SIR IUS 5/18

SLOVENSKI INŠTITUT za REVIZIJO

Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

Kazalo

stran

IZ PRAKSE ZA PRAKSO

NOVOSTI IN OBVESTILA

Dr. Marjan Odar

Uvodnik

Editorial

Dopusti in počitnice so minili. Jesen je tu, pa nova Vlada tudi. Še preden je postala operativna, se je že začela burna razprava predvsem o razlagi koalicijskega sporazuma glede davkov. Najbolj so razvnele strasti napovedane predvidene spremembe obdavčitve kapitalskih dobičkov. Nekateri drugačno obdavčitev kapitalskih dobičkov podpirajo in pozdravljajo, drugi ji odločno nasprotujejo. Vsaka stran seveda zagovarja lastne interese in jih poskuša s takimi ali drugačnimi argumenti tudi podkrepiti. Logično in legitimno. Prepričan sem, da so tudi bralci tega uvodnika razdeljeni. Nočem in ne bom ugibal, katerih je več, čeprav se mi nekako dozdeva, da je večina proti vključitvi kapitalskih dobičkov v dohodninsko osnovo. Tako je pač stanje in na tej točki tudi ne bom ugibal, kakšne bodo dejanske spremembe davčne zakonodaje, ki jih bo predlagala nova Vlada. Menim, da je za razvoj podjetništva pomembno še nekaj drugega – pogosto spreminjanje davčne zakonodaje. Vsakdo, ki se resno spusti v podjetniške vode, bo izdelal podjetniški načrt in načrtoval razvoj podjetja za več let. Gotovo bo pri tem pričakovani poslovni izid eden izmed ključnih elementov cilja poslovanja podjetja. Pa ne le poslovni izid podjetja, ampak tudi donosnost na vložena sredstva vlagateljev oziroma lastnikov. Davki igrajo pri tem zelo pomembno vlogo. Kaj pomaga še tako dober načrt, ki je lahko tudi uresničen, če pa so kasneje končni učinki poslovanja zaradi sprememb davčne zakonodaje pomembno drugačni. V podjetništvu je že tako veliko negotovosti, so lahko dobički in ali pa izgube, vendar nanje podjetnik s svojimi odločitvami lahko vpliva. Na spremembo davčne zakonodaje pa posameznik nima prav nobenega vpliva.

Skoraj vsaka nova Vlada pa ima take ali drugačne ideje glede obdavčitve. In smo pri bistvu problema. Ne gre le za vedno prisotni antagonizem med obdavčitvijo dela in kapitala, ampak je ta problematika širša. Moramo pogledati še širši družbeni kontekst in neposrednim in posrednim davkom dodati še prispevke in druge dajatve. Kakorkoli že obravnavamo to problematiko, ne moremo mimo ugotovitve, da gre za zakonsko podprto prerazporeditev sredstev. Od koga h komu in iz katerih virov h katerim. Dati in ali dobiti in obratno. V tem je temeljno vprašanje ustvarjanja nove vrednosti in redistribucije. Kakšno vizijo razvoja ima

naša država? Katere dejavnosti, interesne skupine so pomembnejše, koga bomo podpirali in kdo bo k temu prispeval? Ali bomo podpirali šolstvo, zdravstvo, podjetništvo, morda turizem, rudarstvo ali kmetijstvo? Ali se želimo odpreti tujim investitorjem in sploh večji vlogi kapitala ali pa smo morda bolj naklonjeni univerzalnemu temeljnemu dodatku? Kaj razumemo kot socialno državo, kako globoko naj seže solidarnost? Ker nam je ostala le še fiskalna samostojnost, so dajatve najpomembnejši instrument, kjer lahko država vpliva na razvoj. Zato sem prepričan, da bi bilo dobro, da bi kot družbeni konsenz sprejeli strategijo in temeljna izhodišča ter okvire razvoja in jih seveda spodbujali z ustrezno fiskalno politiko. Ko bi bila le-ta sprejeta, pa te zakonodaje konceptualno ne bi spreminjali najmanj devet let. Utopija? Morda. Ampak če nimamo cilja, kam bi radi prišli, potem tudi poti do njega ne moremo poznati, in vsak, ki je trenutno na oblasti, bo izbral lastno traso. Po naslednjih volitvah pa morda nekaj drugega ali pa tretjega. In se vrtimo v začaranem krogu.

Marko Anžič*

Pasti revidiranja sistema upravljanja uporabniških pravic v informacijskem sistemu

Pitfalls in the management system audit of user IS access rights

POVZETEK ● *Revizorji informacijskih sistemov (IS) se pri ocenjevanju ustroja in delovanja notranjekontrolnega okolja pogosto zanašajo na sistem upravljanja uporabniških pravic, ki naj bi zagotovil, da sme vsak uporabnik v sistemu početi le tisto, kar mora po naravi svojega dela. Pri tem se zanašajo na procese odobravanja, pregledovanja in odvzemanja teh pravic ter na proces upravljanja samih pooblastil. Neustrezno opredeljene procesne kontrole pa lahko izničijo koristi še tako dobro delujočega sistema upravljanja uporabniških pravic, zato je sodelovanje notranjega revizorja in revizorja IS-jev zaradi njunega različnega fokusa in znanj pogosto nujno potrebno.*

Ključne besede ● *uporabniške pravice v IS-jih, procesne kontrole v IT-jih, sodelovanje notranjega in revizorja IS-jev*

SUMMARY ● *IS auditors frequently rely upon the user (access) rights management system (URMS), intended to ensure that each user performs only the activities related to their work position, based on the assessment of design and operational efficiency of internal control environment. Auditors rely on the access approval, review, revocation as well as role management processes, supported by URMS. However, improperly designed process controls can void the benefits of an effectively designed URMS. This, along with differences in their audit focus and expertise, often requires close cooperation of internal and IT auditors.*

Key words ● *User IS access rights, IT process controls, cooperation between internal and IS auditors*

JEL: D 83, G 31, O 33

* Marko Anžič, specialist za menedžment, CISA, PRIS, CIA, markoff76@gmail.com.

1. UVOD

1.1. Delitev dela

Človek že od pradavnine poizkuša s kar najmanj truda in sredstev (vložek) ustvariti kar največ izdelkov ali storitev (izložek). Med pomembnejše dejavnike doseganja maksimizacije izložka poleg naravnih virov in orodij uvrščamo visoko stopnjo specializacije, zadnje pa omogoča delitev procesa na kar najmanjše število enostavnih korakov. Delitev dela je ločevanje nalog v kateremkoli delovnem sistemu zaradi specializacije sodelujočih v procesu in posledično doseganja visoke učinkovitosti procesa.

1.2. Ločevanje dolžnosti

Dela pa ne delimo vedno le zaradi doseganja višje specializacije sodelujočih v procesu – konec koncev zaradi omejenega števila zaposlencev v nekaterih organizacijah in enostavnosti posameznega procesa nekaterega dela ni smiselno razdeliti med več oseb. Nekateri procesi so namreč povezani z višjo stopnjo tveganja, npr. procesi naročanja storitev, potrjevanja in plačevanja računov. Čeprav so ti procesi samostojni, so med seboj z vložki oz. izložki povezani v verigo, ki jo v praksi imenujemo tudi "od naročila do plačil" (angl. *order-to-payment*). Posameznik, ki sme ali lahko izvaja celotno verigo procesov, ima enostavno možnost izvajati transakcije, ki pri odsotnosti ustreznih kontrol za organizacijo pomenijo tveganje nesmotrnega ali celo škodljivega ravnanja.

Z namenom obvladovati tveganja tako nenamernih napak kot namernih zlorab poslovodstvo v delovne procese uvaja različne kontrole, ki predstavljajo mehanizme zmanjševanja teh tveganj – tako v obliki izboljšanja kakovosti procesa kot tudi preprečevanja prevar. Najpogostejši primer takšnih kontrol je ločevanje dolžnosti (angl. *separation/segregation of duties*). Pri navedeni verigi procesov se delovne naloge tipično razdelijo na način, da nobena oseba ne more npr. pripraviti naročilnice, prevzeti materiala na zalogo, potrditi ustreznost dobaviteljevega računa in hkrati plačati računa. Pogosto je že kombinacija le nekaterih od teh delovnih nalog dovolj, da lahko brez ustreznih kontrol pride do zlorabe s strani zaposlenca (npr. knjiženje in plačevanje računov).

Najpogostejše in najbolj znano načelo ločevanja dolžnosti je načelo štirih oči (angl. *four-eyes principle* ali *two-man rule*), s katerim se zagotavlja, da aktivnosti, ki predstavljajo povišano stopnjo tveganja za organizacijo, v delovnem procesu ne more izvajati ena sama oseba. V primeru iz prejšnjega odstavka bi to pomenilo, da en zaposlenec knjiži vhodne račune, ne more pa jih plačevati. Drug zaposlenec račune plačuje, ne more pa jih knjižiti. Za izvedbo verige procesov torej potrebujemo oba.

