpostavlja dve med seboj povezani bistveni vprašanji glede revizijskih sledi:

- **Nadzor nadzornikov** oziroma pooblastila skrbnikom z najvišjimi pravicami (sistemski skrbniki). Z organizacijskimi in tehničnimi ukrepi mora biti zagotovljen nadzor nad sistemskimi skrbniki oziroma jim ne sme biti s pooblastili dana možnost, da bi onemogočili avtentičnost in celovitost revizijske sledi.
- **Avtentičnost in celovitost** revizijskih sledi obdelave osebnih podatkov. Z organizacijskimi in tehničnimi ukrepi mora biti zagotovljeno, da beleženje dostopov ne more biti trajno ali začasno izključeno. Prav tako nikomur ne sme biti dana možnost naknadnega popravljanja, spreminjanja, brisanja dela ali celotne revizijske sledi – ne

glede na to, ali gre za aktivnosti sistemskega skrbnika ali aktivnosti drugih.

ZVOP-1 določa, da mora biti zagotovljena tako **notranja sledljivost** (sledljivost obdelave osebnih podatkov pri upravljavcu) kot **zunanja sledljivost** obdelave osebnih podatkov (katerim zunanjim uporabnikom so bili posredovani osebni podatki).

2.1 Opredelitev revizijske sledi

»Revizijska sled je nespremenljiv podroben dokumentiran zapis, ki nedvoumno, neizpodbitno in celovito dokumentira zapisovanje in spreminjanje zapisov v njihovi celotni življenjski dobi od izvornega zapisa do trenutno veljavnega zapisa in iz katere je razvidno vsaj, kdo, kdaj, s katerimi podatki in kakšno operacijo je izvedel nad posameznim zapisom, ter s tem omogoča naknadno prepoznavanje časovne točke, vršilca, načina in vsebine naknadne obdelave podatkov, na katere se revizijska sled nanaša.

Revizijska sled naj bo torej ločen zapis dogodka, ki se je zgodil v informacijskem sistemu z navedbo vseh ključnih podatkov za enolično prepoznavo okoliščin nastanka dogodka kot njegovih posledic. Revizijska sled naj bo nesprejemljiva in trajna, morebitne spremembe zaradi zastaranja ali zahtev zakonodaje se morajo beležiti ločeno, prav tako vsi vpogledi v revizijsko sled z navedbo razloga za vpogled. Dostop do revizijskih sledi naj bo omejen na notranje in zunanje revizorje oziroma uporabo v posebnih primerih (npr. incidenti, uradne pritožbe, izvajanje pooblaščenega nadzora)« (Slovenski inštitut za revizijo, 2013, str. 167–168).

Poznamo različne opredelitve revizijskih sledi. Delak (2014, str. 12) meni, da je zgoraj navedena opredelitev osnova za uvedbo in uporabo revizijske sledi v informacijskih sistemih. Poleg revizorjev informacijskih sistemov je namenjena tudi poslovodstvu, strankam, lastnikom v podjetju, strokovnjakom informacijsko-komunikacijske tehnologije, nadzornikom in notranjim revizorjem. V bistvu gre za prvo enotno opredelitev strokovnjakov, prej enotne opredelitve in uporabe revizijske sledi v slovenskem prostoru ni bilo.

2.2 Zgodovina teorije revizijske sledi

Izraz revizijska sled se je prvič pojavil v računalništvu v 50. letih prejšnjega stoletja. Revizijske sledi se beležijo še vedno, beležijo se tako ročno kot avtomatsko, nekateri zapisi se še vedno beležijo klasično, večina pa jih je del informacijskih sistemov, ki so vse okoli nas. V prispevkih na temo revizijskih sledi je revizijska sled predstavljena iz različnih zornih kotov, končni cilj vseh pa je izboljšati varovanje informacij in zmanjšanje možnosti, da informacije uhajajo iz sistema. Trend objav prispevkov na temo revizijskih sledi v tujini narašča, kar je razvidno iz Tabele 1 (Delak, 2014, str. 7–11).

Tabela 1: Število tujih objav na temo revizijske sledi v informacijskem sistemu

Obdobje objave	Število objav	Delež (v %)
pred letom 1980	1	1
1980–1989	5	5
1990–1999	21	23
2000–2009	39	42
po 2010	26	28
Skupaj:	**92**	**100**

Vir: B. Delak, Revizijska sled v informacijskih sistemih v teoriji in praksi, 2014, str. 9, tabela 3.

Prva enotna strokovna opredelitev revizijske sledi v slovenskem prostoru (navedena v točki 2.1 tega diplomskega dela) je bila objavljena leta 2013. Definicijo je določila delovna skupina, katere člani so bili predstavniki Ministrstva za finance, Davčne uprave Republike Slovenije, Združenja za informatiko in telekomunikacije Gospodarske zbornice Slovenije, Združenja računovodskih servisov Gospodarske zbornice Slovenije ter Slovenskega inštituta za revizijo (Slovenski inštitut za revizijo, 2013, str. 167–168).

Pri iskanju gradiva za predmetno diplomsko delo sem naletela na prispevke o revizijskih sledeh v slovenskem jeziku, ki so na voljo od leta 2010 dalje. Prispevki so objavljeni v reviji Slovenskega inštituta za revizijo SIR*IUS (v letih 2013 in 2014) ter v zbornikih referatov mednarodnih konferenc o revidiranju in kontroli informacijskih sistemov, ki jih organizirata Slovenski inštitut za revizijo ter slovenski odsek mednarodnega združenja ISACA. ISACA je neprofitno, neodvisno članske združenje, ki skuša zagotoviti »zaupanje v informacijske sisteme in korist od njih« (Slovenski odsek ISACA, v nadaljevanju ISACA).

2.3 Čas hrambe revizijskih sledi

ZVOP-1 določa, da je rok hrambe podatkov določen glede na namen obdelave podatkov, razen če drugi zakoni na določajo drugače. Ne določa pa posebej roka hrambe revizijskih sledi.

»Revizijske sledi imajo informacijsko vrednost dalj časa, ne samo v času nastanka. Potrebno jih je ustrezno varovati in hraniti (Uratnik, 2011, str. 168).«

Pri tem je treba poudariti, da morajo podjetja razlikovati med roki hrambe podatkov in roki hrambe revizijskih sledi. Po poteku roka hrambe podatkov ni nujno, da poteče tudi rok hrambe za revizijske sledi, ki se nanašajo na te podatke. Revizijsko sled obdelave podatkov je treba hraniti še po obdelavi podatkov oziroma še po končanju hrambe podatkov (uničenju). To velja še posebej za obdelavo osebnih podatkov. Nadalje je treba voditi revizijsko sled vseh obdelav revizijskih sledi (tudi revizijsko sled načina konca hrambe

podatkov, saj je le-ta predpisan z ustreznim postopkom), tudi osebne podatke tistih, ki bodo uničili predhodne sledi. To pomeni, da morajo upravljavci osebnih podatkov omogočiti številne cikle upravljanja z revizijskimi sledmi. Zagotavljanje revizijskih sledi postaja za podjetja vse večji izziv, predvsem zaradi obsežne količine podatkov, kar pomeni, da je pomen primerne informacijske podpore notranjim procesom podjetij vse pomembnejši (Merc & Šavnik, 2015).

Čas hrambe revizijskih sledi za posamezno podjetje je odvisen od zakonodaje, ki velja za dejavnost, za katero je podjetje registrirano. Revizijske sledi, ki nastanejo med izvajanjem dejavnosti oziroma izvajanjem procesov, je treba hraniti trajno ali pa za različno dolga obdobja, od 4 do 20 let (Delak, 2014, str. 15–16).

3 REVIZIJSKE SLEDI V INFORMACIJSKEM SISTEMU

Eden največjih sodobnih izzivov je zagotavljanje informacijske varnosti (Markelj & Bernik, 2012) povsod okoli nas: za posameznika, v gospodarstvu, v javni upravi. Področje informacijske varnosti ločimo kot:

- **Informacijsko varnost v poslovanju**; pomeni vzpostavljanje, vzdrževanje in upravljanje informacijske varnosti v poslovnih sistemih.
- **Informacijsko varnost na področju kriminalitete;** pomeni preiskovanje računalniške kriminalitete, preprečevanje nedovoljenih, nezakonitih vdorov in zaščito.

V tem diplomskem delu je revizijska sled obravnava kot del zagotavljanja informacijske varnostni v poslovno-informacijskih sistemih.

Z vidika informacijskega sistema revizijska sled pomeni beleženje vstopov ali poizkusov vstopov v sistem ali del sistema, zavračanja dostopa do sistema, beleženje vpogledov v podatke, vnos, brisanje, spreminjanje, izpis podatkov (Uratnik, 2011, 159).

Z vidika informacijske varnosti je po mojem mnenju pomembna opredelitev Delaka (2014, str. 7), ki revizijske sledi ne pojmuje samo kot vrste zapisa, ampak tudi sredstvo, dnevnik, »ki omogoča nadzor v smislu varovanja informacij nad beleženjem aktivnosti, obdelavami podatkov, drugimi zapisi in aktivnostim, ki jih izvajajo uporabnik, programi in vzdrževalci«.

Oblak (2011, str. 197) revizijsko sled vidi kot način za ugotavljanje nepravilnosti v informacijskem sistemu. Navaja, da revizijska sled ne bo preprečila zlorabe podatkov, se bo pa s pomočjo revizijske sledi lažje našlo krivca.

Ko v podjetju pride do nekega dogodka ali stanja, je treba ugotoviti, kako se je zgodil, kdo in kdaj ga je povzročil, kakšno je bilo stanje v podjetju pred tem dogodkom. Če ima

podjetje ustrezno uvedene in uporabljene (v nadaljevanju vodene) revizijske sledi v programski opremi in v informacijskem sistemu, odgovor lahko enostavno pridobi. Tudi varnost informacijskega sistema v podjetju je večinoma odvisna od vodenja revizijskih sledi. Vodenje revizijske sledi v informacijskem sistemu omogoča naslednje **aktivnosti in njihove učinke** (Uratnik, 2011, str. 157–159):

- **Nadzor aktivnosti uporabnikov.** Revizijske sledi, vključno z njihovim rednim preventivnim pregledovanjem, omogočajo lastnikom, vodstvu, notranji reviziji nadzor nad uporabniki ob standardni uporabi sistema. Če so odstopanja pri uporabi, lahko prav redno preventivno pregledovanje prepreči morebitno škodo. Uporabniki predstavljajo različna varnostna tveganja. Na primer večje varnostno tveganje predstavljajo sistemski skrbniki.
- **Zagotavljanje večje varnosti v informacijskih sistemih.** Z rednim pregledovanjem sistemskih dnevnikov (t.i. zapisov dogodkov v času delovanja sistema v mrežnih, varnostnih napravah, operacijskih sistemih) se lahko pravočasno pokažejo morebitni poizkusi vdorov ali druge nepooblaščene aktivnosti oziroma odstopanja od standardne uporabe.
- **Zagotavljanje skladnosti z zahtevami zakonov in drugih predpisov.** Vrsta zakonov in drugih predpisov zahteva izvajanje poslovanja tako, da je vsak trenutek mogoče ugotoviti potek in vsebino uporabe informacijskega sistema. S tem je dokazana skladnost poslovanja.
- **Preventivno učinkovanje.** Uvedene in redno pregledovane revizijske sledi bodo odvrnile potencialne (notranje) storilce od nepooblaščenih dostopov (protipravnih in kaznivih dejanj).
- **Raziskovanje dogodkov.** Ob nepooblaščenem dostopu, incidentu v informacijskem sistemu je zelo pomembno, kako dobro, hitro in natančno lahko raziščemo dogodek ter ugotovimo način in izvedbo incidenta. Hkrati se ugotovijo tudi slabosti sistema. Posledično se sistem lahko zaščiti pred podobnimi incidenti.
- **Dokazovanje dogodkov.** V informacijskih sistemih posamezne dogodke uporabniki izvedejo nepooblaščeno. V takih primerih je zelo pomembno, da so na voljo pravočasne in pravilne revizijske sledi o teh dogodkih, vpogledih, spreminjanju podatkov, transakcijah. Te revizijske sledi so v nadaljnjih postopkih (internih disciplinskih postopkih, sporih, postopkih pred sodiščem) dokazilo o dogajanju v informacijskih sistemih.
- **Dokazovanje škode.** S pomočjo revizijskih sledi se lažje določi materialno škodo, ki je nastala kot posledica nepooblaščenega dostopa, incidenta.

3.1 Zagotavljanje celovite revizijske sledi v informacijskem sistemu

Opredelitev revizijske sledi v točki 2.1 in prav tako informacijski pooblaščenec (Informacijski pooblaščenec, 2010) v svojih usmeritvah navajata, da mora biti revizijska

sled celovita, celotno dokumentirana. V informacijskih sistemih je celovitost revizijske sledi glede na stanje in uporabnost razumljena kot (Delak, 2014, str. 16, 19):

- aplikativna revizijska sled oziroma revizijska sled za aplikativno programsko opremo,
- sistemska revizijska sled oziroma revizijska sled za sistemsko programsko opremo,
- orodje, s katerim se revizijska sled pregleduje.

Priporočeno je, naj bo zagotovljena celotna revizijska sled, tako za aplikativno kot za sistemsko programsko opremo. Če to ni mogoče, je priporočeno vsaj zagotavljanje revizijske sledi za aplikativno programsko opremo, ki obdeluje osebne podatke. Revizijska sled za aplikativno programsko opremo se naredi v podatkovni bazi, kjer aplikacije hranijo podatke. Revizijska sled za sistemsko programsko opremo sledi dogodkom v sistemu, kot so na primer prižiganje oziroma ugašanje računalnika, prijava oziroma odjava uporabnika v sistem, iskanje virusov, zagon oziroma zaustavitev baze podatkov (B. Oblak, osebna komunikacija, 16. junij 2016).

3.2 Revizijske sledi in revizija informacijskega sistema

»**Revizija informacijskega sistema** (v nadaljevanju revizija) je sistematičen strokovni pregled tehničnega in organizacijskega vidika zagotavljanja informacijske podpore v podjetju, katerega namen je preveriti skladnost delovanja informacijske tehnologije s predpisi, standardi in dobrimi praksami« (Slovenski inštitut za revizijo, 2016).

»**Revizor informacijskih sistemov** (v nadaljevanju revizor) z veljavno licenco Slovenskega inštituta za revizijo je strokovno usposobljen za izvajanje revizijskega pregleda ter izpolnjuje najvišje strokovne in etične standarde« (Slovenski inštitut za revizijo, 2016).

Zaradi zahtev po vodenju revizijskih sledi morajo revizorji v okviru revizij preverjati tudi, ali je revizijska sled v programski opremi, ki jo uporablja revidirano podjetje, vodena ustrezno. Z vidika revizije je poudarek na aplikativni programski opremi. Aplikativna revizijska sled je pomemben dokaz o dogodkih v informacijskem sistemu. To je podatek o tem, kdo je izvedel katero dejanje v sistemu in kdaj ga je izvedel. V praksi je ob upoštevanju veljavnih predpisov beleženja revizijskih sledi še vedno veliko problemov. Problemi so povezani z zasnovo revizijske sledi, zagotavljanjem beleženja revizijske sledi ob uporabi informacijskega sistema, katerega del je tudi aplikativna programska oprema z lastno funkcijo zapisa revizijske sledi ter hkrati vzdrževanja tega zapisa, kar vključuje varno hrambo. Samo sledljivost še ne zadošča. Vpeljani morajo biti tudi postopki za pregledovanje revizijske sledi, podana morajo biti zagotovila, da so dejanja, ki se kažejo v revizijski sledi, veljavna in pravilno potrjena. Revizor mora najti dokaze, da se revizijske sledi pregledujejo in se po njih ukrepa. Revizorji pri svojih zahtevah iz poleg že predstavljenih zakonskih zahtev v prvem poglavju predmetnega diplomskega dela in

opredelitve revizijske sledi v poglavju 2.1 predmetnega diplomskega dela izhajajo tudi iz smernic in priporočil mednarodnih standardov iz družine ISO/IEC 27000, t.i. standardi za zagotavljanje informacijske varnosti (ISO 2700 Directory, 2016), Mednarodnega standarda revidiranja 500 (Mednarodni standard revidiranja, MSR 500, Revizijski dokazi, 2016, nadaljevanju MSR 500) in priporočil ISACA. MRS 500 med drugim navaja, da revizor pri načrtovanju in izvajanju revizijskih postopkov kot revizijske dokaze upošteva tiste informacije, ki so primerne in zanesljive (Slovenski inštitut za revizijo, 2013, str. 165–167).

Revizijske sledi bi morale biti uvedene v vse sisteme: v sistem za upravljanje podatkovnih baz, sistemsko opremo na strežnikih in v sistemsko opremo na komunikacijah. Hkrati morajo imeti podjetja na voljo orodje za hitro in učinkovito pregledovanje revizijskih sledi. Z orodjem se revizijska sled pregleduje, raziskuje in išče po njej**.** Revizorji morajo imeti določena znanja o orodjih, navadno so jim na volji priročniki za osnovno uporabo in razumevanje (B. Oblak, osebna komunikacija, 16. junij 2016).

4 PROGRAMSKE REŠITVE ZA VODENJE REVIZIJSKIH SLEDI

Za vodenje revizijskih sledi v informacijskem sistemu so na voljo različne rešitve. Po mnenju strokovnjaka (B. Oblak, osebna komunikacija, 16. junij 2016) je ne glede na vrsto rešitev oziroma programskega orodja, ki se za vodenje revizijskih sledi uporablja, uvajanje zapleteno, nepriljubljeno tako pri podjetjih (naročnikih) kot dobaviteljih ustreznih rešitev. Podjetja namreč upravljajo z ogromnimi količinami podatkov v elektronski obliki in treba je beležite **vse spremembe** teh podatkov, **dostope** do njih ter **stare vrednosti** podatkov pri spremembah. Stanje v praksi je takšno, da starejše aplikacije posebnega orodja za beleženje revizijskih sledi nimajo, medtem ko so orodja za beleženje revizijskih sledi pri novejših aplikacijah že vgrajena. Za beleženje revizijskih sledi se uporablja **namenski uporabniški vmesnik.**

4.1 Lastnosti vodenja revizijskih sledi

Glede na to, kje se revizijske sledi nahajajo oziroma kam se namestijo, govorimo o vzpostavitvah revizijskih sledi na delovnih postajah, v aplikacijah, podatkovnih bazah, operacijskih sistemih, na strežnikih, na mrežnih, komunikacijskih in varnostnih napravah (Rakar & Žele, 2010, str. 144).

Uvedba revizijske sledi je zakonsko predpisana, zaradi svoje zahtevnosti vključitve v sistem pa hkrati med razvijalci nepriljubljena. Zahtevnost in hkrati nepriljubljenost je posledica splošnosti ZVOP-1, saj je njegove zahteve zaradi splošnosti težko vključiti v rešitev (Vezjak, 2012, str. 171).

4.1.1 Ravni revizijske sledi

Povzeto po Vezjaku (2012, str. 173) ločimo **tri ravni beleženja** dogodkov oziroma zagotavljanja **revizijskih sledi:**

1. Raven oziroma beleženje aktivnih dostopov do podatkov, t.i. sledljivost sprememb podatkov; ta raven sledljivosti omogoča, da pozneje ugotovimo, kdo, kdaj in kjer je spreminjal podatke (vnesel, spremenil, izbrisal).
2. Raven oziroma beleženje aktivnih in pasivnih dostopov do podatkov, t.i. sledljivost dostopa do podatkov; ta raven sledljivosti omogoča, da poleg tega, kdo je spreminjal podatke, tudi pozneje lahko ugotovimo, kdo je dostopal do podatka (vpogled, seznanitev), vendar (zapisa) podatka ni spreminjal.
3. Raven oziroma beleženje dostopov, beleženje sprememb podatkov ter beleženje tako izvornih kot popravljenih podatkov, kar pomeni, da na podlagi sledljivosti lahko pozneje ugotovimo, kdo je do podatkov dostopal, jih spreminjal, hkrati pa tudi, kakšen je bil prvoten podatek in v kaj je bil spremenjen.

4.1.2 Ustreznost in učinkovitost revizijske sledi

Ustrezna nastavitev revizijske sledi vedno pomeni izredno zahteven proces – tako za naročnike kot za dobavitelje rešitev, ki ga je treba natančno načrtovati, izvesti, redno pregledovati in posodabljati. Zelo pomembno pa je, da podjetje **naredi ustrezno analizo tveganja** za svoj informacijski sistem, tako poslovni kot tehnični del. Na podlagi analize tveganja določi svoje potrebe po beleženju revizijskih sledi, na podlagi potreb pa tudi vsebino revizijskih sledi oziroma podatke, ki se z revizijskimi sledmi beležijo. Podjetje mora izdelati **politiko revizijskih sledi**, ki med drugim določa:

- kritične sisteme in podatke, za katere je treba zagotoviti revizijske sledi,
- dogodke, ki jih je treba beležiti,
- elemente, ki jih morajo beleženja vsebovati,
- analiziranje, pogostost pregledovanja, prenašanje beleženja, shranjevanje podatkov,
- odstranjevanje podatkov iz revizijskih sledi,
- procese za upravljanje revizijskih sledi,
- odgovornost za upravljanje revizijskih sledi.

Pri tem je pomembno, da je **vzpostavljanje in upravljanje revizijskih sledi usklajeno s** poslovnimi zahtevami za delovanje sistemov, z varnostnimi zahtevami za sisteme in podatke, z zakonodajo, pogodbenimi obveznostmi in standardi na področju varovanja (Uratnik, 2011, str. 164–165).

Strokovnjaki navajajo različne dejavnosti, ki jih mora beležiti učinkovita revizijska sled. Oblak (2011, str. 192, 193) navaja, da je za učinkovito revizijsko sled treba voditi:

- vse prijave in odjave v sistem oziroma iz njega,
- vse ukaze za vpogled v podatke,
- vse uspešno izvedene poizvedbe,
- vse poskuse poizvedb, ki so se končale neuspešno,
- vse ukaze s spreminjanjem pooblastil,
- revizijske sledi vklopa ali izklopa vodenja revizijske sledi nad posameznim objektom,
- vse ukaze nad objekti.

Zgoraj navedene so revizijske sledi, ki opisujejo poizvedbe nad objekti (Oblak, 2011, str. 192). Druga vrsta so revizijske sledi, ki opisujejo spremembe podatkov. Delak (2014, str. 16) tovrstno razdelitev revizijskih sledi navaja kot aplikativne revizijske sledi in sistemske revizijske sledi (poglavje 3.1).

4.1.3 Koraki in predpostavke revizijske sledi

Rakar in Žele (2010, str. 145) navajata naslednje **korake za vzpostavitev revizijskih sledi** v podjetju:

- popis informacijskih sredstev (vključuje mrežno opremo, strežnike, programsko opremo, baze podatkov, dokumente),
- ocena tveganja za možnost nepooblaščenih dostopov in zlorabe pravic,
- izdelava politike revizijske sledi,
- izdelava izvedbenih dokumentov,
- nastavitev sistemov, naprav in aplikacij v skladu z izvedbenimi dokumenti.

Pri vzpostavitvi sistema za zagotavljanje revizijske sledi (vključno z moduli in poročili) morajo biti upoštevane naslednje **predpostavke** (Vezjak, 2012, str. 176):

- **Sistem oziroma aplikacija ne sme delovati, če sistem revizijskih sledi ne deluje**. Gre za strog predpis, ki preprečuje, da bi bila ranljivost sistema zlorabljena.
- Zagotovljena mora biti **splošnost sistema;** rešitev mora biti odprta za različne sisteme, formate, ki so in bodo v informacijskem sistemu.
- Zagotovljena mora biti **skladnost sistema z zakonodajo;** sistem mora biti skladen z zakonodajo.
- Zagotovljena mora biti **optimalna količina podatkov revizijske sledi**; zapisovati je treba **le tiste podatke, ki so nujni in smiselni** za potrebe revizijske sledi.
- **Časovni pribitek operacijam** zaradi revizijske sledi mora biti **minimalen**; revizijska sled mora biti izvedena optimalno, saj dodatno upočasnjuje delovanje aplikacije.
- Zagotovljena mora biti **čim manjša povezanost sistema za zagotavljanje revizijskih sledi in aplikacij;** sistem za zagotavljanje revizijskih sledi mora biti programsko in podatkovno neodvisen od aplikacij.

- Zagotovljena mora biti **dostopnost revizijske sledi;** revizijska sled mora biti hitro in enostavno dostopna (na voljo mora biti enostavno povpraševanje) in enostavno berljiva.
- Zagotovljena mora biti **neodvisnost podatkov od programiranja;** sistem mora podatke izpisovati v standardni format (bazo, tekstovno datoteko).

Ko je projekt uvedbe revizijskih sledi končan, je nujno, da se revizijske sledi tudi redno **pregledujejo**, saj le tako ustrezno služijo svojemu namenu, zagotavljanju varnosti informacij v sistemu. Na osnovi pregledovanj se lahko ugotovijo dogodki, kot so na primer nedovoljeni notranji dostopi ali celo zunanji vdori. Tako se odkrijejo pomanjkljivosti v sistemu. Pomembno je, da so na voljo ustrezna orodja za pregledovanje revizijskih sledi in da jih pregleduje neodvisna oseba. To je lahko revizor informacijskega sistema ali pooblaščena oseba (Uratnik, 2011, str. 166–167).

Kot bo navedeno v nadaljevanju, je pregledovanje potrebno tudi z vidika rešitve za vodenje revizijske sledi, saj je le tako možno ustrezno nadgrajevati oziroma posodabljati programsko rešitev za vodenje revizijskih sledi.

Če povzamem do sedaj navedene lastnosti revizijskih sledi in mnenje strokovnjaka (B. Oblak, osebna komunikacija, 16. junij 2016), mora biti revizijska sled v informacijskem sistemu vodena (vodenje zajema beleženje oziroma zapisovanje revizijske sledi ter pregledovanje oziroma iskanje po revizijskih sledeh) **zakonsko ustrezno, učinkovito in zadostno za podjetje**. Kakšna je zadostna revizijska sled, podjetje ugotovi na podlagi izvedene analize varnostnega tveganja, ki je osnova za določitev politike revizijskih sledi. Razvoj ustrezne rešitve poteka na podlagi izdelane politike revizijske sledi podjetja.