2. NOTRANJEKONTROLNI SISTEM INFORMACIJSKIH SISTEMOV

2.1. Uporabniške pravice v IS-jih

Uporabniške pravice v informacijskem sistemu (v nadaljevanju IS) so digitalna analogija pristojnostim in odgovornostim, ki jih posameznikom dodeli vodstvo organizacije zaradi izvajanja delovnih nalog. Za delo v IS-jih uporabnik potrebuje ustrezne uporabniške pravice, ki obsegajo dostop do:

- računalniškega omrežja (npr. preko aktivnega imenika Windows ali Linux LDAP),
- aplikacij, ki omogočajo izvajanje delovnih procesov,
- posameznih funkcionalnosti aplikacij, s katerimi je mogoče izvajati del ali celoten delovni proces,
- virov podatkov (baze podatkov, datotečni sistemi, spletni portali ipd.) in
- dostop do branja, zapisovanja, spreminjanja ali brisanja konkretnih podatkov.

2.1. Pomen dodeljevanja uporabniških pravic

Med notranje varnostne grožnje sodijo predvsem:

- finančne zlorabe,
- nepooblaščen dostop do podatkov,
- kraja intelektualne lastnine,
- industrijsko vohunjenje,
- uničevanje podatkov ipd.

Praktično vse pa je mogoče izvesti z (preširokim) dostopom do IS-jev in podatkov organizacije. Pomembnost ustreznega dodeljevanja uporabniških pravic kot enega od ključnih mehanizmov varovanja IS-jev jasno pokaže tudi statistika (Cybersecurity Insiders, 2018), ki kaže, da strokovnjaki s področja IT-ja in varnosti ocenjujejo notranje varnostne grožnje kot večji izziv kot zunanje, ne glede na to, ali so te grožnje posledica napak in malomarnosti ali namernih ravnanj. Kar 90 % jih ugotavlja, da so ranljivi za notranje napade, 37 % pa jih meni, da največje tveganje predstavljajo ravno preširoko dodeljene uporabniške pravice v IS-jih.

2.2. Uporabniške vloge

Uporabniške vloge v IS-jih (angl. *user roles*) predstavljajo nabor uporabniških pravic znotraj posameznega dela informacijskega sistema (aplikacije, baze omrežja), ki predstavljajo pravico do izvedbe določenega nabora nalog in dostopa do določenih podatkov. Vsebinsko predstavljajo digitalni ekvivalent delovni funkciji, delovni nalogi ali (sistematiziranemu) delovnemu mestu.

Namen uporabniških vlog je:

- zagotoviti dodeljevanje natanko takšnih uporabniških pravic, kot jih uporabnik potrebuje za celovito in kakovostno izvedbo svojih delovnih nalog;
- sistematično ločevati uporabniške pravice, ki predstavljajo kršitev načela ločevanja dolžnosti;
- standardizirati uporabniške profile in s tem poenostaviti tako dodeljevanje lastnikom procesa oz. ključnim uporabnikom kot tudi upravljanje samih pravic odgovorne osebe v službi informacijskih tehnologij.

Njihov obseg je odvisen predvsem od:

- velikosti organizacije,
- kompleksnosti delovnih procesov ter
- preferenc oz. sprejemljivosti tveganja (angl. risk appetite) vodstva.

Na tem mestu je smiselno poudariti, da se v organizacijah pogosto uporablja koncept referenčnega uporabnika. To pomeni, da npr. novemu zaposlencu dodelimo enake uporabniške pravice, kot jih že ima eden od obstoječih zaposlencev, ki opravlja podobne naloge kot novi zaposlenec. V sistemih, v katerih se uporabniku ob menjavi delovnega mesta uporabniške pravice, ki jih ne potrebuje več, ne odvzemajo, to povzroči kopičenje uporabniških pravic pri posameznem uporabniku, to kopičenje pa se nato širi tudi na nove zaposlence. Takšno dodeljevanje uporabniških pravic je slaba praksa, ki sčasoma povzroči neučinkovitost kontrolnih mehanizmov.

2.3. Druge sorodne kontrole

Za prepoznavanje istovetnosti oz. identitete uporabnika se kot pomembna predpostavka za učinkovito dodeljevanje pravic uporabnikom uporabljajo drugi kontrolni mehanizmi (združeni v koncept upravljanja uporabniških identitet; angl. (*user, identity management*), ki pa jih v okviru tega članka ne bomo obravnavali. Ravno tako ne bomo obravnavali revizijske sledi, ki predstavlja mehanizem zagotavljanja sledljivosti uporabnikove aktivnosti v IS-jih. Ta namreč predstavlja detektivno (zaznavalno) in ne preventivno (preprečevalno) kontrolo, zaradi česar ne moremo govoriti o enakovredni alternativni kontroli, ki bi zmanjševala tveganje neustreznih uporabniških pravic.

2.4. Procesne kontrole

Procesne kontrole (angl. *processing controls*) spadajo po napotkih za revidiranje *GTAG 8* v družino aplikativnih kontrol, ki se nanašajo na posamezne delovne procese ali aplikativne informacijske sisteme. Med te spadajo tudi vnosne kontrole, izhodne kontrole, kontrole integritete ter revizijska sled.

Procesne kontrole so tiste, ki omogočajo samodejni (avtomatiziran) način zagotavljanja, da je procesiranje podatkov celovito, natančno in odobreno. V informacijskem sistemu najdemo različne oblike procesnih kontrol:

- dodeljevanje statusa dokumentu, ki opredeljuje korak procesa, v katerem se dokument nahaja, in možnosti dela z njim (npr. status Zaključen običajno ne dovoljuje spreminjanja dokumenta);
- samodejno dodeljevanje dokumenta v potrjevanje ustreznim osebam glede na lastnosti dokumenta (npr. dodelitev ustreznemu potrjevalcu glede na stroškovno mesto);
- primerjava in uporaba ali usklajevanje podatkov med različnimi dokumenti (npr. med naročilnico in vhodnim računom);
- spreminjanje ali ustavljanje procesnega toka glede na lastnosti dokumenta (npr., če vhodni račun ne temelji na naročilnici ali pogodbi ali je znesek računa višji od opredeljenega parametra) ipd.

Procesne kontrole so večinoma, podobno kot uporabniške pravice, preventivne kontrole, torej preprečujejo neželen potek procesa.

3. SISTEM UPRAVLJANJA UPORABNIŠKIH PRAVIC

3.1. Procesi URMS

Sistem upravljanja uporabniških pravic (angl. *user (access) rights management system* ali *URMS*) je sestavljen iz naslednjih ključnih (upravljavskih) procesov:

- dodeljevanja,
- spreminjanja,
- odvzemanja in
- obdobnega pregledovanja ustreznosti dodeljenih uporabniških pravic.

Sistem mora biti vzpostavljen na način, pri katerem smejo uporabniške pravice upravljati izključno tiste osebe, ki jim je bila delegirana pristojnost upravljanja procesov, na katere se nanašajo pravice. Npr., direktor prodaje kot lastnik prodajnih procesov sme upravljati izključno tiste uporabniške pravice, ki se nanašajo na te procese. Uporabniške pravice dela z drugimi procesi smejo upravljati lastniki drugih procesov.

Pri pregledu ustreznosti zasnove in učinkovitosti teh procesov ali ob njihovem vzpostavljanju se je smiselno ozreti po mednarodnih standardih in okvirih, ki predstavljajo nabor dobre prakse.

3.2. Družina mednarodnih standardov ISO 2700x

Referenčni cilji kontrol in kontrole, kot jih opredeljuje mednarodni standard informacijske varnosti ISO 27001:2013 in so relevantni za upravljanje uporabniških pravic, so opredeljeni v okviru področja A.9 Nadzor dostopa.

Kontrole, ki omogočajo izpolnjevanje ciljev tega področja in so še posebej relevantne za upravljanje uporabniških pravic, so (referenčni kontrolni cilji od A.9.1.1 do A.9.2.6):

- Izvesti se mora formalni postopek za registracijo in izbris registracije uporabnika, da se omogoči dodeljevanje pravic dostopa.
- Izvesti se mora formalni proces zagotavljanja dostopa uporabnikom, da se pravice dostopa dodelijo ali prekličejo za vse vrste uporabnikov za vse sisteme in storitve.
- Dodelitev in uporaba posebnih pravic dostopa se morata omejiti in nadzorovati.
- Dodeljevanje tajnih informacij za preverjanje verodostojnosti se mora nadzorovati s formalnim procesom upravljanja.
- Lastniki dobrin morajo pregledovati uporabniške pravice dostopa v rednih časovnih presledkih.
- Pravice dostopa vseh zaposlenih in zunanjih uporabnikov do informacij in naprav za obdelavo informacij se morajo odstraniti po prekinitvi njihove zaposlitve, pogodbe ali dogovora oziroma se prilagoditi spremembam.

ISO 27001 ločevanje (razmejitev) dolžnosti obravnava sicer v okviru kontrolnega cilja A.6.1.2: "Nasprotujoče si naloge in področja odgovornosti se morajo razmejiti, da se zmanjšajo možnosti za nepooblaščeno ali nenamerno spreminjanje ali zlorabo dobrin organizacije."

3.3. Zanašanje na učinkovitost procesov URMS

Zasnovo kontrol sistema URMS običajno revizorji ocenijo kot ustrezno takrat, kadar je ta tako dokumentno (opis procesov in pravil) kot sistemsko (vpeljava procesov v IS) podprt in sledi načelom dobre prakse. Za preverjanje njegove dejanske (operativne) učinkovitosti revizorji običajno izvedejo pregled vzorčnih uporabnikov, pri teh pa primerjajo dejansko dodeljene uporabniške pravice v izbranih aplikacijah s formalno odobrenimi.