4.2 Predstavitev rešitev za vodenje revizijskih sledi

Po mnenju strokovnjaka (B. Oblak, osebna komunikacija, 16. junij 2016) je za poslovne uporabnike pri uvajanju rešitev za vodenje revizijske sledi pomembno, da dobro poznajo aplikacije in model podatkovne zbirke aplikacij, za katere želijo voditi revizijske sledi, kar je hkrati tudi najbolj problematično. Le z dobrim poznavanjem lahko označijo prave entitete, za katere naj se revizijska sled vodi in s tem zmanjša količino revizijske sledi. Podjetje mora sodelovati z avtorjem aplikacije (če ne gre za lastno aplikacijo) in tudi zagotoviti ustrezno zmogljivo strojno opremo.

Delitve in priporočila glede uporabe programskih rešitev za vodenje revizijskih sledi so različni. V nadaljevanju so predstavljene osnovne lastnosti posamezne rešitve uvajanja revizijskih sledi glede na vrsto operacijskega sistema oziroma sistema za upravljanje podatkovnih baz. V splošnem velja, naj se ne glede na uporabljeno programsko rešitev oziroma operacijski sistem revizijske sledi kot dnevniški zapis **nastavijo ustrezno za posamezno okolje.** Vsaka rešitev namreč ni ustrezna za vsako okolje (podjetje), upoštevati

je treba tudi pomanjkljivosti, ki jih ima vsaka od v nadaljevanju opisanih rešitev za vodenje revizijskih sledi in so pri opisu posamezne rešitve tudi omenjene. Predstavitev je povzeta po Delaku (2014, str. 19–22).

4.2.1 Operacijski sistem Microsoft

Na operacijskih sistemih Microsoft (različne verzije Windowsov) je možno ustrezno nastavljati revizijske sledi v obliki določenih dnevniških zapisov, ki omogočajo beleženje uspešnih in neuspešnih dostopov do posameznih delov informacijskih sistemov. Te dostope v nadaljevanju imenujemo dogodki. Ti dnevniški zapisi se lahko nastavijo na delovne postaje (nastavi uporabniški skrbnik) in strežnike (nastavi skrbnik domene). Dnevniški zapisi se pregledujejo s pomočjo pregledovalnika dogodkov (angl. *event viewer*). Na delovnih postajah lahko pregledujemo dnevniške zapise operacijskega sistema, kot so uporabniški dnevnik, sistemski dnevnik, dnevnik nastavitev, dnevnik posredovanih dogodkov in varnostni dnevnik, ki ga lahko pregleduje le skrbnik. Nastavitev dnevniških zapisov oziroma beleženja dogodkov na strežniku je sicer podobna kot na delovnih postajah, vendar z vidika varnosti pomembnejša in zahtevnejša. Strežnik namreč preverja uporabnike in računalnike v celi domeni, posledično se na njem beležijo tudi vse prijave na računalnike v domeni. Kadar gre za večja omrežja in večji obseg dnevniških zapisov, je poleg pregledovalnika dogodkov treba uporabljati dodatna orodja za pregledovanje zapisov. Opisana rešitev ima naslednje pomanjkljivosti:

- če gre za beleženje veliko različnih dnevniških zapisov, je za iskanje posameznega dogodka potrebnega veliko časa in izkušenj;
- če se zagon delovne postaje ali strežnika izvede iz zunanjega medija, je možen vklop računalnika in dostop do podatkov v računalniku brez beleženja dnevniških zapisov;
- možnost zlorabe pravic skrbnika domene – ta lahko izbriše dnevniški zapis (delno ali v celoti).

4.2.2 Odprtokodni operacijski sistemi

Nastavitev revizijskih sledi v odprtokodnih operacijskih sistemih, kot sta na primer operacijska sistema Linux ali ReactOS, se med seboj razlikuje glede na vrsto odprtokodnega operacijskega sistema in glede na uporabo (namizna ali strežniška). Ti sistemi omogočajo izdelavo različnih revizijskih poročil, ker so dnevniški zapisi lahko nerazumljivi. Z ustreznimi ukazi se lahko poišče zapis določenega dogodka. Nastavitev revizijskih sledi v odprtokodnih operacijskih sistemih je možna s tako imenovanimi prikritimi procesi (angl. *auditing daemon),* ki omogočajo:

- beleženje različnih dostopov do datotek, imenikov in posameznih virov.
- sledenje sistemskim klicem, ki temeljijo na prej določenih pravilih, za katere je značilno, da se lahko nastavijo v t.i. korenski particiji (del diska, ki ga računalnik

uporablja kot ločeno enoto in se priklopi na korenski datotečni sistem). Z ustrezno nastavitvijo dovoljenj za sistemske klice se lahko beležijo različni posegi (branje, pisanje, spreminjanje, izvajanje).

4.2.3 Operacijski sistem Mac OS

Gre za operacijske sisteme proizvajalca Apple – Mac OS, katerih osnova je operacijski sistem Unix, osnova za revizijske sledi pa je format datotek Sun´s BMS (Base Security Model). Nastavitev revizijskih sledi je podobna kot pri odprtokodnih operacijskih sistemih s smiselno uporabo preverjenih dobrih praks.

4.2.4 Operacijski sistem na komunikacijski opremi

Gre za pravilno namestitev operacijskega sistema na aktivno komunikacijsko opremo (na primer Cisco). Osnovnemu izdelku se doda pakete z določenimi lastnostmi (podatkovni, varnostni ali združeni ukazi), ki se jih lahko ustrezno nastavi.

4.2.5 Sistemi za upravljanje podatkovnih baz

V nadaljevanju so predstavljeni trije najpogostejši sistemi za upravljanje podatkovnih baz (v nadaljevanju SUPB): DB2, MS SQL in Oracle. Navedeni SUPB so nameščeni na različnih operacijskih sistemih, vsak od njih pa ima svoje nastavitve zapisov oziroma revizijske sledi v posameznih sistemskih rešitvah.

4.2.5.1 DB2

V okviru obravnavane podatkovne baze sta dve ravni revizijskih aktivnosti: primarna raven in raven podatkovne baze ter dva profila skrbnikov, ki imata razdeljena pooblastila oziroma pravice: pravice skrbnikov na primarni ravni (v nadaljevanju SYSADM) in pravice skrbnikov na ravni podatkovne baze (v nadaljevanju SECADM). Revizijski dnevniški zapis in revizijska nastavitvena datoteka sta na primarni ravni. Revizijske nastavitve na primarni ravni upravlja SYSADM. Politiko revizijske sledi upravlja skrbnik SECADM. Revizijska sled za obdelave, ki jih izvajajo skrbniki SYSADM, ni vzpostavljena.

4.2.5.2 MS SQL

Je sistem za SUBP. Deluje kot samostojni podatkovni strežnik, ki je lahko porazdeljen na več strežnikov. Obstajajo standardne in poslovne različice strežnikov, med katerimi so velike razlike. Bolj funkcionalne so poslovne različice, pri katerih ločimo nastavitvi revizijskih sledi CC in C2. C2 beleži večji obseg aktivnosti in je z vidika zapisovanja

obdelave osebnih podatkov skladna z ZVOP-1. Posledično to pomeni veliko dnevniških zapisov v bazi, zaradi katerih je tudi odzivni čas slabši.

4.2.5.3 ORACLE

Oracle je SUPB, ki omogoča dva načina: osnovni SUPB ali pa osnovni SUPB z dodatno rešitvijo, ki zahteva posebno licenco Oracle Audit Vault (v nadaljevanju OAV). OAV omogoča: skladnost z zahtevami predpisov, s pomočjo varnega in nadgradljivega revizijskega podatkovnega skladišča zmanjšanje varnostnih tveganj, po potrebi integracijo s SUPB DB2 in MS SQL. Tudi pri Oraclu obstajajo standardne in poslovne različice strežnikov. Za problematiko, predstavljeno v tej nalogi, so uporabne poslovne različice, saj le-te vključujejo lastnosti za zagotavljanje varnosti. Orodje Arbiter za vodenje revizijskih sledi, ki bo predstavljeno v naslednjem poglavju, omogoča vse lastnosti za zagotavljanje varnosti tako pri poslovnih kot tudi standardnih različicah strežnikov Oracle in za potrebe Oracla nadomešča OAV.

4.3 Neustrezne rešitve za vodenje revizijskih sledi

V Sloveniji je zakonodaja glede varstva osebnih podatkov zahtevna, ozaveščenost o vodenju revizijskih sledi oziroma ustrezni vključitvi le-te v informacijski sistem pa je še zelo na začetku (Delak, 2014, str. 5).

V praksi se uporabljajo neustrezne rešitve za vodenje revizijskih sledi. Čeprav dokumentacija rešitve navaja in uporabljena rešitev zagotavlja beleženje revizijskih sledi, je izvedba večkrat neustrezna. To posledično pomeni, da zapis revizijske sledi ne obstaja. Primeri neustreznega zagotavljanja revizijskih sledi v aplikativni programski opremi so (Slovenski inštitut za revizijo, 2013, str. 167–168):

- beleženje iste podatkovne zbirke v ločeno tabelo iste podatkovne zbirke,
- zapis datuma in podatka, ki se je spremenil, v datoteko,
- zapis revizijske sledi kot sistemske dnevniške datoteke, ki se uporablja za diagnostiko nepravilnega delovanja programske opreme,
- zapis delnih podatkov o dogodku, kot na primer samo stara vrednost podatka ali samo nova vrednost podatka.

Če podjetje potrebuje vodenje revizijskih sledi in jih ima vodene neustrezno, potem je bolje, da jih ne vodi. Podjetje namreč tako dobi napačen občutek, da revizijske sledi vodi, rezultati so pa neuporabni. Vsa vložena sredstva (finančna, čas, zaposleni) tako pomenijo izgubo (B. Oblak, osebna komunikacija, 16. junij 2016).

5 ARBITER

V nadaljevanju bo predstavljena ena izmed rešitev za zagotavljanje revizijskih sledi v informacijskem sistemu **Sistemsko vodenje revizijskih sledi Arbiter. Programsko orodje Arbiter** (v nadaljevanju Arbiter) **je aplikacijska programska oprema za celovito upravljanje revizijskih sledi brez posega v aplikacije**. Arbiter je razvilo podjetje Abakus plus, d. o. o., iz Kranja (v nadaljevanju Abakus plus). Zanj je prejelo srebrno priznanje za inovacije Gorenjske gospodarske zbornice (Arbiter, 2016).

5.1 Predstavitev Arbitra

Arbiter za beleženje revizijske sledi uporablja dnevniške datoteke podatkovne zbirke. Iz podatkovne zbirke Oracle vzame podatke o spremembah in dostopih do podatkov ter jih zapisuje v ločeno podatkovno zbirko. To omogoča poznejše sledenje revizijskih sledi. V nadaljevanju so navedene glavne lastnosti Arbitra:

- Program je podprt izključno s tehnologijo Oracle.
- Arbiter je na svojem strežniku, kjer se izvaja glavnina obdelav, zato ne obremenjuje in ne upočasnjuje delovanja preostalih aplikacij.
- Arbiter ni odvisen od preostalih aplikacij.
- Uporablja dnevniške datoteke podatkovne zbirke. Brez posega v aplikacije omogoča združitev revizijskih sledi iz različnih aplikacij in različnih podatkovnih zbirk.
- Revizijske sledi vodi ločeno od podatkovnih zbirk, v svoji zbirki.
- Preko enostavnega, zmogljivega spletnega vmesnika se z Arbitrom beležijo vsi dogodki, kot so na primer prijava v sistem, spreminjanje podatkovne strukture, spreminjanje podatkov in vpogledi vanje. Tako dobimo **odgovor na bistvena vprašanja o nastanku dogodka: kdo, kaj in kdaj. Beleži nove in stare vrednosti podatkov.**
- Z Arbitrom lahko potrdimo pravilno delovanje informacijskega sistema v podjetju, saj omogoča **centralno vodenje, pregled in analizo revizijskih sledi ter postopek združuje in avtomatizira**.
- Omogoča sistem alarmiranja, s katerim zaznava in takoj poroča o nedovoljenih posegih in spremembah podatkov (Z Arbitrom do revizijske sledi, 2016).

5.2 Delovanje in prednosti Arbitra

Delovanje Arbitra je v nadaljevanju s pomočjo izsledkov iz intervjuja z avtorjem Arbitra (B. Oblak, osebna komunikacija, 16. junij 2016) predstavljeno kot primerjava z drugimi rešitvami za vodenje revizijskih sledi ter z vidika prednosti, ki jih ima Arbiter pred drugimi rešitvami.

5.2.1 Primerjava delovanja Arbitra z drugimi aplikacijami

Podatkovne zbirke same navadno revizijskih sledi ne beležijo. V zbirki je zapisana samo zadnja sprememba. Pravilno pa je, da bi imeli zapisano vsako spremembo, vsak dostop do podatkovne zbirke. Za pravilno revizijsko sled je treba najti način, da se vse te informacije zapišejo. Eden izmed načinov je, da se vsaka sprememba, dogodek zapiše takrat, ko se zgodi. To je možno izvesti s tako imenovanimi prožilci v podatkovni zbirki. Treba je spremeniti aplikacijo, po drugi strani se pa s shranjevanjem dodatnih podatkov povečuje velikost podatkovnih zbirk.