Tako na podlagi lastne pretekle prakse kot ob opazovanju tuje (predvsem, ne pa tudi izključno slovenske) avtor članka ugotavlja, da se za ocenjevanje tveganj v posameznih delovnih (poslovnih) procesih tako notranji revizorji (ki revizorjem IS-jev, ki jih najemajo, običajno predpisujejo obseg revizijskega posla) kot tudi

revizorji IS-jev pogosto uporabljajo le kontrolne cilje standarda informacijske varnosti ISO 27001, ki se nanašajo na ocenjevanje uspešnosti in učinkovitosti upravljanja uporabniških pravic. Pri tem je treba poudariti, da je pregled mehanizmov, ki izpolnjujejo kontrolni cilj A.6.1.2 (Razmejitev dolžnosti), pogosto predmet poenostavljenega pregleda ali sploh ni predmet pregleda, saj (1) mnogo organizacij ne ločuje dolžnosti sistematično, (2) pričakovani obseg revizijskega posla ne dovoljuje podrobnejše analize opredeljenih vlog, hkrati pa (3) nimajo niti notranji niti revizorji IS-jev sami dovolj znanja, da bi celovito poznali vse tipične vloge v različnih delovnih procesih in konflikte, ki jih kombinacije posameznih vlog predstavljajo.

Kljub temu da revizor lahko omeji obseg in namen revizije na izključno dajanje mnenja o delovanju URMS-ja za naročnika revizijskih storitev (kamor sodijo tudi zunanji revizorji, ki najemajo storitve revizije IS-jev znotraj ali zunaj lastne organizacije) le na podlagi omejitev, ni nujno jasno, na delovanje katerih kontrol oz. izpostavljenost katerim tveganjem revizor sploh daje mnenje.

Najpogosteje se ustreznost ločevanja dolžnosti zaradi navedenega izvaja kot ločen, samostojni revizijski posel, pri tem pa se uporabljajo specializirane matrike tipičnih poslovnih vlog in konfliktov med njimi. Takšne matrike so običajno na voljo le večjim revizijskim družbam, ki imajo dovolj virov in znanja za pripravo takšnih pripomočkov.

Na podlagi (pre)ozko opredeljenega obsega revizijskega posla mora nato revizor IS-jev podati mnenje o uspešnosti zasnove in operativni učinkovitosti kontrol, ki obvladujejo tveganja, ki izhajajo iz aktivnosti zaposlencev organizacije v informacijskem sistemu. Kot bo pokazal primer v nadaljevanju, je lahko oblikovanje ali dajanje takšnega mnenja brez razumevanja delovanja procesnih kontrol z vidika presoje le pregledanih kontrol morda ustrezno, z vidika celovitega razumevanja tveganj napak in zlorab, povzročenih s strani uporabnikov, pa napačno. Zanašanje izključno na delovanje procesov URMS-ja tako brez razumevanja sovpliva, ki ga imajo procesne kontrole na sistem uporabniških pravic, tako ni priporočljivo.

4. PRIMER REVIZIJE PROCESA LIKVIDATURE RAČUNOV

V nadaljevanju bom za praktično ponazoritev navedenih omejitev pregleda sistema upravljanja uporabniških pravic uporabil izkušnjo iz notranjerevizijskega posla pregleda procesa likvidature vhodnih računov, ki sem ga v preteklosti izvajal v ilustrativnem podjetju.

4.1. Obseg revizije

Revizija je prvotno obsegala pregled naslednjih ključnih kontrolnih ciljev (navajam samo za vsebino tega članka relevantne) procesa likvidature računov:

- potek dela procesa likvidacije je sistematičen, predvidljiv in v skladu z internimi akti;
- aplikativne kontrole preprečujejo naključne in namerne napake pri vnosu podatkov;
- dostopi do informacijskega sistema se ustrezno upravljajo;
- informacijski sistemi medsebojno samodejno, pravilno in ažurno izmenjujejo podatke.

Med izvedbo se je obseg revizije razširil še na pregled kontrol na področju priprave in potrjevanja storitvenih naročilnic, saj sem že ob pregledu zasnove notranjekontrolnega okolja priprave različnih vrst naročilnic prepoznal določene sistemske pomanjkljivosti, kot jih navajam v nadaljevanju članka. Procesa knjiženja in plačevanja računov, ki se izvajata po izvedeni likvidaturi, nista bila predmet revizije.

4.2. Kratek opis pregledanih procesov

Likvidatura računov je proces potrjevanja količinske in kakovostne ustreznosti izvedenih storitev (le v primeru storitvenih naročilnic, v primeru materialnih se prevzem izvaja v enem od skladišč, v primeru blaga na poti pa na podlagi transportnice in računa), skladnosti cen in drugih komercialnih pogojev z dogovorjenimi ter skladnosti z zakonodajnimi (predvsem davčnimi) zahtevami, proces pa se zaključi s knjiženjem računa. Vsak račun ima v procesu skrbnika (večinoma administrator, ki običajno pripravi tudi naročilnico), vsebinskega potrjevalca (pripravljalec naročilnice ali naročnik storitve oz. blaga) in parafista (lastnik stroškovnega mesta, ki ga račun bremeni). Brez potrditve potrjevalca in parafista likvidatura računa ni mogoča. Posamezni račun lahko potrdi tudi več kot en potrjevalec in več kot en parafist. Po potrditvi računa podatke na njem preveri likvidator (eden od zaposlencev v računovodstvu). V primeru pravilnosti ga poknjiži, sicer ga vrne v dopolnitev skrbniku.

Proces likvidature je na vhodu povezan s procesom zajemanja vhodnih računov v ustrezno digitalno obliko, povezuje pa se tudi s predhodno potrjenimi naročilnicami.

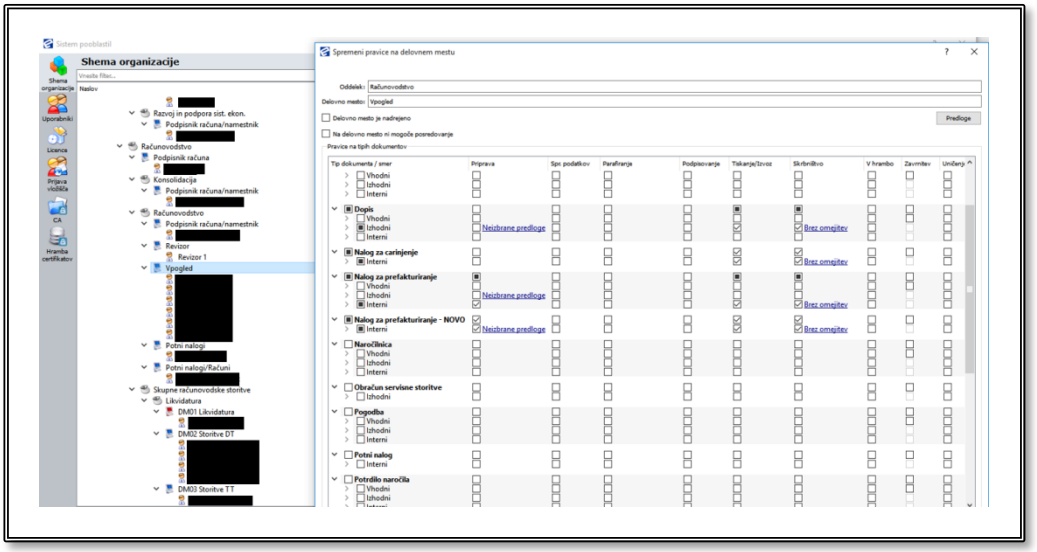
4.3. Podporni informacijski sistem

Procesa likvidature računov ter potrjevanja storitvenih naročilnic sta podprta z informacijskim sistemom L (kot likvidatura), ki je preko določenih ročnih

mehanizmov povezan z informacijskim sistemom K (kot knjiženje), ta pa se uporablja za knjiženje vhodnih računov in za pripravo storitvenih naročilnic.

Za potrebe presoje procesov likvidature računov in potrjevanja storitvenih naročilnic so bile za revizorja IS-jev pomembne le uporabniške pravice v okviru sistema L. L sicer vzdržuje lastno bazo uporabnikov, ki pa se (ob ročnem proženju) samodejno usklajuje s podatki o zaposlencih v K-ju (modul, ki pokriva področje upravljanja kadrov oz. *HR*). Poleg uporabnikov se iz K-ja v L prenaša tudi organizacijska shema zaposlencev. Ta se v L-ju uporablja kot izhodišče za shemo potrjevalcev, saj se pravice dodeljujejo na delovno mesto, posameznega uporabnika pa se prav tako dodeli na delovno mesto. Dostop do sistema se uporabniku aktivira na podlagi odobritve s strani njegovega neposrednega vodje (shema pooblastil se nahaja v sliki 1).

Slika 1: Zaslonska slika sheme pooblastil v L-ju



4.4. Procesne kontrole v L-ju

Poleg že navedene obvezne potrditve računa s strani potrjevalca in parafista potek dela (angl. *workflow*) procesa likvidature računa v L-ju vključuje tudi druge procesne kontrole (navajam le pomembnejše):

- obveznost naročilnice za vsak račun, ki se nanaša na izvedbo storitev, in obvezno povezovanje računa z naročilnico;
- obvezno kreiranje "letne" naročilnice v primeru sukcesivne dobave oz. pričakovanja več vhodnih računov za isto naročilnico ("enkratna" naročilnica se s prvim vhodnim računom zapre in arhivira);

- usmerjanje računa k ustreznim uporabnikom na podlagi več tipov pravil:
  - tabela povezav med dobaviteljem in likvidatorjem,
  - podatek o kreatorju ali naročniku iz naročilnice, terminskega sporazuma, dobavnice – ta postane odgovorni uporabnik (podpisnik),
  - druga specifična pravila, ki se izvajajo ob prejemu, pošiljanju, nastanku, na podlagi podatkov v dokumentu ali na podlagi časovnih pravil),
  - ko en od teh mehanizmov samodejno izbere podpisnika, se to posebej zabeleži v revizijski sledi dokumenta z oznako "Skripta" ali "Pravilo", v primeru ročnega posredovanja pa kot "Posredovano";
- preverjanje skladnosti podatkov o količinah in ceni na nivoju postavke ter skupni ceni med računom in naročilnico; v primeru neskladja mora uporabnik popraviti podatke na naročilnici ali zavrniti račun;
- različni statusi dokumenta, ki enim uporabnikom omogočijo, drugim pa onemogočijo delo na dokumentu.

4.5. Ključne ugotovitve revizije

Revizija je ugotovila različne vrste pomanjkljivosti, v tem članku bom navedel le tiste, ki so povezane z neustreznimi ali neobstoječimi procesnimi kontrolami.

Uporabniške pravice v sistemu L se ne upravljajo sistematično, smernic ali pravil dodeljevanja dostopov družba nima. Dostop do sistema odobrava nadrejena oseba zaposlenca po formalni proceduri v okviru intranetnega portala. Sistematični pregled uporabniških pravic se ne izvaja periodično. Tveganje do neke mere zmanjšuje dejstvo, da se brez aktivnega uporabniškega računa v omrežju ni mogoče prijaviti v aplikacijo. Uporabnike je treba po prenosu podatkov iz modula K HR ročno razvrstiti v skupine uporabnikov (delovna mesta), za katere so dodeljene uporabniške pravice. Izpisa podatkov o uporabnikih sistema (razen dostopa do podatkov posameznega uporabnika), vključno z njihovimi uporabniškimi pravicami, iz sistema nisem mogel pridobiti zaradi strukture podatkov v sistemu. Zato nisem mogel izvesti sistematične analize uporabniških dostopov (npr. primerjava med številom lastnikov stroškovnim mest iz sistema pooblastil in številom uporabnikov s pravico parafiranja). Kljub temu na podlagi preverjenega vzorca uporabnikov nisem opazil odstopanj med vlogo v organizaciji podjetja in dodeljenimi uporabniškimi pravicami. Na podlagi navedenega bi lahko prišel do zaključka, da sistem upravljanja uporabniških pravic ni zasnovan v celoti v skladu s standardom ISO 27001:2013, kljub temu pa pregled operativne učinkovitosti dejanskih uporabniških pravic ne kaže povišanega tveganja neustrezno dodeljenih pravic.

Ne glede na to, ali se lahko glede na opisan rezultat pregleda sistema upravljanja uporabniških pravic na njegovo delovanje zanesemo ali ne, naslednje ugotovitve,

povezane s procesnimi kontrolami, pokažejo, da prepoznanih tveganj ne bi mogli obvladovati niti s sistemom, ki bi bil tako v zasnovi kot v operativni učinkovitosti v celoti skladen s standardom ISO 27001:2013.

Storitveno naročilnico v L-ju lahko parafira kdorkoli, ki ima pravico do parafiranja, čeprav ni dejanski lastnik relevantnega stroškovnega mesta in s pripravljavcem oz. potrjevalcem naročilnice ni v nadrejenem hierarhičnem položaju. Poenostavljeno povedano: storitveno naročilnico lahko v imenu lastnika kateregakoli stroškovnega mesta parafira katerikoli uporabnik z uporabniško pravico parafista. Ker v fazi priprave naročilnice ne sodeluje nobena druga funkcija (nabava, likvidatura), je kontrolo pristojnosti parafista in stroškovnega mesta, ki ga račun bremeni, mogoče izvesti (ročno) izključno v procesu likvidature računa s strani računovodstva.

Uporabnik, ki ima v L-ju uporabniške pravice do podpisovanja in parafiranja dokumentov, lahko tako kreira, podpiše in parafira storitveno naročilnico, hkrati pa podpiše in parafira vhodni račun, ki se na to naročilnico nanaša. Takih primerov sem v pregledanem obdobju enega leta odkril več deset. Sistem tako v navedenem scenariju ne zagotavlja pravila štirih oči.

Procesi, ki urejajo tok dokumentov v L-ju, so v določeni meri avtomatizirani (dodelitev prvega podpisnika/parafista, primerjava med naročilnico materiala in računom ter samodejna likvidacija), vendar pa proces likvidature v L-ju omogoča posameznemu uporabniku prosto posredovanje dokumenta poljubni drugi osebi v podpis ali parafo. Pri tem lahko katerakoli oseba, ki ji je bila dodeljena pravica podpisovanja ali parafiranja dokumentov, to akcijo izvede na poljubnem dokumentu, če ji je ta posredovan v potrditev, čeprav nima dejanske pristojnosti odobravanja stroškov na podlagi prejetega računa. Čeprav uporabniški pravici podpisovanja oz. parafiranja nista dodeljeni vsakemu zaposlencu, je zaradi obsega organizacije dodeljena več sto uporabnikom.

Poleg omogočanja neavtoriziranega podpisovanja računov omogoča navedena fleksibilnost sistema uporabnikom neposredno izogibanje naslednji kontroli: računovodstvo redno pripravlja poročila o računih, ki v sistemu čakajo aktivnost uporabnika več kot 3 dni (formalni rok za potrditev ali zavrnitev računa s strani uporabnika). Vključitvi posameznega računa (s tem pa tudi uporabnika) v takšno poročilo in posledično zagovoru pri nadrejeni osebi se uporabniki enostavno izognejo s preposredovanjem računa poljubni drugi osebi. V okviru pregleda nekaterih računov smo ugotovili, da takšno preposredovanje računov med dvema uporabnikoma ni redko.

Storitveno naročilnico, ki se jo ustvari v K-ju, je treba v L-ju podpisati le enkrat – vsaka nadaljnja sprememba naročilnice v K-ju se v L preslika kot nova različica,

zanjo pa ponovni podpis ni več potreben. Nova različica naročilnice se lahko tako po predmetu naročila in obsegu bistveno razlikuje od prejšnje, vendar pa parafist teh sprememb ne vidi. Tveganje bi sicer moralo zmanjševati dejstvo, da mora tudi račun parafirati parafist, vendar pa je v povezavi s predhodno ugotovitvijo (vsak uporabnik z uporabniško pravico parafista lahko parafira račun) tveganje zlorabe nezmanjšano. Edini mehanizem za preprečitev tovrstne zlorabe je že omenjena ročna kontrola pravilnosti podatkov na računu, ki ga izvaja računovodstvo.

Nabava v proces potrjevanja storitvenih naročilnic in v nekaterih primerih nabave storitev ni vključena, razen v primeru eksplicitnega ročnega posredovanja uporabnika. Kljub nevključenosti nabave v proces potrjevanja storitvenih naročilnic je iz naročilnic, kreiranih v K-ju in posredovanih v L, razvidno, da sta na dokumentu podpisana nabavni referent in podpisnik. V resnici naročilnico v K-ju kreira le ena oseba, na podlagi podatka o nabavni skupini pripravljavca naročilnice pa se izpiše druga oseba (nabavnik ali podpisnik), ki je članica nabavne skupine. V več primerih sem ugotovil, da na naročilnici navedeni nabavnik ni ne kreiral naročilnice K ne sodeloval pri njeni potrditvi v L-ju.

Ko je račun likvidiran v L, se z ročnim sprožilcem prenese v K, kjer je račun parkiran, ni pa še knjižen. V tej fazi je mogoče na računu spremeniti datum računa, številko računa in rok za plačilo. Podatki se sicer popravljajo že ob vnosu računa v L, a se lahko napaka spregleda in ugotovi kasneje. Takšna fleksibilnost sistema predstavlja tveganje nepooblaščenega spreminjanja (skrajševanja ali podaljševanja) roka plačila po pregledu in likvidaciji računa.

4.6. Odprava pomanjkljivosti

Na podlagi revizijskih ugotovitev in priporočil je vodstvo podjetja potrdilo izvedbo naloge prenove procesov priprave storitvenih naročilnic in likvidature računov, ki se bodo uvedli v nov informacijski sistem. Z namenom sprotnega preverjanja, katerim tveganjem je proces izpostavljen in ali so v procesu opredeljene ustrezne kontrole, ki bi tveganja zmanjševale, sem bil kot svetovalec v nalogo vključen tudi sam.

5. ZAKLJUČEK

Kot izhaja iz ugotovitev revizije, le na podlagi pregleda uspešnosti zasnove in operativne učinkovitosti sistema upravljanja uporabniških pravic ni mogoče dati razumnih zagotovil o celovitem obvladovanju tveganj napak in zlorab, ki izvirajo iz neustreznega ločevanja dolžnosti v delovnem procesu, temveč je treba v ta namen presojati tudi skladnost uporabniških vlog z načelom ločevanja dolžnosti, še posebej pa procesne kontrole, ki lahko zaobidejo vse mehanizme, povezane z

upravljanjem uporabniških pravic. Pregled URMS-ja je nujen, ni pa zadosten pogoj za dajanje mnenja o obvladovanju navedenih tveganj.