Arbiter deluje drugače. Posegi v aplikacije niso potrebni. Za beleženje revizijskih sledi uporablja dnevniške datoteke podatkovnih zbirk (Oracle ali MS SQL), iz katerih razbere podatke o spremembah in vpogledih v podatke in jih zapisuje v ločeno podatkovno zbirko. Revizijsko sled, ki jo beleži na podlagi ugotovljenih sprememb, dogodkov, vodi v ločeni podatkovni zbirki. Tako ne obremenjuje osnovne aplikacije pa tudi nič je ni treba spreminjati zaradi vodenja revizijskih sledi. Arbiter deluje zgolj nad dnevniškimi datotekami in je od aplikacije popolnoma neodvisen. **Revizijska sled je resnično ločena od podatkov v podatkovnih zbirkah.**

5.2.2 Prednosti Arbitra pred drugimi aplikacijami

Glavne prednosti Arbitra pred drugimi aplikacijami za vodenje revizijskih sledi so:

- Vodenje revizijskih sledi brez dodatnih posegov v aplikacije.
- Arbiter **omogoča analizo poizvedb** iz podatkovnih zbirk Oracle. To je inovativna rešitev tega orodja, ki predhodno ni bila zasledena še v nobenem izdelku.
- Podjetja lahko sama izdelujejo lastne vtičnike za pregled in iskanje po podatkih, saj je zasnova Arbitra na dokumentiranem in odprtem podatkovnem modelu. Uporabnikom je na voljo tudi programska knjižnica za iskanje starih vrednosti podatkov po posameznih tabelah (API).
- V Arbiter je možno vključiti podporo za različno programsko opremo. Za uvajanje Arbitra je značilna prilagodljivost. Prilagaja se potrebam in željam uporabnikov ter zahtevam revizorjev:
  - Če primanjkuje prostora v zbirki, kjer so shranjene revizijske sledi, je mogoč izvoz in uvoz starih podatkov. Revizijske sledi je mogoče arhivirati in po potrebi obnoviti.
  - Nastavitve, kot je na primer nastavljanje prenosov, spreminjanje gesel, se lahko izvajajo z grafičnim uporabniškim vmesnikom GUI.
  - Lahko se doda podpora za različne programske jezike.
- Lahko se doda različna programska oprema, ki jo uporabnik že uporablja, na primer zajem tabel za vodenje in registracijo delovnega časa določene programske opreme, ki jo naročnik že uporablja.

- Arbiter med drugim zna beležiti revizijsko sled za prenose sprememb podatkov med primarno in nadomestno lokacijo, če gre za visoko odporne sisteme oziroma sisteme, odporne na katastrofe. Arbiter omogoča sinhronizacijo podatkov med primarno in nadomestno lokacijo (Z Arbitrom do revizijske sledi, 2016; B. Oblak, osebna komunikacija, 16. junij 2016).

Z Arbitrom v podjetjih lahko sledijo nedovoljenim posegom in jih tudi analizirajo, s čimer ugotovijo pomanjkljivosti informacijskega sistema. Ugotovijo lahko, da so na primer ob določenih terminih, intervalih večje aktivnosti v podatkovnih zbirkah od povprečja. Analizirajo lahko, zakaj. Prav tako izdelek omogoča tvorjenje opozorilnih znakov, če gre za odstopanja od običajnih aktivnosti ali vrednosti. Glede konkurence v primerjavi z drugimi izdelki avtor namreč zagotavlja, da ostali izdelki niso primerljivi z Arbitrom, ker ne omogočajo vseh uporabnosti, ki jih Arbiter. Možnost izdelave analize poizvedb je velika prednost Arbitra. Po navedbah avtorja sta mu konkurenčna dva izdelka na trgu, ki prav tako omogočata beleženje novih in starih vrednosti podatkov, ne znata pa izdelati analize poizvedb. Eden od njiju je OAV, ki je bil kot ena izmed rešitev predstavljen v prejšnjem poglavju.

Prav zaradi zgoraj poudarjene možnosti izvedbe analiz poizvedb iz revizijskih sledi je eden izmed uporabnikov Arbitra (neimenovano podjetje) prav z uporabo tega programa ugotovil vzrok za nepooblaščeno uhajanje informacij iz podjetja in vzpostavil ustrezne ukrepe za preprečitev. Po navedbah avtorja se je v večini podjetij, kjer so začeli uporabljati Arbiter, nepooblaščeno odtekanje informacij ustavilo.

Na podlagi praktičnih izkušenj avtor Arbitra navaja, da uporabniki orodja za beleženje revizijske sledi, ko jih imajo enkrat vgrajene, redko uporabljajo. Zato tudi ne ugotovijo morebitnih nepravilnosti. Avtorji so zato pri razvoju Arbitra namenili veliko pozornosti nadzoru. Arbiter se, kolikor le lahko, vzdržuje sam in napako, ki je sam ne zna rešiti, javi. Njegovo vzdrževanje je zahtevno predvsem zaradi velike podatkovne zbirke, ki v več letih zraste do 10 ali 15 TB. Če gre za nezgodo s podatki in je treba vračati staro stanje podatkov iz varnostne kopije, lahko to traja več dni, tudi teden. Ker je osnova dejavnost podjetja Abakus plus skrbništvo nad podatkovnimi zbirkami, so z vgraditvijo inovativnih rešitev omilili tudi ta problem.

5.3 Poslovni vidik Arbitra

Po navedbah avtorja je bil razlog za razvoj Arbitra naročilo stranke. Obenem je bil razvoj rešitve za vodenje revizijskih sledi s tako unikatnimi lastnostmi potencialna tržna niša. Arbiter je splošno orodje za vodenje revizijskih sledi v podatkovnih zbirkah Oracle. Kot tak se prodaja kot samostojni izdelek. Razvoj izdelka se je začel z naročilom Aerodroma Ljubljana, kot bo predstavljeno v nadaljevanju. Finančni učinek projekta Arbiter je pokril

razvojne stroške. Izdelek prinaša nekaj finančnega dohodka. Še vedno načrtujejo širjenje v druga podjetja.

Poleg Aerodroma Ljubljana in Abakusa plus Arbiter trenutno uporabljajo še v petih podjetjih. Od tega v dveh bankah, zavarovalnici in dveh podjetjih za informacijski inženiring (Arbiter, 2016).

Abakus plus je podjetje, ki je znano po svojem strokovnem znanju. Pri uvajanju novih rešitev in izdelkov so vedno med prvimi. Znani so po izredno dobrem poznavanju podatkovnih zbirk Oracle. Razvoj Arbitra je bil tehnično izredno zahteven izdelek, kjer je bilo potrebnega veliko podrobnega znanja o delovanju podatkovne zbirke Oracle. Glede strokovnosti je Arbiter pripomogel k ugledu podjetja. Hkrati pa se pri takih izdelkih zgodi, da se, ker rešuje nepriljubljeno problematiko, nepriljubljenost prenese tudi na izdelovalca izdelka. **Ob upoštevanju dosedanjih izkušenj avtor pravi, da se razvijanja tega izdelka ne bi ponovno lotil** (B. Oblak, osebna komunikacija, 16. junij 2016).

5.4 Razvoj Arbitra z Aerodromom Ljubljana

Že v prejšnjih poglavjih je bilo predstavljeno dejstvo, da je danes del vsake revizije v podjetju tudi revidiranje informacijskega sistema oziroma pregledovanje računalniške obdelave podatkov. Vedno pomembnejši sestavni del revizije informacijskega sistema je tudi pregledovanje revizijskih sledi.

»Revizijska hiša Deloitte je tudi zaradi uporabe Arbitra potrdila ustreznost informacijskega sistema v Aerodromu Ljubljana. Boštjan Rakovec, vodja informacijskih projektov, Aerodrom Ljubljana, d. d.« (Z Arbitrom do revizijske sledi, 2016).

Iz predhodno navedenega je bilo razbrati, da za vodenje revizijskih sledi uporablja Arbiter tudi Aerodrom Ljubljana (v nadaljevanju letališče). Arbiter v Aerodromu Ljubljana zagotavlja vodenje revizijske sledi v aplikacijah.

Prek letališča letno potuje 1,5 milijona potnikov, kar pomeni, da gre za upravljanje z ogromno količino podatkov v elektronski obliki. Zato je uvajanje orodij za vodenje revizijskih sledi v takem sistemu zelo zapleteno. Po drugi strani je nujno, ker imajo zaposleni dostop do ogromne podatkovne zbirke, s čimer je dana možnost zlorabe podatkov oziroma uhajanje podatkov prek zaposlenih. Beleženje dostopa do podatkov mora biti nujno zagotovljeno. Na letališču so morali vzpostaviti sistem zagotavljanja revizijskih sledi, saj jim prej aplikacije tega niso zagotavljale, kar ni skladno z ZVOP-1. To pomanjkljivost so ugotovili tudi revizorji in letališče na to opozarjali. Na letališču so **morali zagotoviti sledljivost dostopov do osebnih podatkov potnikov** (Vučić, 2010).

Ena izmed aplikacij, ki jo uporabljajo na letališču, je tudi Letališki programski paket (v nadaljevanju FIS). FIS je izdelek Abakusa plus, ki tako kot druge aplikacije na letališču uporablja podatkovno zbirko Oracle. Abakus je na letališču tudi skrbnik podatkovnih zbirk. Prvotna zamisel je bila, da bi v aplikacije vgradili revizijske sledi, podjetje Abakus plus pa bi pri tem kot skrbnik podatkovnih zbirk pomagalo različnim izvajalcem. Po analizi in oceni stroškov za predelavo je bilo ugotovljeno, da to ni ekonomsko ugodna rešitev. Domislili so se izdelave splošnega orodja in ga razvili v Arbiter. Po analizi stroškov je bila ta rešitev tri- do štirikrat cenejša, kot če bi bilo treba nadgrajevati vse aplikacije na letališču. Hkrati so se z uporabo splošnega orodja izognili tudi verjetnim napakam v aplikacijah ter potrebi po nadzoru skrbnikov za posamezno aplikacijo. Razvoj Arbitra je trajal nekaj več kot leto dni. Pri projektu je stalno ali občasno delalo šest ljudi. Po obsežnih testiranjih je bil vgrajen leta 2010 (B. Oblak, osebna komunikacija, 16. junij 2016).

Glavne značilnosti uvajanja Arbitra na letališču (Vučić, 2010):

- Uvajanje je bilo tehnično zelo zahtevno, kar je tudi značilno za podjetje, ki upravlja z veliko količino podatkov v elektronski obliki, v sistem pa je vključenih več različnih aplikacij.
- Pred začetkom razvoja so pripravili spisek aktivnosti in zahtev za razvoj aplikacije.
- Pred vgradnjo Arbitra v sistem so nadgradili podatkovno zbirko z novejšo verzijo.
- Pri nadgradnji podatkovne zbirke in vključitve Arbitra v sistem so izkoristili priložnost zaprtja letališča zaradi večjih obnovitvenih del.
- Z uvedbo Arbitra je bila na letališču zagotovljena sledljivost v vseh delih poslovanja.
- Arbiter je na letališču povezan z več različnimi aplikacijami, ki temeljijo na podatkovni zbirki Oracle. Nekatere izmed teh aplikacij omogočajo izvoz podatkov v Excel. Z uvedbo Arbitra je zagotovljena med drugim tudi sledljivost izvažanja podatkov v Excel. Podatki o takšnih izvozih se zapišejo v dnevniške datoteke, iz katerih Arbiter razbere podatke o spremembah. Tako se ve, kdo in kdaj je podatke izvozil v Excel.
- Vpogled v revizijske sledi imajo le določene osebe, ki si različne poglede lahko prilagodijo z vtičnikom.
- Način pregledovanja podatkov, kot ga omogoča Arbiter, deluje v ozadju, uporabniki ga pri svojem delu ne opazijo, zato zaradi uvajanja Arbitra ni bilo treba posebej uvajati zaposlenih.

5.5 Izpolnjevanje priporočil stroke

V nadaljevanju bo v tabelah 2 in 3 prikazano, kako Arbiter izpolnjuje priporočila strokovnjakov glede lastnosti revizijskih sledi v informacijskem sistemu.

5.5.1 Arbiter in ravni revizijske sledi

V poglavju 4.1.1 so bile predstavljene tri ravni beleženja revizijske sledi. Na podlagi intervjuja s strokovnjakom sem preverila, ali Arbiter zagotavlja vse tri ravni revizijske sledi.

Tabela 2: Zagotavljanje ravni revizijskih sledi z Arbitrom

Raven	Opis ravni beleženja	Arbiter zagotavlja DA/NE	Kako raven zagotavlja Arbiter
1.	Beleženje aktivnih dostopov do podatkov; kdo, kdaj, kje je spreminjal podatke.	DA	Arbiter zapiše vse ukaze, ki delujejo s podatki (v nadaljevanju stavke SQL): kdo in kdaj je kaj spreminjal (vnesel, spremenil, izbrisal). Tako, da lahko naknadno pogledamo v spisek dogodkov.
2.	Beleženje aktivnih in pasivnih dostopov do podatkov; kdo je dostopal do podatka, vendar podatka ni spreminjal.	DA	Arbiter vodi tudi ostale dogodke, za katere se vzpostavi beleženje: spremembe pooblastil, prijave v podatkovno bazo. Ker vodi vse stavke SQL, s tem omogoča tudi sledljivost, kdo je dostopal do podatka, oziroma vpoglede.
3.	Beleženje dostopov, beleženje sprememb podatkov ter beleženje tako izvornih kot popravljenih podatkov.	DA	Arbiter za vse podatke vodi tudi vse spremembe. Pri spremembah zabeleži stare in nove vrednosti tako, da pri spremembi podatka vidimo, iz katerega in v kaj se je podatek spremenil. Pri brisanju so shranjene tudi vrednosti, ki jih je imela entiteta pred brisanjem. Torej lahko vidimo, kateri podatki so bili brisani in kdo ter kdaj jih je brisal.