Revizor se pri pregledu kontrolnega cilja A.6.1.2 Razmejitev dolžnosti pogosto sooča z določenimi omejitvami: (1) mnogo organizacij ne ločuje dolžnosti sistematično, (2) pričakovani obseg revizijskega posla ne dovoljuje podrobnejše analize opredeljenih vlog, hkrati pa (3) nimajo niti notranji niti revizorji IS-jev sami dovolj znanja, da bi celovito poznali vse tipične vloge v različnih delovnih procesih in konflikte, ki jih predstavljajo kombinacije posameznih vlog.

Nekateri ukrepi, s katerimi lahko revizor na revizijskem poslu obvlada tveganja, ki izvirajo iz teh omejitev, so lahko:

- izpostavitev omejitve dajanja zagotovil na izključno delovanje kontrol URMS v okviru ponudbe, revizijskega načrta in/ali revizijskega poročila;
- razširitev obsega revizijske naloge na vsaj enega od bolj kritičnih oz. tveganih procesov za organizacijo;
- aktivna vključitev notranjega revizorja v revizijski posel in njuno sorevidiranje sistema URMS, presoja vsebine uporabniških vlog, dodeljenih uporabnikom, z vidika ločevanja dolžnosti ter pregled procesnih kontrol s presojo medsebojnih vplivov vseh.

Na tak način bo revidiranec pridobil jasnejšo sliko o tem, kakšna zagotovila revizor informacijskih sistemov sploh daje, oz. natančnejšo sliko o preostalem tveganju napak in predvsem zlorab v delovnem procesu.

6. LITERATURA IN VIRI

1. Bellino et al. (2007). GTAG 8 – Auditing Application Controls. The Institute of Internal Auditors. Julij 2007.
2. Cybersecurity Insiders. 2018 Insider Threat Report. Najdeno 8. 7. 2018 na naslovu https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf.
3. Slovenski inštitut za standardizacijo. Slovenski standard SIST ISO/IEC 27001:2013. Januar 2014.
4. Wikipedia: Digital identity. Najdeno 8. 7. 2018 na naslovu https://en.wikipedia.org/wiki/Digital_identity.
5. Wikipedia: Division of labour. Najdeno 8. 7. 2018 na naslovu https://en.wikipedia.org/wiki/Division_of_labour.
6. Wikipedia: Separation of duties. Najdeno 8. 7. 2018 na naslovu https://en.wikipedia.org/wiki/Separation_of_duties.
7. Wikipedia: Two-man rule. Najdeno 8. 7. 2018 na naslovu https://en.wikipedia.org/wiki/Two-man_rule.

Boštjan Kežmah*

Pametne pogodbe

Smart Contracts

POVZETEK ● *Bistvo pametnih pogodb je njihova samodejna izvršitev, na katero ni mogoče vplivati, kar naj bi pogodbenim strankam zagotavljalo višjo stopnjo varnosti. Vendar se izkaže, da je kljub temu tehnično mogoče, da se pametna pogodba ne bo izvedla ali pa ne na dogovorjen način. Najpogosteje se danes pametne pogodbe uporabljajo za izdajo kovancev in so zaradi pomanjkljivega nadzora velikokrat povezane z goljufijami. To sicer ne pomeni, da nimajo uporabne vrednosti, vendar je smiselno pred njihovo uporabo pretehtati prednosti in slabosti njihove uporabe, predvsem pa njihovo vpeljavo obravnavati kot vsak drug tehnološki projekt, vključno z analizo povračila investicije.*

Ključne besede ● *pametne pogodbe, Ethereum, bitcoin, kriptovalute*

SUMMARY ● *The essence of smart contracts lies in their ability of automatic execution without external influence, which should provide a higher level of security for contracting parties. However, it turns out that it is technically possible that a smart contract will not be carried out in an agreed manner. Today, smart contracts are most commonly used to issue coins and are often associated with fraud due to lack of supervision. This does not mean that they do not have any useful value, though they call for consideration of advantages and disadvantages before their use, and above all, shall be treated as any other technological project, including the analysis of the return on investment.*

Key words ● *smart contracts, Ethereum, Bitcoin, cryptocurrencies*

JEL: M 42

1. UVOD

Pametno pogodbo je opredelil Nick Szabo kot pristop, s katerim bi lahko mnoge vrste pogodbenih določil vključili v programsko ali strojno opremo na takšen način, da bi imela kršitev pogodbe za kršitelja visoko ceno (kadar je to zaželeno celo nedosegljivo).[1]

* Dr. Boštjan Kežmah, aktivni PRIS, CISA, UM FERI, Smetanova ulica 17, 2000 Maribor, bostjan.kezmah@um.si.

Kot najširši pomen ideje si je Szabo predstavljal, da bi morale biti pogodbe "vključene v svet"[1] v smislu, da postanejo nedeljiv del naše predstave o svetu, kot npr. zakoni fizike. Pri tem bi morali biti mehanizmi sveta strukturirani na takšen način, da bi bile pogodbe:[1]

a) odporne proti preprostemu vandalizmu in
b) odporne proti naprednim, motiviranim kršitvam.

Pametna pogodba je poseben protokol, ki je namenjen prispevanju, preverjanju ali izvedbi pogajanj ali pogodbe. Pametne pogodbe omogočajo izvajanje kredibilnih transakcij brez sodelovanja tretjih strank. Te transakcije so sledljive in niso reverzibilne. Vsebujejo vse informacije glede pogodbenih pogojev ter samodejno izvedejo vse zastavljene aktivnosti.[2]

2. SVET PAMETNIH POGODB

Szabo je svet pametnih pogodb opredelil, ko še ni obstajalo primerno okolje, v katerem bi se lahko izvajale.

V trenutnem stanju tehnike se odražajo v obliki tehnologij, ki jih imenujemo tehnologija porazdeljene glavne knjige (angl. distributed ledger technology – DLT). Za te tehnologije je značilno, da so podatki in pravila odločanja razpršeni, ponovljeni ter usklajeni z množico vozlišč, ki si med seboj ne zaupajo in praviloma predstavljajo veliko število posameznikov, interesnih skupin ali institucij.

Prvi in najbolj razširjen svet pametnih pogodb je omrežje Bitcoin, ki ga je izumil Satoshi Nakamoto[3] [1] v letu 2008. Obljubljalo je predvsem zmanjšanje stroškov in pospešitev prenosov sredstev med računi (Bitcoin naslovi), s tem da bi iz poslovanja izvrševanja pogodb izločilo banke. Nakazila med naslovi so izjemno poenostavljen, primitiven primer pametne pogodbe, kjer uporabnik, ki želi nakazati sredstva, dokaže, da je lastnik naslova, zato mu omrežje dovoli, da na drugi naslov nakaže določeno število enot valute (bitcoin). Pri tem svet pametnih pogodb (omrežje Bitcoin) izvaja oziroma preverja pogodbena določila tako, da preverja, ali je na izvornem računu dovolj sredstev, da je zahtevano število enot valute mogoče pripisati drugemu naslovu, in hkrati preverja, da se ob prenosu sredstev ne bi ustvarile nove vrednosti valute, kar preprosto preveri tako, da mora biti za vsako transakcijo vsota "dvigov" sredstev enaka vsoti "pologov" sredstev. Če sta vsoti enaki, potem je svet pametnih pogodb prepričan oziroma je zagotovil, da s transakcijo ne bodo ustvarjena nova sredstva.

[1] Psevdonim, prave identitete avtorja ali avtorjev še vedno ne poznamo.

Nova sredstva lahko ustvarijo le rudarji, ki so z ustvarjenimi novimi sredstvi nagrajeni za svoje delo. Njihovo delo je preverjanje določil pogodbe, kar opravijo tako, da izvajajo algoritme, ki jih določa omrežje, s svojimi viri (računalniško opremo, električno energijo, internetno povezavo). Ob tem rešujejo tudi izjemno računsko zahtevno matematično uganko, katere namen je preprečiti vandalizem in motivirane kršitve, ki jih je predvidel Szabo. Ker vnaprej ni mogoče določiti, kateri rudar bo prvi rešil uganko, so s tem tudi manipulacije in vplivi na rudarje težje izvedljivi, kar daje omrežju nujno potrebno varnost za sodelovanje med vozlišči, ki si medsebojno ne zaupajo.

Način delovanja omrežja je izrazito asimetričen. Reševanje uganke je računsko izjemno zahtevno, medtem ko je preverjanje rešitve uganke preprosto. To omogoča vsem vozliščem, ki sestavljajo omrežje, da se lahko enostavno, brez velikega računskega vložka prepričajo, da je rudar res našel rešitev matematične uganke. Ob tem lahko vozlišča preverijo tudi ostale določbe pogodbe, predvsem, ali so res vse transakcije zastavljene tako, da z izvedbo transakcij ne bodo ustvarjene nove enote valute.

Zaradi narave problema (prenosa sredstev) imajo vozlišča na razpolago vse informacije, ki so potrebne za preverjanje skladnosti s pogodbo že znotraj vsake posamezne transakcije, zato ne potrebujejo nobenih dodatnih informacij zunaj omrežja.