Vir: Prirejeno in povzeto po D. Vezjak, Revizijske sledi – nuja in mora, 2012, str. 173; B. Oblak, osebna komunikacija, 16. junij 2016.

Arbiter zagotavlja vse tri ravni revizijskih sledi. V osnovi zagotavlja tako sledljivost v bazah podatkov Oracle, vendar je sistem odprt, tako da se vanj lahko zapisujejo tudi revizijske sledi iz drugih virov. Programski jezik je SQL.

5.5.2 Arbiter in predpostavke revizijskih sledi

V poglavju 4.1.3 so bile naveden predpostavke, ki morajo biti izpolnjene pri vzpostavitvi vodenja revizijske sledi v sistemu. Na podlagi intervjuja s strokovnjakom sem preverila ali Arbiter izpolnjuje navedene predpostavke in jih predstavila v Tabeli 3.

Za lažje razumevanje besedila v Tabeli 3 navajam, da je arhivska log-datoteka arhivska dnevniška datoteka, v katero podatkovne baze zapisujejo vse operacije, da lahko ob napaki iz tega obnovijo podatke. Vsaka podatkovna zbirka ustvarja te datoteke, saj so nujne za njeno okrevanje po morebitni napaki.

Iz Tabele 3 v nadaljevanju je razbrati, da Arbiter zagotavlja vseh osem predpostavk za ustrezno vodenje revizijskih sledi v sistemu.

Tabela 3: Izpolnjevanje predpostavk za vodenje revizijskih sledi z Arbitrom

Zaporedna številka predpostavke	Predpostavka	Arbiter zagotavlja DA/NE	Opis, kako je predpostavka zagotovljena
1.	Sistem oziroma aplikacija ne sme delovati, če sistem revizijske sledi ne deluje.	**DA**	To predpostavko je na tehnični ravni mogoče doseči, ni nobene ovire. Gre pa v osnovi za odločitev oziroma nastavitev naročnikove politike. Pri tem je treba izpostaviti lastnost Arbitra, ki omogoča, da če Arbiter nekaj časa ne deluje (zaradi na primer vzdrževalnih ukrepov, selitve strežnika, prekinitve povezave med podatkovno bazo in Arbitrom), se ne izgubi nobena revizijska sled. Ko se Arbiter ponovno vklopi, vzame iz podatkovne zbirke vse podatke tudi za čas, ko je bil izklopljen.
2.	Zagotovljena mora biti splošnost sistema – rešitev mora biti "odprta".	**DA**	Arbiter je popolnoma odprta rešitev. Vpis revizijske sledi je mogoč iz različnih virov. Trenutno podprti viri podatkovnih baz so: podatkovna zbirka Oracle, Rsyslog in MS SQL Server. Uporabnikom je na voljo tudi priročnik za administratorje.
3.	Skladnost sistema z zakonodajo.	**DA**	Arbiter je skladen s priporočili informacijskega pooblaščenca.
4.	Zagotovljena mora biti optimalna količina podatkov revizijske sledi.	**DA**	Pri uvajanju Arbitra se točno določi, čemu je treba slediti; tako se tudi določi minimalno količino podatkov za potrebe revizijske sledi.
5.	Minimalni časovni pribitek operacijam.	**DA**	Časovni pribitek Arbitra zaradi narave njegovega delovanja je minimalen, najmanjši možni, kar jih je. Arbiter namreč obdeluje arhivske log-datoteke na svojem strežniku in s tem nič ne obremenjuje aplikacij. Obremenitev aplikacij je ta, da morajo aplikacije vklopiti revizijsko sled, to pa je neodvisno od Arbitra in je odvisno samo od tipa podatkovne zbirke aplikacije.
6.	Zagotovljena mora biti čim manjša povezanost sistema za zagotavljanje revizijskih sledi in aplikacij.	**DA**	Arbiter ni nujno povezan z aplikacijami, kjer so revizijske sledi vodene. Na Arbitrov strežnik je treba samo prenašati arhivske log-datoteke. Ker se te ustvarjajo neodvisno od tega, ali vodimo revizijsko sled ali ne, ne predstavljajo dodatnih obremenitev.
7.	Zagotovljena mora biti dostopnost revizijske sledi.	**DA**	Revizijska sled je enostavno dosegljiva, vseeno pa mora revizor poznati podatkovni model, za katerega se vodijo revizijske sledi. Za revizorje je na voljo tudi priročnik za začetek uporabe Arbitra.
8.	Zagotovljena mora biti neodvisnost podatkov od programiranja.	**DA**	Predpostavka je popolnoma zagotovljena. Arbiter namreč vodi revizijsko sled na osnovni ravni: podatkovni zbirki. Vse aplikacije so nad osnovno ravnjo. Tako ni možnosti, da bi se »programsko« obšlo vodenje revizijskih sledi. Prav tako se vodi tudi revizijske sledi za skrbnike podatkovnih baz, ki lahko »ročno« dostopajo do osnovnega dela podatkov (podatkovne zbirke). S tem so torej zabeleženi vsi dostopi do podatkov.

Vir: Prirejeno in povzeto po D. Vezjak, Revizijske sledi – nuja in mora, 2012, str. 176; B. Oblak, osebna komunikacija, 16. junij 2016.

6 VODENJE REVIZIJSKIH SLEDI V PRAKSI

Vodenje revizijskih sledi v praksi je v nadaljevanju prikazano na podlagi revizije informacijskih sistemov v 65 slovenskih podjetjih in organizacijah (v nadaljevanju podjetja), ki so razvrščene glede na dejavnost, ki jo opravljajo.

Iz Tabel 4, 5 in 6, ki so prikazane v nadaljevanju, je razbrati, da je vodenje celovite revizijske sledi v podjetjih (aplikativne, sistemske in orodja za pregledovanje revizijskih sledi) po trenutnih raziskavah bolj izjema kot pravilo. Uvedene so delne rešitve za vodenje revizijskih sledi, stanje na področju varovanja osebnih podatkov ni usklajeno z zahtevami zakonodaje.

Tabela 4: Stanje vodenja aplikacijskih revizijskih sledi v podjetjih

Oznaka dejavnosti	**Dejavnost**	**Stanje aplikativnih revizijskih sledi v podjetju**			
		DA	DELNO	NE	NI
G	Trgovina, vzdrževanje in popravila motornih vozil	0	1	0	0
I	Informacijske in komunikacijske dejavnosti	0	2	1	0
K	Finančne in zavarovalniške dejavnosti	1	23	15	4
M	Strokovne, znanstvene in tehnične dejavnosti	2	7	1	0
O	Dejavnosti javne uprave in obrambe, dejavnost obvezne socialne varnosti	0	0	3	0
S	Druge dejavnosti	1	1	2	1
Skupaj:		**4**	**34**	**22**	**5**
Delež (v%):		**6**	**52**	**34**	**8**

Legenda: DA – uvedene ustrezno v vseh aplikacijah; DELNO – uvedene delno, le v nekaterih aplikacijah; NE – niso uvedene; NI – ni vključeno, revizijski pregled ni vključeval neposrednega pregleda revizijskih sledi.

Vir: Prirejeno in povzeto po B. Delak, Revizijska sled v informacijskih sistemih v teoriji in praksi 2014, str. 17, tabela 8.

V Tabeli 4 je prikazano, da ima le 6 % obravnavanih podjetij oziroma 4 od 65 vodene aplikacijske revizijske sledi v vseh aplikacijah. 52 % podjetij ima vodene aplikacijske revizijske sledi le v nekaterih aplikacijah, 34 % obravnavnih podjetij oziroma kar 22 od 65 podjetij uporabniških revizijskih sledi nima vodenih oziroma le-te v aplikacije niso uvedene.

Tabela 5: Stanje uporabe orodij za pregledovanje revizijskih sledi v podjetjih

Oznaka dejavnosti	Dejavnost	Stanje orodij za pregl. rev. sledi v podjetju			
		DA	DELNO	NE	NI
G	Trgovina, vzdrževanje in popravila motornih vozil	0	0	1	0
I	Informacijske in komunikacijske dejavnosti	0	0	3	0
K	Finančne in zavarovalniške dejavnosti	0	9	30	4
M	Strokovne, znanstvene in tehnične dejavnosti	0	4	6	0
O	Dejavnosti javne uprave in obrambe, dejavnost obvezne socialne varnosti	0	0	3	0
S	Druge dejavnosti	1	1	2	1
Skupaj:		**1**	**14**	**45**	**5**
Delež (v %):		**2**	**22**	**69**	**8**

Legenda: DA – podjetje ima orodje za hitro in učinkovito pregledovanje revizijskih sledi; DELNO – pregled revizijskih sledi je mogoč z različnimi orodji ali s pomočjo zunanjega izvajalca; NE – podjetje nima znanj, navodil za pregledovanje revizijskih sledi; NI – ni vključeno, revizijski pregled ni vključeval neposrednega pregleda revizijskih sledi.

Vir: Prirejeno in povzeto po B. Delak, Revizijska sled v informacijskih sistemih v teoriji in praksi 2014, str. 17, tabela 9.

V Tabeli 5 je prikazano, da 69 % obravnavanih podjetij, ki sicer ima vodene revizijske sledi v informacijskem sistemu, nima na voljo navodil in znanja za pregledovanje revizijskih sledi. Orodje za ustrezno in učinkovito pregledovanje revizijskih sledi imata le 2 % podjetij oziroma eno podjetje od 65. Pregledovanje revizijskih sledi z različnimi orodji ali pa s pomočjo zunanjega izvajalca je možno pri 22 % podjetjih.

V Tabeli 6 je prikazano, da 55 % obravnavanih podjetij nima uvedenih revizijskih sledi na sistemski računalniški opremi. Le 2 % oziroma eno podjetje od 65 ima uvedene revizijske sledi v vse sisteme. 23 % od obravnavanih podjetjih ima sistemsko revizijsko sled uvedeno le v nekaterih sistemih podjetja.

Tabela 6: Stanje vodenja sistemskih revizijskih sledi v podjetjih

Oznaka dejavnosti	Dejavnost	Stanje sistemske revizijske sledi v podjetju			
		DA	DELNO	NE	NI
G	Trgovina, vzdrževanje in popravila motornih vozil	0	0	1	0
I	Informacijske in komunikacijske dejavnosti	0	2	1	0
K	Finančne in zavarovalniške dejavnosti	0	12	28	3
M	Strokovne, znanstvene in tehnične dejavnosti	0	0	0	10

se nadaljuje

Tabela 6: Stanje vodenja sistemskih revizijskih sledi v podjetjih (nad.)

Oznaka dejavnosti	Dejavnost	Stanje sistemske revizijske sledi v podjetju			
O	Dejavnosti javne uprave in obrambe, dejavnost obvezne socialne varnosti	0	0	3	0
S	Druge dejavnosti	1	1	3	1
Skupaj:		**1**	**15**	**36**	**14**
Delež (v %):		**2**	**23**	**55**	**22**

Legenda: DA – revizijska sled je vključena v sistem za upravljanje podatkovnih baz, sistemsko opremo na strežnikih in na komunikacijah; DELNO – revizijska sled v podjetju je uvedena le za nekatere sisteme, ki jih uporabljajo v podjetju; NE – podjetje nima uvedenih sistemskih revizijskih sledi; NI – ni vključeno, revizijski pregled ni vključeval neposrednega pregleda revizijskih sledi.

Vir: Prirejeno in povzeto po B. Delak, Revizijska sled v informacijskih sistemih v teoriji in praksi 2014, str. 18, tabela 10.

Iz prikazanega lahko povzamemo, da imajo uvedene celovite revizijske sledi predvsem podjetja, ki delujejo na področju finančne in zavarovalniške dejavnosti ter v strokovnih, znanstvenih in tehničnih dejavnostih. Še posebej na področju finančne in zavarovalniške dejavnosti gre za velike informacijske sisteme z velikim številom podatkovnih zbirk in strank. Hkrati pa tudi za veliko odgovornost upravljanja z osebnimi podatki. Po mnenju strokovnjaka (B. Oblak, osebna komunikacija, 16. junij 2016) povečanja števila podjetij z vodenimi revizijskimi sledmi v drugih dejavnostih ni pričakovati.

Sistem beleženja revizijskih sledi v praksi je težaven. Sploh v podjetjih z obsežnimi informacijskimi sistemi, ki vključujejo več aplikacij. V praksi gre lahko za več 10 do 100 aplikacij. Zelo težko je kupiti ustrezno rešitev, ker se jih ne da spreminjati in jih je težko prilagoditi vsem zahtevam, tako zakonodaje kot sistema. Splošne aplikacije so namenjene tudi tujemu trgu, kar pomeni, da nimajo zagotovljenega beleženja sledi, kot zahteva ZVOP-1 (Vezjak, 2012, str. 171, 179).

V primeru obsežnih informacijskih sistemov je rešitev, kot jo zagotavlja Arbiter in ki sem jo predstavila v prejšnjem poglavju, zelo učinkovita, saj brez posega v že delujoče aplikacije omogoča združitev revizijskih sledi iz različnih aplikacij in različnih podatkovnih zbirk. Lahko se doda različna programska oprema, ki jo naročnik že uporablja. Ne obremenjuje in ne upočasnjuje delovanja obstoječih aplikacij.