Razpoložljivost informacij in enostavnost problema sta vodili k razvoju omrežja (Bitcoin), ki je specializirano izključno za prenos sredstev in zna zato izvajati samo eno vrsto pametne pogodbe.

3. PROBLEM ZAUPANJA ALI PROBLEM BIZANTINSKIH GENERALOV

Svet pametnih pogodb primarno rešuje problem zaupanja med strankami, med katerimi ni zaupanja in ga tudi ni mogoče vzpostaviti.

Tak primer so opisali že Lamport, Shostak in Pease kot problem bizantinskih generalov. V osnovi problem izhaja iz splošnega problema v računalništvu, zaradi katerega deli informacijskega sistema, ki nepravilno delujejo, sporočajo drugim delom informacijskega sistema napačne, lahko tudi nasprotujoče si podatke.

Problem so slikovito predstavili kot problem bizantinske vojske, ki oblega mesto. Okrog mesta so nastanjene vojaške enote in generali se morajo uskladiti glede vojaške taktike, pri tem pa komunikacijo zagotavljajo sli. Eden ali več generalov je

lahko izdajalcev, ki bodo poskušali vnesti zmedo med ostale. Cilj je poiskati algoritem, ki bo omogočal zvestim generalom, da dosežejo dogovor glede vojaške taktike. Izkaže se, da je pri uporabi ustnih sporočil problem rešljiv samo, če sta zvesti vsaj dve tretjini generalov, če pa bi uporabljali pisna sporočila, ki jih ni mogoče ponarediti, je problem rešljiv za katerokoli število generalov in izdajalcev.[4]

Verige blokov dosežejo skupni dogovor na podlagi tega spoznanja z decentralizacijo odločanja in javno porazdelitvijo glavne knjige.

4. VERIŽENJE BLOKOV

Veriga blokov je veriga med seboj kriptografsko povezanih in zaščitenih zapisov, ki jih imenujemo bloki. Praviloma vsak blok vsebuje kriptografsko zgostitev (prstni odtis, zgoščeno vrednost) prejšnjega bloka, časovno značko in podatke o transakcijah, ki sestavljajo blok.

4.1. Zgoščevalne funkcije

Bistveno vlogo v verigah blokov imajo zgoščevalne funkcije. To so enosmerne funkcije v obliki algoritmov, ki vhodne podatke preoblikujejo v izhodne na takšen način, da imajo izhodni podatki vedno enako dolžino. Lahko si jo predstavljamo tudi kot izjemno učinkovito funkcijo za stiskanje podatkov, ki podatke zgosti do te mere, da se pri tem izgubi toliko informacij, da iz izračunanega rezultata ne moremo več dobiti izvornih podatkov (zato jih tudi imenujemo enosmerne funkcije, saj je mogoče opraviti izračun le v eno smer).

Primer zgoščevalne funkcije, ki se uporablja le za kontrolo pravilnosti podatkov, je kontrolna cifra, ki je zadnja cifra davčne številke ali EMŠO, in kontrolni cifri na koncu številke transakcijskega računa. Vendar so te kontrolne cifre določene po izjemno enostavnih algoritmih, imajo pa tudi zelo majhno zalogo vrednosti – število kombinacij, ki jih lahko opišejo. Tako na primer pri EMŠU lahko z eno cifro opišemo le 10 različnih številk, pri nadaljnjih številkah EMŠA pa se začne kontrolna številka (zgostitev) ponavljati.

Za kriptografske zgoščevalne funkcije zato velja, da imajo dovolj veliko zalogo vrednosti, da je verjetnost, da bi imela dva podatka enako zgostitev, zanemarljivo majhna. Takemu prekrivanju vrednosti pravimo tudi kolizije. Ta lastnost je pomembna med drugim zato, ker imajo zgostitve bistveno vlogo pri elektronskem podpisovanju in ne želimo, da bi imeli dve pogodbi enak "prstni odtis" oziroma enako zgostitev, saj bi lahko katerakoli od pogodbenih strank trdila, da je

podpisala neko drugo pogodbo (ali podatek), ki ima enako zgostitev kot pogodba, ki je bila dejansko elektronsko podpisana.

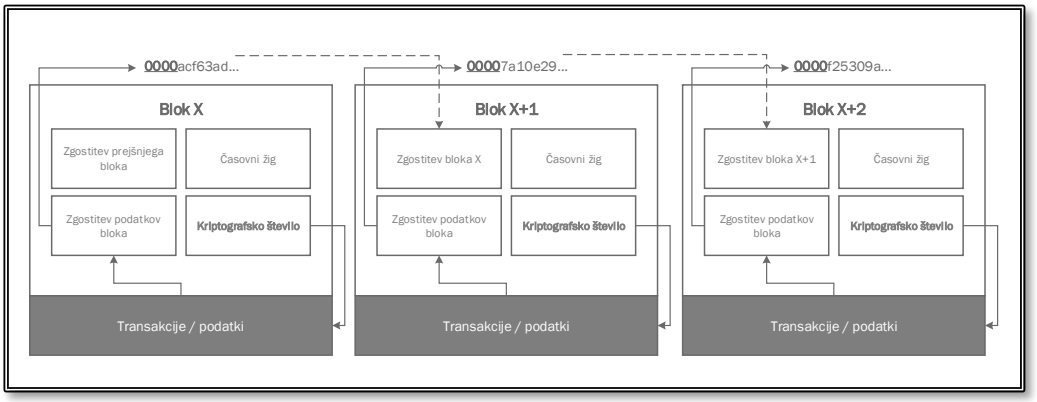
Druga kriptografska značilnost je nepredvidljivost zgoščevalne funkcije, ki pomeni, da že izjemno majhna sprememba vhodnih podatkov bistveno spremeni zgostitev. To je pomembno zato, da je matematično izjemno zahtevno poiskati kolizijo, saj je vpliv spremembe vhodnega podatka na zgostitev izjemno težko predvideti. Če to razložimo na primeru elektronsko podpisanih pogodb, je pomembno, da je za pogodbeno stranko, ki bi želela spremeniti pogodbo, postopek ponarejanja prezahteven, saj ne more s preprosto spremembo nekaj črk ali številk na enem mestu in odvzemom črk ali številk na drugem mestu sestaviti pogodbe, ki ima enako zgostitev kot pogodba, ki je bila elektronsko podpisana.

4.2. Matematična uganka ali dokaz opravljenega dela

V omrežju Bitcoin temelji matematična uganka na zgoščevalni funkciji[3]. Del vsakega bloka je enkratno kriptografsko število (angl. nonce). Idejno izvira iz načinov omejevanja neželene pošte[5] ter algoritma Hashcash[6]. Hashcash je sistem za dokazovanje opravljenega dela, ki ga v verigah blokov imenujemo rudarjenje.

Rudar izračuna zgoščeno vrednost bloka po pravilih za izračun zgostitve bloka, ki med drugim vsebuje tudi zgostitev transakcij, ki sestavljajo blok z uporabo Merklovega drevesa. Sestavni del podatkov, na podlagi katerih izračuna zgostitev, je tudi kriptografsko število. Rudar mora najti zgostitev, ki se začne z zaporedjem ničel. Kadar izračuna zgostitev bloka, praviloma izračunana vrednost ne ustreza temu pravilu. Zato rudar izbere naslednje kriptografsko število in ponovno izračuna zgostitev. Preveri, ali se zgostitev začne s predpisanim številom ničel. Če se ne, ponovno izbere kriptografsko število in izračuna zgoščeno vrednost ter to ponavlja tako dolgo, dokler ne najde kriptografskega števila, ki da zgoščeno vrednost v zahtevani obliki. Ko je našel ustrezno kriptografsko število, je rešil matematično uganko in s tem potrdil blok. Matematične bližnjice pri tem ne poznamo. Zaradi enosmernega delovanja zgoščevalnih funkcij ne more preprosto izračunati kriptografskega števila neposredno iz zgoščene vrednosti in mora uporabiti metodo "grobe sile", kar pomeni, da preizkuša kombinacije druga za drugo, dokler ne najde prave.