6.1 Zakaj v podjetjih ne vodijo revizijskih sledi

Na podlagi obravnavane literature in mnenja strokovnjaka (B. Oblak, osebna komunikacija, 16. junij 2016) v nadaljevanju povzemam razloge, zakaj podjetja ne vodijo (celovitih) revizijskih sledi oziroma zakaj jih ne vodijo ustrezno:

- Podjetja niso seznanjena z vsebino ZVOP-1, zato se ne zavedajo in ne razumejo, kaj resnično pomeni uvajanje in vodenje revizijskih sledi v podjetju.
- ZVOP-1 je napisan splošno, težko ga je uporabiti v praksi. Splošna rešitev, ki bi izpolnjevala vse zahteve ZVOP-1, ne obstaja.
- Investicija uvajanja rešitve za vodenje revizijske sledi je draga in zahteva veliko časa (stroški opreme, stroški dela pri uvajanju, pregledovanju in analiziranju). Potrebna je tudi nadgradnja že delujoče programske opreme. Še posebej zahtevno je uvajanje v velikem podjetju z več podatkovnimi zbirkami in velikim številom strank.
- Čas hrambe revizijske sledi ni ustrezen, ker ni na voljo dovolj pomnilniškega prostora.
- Izdelek, ki ne prinese neposredne vrednosti, je v osnovi nepriljubljen. Če je njegova uporaba predpisana z zakonom, nepriljubljenost narašča. Če podjetje v vodenju revizijske sledi ne vidi neke poslovne vrednosti in začne revizijske sledi beležiti samo zato, da zadosti zahtevam zakonodajalca, priljubljenosti izdelka tudi ni pričakovati. Hkrati se pri takih izdelkih zgodi, da se nepriljubljenost prenese na izdelovalca izdelka. Pisanje rešitev za vodenje revizijskih sledi je nepriljubljeno tudi med razvijalci, načrtovalci programskih rešitev.
- Še vedno je veliko uporabnikov (podjetij), ki želijo samo zadostiti zakonskim zahtevam. Mnenje uporabnikov glede vodenja revizijskih sledi se je spremenilo le pri tistih uporabnikih, ki se zavedajo posledic uhajanja informacij iz podjetja in želijo to v svojih podjetjih preprečiti.
- Večina uporabnikov (podjetij) še vedno ne uporablja redno orodij za pregledovanje revizijske sledi. Želijo jih uporabiti samo takrat, ko bi morali na podlagi zakonskih zahtev narediti poročilo. Takrat bi želeli poročilo takoj, kar ni enostavno, saj glede na to, da orodij ne uporabljajo, teh niti ne poznajo in ne vedo, kaj vse jim nudijo. Zato razvijalci rešitev ne dobivajo povratnih informacij z željami in pripombami uporabnikov, ki bi bile osnova za nadgradnjo in posodobitev orodja.
- Vzpostavitev beleženja revizijskih sledi v podjetju, kot ga določa ZVOP-1, in hkrati omogočiti, da bo uporabnik oziroma naročnik enostavno prišel do odgovorov, je zelo zapleten in drag projekt. ZVOP-1 namreč zahteva, da je treba vsak trenutek odgovoriti, kaj je določen uporabnik videl od osebnih podatkov osebe, ki zahteva poročilo. Če se ne da ugotoviti, točno katere podatke je uporabnik videl, se šteje, da je vpogledal v vse podatke. S trenutnimi tehničnimi zmožnostmi je težko enostavno zagotoviti vse, kar zahteva ZVOP-1. Zato je vodenje revizijskih sledi drago. Hkrati se ob trenutnem razvoju in potrebah podatki hranijo na različnih lokacijah, na primer poslovanje v oblaku. Revizijsko sled je težko zagotoviti povsod.

Tehnični problem zagotavljanja revizijskih sledi je težko razumeti, zato je v nadaljevanju ponazorjen s primerom.

6.1.1 Predstavitev tehničnega problema vodenja revizijskih sledi

Imamo podatkovno zbirko, v kateri imamo 100 GB podatkov. Zanje moramo voditi

revizijske sledi. S podatki se izvajajo različne akcije. Največ je vpogledov ali poizvedb (ukaz SELECT), manj je dodajanja (ukaz INSERT), spreminjanja (ukaz UPDATE) ali brisanja (ukaz DELETE). Poenostavljeno postavimo trditev, da imamo tabelo DELAVCI s tremi kolonami: ime, naslov, davčna številka.

Tabela 7: Delavci – primer tehničnega problema vodenja revizijske sledi

Ime	Naslov	Davčna številka
Janez Novak	Naslov 1	90809790
Marija Novak	Naslov 2	89079876
Metka Novak	Naslov 3	79889999
Franci Novak	Naslov 4	68796999

Uporabnik naredi poizvedbo, ki bo vrnila vsa imena na M.
*SELECT * FROM delavci WHERE ime LIKE 'M%'*

Taka poizvedba vrne dva zapisa: Marijo in Metko Novak. Za to poizvedbo bi morala nastati revizijska sled: kdo, kdaj in kaj je dostopal, torej, ali je poizvedoval uporabnik JANEZ.

Tabela 8: Revizijska sled za uporabnika Janeza

Kdo	Kdaj	Ime	Naslov	Davčna številka
JANEZ	16. 6. 2016 06:00:00	Marija Novak	Naslov 1	89079876
JANEZ	16. 6. 2016 06:00:00	Metka Novak	Naslov 3	79889999

V revizijski sledi imamo sedaj zapise in lahko pregledamo, kdo, kdaj in kaj je videl. Zdaj pa si predstavljajmo, da je takih in podobnih poizvedb na dan vsaj sto, kar je sicer malo, navadno se štejejo poizvedbe v tisočih ali deset tisočih. V povprečju vsaka poizvedba vrne dva zapisa. Tako dobimo v revizijski sledi na dan ali na leto:

1) 100 * 2 = 200 zapisov/dan
2) 200 * 200 = 40.000 zapisov/leto, če štejemo 200 delovni dni

Iz primera je razvidno, da iz osnovne tabele s štirimi vrsticami v revizijski sledi naredimo 40.000 vrstic letno. Vrstice v revizijskih sledi so prostorsko še večje, ker moramo zapisati še nekaj dodatnih informacij. Poenostavljeno to za naš primer pomeni, da bi bila samo za poizvedbe letna podatkovna zbirka 10.000-krat večja od podatkovne zbirke, v kateri imamo osnovne podatke. Poleg tega moramo upoštevati še, da je treba pri spremembah (ukaz UPDATE) shraniti še vrednosti pred spremembo, potem vidimo, da se količina podatkov, ki se jih hrani, še dodatno povečuje. V našem primeru, ko je osnovna podatkovna zbirka velika 100 GB, bi bila po enem letu podatkovna zbirka revizijske sledi velika 1.000.000 GB oziroma 1.000 TB. To predstavlja ogromno prostora, zato take

tehnike zajemanja podatkov niso učinkovite oziroma so bistveno predrage.

Da bi zmanjšali količino podatkov v revizijski sledi, so na razpolago različne tehnike. Predvsem pa se to odraža v kakovosti končnega poročila, ki ga dobi uporabnik. Da ne bi zapisovali vsega, kar je uporabnik videl, navadno v revizijski sledi zapišemo samo ukaz, s katerim je uporabnik poizvedoval (ukaz SELECT) med podatki kot v našem primeru. S tem se količina podatkov v revizijski sledi zmanjša, v našem primeru na vsaj dvakrat manj zapisov. Tako potem na podlagi ukaza sklepamo, kaj je uporabnik videl. Seveda so take ugotovitve lahko tudi napačne. Če je na primer uporabnik dostopal do podatkov 1. 1. 2016, je videl stanje, kakršno je bilo v podatkih takrat. Kasneje, na primer 15. 1. 2016, pa smo morda dodali novega delavca – Milana Novaka. Če danes preverjamo revizijske sledi, bi za uporabljeno poizvedbo sklepali, da je uporabnik videl tudi tega novega uporabnika, ker merila ustrezajo. V resnici pa ga ni videl. **Tako vodenje revizijskih sledi je sicer v skladu z ZVOP-1, ki določa, da če ne moremo točno povedati, kaj je uporabnik v danem trenutku videl, potem sklepamo, da je videl vse.** Vseeno pa ni res, da je uporabnik videl tudi podatke Milana Novaka.

Kakšne možnosti revizijska sled uporablja, je odvisno od rešitve za vodenje revizijske sledi. Vsem pa je skupno to, da je količina revizijskih sledi, ki jih hranimo, mnogokratnik količine vseh podatkov, ki jih imamo. Poleg tega revizijska sled potrebuje veliko več resursov kot vir revizijske sledi. Zato so že zahteve po sami strojni opremi mnogo večje kot za produkcijski strežnik vira revizijske sledi. Po praktičnih izkušnjah podatkovna zbirka od pet- do desetkrat preraste velikost vira revizijske sledi. In če pomislimo, da zakonodaja zahteva hrambo podatkov o revizijski sledi za več let, potem si lahko zamislimo, kakšen strošek to predstavlja za naročnika (B. Oblak, osebna komunikacija, 16. junij 2016).

6.2 Posledice pomanjkanja revizijskih sledi

Vezjak (2012, str. 175) navaja naslednje negativne posledice pomanjkanja revizijskih sledi za podjetje:

- sankcije zaradi neupoštevanja ZVOP-1,
- podjetje zaradi pomanjkanja podatkov o dostopanju do podatkov ne more preprečiti zlorab zaposlenih, zato pride do tožb, sporov, kazni,
- število nepooblaščenih dostopov narašča, saj ni zagotovljen nadzor nad uporabo podatkov,
- nižja kakovost poslovanja,
- manjši ugled podjetja,
- dodatni stroški zaradi zamud, iskanja različnih podatkov po različnih poročilih, zapisih, da se jih potem združi v enotno poročilo.

S celovitim, za podjetje ustreznim in učinkovitim vodenjem revizijskih sledi v informacijskem sistemu lahko podjetja zgoraj naštete posledice pomanjkanja revizijskih sledi odpravijo ali jih vsaj omilijo.

7 POSLOVNA VREDNOST REVIZIJSKE SLEDI

Poslovna vrednost revizijskih sledi bo analizirana **z vidika poslovne vrednosti informatike** s **stroški** vključitve in vodenja revizijskih sledi v informacijskem sistemu, s **koristmi**, ki jih podjetje s tem pridobi, ter z vplivom, ki jih imajo te koristi na poslovanje podjetja.

7.1 Poslovna vrednost informatike

Groznik, Indihar Štemberger in Kovačič (2005, str. 213–222) navajajo, da naložbe v informatiko same po sebi ne prinašajo poslovne vrednosti. **Poslovno vrednost informatike je treba obravnavati kot izboljšave**, ki jih informatika prinese v poslovne procese. Informatika pozitivno vpliva na uspešnost poslovanja, ponuja priložnosti za ustvarjanje konkurenčne prednosti, ob pogoju, da podjetje k informatizaciji **pravilno pristopi,** jo strateško načrtuje. Podjetja, ki merijo vrednost in pomen informatike samo s finančnimi kazalci, bodo lahko razočarana. Zelo pomembno je, da v podjetju na informatiko ne gledajo le kot na stroške, ampak upoštevajo tudi koristi. Čeprav vemo, kje iskati vrednost informatike, jo je zelo težko izraziti v številkah.

Groznik in Vičič (2005, str. 198–202) menita, da je namen vlaganja v informatiko povečanje konkurenčne prednosti in s tem povečanje poslovne uspešnosti. Problem je, da v podjetjih vidijo le stroške, ne pa neposredne poslovne vrednosti informatike. Glavni nosilci vrednosti informatike so poslovni procesi, kadri z ustreznim znanjem ter inovativna uporaba informacijske tehnologije. Podjetja morajo izbrati prave investicije v informatiko, kar pomeni, da ni bistveno, koliko se vlaga, ampak kam in s kakšnim namenom. Učinke informatike je treba meriti z ustreznimi parametri, ki morajo upoštevati otipljive in neotipljive dele poslovanja. Avtorja navajata, da za vrednotenje informatike poznamo različne metode, pogoj za realno merjenje pa je obravnava stroškov kot tudi koristi. Merjenje stroškov naj bi bilo dokaj enostavno. Z vidika koristi ločimo dva načina merjenja:

a) **Posredne in neposredne koristi.** Pri tej delitvi ugotavljamo, ali pridobljena korist izhaja neposredno iz investicije v informatiko ali pa iz neke skupne organizacijske rešitve.
b) **Otipljive (merljive) in neotipljive koristi.** Otipljive koristi lahko izrazimo in izračunamo s številkami in ugotovimo, kakšen je resnični vpliv informatike na uspešnost poslovanja po različnih merilih (kot so na primer dobiček, produktivnost, dodana vrednosti). Neotipljive koristi lahko le ocenimo, čeprav vemo, da obstajajo. So sicer manj raziskane, vendar z vidika upravičenosti investicij v informatiko vse

pomembnejše. Avtorja navajata naslednje primere neotipljivih koristi: višje zadovoljstvo strank, povečana prilagodljivost poslovanja, višja kakovost informacij, izboljšan nadzor virov, izboljšanje načrtovanja, zvišanje naklonjenosti zaposlenih, izboljšano upravljanje premoženja, boljši poslovni ugled podjetja.