Slika 1: Medsebojna povezanost blokov v verigi blokov



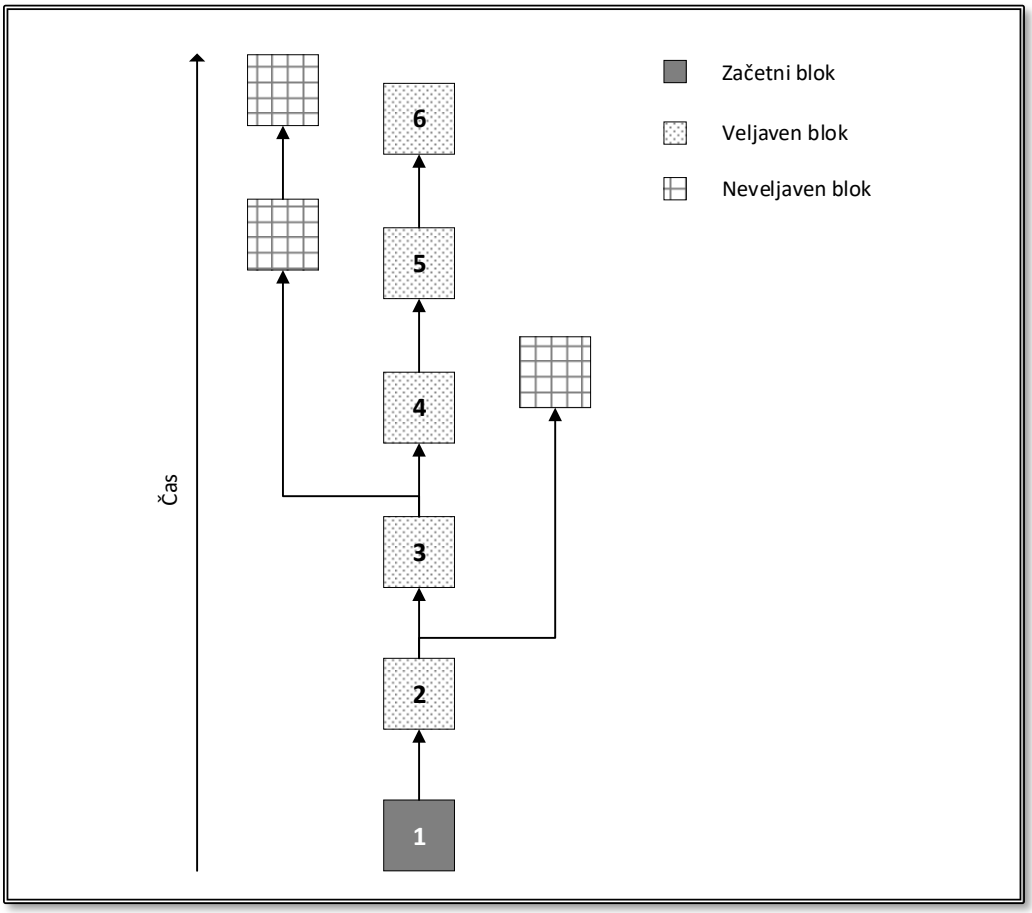
Odvisno od tega, kako zmogljivo je omrežje, torej odvisno od tega, koliko vozlišč ga sestavlja in kakšne računske kapacitete dosegajo ta vozlišča, se sčasoma spreminja hitrost reševanja matematične uganke. Omrežje doseže stabilnost potrjevanja blokov in s tem varnost delovanja omrežja tako, da spreminja zahtevnost matematične uganke s sprotnim prilagajanjem števila vodilnih ničel v zgoščeni vrednosti. Več ko je vodilnih ničel zgoščene vrednosti, težja je matematična uganka. Tako lahko omrežje dinamično prilagaja zahtevnost rudarjenja. Zahtevnost reševanja uganke se eksponentno povečuje s številom zahtevanih vodilnih ničel.

4.3. Dolžina verige

Uradna veriga je tista, ki je najdaljša. To preprečuje vozliščem, da bi s spremembo in potrjevanjem posameznega bloka lahko spremenila že potrjene bloke. Ker je potrjevanje posameznega bloka računsko zahtevno, bodo v času, ko bi potrjevali ponarejeni blok, v omrežju potrjeni že novi bloki, ki bodo skupaj sestavljali daljšo verigo. Ker bodo vozlišča v omrežju nadaljevala vzdrževanje in potrjevanje najdaljše verige, je potrjevanje ali ponarejanje starih blokov brezpredmetno, saj krajših verig omrežje ne bo uporabljalo kot trenutno veljavne verige blokov, s tem pa tudi ne ponarejenih blokov, ki so v krajši verigi.

Ponarejanje bi bilo mogoče samo v primeru, če bi ponarejevalec obvladoval več kot polovico računske moči celotnega omrežja, saj bi v tem primeru lahko potrjeval bloke hitreje kot preostali del omrežja, kar pa bi moralo biti v praksi dovolj velikega, porazdeljenega omrežja, nemogoče. Tako v praksi najdaljša veriga vključuje največ opravljenega (računskega) dela in ker večino omrežja obvladujejo poštena vozlišča, je najdaljša veriga tudi poštena.[3]

Slika 2: Veljavna je le najdaljša veriga blokov



Pri tem se je treba zavedati, da algoritem kot bistveni element varnosti uporablja verjetnost. Stopnja varnosti se zato povečuje, kadar se povečuje število rudarjev, in zmanjšuje pri njihovem upadanju.

Ta značilnost lahko predstavlja pomembno omejitev pri dolgoročnem delovanju verig blokov, saj to pomeni, da bi morali uporabniki verige blokov, še posebej tisti, ki imajo v njej shranjene pomembne informacije, poskrbeti za dolgoročno privlačnost takšne verige. Z zmanjševanjem privlačnosti se bo pričakovano zmanjševalo število rudarjev, s tem pa varnost informacij. Ker rudarje v trenutnih modelih najbolj privlači zaslužek, bodo morali dolgoročni uporabniki verig blokov skrbeti za ustrezne inovacije v poslovnih modelih, ki bodo rudarjem omogočale nadaljnje dobičke.

5. PAMETNE POGODBE

Bitcoin predstavlja le najpreprostejšo možnost izvajanj pametnih pogodb. Te pridobivajo uporabnost z naraščanjem števila funkcionalnosti, ki jih podpirajo. V omrežju Bitcoin je ta funkcionalnost omejena na preprečevanje nedovoljenega oziroma nenadzorovanega ustvarjanja novih kovancev v omrežju.

Sčasoma sta vzniknili dve različni šoli: Satoshijeva šola zagovarja omejevanje števila funkcionalnosti pametne pogodbe (omejevanje funkcionalnosti ukazov), medtem ko šola Vitalika Buterina poudarja prednosti uporabe verige blokov kot računalniške platforme, ki lahko izvaja dobro opredeljene funkcije s pomočjo pogodb in parametrov[7].

Na podlagi idej šole Vitalika Buterina se je razvilo omrežje Ethereum. Omrežje Ethereum predstavlja Ethereum navidezni stroj (angl. Ethereum Virtual machine), ki v porazdeljenem omrežju izvaja ukaze, ki predstavljajo pametno pogodbo.

Zaradi značilnosti verige blokov je pogodba, ko je enkrat objavljena v omrežju, nespremenljiva in nihče od uporabnikov ne more vplivati niti na njeno vsebino niti na njeno delovanje.

Pogodbe v programskem omrežju Ethereum praviloma nastanejo s pomočjo programskega jezika Solidity.

Primer pogodbe, ki razdeli "dobiček" med določeno število lastnikov, prikazuje slika 3. Evidentno se pisanje pametnih pogodb bistveno razlikuje od pisanja običajnih pogodb, kot jih poznamo danes, in zahteva sodelovanje razvijalcev.

Slika 3: Primer izvorne kode pametne pogodbe v programskem jeziku Solidity

```
pragma solidity ^0.4.16;

contract DelitevDobicka {
    address private pobudnik;
    mapping(uint => address) private lastniki;
    uint public steviloLastnikov;

    event Razdeli(uint _amount, uint _steviloLastnikov);

    function DelitevDobicka(address[] naslovi) public {
        pobudnik = msg.sender;
        steviloLastnikov = naslovi.length;
        for (uint i=0; i< naslovi.length; i++) {
            lastniki[i] = naslovi[i];
        }
    }

    function deliDobicek() public payable returns (bool uspeh) {
        uint znesek = msg.value / steviloLastnikov;
        for (uint i=0; i<steviloLastnikov; i++) {
            if (!lastniki[i].send(znesek)) revert();
        }
        Razdeli(msg.value, steviloLastnikov);
        return true;
    }

    function kill() private {
        if (msg.sender == pobudnik) selfdestruct(pobudnik);
    }
}
```

Najpogostejši primeri praktične uporabe pametnih pogodb danes predstavljajo začetne ponudbe kovancev (angl. Initial Coin Offering – ICO).

ICO predstavljajo odgovor na zapletene postopke zbiranja kapitala za podjetniške podvige. Izdajanje vrednostnih papirjev nadzirajo zakonodajalci po vsem svetu in pri tem ICO predstavljajo sivo področje "vrednostnih papirjev", saj spretni izdajatelji kovancev izdajo svojega kovanca organizirajo tako, da ne bi imela značilnosti vrednostnega papirja.

Pomanjkanje nadzora nad izdajo kovancev se odraža v obliki množice novih Ponzijevih shem in drugih oblik goljufij, pri katerih izdajatelji po tem, ko zberejo sredstva, preprosto izginejo[8].

Poleg Ponzijevih shem so goljufije povezane tudi z manipulacijo trga oziroma vrednosti kovancev. Na podlagi analize, ki jo je izvedel Wall Street Journal, so goljufi samo na najbolj znanih menjalnicah kriptovalut od januarja do konca julija 2018 ustvarili trgovalne aktivnosti v vrednosti več kot 825 milijonov USD po shemi "pump-and-dump", kar je povzročilo vlagateljem na "napačni" strani več sto milijonov dolarjev izgub[9].

Posledično se zanimanje javnosti za kriptovalute zmanjšuje. Tržna kapitalizacija kriptovalut se je od januarja do avgusta 2018 zmanjšala z 835 milijard dolarjev na 193 milijard dolarjev[10], do septembra 2018 pa še dodatno na le 112 milijard dolarjev[11].

Zmanjšano zanimanje se odraža tudi na manjšem povpraševanju po strojni opremi za rudarjenje kriptovalut. Proizvajalec grafičnih kartic Nvidia je v letu 2018 pričakoval zmanjšanje povpraševanja na 100 milijonov dolarjev, dejanski prihodek pa je obsegal le 18 milijonov dolarjev[12].