Menim, da mora biti vključitev revizijskih sledi v informacijski sistem ustrezno načrtovana in izvedena na pravi način (ustrezna vključitev revizijskih sledi v podjetje je bila predstavljen v prejšnjih poglavjih), sicer vodenje revizijskih sledi za podjetje nima ustrezne poslovne vrednosti, saj investicija ne pomeni izboljšave za podjetje. Če so revizijske sledi v podjetju vodene neustrezno, vsa vložena sredstva v uvajanje pomenijo izgubo, kar je bilo predstavljeno v poglavju 4.3.

Poslovne vrednosti investicije vodenja revizijskih sledi ni mogoče neposredno določiti. Kot so povzeli avtorji že predhodno, je stroške investicij v informatiko enostavno oceniti, ne velja pa to za koristi. Za koristi vodenja revizijskih sledi je značilno, da del njih spada med neotipljive koristi. Tri primere neotipljivih koristi revizijskih sledi sta podala avtorja zgoraj: višje zadovoljstvo strank, višja kakovost informacij, večji ugled podjetja. Podrobneje bom koristi predstavila v nadaljevanju, v točki 7.2.2.

»Vloga in pomen informatike postane opazna v dramatičnih obdobjih poslovanja« (Groznik & Vičič, 2005, str. 198–202). V povezavi s predhodno navedbo se navezujem na revizijske sledi. Če v podjetju nepooblaščeni dostopajo do podatkov ali podatki uhajajo, je z ustrezno vodenimi revizijskimi sledmi mogoče ugotoviti krivca za nastalo situacijo in jo omiliti. Po drugi strani je mogoče z ustreznimi analizami predhodno ugotoviti nepravilnosti v sistemu, jih odpraviti in s tem odpraviti možnost za nastanek dramatičnih trenutkov v podjetju. Tako lahko stroške v podjetju znižajo ali pa ti sploh ne nastanejo.

7.2 Analiza poslovne vrednosti revizijskih sledi

Vključitev revizijskih sledi v informacijski sistem za podjetje pomeni izboljšavo v poslovanju, ki vpliva na višjo poslovno vrednost podjetja. Ekonomska upravičenost uvedbe in vodenja revizijskih sledi bo v nadaljevanju prikazana s preprosto analizo stroškov in koristi (angl. *Cost Benefit Analysis*).

Turk (2005, str. 153) navaja, da podjetja želijo izboljšati poslovne rezultate, zato na eni strani zmanjšujejo stroške (vsako naložbo morajo utemeljiti), po drugi strani pa ugotavljajo prednosti nove tehnologije. Z analizo stroškov in koristi lahko pridobijo ustrezne odgovore.

Investicijo uvedbe in vodenja revizijskih sledi v informacijskem sistemu podjetja (v nadaljevanju investicija) bom ovrednotila glede na ocenjene stroške in ocenjene koristi investicije. Cikajlo & Gider (2010, str. 104) navajata, da pri analizi stroškov in koristi (v

nadaljevanju ASK) seštejemo vse stroške projekta (stroške razvoja in obratovanja), ki so potrebni za uresničitev projekta, na drugi strani pa vse učinke (v našem primeru: koristi), ki bi jih pri tem imeli. Koristi projekta analiziramo v določenem obdobju, na primer petih let.

Najpomembnejši in hkrati najzahtevnejši del ASK je oceniti stroške in koristi investicije.

7.2.1 Stroški revizijskih sledi

Stroški obravnavane investicije so razdeljeni na:

a) **stroške razvoja** (stroški tako imenovanih korakov za vzpostavitev revizijskih sledi iz poglavja 4.1.3, razvoj programske rešitve pri razvijalcu, vključitev rešitve v informacijski sistem, nadgradnja programske opreme);
b) **stroške obratovanja** (beleženje, pregledovanje revizijskih sledi, iskanje po revizijskih sledeh, izdelava in analiziranje poizvedb, poročil, odprava nepravilnosti v sistemu na podlagi poizvedb in poročil).

Stroški so s pomočjo avtorja Arbitra ocenjeni za obdobje petih let na podlagi števila ur vloženega dela in ocenjene vrednosti bruto vrednosti urne postavke. Ocena je narejena ob domnevi, da je strošek fiksen, ne glede na obseg poslovanja podjetja, ter da je programska rešitev izdelana zunaj podjetja (za podjetje rešitev izdelajo zunanji izvajalci, ne gre za lastno rešitev podjetja). Upoštevana je tudi predpostavka, da vodenje revizijskih sledi poteka ustrezno, saj v nasprotnem primeru vsi stroški pomenijo neposredno izgubo vloženih sredstev, kot je bilo predhodno že predstavljeno.

Tabela 9: Ocena stroškov investicije za obdobje petih let (v EUR)

Vrsta stroška (razvoj/ obratovanje)	Opis stroška	Izvajalec naloge (podjetje/ razvijalec)	Število mesecev	Ocenjen strošek
Razvoj	Popis informacijskih sredstev, ocena tveganja, izdelava politike revizijske sledi, izdelava izvedbenih dokumentov, nastavitev sistemov	podjetje	1	16.800
Razvoj	Razvoj rešitve	razvijalec	12	604.800
Obratovanje	Beleženje, pregledovanje revizijske sledi, iskanje po revizijskih sledeh, izdelava poročil	podjetje	60	12.000
Razvoj	Nadgradnja programske opreme	podjetje	3	50.400
Obratovanje	Strošek dodatnih ukrepov v podjetju, na podlagi analiz (odprava nepravilnosti v sistemu)	podjetje	60	3.000
Stroški skupaj:				**687.000**

Ocenjen strošek investicije za obdobje petih let je **687.000 EUR.**

7.2.2 Koristi revizijskih sledi

Koristi revizijskih sledi sem razdelila na otipljive in neotipljive in jih prikazala v Tabeli 10.

Tabela 10: Otipljive in neotipljive koristi investicije

Otipljive koristi revizijskih sledi	Neotipljive koristi revizijskih sledi
Nižji stroški kazni (Kazni so posledica neupoštevanja ZVOP-1 ali odškodninskih postopkov in tožb zaradi uhajanja podatkov. Vodenje revizijskih sledi v podjetju razloge za kazni odpravi ali jih vsaj zmanjša.)	**Večji ugled in zaupanje v podjetje**
	Večja kakovost informacij v podjetju (Posledica odpravljenih nepravilnosti v delovanju informacijskega sistema, ki so bile ugotovljene na podlagi analiziranja poizvedb iz revizijskih sledi.)
Višji prihodki (Posledica pridobitve novih strank in ohranitev obstoječih strank, zaradi večjega ugleda in zaupanja v podjetje.)	**Večja informacijska varnost v podjetju** (Posledica zmanjšanja nepooblaščenih dostopov do podatkov in zmanjšanja možnosti za uhajanje podatkov iz podjetja.)
	Pozitiven učinek na uporabnika z vidika zanesljivosti, mirnosti (Posledica zavedanja uporabnika, da na podlagi vodenih revizijskih sledi lahko izve, kdo je dostopal do podatkov in kaj je pregledoval).

Ocena vrednosti koristi revizijskih sledi je zapletena, ker je večina koristi neotipljivih, zato jih ne moremo neposredno ovrednotiti. Turk (2005, str. 164) navaja, da so neotipljivi stroški in koristi samo tisti, ki jih nikakor ne moremo ugotoviti na trgu, ker ne nastopajo kot blago. Za potrebe ASK so v nadaljevanju navedene ocenjene vrednosti otipljivih koristi obravnavane investicije. Otipljive koristi so ocenjene kot:

a) 0,5 % od javno objavljenih prihodkov poslovanja v letu 2014 za tista podjetja, ki za vodenje revizijskih sledi uporabljajo Arbiter. Podjetja so glede na dejavnosti in obseg poslovanja različna med seboj, zato je za oceno letnih koristih uporabljeno povprečje vseh podjetij. Podatki so razvidni iz Tabele 11.
b) Kazni za tri prekrške letno na podlagi 91. in 93. člena ZVOP-1 (za podjetje, odgovorno osebo podjetja in posameznika, ki je prekršek storil). Podatki so razvidni iz Tabele 12.

Tabela 11: Ocenjene letne koristi investicije na podlagi poslovnih prihodkov (v EUR)

Podjetje	Poslovni prihodki 2014	0,5 % poslovnih prihodkov
Abakus plus, d. o. o.	948.798	4.744
Aerodrom Ljubljana, d. o. o.	32.048.626	160.243
Gorenjska Banka, d. d.	52.272.000	261.360
Hranilnica Lon, d. d.	9.749.000	48.745
Laser Line, d. o. o.	171.422	857
NLB Vita, d. d.	54.829.882	274.149
Pronet, d. o. o.	803.192	4.016

se nadaljuje

Tabela 11: Ocenjene letne koristi investicije na podlagi poslovnih prihodkov (v EUR) (nad.)

Podjetje	Poslovni prihodki 2014	0,5 % poslovnih prihodkov
Pronet, d. o. o.	803.192	4.016
SKUPAJ:	150.822.920	754.115
Povprečje/ocenjene koristi letno:	21.546.131	**107.730**

Vir: Prirejeno in povzeto po Arbiter, 2016.

Tabela 12: Ocenjene letne koristi investicije na podlagi glob za prekrške (v EUR)

Ocenjen strošek enega prekrška	14.590
Ocenjen strošek treh prekrškov na leto	**43.770**

Vir: Prirejeno in povzeto po 91. in 93. člen ZVOP-1.

Ocenjen skupni letni strošek otipljivih koristi za obravnavano investicijo je **151.500 EUR.**

7.2.3 Analiza stroškov in koristi revizijskih sledi

V Tabeli 13 so predstavljeni podatki za ASK obravnavane investicije. Podatki v tabeli so prikazani za obdobje petih let. Kot diskontna stopnja je uporabljena 2,7-odstotna bančna obrestna mera za podjetja, maj 2016 (Banka Slovenije, 2016).

Tabela 13: Tabela za ASK obravnavane investicije (v EUR)

OPIS VSEBINE/ ZAPOREDNO LETO	0	1	2	3	4	5
STROŠKI RAZVOJA	**672.000**					
STROŠKI VZDRŽEVANJA		**3.000**	**3.000**	**3.000**	**3.000**	**3.000**
Obrestni faktor 2,7 %	1,000	0,974	0,948	0,923	0,899	0,875
SEDANJA VREDNOST (v nadaljevanju PV) STROŠKOV	672.000	2.921	2.844	2.770	2.697	2.626
Kumulativa stroškov absolutno	672.000	675.000	678.000	681.000	684.000	687.000
Kumulativa PV stroškov	672.000	674.921	677.765	680.535	683.232	**685.858**
KORISTI REVIZIJSKIH SLEDI		**151.500**	**151.500**	**151.500**	**151.500**	**151.500**
PV KORISTI		147.517	143.639	139.863	136.185	132.605
Kumulativa PV koristi		147.517	291.156	431.018	567.204	**699.809**
NETO PV (v nadaljevanju NPV)	– 672.000	– 527.404	– 386.610	– 249.517	– 116.028	**13.951**
Neto denarni tok v letu	– 672.000	148.500	148.500	148.500	148.500	**148.500**
Kumulativni neto denarni tok – prag rentabilnosti	– 672.000	– 523.500	– 375.000	– 226.500	– 78.000	70.500

Vir: Prirejeno in povzeto po I. Cikajlo & F. Gider, Tehnike reševanja problemov, 2010, str. 109, 111.

Na podlagi podatkov iz Tabele 13 bodo v nadaljevanju izračunani finančni kazalci z namenom dokazati ekonomsko upravičenost obravnavane investicije. Izračunani bodo naslednji finančni kazalci: analiza dobe odplačevanja (angl. *Payback Time,* v nadaljevanju PBT), naložbeni donos (angl. *Return of Investment,* v nadaljevanju ROI), neto sedanja vrednost (angl. *Net present Value,* v nadaljevanju NPV) ter indeks donosnosti (angl. *Profitability Index,* v nadaljevanju PI).

***PBT** = leto pred poplačilom + nepoplačani znesek/koristi v letu poplačila*
PBT = 4 leta, 6 mesecev

T.i. prag rentabilnosti, pri katerem investicija prične prinašati dobiček, je 4 leta in 6 mesecev od začetka investicije.

***ROI** = (skupna vrednost koristi – skupna vrednost stroškov)/skupna vrednost stroškov*
ROI = 2 %

Analizirana investicija ima v 5 letih donosnost 2 %.

***NPV** = kumulativna cena, preračunana na PV = 13.951 EUR*
Odločitveni kriterij: če je NPV > 0, je investicijski projekt sprejemljiv (Berk, Lončarski, & Zajc, 2007, str. 99)

Na podlagi izračunane NPV obravnavane investicije lahko potrdimo, da je investicija sprejemljiva.

***PI** = PV »koristi« / PV »stroškov« = 1,02*
Odločitveni kriterij: če je PI > 1, je investicijski projekt sprejemljiv (Berk et al., 2007, str. 105–106)

Na podlagi izračunanega PI v obravnavano investicijo lahko potrdimo, da je investicija sprejemljiva.

Iz izvedene preproste analize stroškov in koristi ter izračunanih finančnih kazalcev je razbrati, da je investicija uvedbe in vodenja revizijskih sledi v podjetju ekonomsko upravičena. Stroški investicije se povrnejo prej kot v petih letih, investicijski projekt je sprejemljiv. Pri tem je treba poudariti, da so bile v okviru ASK upoštevane le otipljive koristi revizijskih sledi. Poleg predstavljenih »otipljivih« rezultatov ASK je treba upoštevati še neotipljive koristi revizijskih sledi, ki dodatno potrjujejo upravičenost investicije ter so hkrati lahko za podjetje pomembna konkurenčna prednost. Koristi revizijskih sledi v podjetju so posledice izboljšav, ki jih je investicija v revizijske sledi povzročila v poslovnih procesih podjetja. Na podlagi predstavljenih ugotovitev lahko potrdimo, da vodenje revizijskih sledi za podjetje ima poslovno vrednost.

Menim, da je poslovna vrednost revizijske sledi večja za tista podjetja, ki pri opravljanju svoje dejavnosti upravljajo z veliko količino osebnih podatkov, kot so na primer finančne ustanove, zavarovalnice, letališča. To je tudi razbrati iz prikazanega stanja v poglavju 6, mnenja strokovnjaka (B. Oblak, osebna komunikacija, 16. junij 2016), predstavljenega primera letališča v poglavju 5. Večji je obseg osebnih podatkov, s katerimi upravlja podjetje, večje so koristi revizijskih sledi za podjetje in s tem je večja poslovna vrednost revizijskih sledi.

SKLEP

V diplomskem delu sem s teoretičnega in praktičnega vidika preučila vodenje revizijskih sledi v podjetjih ter na osnovi ugotovitev analizirala poslovno vrednost revizijskih sledi. Končna ugotovitev je, da ima vodenje revizijskih sledi za podjetje poslovno vrednost.

Poslovna vrednost je v izboljšavah, ki jih koristi vodenja revizijskih sledi povzročijo v poslovnih procesih podjetja. Še posebej pomembne so t.i. neotipljive koristi vodenja revizijskih sledi v podjetju: večji ugled in zaupanje v podjetje, večja kakovost informacij v podjetju, večja informacijska varnost, pozitiven učinek na uporabnika z vidika zanesljivosti, mirnosti kot posledica zavedanja, da je v podjetju zagotovljena sledljivost obdelave podatkov (kdo je do podatkov dostopal, kaj je pregledoval, ali je podatke spreminjal, kakšne so nove in stare vrednosti podatkov). Z vodenjem revizijskih sledi v podjetjih preprečijo nepooblaščene dostope do podatkov in uhajanje podatkov.

Kljub temu so programske rešitve za vodenje revizijskih sledi pri uporabnikih (podjetjih) in razvijalcih rešitev nepriljubljene. Zaskrbljujoče je dejstvo, da je predmetna tematika (pre)zahtevna in glede na vloženo delo tudi ne dovolj donosna za razvijalce rešitev. Strokovnjak, ki mi je omogočil vpogled v praktični vidik vodenja revizijskih sledi, namreč pravi, da se ob upoštevanju dosedanjih izkušenj razvijanja te rešitve ne bi ponovno lotil.

Zahteve zakonodaje za vodenje revizijskih sledi so splošne, ohlapne, zato je proces njihovega uvajanja tehnično zahteven in drag. Stanje zagotavljanja revizijskih sledi v podjetjih je slabo, velikokrat so vodene le zato, ker tako zahteva zakonodaja. V podjetjih premalo poznajo in se zavedajo pomena ustrezno vodenih revizijskih sledi v informacijskih sistemih in odgovornosti upravljanja z osebnimi podatki.

Kot eno izmed možnih rešitev za izboljšanje opisanega stanja vidim v dopolnitvi zakonodaje (spremembe ZVOP-1 ali pa izdaja ustreznega podzakonskega akta), ki bi natančneje opredelila zahteve za sledljivost obdelave podatkov in tako poenostavila delo razvijalcem programskih rešitev ter hkrati poenostavila in znižala stroške uvajanja revizijskih sledi za uporabnika. Za neupoštevanje določil ZVOP-1 pa bi predpisala višje kazni s ciljem povečati zavedanje in odgovornost upravljanja z osebnimi podatki v podjetjih.

LITERATURA IN VIRI

1. *Arbiter*. Najdeno 30. aprila 2016 na spletnem naslovu http://www.abakus.si/sl/produkti/programska_oprema/arbiter
2. Banka Slovenije. (2016, julij). *Mesečna informacija o poslovanju bank.* Najdeno 20. julija 2016 na spletnem naslovu https://www.bsi.si/iskalniki/porocila.asp?MapaId=1329
3. Berk, A., Lončarski, I., & Zajc, P. (2007). *Poslovne finance*. Ljubljana: Ekonomska fakulteta.
4. Cikajlo, I., & Gider, F. (2010). *Tehnike reševanja problemov.* Nova Gorica: Univerza.
5. Delak, B. (2014). Revizijska sled v informacijskih sistemih v teoriji in praksi. *SIR*IUS*, 5, 5–28.
6. Groznik, A., Indihar Štemberger, M., & Kovačič, A. (2005). Vloga menedžmenta pri zagotavljanju poslovne vrednosti informatike. *Uporabna informatika, 13*(4), 213–222.
7. Groznik, A., & Vičič, D. (2005). Vrednost in pomen informatike v podjetju. *Organizacija, 38*(4), 198–202.
8. Informacijski pooblaščenec. (2010, 6. december). *Smernice za razvoj informacijskih rešitev.* Najdeno 18. julija 2016 na spletnem naslovu https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_razvoj_informacijskih_resitev.pdf
9. *ISO 2700 Directory*. Najdeno 30. aprila 2016 na spletnem naslovu http://www.27000.org
10. Markelj, B., & Bernik, I. (2012, 5. oktober). Nacionalna konferenca Informacijska varnost – odgovori na sodobne izzive. *Revija za teorijo in prakso zagotavljanja varnosti.* Najdeno 15. maja 2016 na spletnem naslovu http://www.fvv.um.si/rV/arhiv/2012-1/08_Markelj_Bernik.pdf
11. Mednarodni standard revidiranja, MSR 500, Revizijski dokazi. (2009) Najdeno 20. maja 2016 na spletnem naslovu http://www.si-revizija.si/sites/default/files/standardi/msr_500.pdf
12. Merc, P., & Šavnik. J. (2015, 22. oktober). Hramba podatkov in revizijska sled. *Pravna praksa*. Najdeno 20. julija 2016 na spletnem naslovu https://www.iusinfo.si/Login/FormsLogin/FormsLogin.aspx?ReturnUrl=%2fLITE%2fBesedilo.aspx%3fSOPI%3dL010Y2015V41P9-11N1&SOPI=L010Y2015V41P9-11N1#op_002
13. Ministrstvo za finance Republike Slovenije, Urad Republike Slovenije za nadzor proračuna. (2004). *Usmeritve za notranje kontrole*. Najdeno 30. aprila 2016 na spletnem naslovu http://www.unp.gov.si/fileadmin/unp.gov.si/pageuploads/zakonske_podlage/predpisi_slo/usmeritve_notr_kontr.pdf
14. O'Kelley, D., Ye, R. L. & Jones, C. G. & Miller, D. W. (2015). Effective network security audit trail management practices: an exploratory study. *Issues in Information Systemsm, 16*(III), 209–218.
15. Oblak, B. (2011). Vodenje revizijskih sledi brez posegov v aplikacije. *Zbornik referatov XIX. Mednarodne konference o revidiranju in kontroli informacijskih sistemov* (str. 187–198). Ptuj: Slovenski inštitut za revizijo.

16. Pravilnik o zahtevah za računalniške programe in elektronske naprave, upravljanje in delovanje informacijskega sistema ter o vsebini, obliki, načinih in rokih za predložitev podatkov. *Uradni list RS* št. 35/2013, 42/2013 – popr., 57/2013, 18/2016.
17. Rakar, A., & Žele, M. (2010). Učinkovito upravljanje revizijskih sledi. *Zbornik referatov XVIII. Mednarodne konference o revidiranju in kontroli informacijskih sistemov* (str. 143–150). Ptuj: Slovenski inštitut za revizijo.
18. Roratto, R., & Dias, E. D. (2014). Security information in production and operations: A study on audit trails in database systems. *JISTEM - Journal of Information Systems and Technology Management, 11*(3), 717–734.
19. Slovenski inštitut za revizijo. (2013). Iz prakse v prakso, Revizijske sledi v aplikativni programski opremi. *SIR*IUS, Slovenski inštitut za revizijo,* 1, 165–168.
20. Slovenski inštitut za revizijo. (2016). *Revizorji informacijskih sistemov*. Najdeno 5. maja 2016 na spletnem naslovu http://www.si-revizija.si/sekcijarevizorjevis/revizorji-informacijskih-sistemov
21. Slovenski odsek ISACA. (2016). *Zavarovanje osebnih podatkov pri uporabi informacijskih tehnologij*. Najdeno 20. maja 2016 na spletnem naslovu http://www.isaca.si/datoteke/2016/02/varstvo-osebnih-podatkov-ikt.pdf
22. Slovenski odsek ISACA. (b.l.). *Poslanstvo.* Najdeno 30. aprila 2016 na spletnem naslovu http://www.isaca.si/o_odseku.php
23. Turk, T. (2005). Analiza stroškov in koristi naložb v informatiko. *Uporabna informatika, 13*(3), 153–169.
24. Uratnik, J. (2011). Obvladovanje revizijskih sledi – upravljanje, procesi, standardi. *Zbornik referatov XIX. Mednarodne konference o revidiranju in kontroli informacijskih sistemov* (str. 157–170). Ptuj: Slovenski inštitut za revizijo.
25. Ustava Republike Slovenije (URS). *Uradni list RS* št. 33/1991, 42/1997-UZS68, 66/2000-UZ80, 24/2003-UZ3a, 47, 68, 69/2004-UZ14, 69/2004-UZ43, 69/2004-UZ50, 68/2006-UZ121, 140, 43, 47/2013.
26. Vezjak, D. (2012). Revizijske sledi – nuja in mora. *Zbornik referatov XX. Mednarodne konference o revidiranju in kontroli informacijskih sistemov* (str. 171–184). Ptuj: Slovenski inštitut za revizijo.
27. Vučić, N. (2010, 13. december). Kako zagotoviti revizijsko sled. *MonitorPro.* Najdeno 19. maja 2016 na spletnem naslovu http://www.monitorpro.si/si/_detajl/?id=41740
28. *Z Arbitrom do revizijske sledi.* Najdeno 30. aprila 2016 na spletnem naslovu http://www.arbiter.si/downloads/misc/Monitor_pro_poslovni_programi_priloga.pdf
29. Zakon o bančništvu (ZBan-2). *Uradni list RS* št. 25/2015, 44/2016 – ZRPPB.
30. Zakon o davčnem postopku (ZDavP-2). *Uradni list RS* št. 117/2006, 24/2008 – ZDDKIS, 125/2008, 85/2009, 110/2009, 1/2010 – popr., 43/2010, 97/2010, 24/2012 – ZDDPO-2G, 24/2012 – ZDoh-2I, 32/2012, 94/2012, 101/2013 – ZDavNepr, 111/2013, 22/2014 – odl. US, 40/2014 – ZIN-B, 25/2014 – ZFU, 90/2014, 95/2014 – ZUJF-C, 23/2015 – ZDoh-2O, 23/2015 – ZDDPO-2L, 91/2015.

31. Zakon o dostopu do informacij javnega značaja. (ZDIJZ). *Uradni list RS* št. 24/2003, 61/2005, 113/2005 – ZInfP, 109/2005 – ZDavP-1B, 28/2006, 117/2006 – ZDavP-2, 23/2014, 50/2014, 72/2014 – skl. US, 19/2015 – odl. US, 102/2015, 32/2016.
32. Zakon o elektronskih komunikacijah (ZEKom-1). *Uradni list RS* št. 109/2012, 110/2013, 40/2014 – ZIN-B, 54/2014 – odl. US, 81/2015.
33. Zakon o gospodarskih družbah (ZGD-1). *Uradni list RS* št. 42/2006, 60/2006 – popr., 26/2007 – ZSDU-B, 33/2007 – ZSReg-B, 67/2007 – ZTFI, 10/2008, 68/2008, 42/2009, 33/2011, 91/2011, 100/2011 – skl. US, 32/2012, 57/2012, 44/2013 – odl. US, 82/2013, 55/2015.
34. Zakon o Informacijskem pooblaščencu (ZInfP). *Uradni list RS* št. 113/2005, 51/2007 – ZUstS-A.
35. Zakon o javnih financah. (ZInfP). *Uradni list RS* št. 79/1999, 124/2000, 79/2001, 30/2002, 110/2002 – ZDT-B, 56/2002 – ZJU, 127/2006 – ZJZP, 14/2007 – ZSPDPO, 109/2008, 49/2009, 38/2010 – ZUKN, 107/2010, 110/2011 – ZDIU12, 46/2013 – ZIPRS1314-A, 101/2013, 101/2013 – ZIPRS1415, 38/2014 – ZIPRS1415-A, 14/2015 – ZIPRS1415-D, 55/2015–ZFisP, 96/2015.
36. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). *Uradni list RS* št. 30/2006, 24/2014 – odl. US, 51/2014.
37. Zakon o varstvu osebnih podatkov (ZVOP-1-1). *Uradni list RS* št. 86/2004, 113/2005 – ZInfP, 51/2007 – ZUstS-A, 67/2007.