Glede na poročila, ki jih objavlja Bloomberg, 90 % projektov, povezanih z verigami blokov, ne bo povezanih s končnimi izdelki in storitvami, Gartnerjev analitik Rajesh Kandaswamy pa izpostavlja, da še nikoli ni bilo takšne razlike med navdušenjem in dejansko uporabo tehnologije[13].

Dosedanje zlorabe pa ne preprečujejo legitimne uporabe, kadar je v uporabo verige blokov vključen ustrezen nadzor. Primer je izdaja obveznic s pomočjo tehnologije verige blokov, ki jo je Svetovna banka odobrila banki Commonwealth Bank of Australia. Vendar se v tem primeru izdaja nanaša z vidika pravne zaščite na "klasične" obveznice, le tehnologija, ki omogoča izmenjavo podatkov o trenutnih lastnikih obveznic, temelji na verigi blokov.

Pametna pogodba je torej še vedno le tako poštena, kot so pošteni nameni avtorja pogodbe. Celotnega problema zaupanja v omrežje trenutno še ne znamo rešiti samo z uporabo verige blokov. Ko enkrat pogodbene stranke poženejo pogodbo, je ni več mogoče niti spremeniti niti ustaviti na zahtevo, ne glede na kasneje odkrite spremenjene okoliščine ali druge vzroke, ki bi v običajnem poslovanju vodili k prekinitvi ali spremembi pogodbe.

5.1. Praktična uporaba pametnih pogodb

Glasniki tehnologije verig blokov in pametnih pogodb predstavljajo najrazličnejše scenarije, v katerih so pametne pogodbe boljše od obstoječih "klasičnih" pogodb.

Primer je pametna pogodba z zavarovalnico. Zavarovanec plača zavarovalno premijo in s tem postane stranka v sklopu pametne pogodbe. Ko nastopi

zavarovalni primer, pametna pogodba zavarovancu samodejno izplača škodo. Pri tem zavarovalnica nima nobenega vpliva na izvajanje pametne pogodbe. Zavarovanec si lahko izvorno kodo (torej pravila) pogodbe sam ogleda v omrežju verig blokov, preden k taki pogodbi pristopi. Torej je bil natančno informiran o pogojih in načinu izvajanja pogodbe, preden jo je sklenil, in je lahko prepričan, da se po sklenitvi pogodbe njena funkcionalnost ne bo spremenila.

Ena pomembnejših omejitev pametne pogodbe je vir podatkov, ki potrdi, da je nastala škoda. Ker si zavarovalnica in zavarovanec ne zaupata, bosta imenovala tretjo, neodvisno osebo, da potrdi oziroma ugotovi, da je nastal škodni dogodek. Pri klasičnih pogodbah je sodišče zaupanja vredna tretja oseba, ki sprejme dokončno odločitev. Če želimo reševanje sporov pri pametnih pogodbah poenostaviti oziroma se jim izogniti, določimo tretjo osebo, ki sporoči samo en podatek in ne proučuje celotne pogodbe. Takemu viru pravimo "orakelj". Primer bi bil neodvisni strokovnjak, ki spremlja vreme in ugotovi količino padavin na določenem območju, kjer ima zavarovanec nepremičnino. Ob dovolj veliki količini padavin, ki je določena že v pametni pogodbi, ta samodejno izplača škodo. Ob tem se postavlja vprašanje, zakaj ne bi zavarovalnica in zavarovanec takšnega "oraklja" določila že danes, saj ju pri tem nič ne ovira. Če bi bila torej to želja zavarovalnic in zavarovancev, bi lahko enak učinek dosegli tudi brez uporabe pametnih pogodb.

Podoben primer je plačilo najemnine. Pametna pogodba spremlja plačila najemnine, in če najemnik najemnine ne plača, izvede samodejno "izvršbo" tako, da zaklene električno ključavnico stanovanja do plačila zaostalih najemnin. Vprašanje je, kako v teh primerih poskrbimo za varnost ljudi. Ker pametna pogodba meri le čas zamude pri plačilu, lahko najemnika kar zaklene v stanovanje (in nato slučajno izbruhne požar) ali pa najemnika zaklene iz stanovanja (ta pa je pred tem majhnega otroka za trenutek samega pustil v stanovanju).

Za celovito, samodejno delovanje pametnih pogodb potrebujemo dovolj senzorjev, ki pametne pogodbe oskrbujejo s podatki. Z vsakim dodanim senzorjem pa je v pogodbi več odločitev, z večanjem števila odločitev v programski opremi pa se povečuje možnost napak. Ko se povečuje možnost napak, se povečuje interes posameznikov, da imajo neko obliko varstva za primere, ki niso bili predvideni, ali za primere, ko pametna pogodba ne deluje skladno s pričakovanji. Pri klasičnem poslovanju takšno varstvo zagotavljajo predpisi in sodišča.

Zmogljivost pametnih pogodb bo odvisna od vzpona interneta stvari (angl. Internet of Things – IoT), saj le v svetu interneta stvari lahko pametne pogodbe dobijo dovolj podatkov, da lahko zaščitijo vse pogodbene stranke. Primer je

prodaja rabljenega avtomobila. Veliko podatkov je potrebnih, da je lahko kupec prepričan, v kakšnem stanju je rabljeni avtomobil prodajalca (ali je bil poškodovan, kako in kdaj je bil servisiran, kakšne okvare so bile odpravljene ipd.).

5.2. Izzivi pametnih pogodb

V praksi se izkaže, da ima tudi nespremenljivost verige blokov svojo mejo. Razen manj verjetne možnosti, da bi napadalec obvladoval več kot polovico računskih kapacitet omrežja, obstaja tudi možnost, da uporabniki z glasovanjem zavestno spremenijo podatke v blokih.

Primer je zloraba pametne pogodbe v sklopu projekta Decentralized Autonomous Organization, ki je bila posledica napake v programski kodi pametne pogodbe. V maju 2016 so se zato uporabniki (celotnega) omrežja Ethereum z glasovanjem odločili, da spremenijo način delovanja omrežja in hkrati "izbrišejo" krajo kovancev[8]. Takšen poseg se imenuje trdi razcep (angl. hard fork).

V primeru individualnih zapletov manjše vrednosti je malo verjetno, da bodo pripravljeni vsi uporabniki omrežja lokalno težavo reševati z glasovanjem za trdi razcep. Pogodbene stranke bodo zato morale iskati druge varnostne mehanizme, ob tem pa še razrešiti vprašanje, kdo je odgovoren za vsebino pogodbe – odvetnik, ki jo je sestavil v obliki besedila, ali razvijalec, ki je to besedilo prepisal v programsko kodo pametne pogodbe. Morda pa kar pogodbene stranke, saj so imele možnost same prebrati pogodbo pred njenim podpisom.

Ker mora izvajanje pogodbe nekdo plačati, se v ta namen v omrežju Ethereum uporablja gorivo. Ob zagonu pogodbe določimo tudi največjo količino goriva, ki ga lahko pogodba porabi, in če tega zmanjka, potem se izvajanje pogodbe ustavi, podatki pa se vrnejo v začetno stanje. Te "določbe" v pogodbi oziroma takšnega načina njenega obnašanja ni mogoče preprečiti, ker to omejitev vsiljuje omrežje. Pogodbene stranke kljub vsem varovalom ne morejo biti prepričane, da se bo pogodba v celoti dejansko tudi izvedla.

Z izzivi se srečujejo tudi zakonodajalci, saj s prehodom v kriptosvet, ki temelji na pametnih pogodbah, izgubljajo nadzor nad posli, ki jih sklepajo uporabniki omrežja. Ker so pogodbe nespremenljive, se represivni organi ne morejo vključiti v izvajanje posamezne pametne pogodbe, prav tako pa zaradi izrazite porazdeljenosti ne morejo preprečiti obstoja omrežja, v katerem se izvajajo pametne pogodbe.

6. SKLEP

Pametne pogodbe predstavljajo zanimivo orodje, ki omogoča, da se pogodbene stranke popolnoma arbitrarno odločijo o njihovi vsebini.

Pred njihovo uporabo je smiselno proučiti omejitve in pasti, ki izhajajo iz načina njihovega delovanja. Razen omejitev, ki jih vsiljujeta tehnologija in omrežje, kot je možnost napak v programski kodi pametne pogodbe ali celo programski kodi omrežja, v katerem se izvaja, omejitev pri zagotavljanju, da se bo pogodba tudi dejansko izvedla v celoti, omejitev pri zagotavljanju nespremenljivosti podatkov v omrežju, varnosti, ki temelji na verjetnosti ter problemih vzpostavitve "orakljev", zaradi katerih smotrnost uporabe pametne pogodbe postane vprašljiva, se pogodbene stranke srečujejo tudi z vprašanjem pravne varnosti.

Z uporabo pametne pogodbe se pogodbene stranke odpovedujejo pravnemu varstvu. Danes je sicer še mogoče izvršiti sodno odločbo na podlagi sodbe sodišča, z morebitnim celovitim prehodom v kriptosvet pa so možnosti vse manjše. Če bi vse premoženje uporabnikov omrežja obstajalo le v omrežju, izvršba ne bi bila več izvedljiva, saj tretja stranka, ne da bi dosegla trdi razcep, ne more vplivati na delovanje omrežja, s tem pa bi se postavilo tudi vprašanje smiselnosti sodišč, posledično predpisov, kar bi lahko vodilo do povsem novih oblik družbene ureditve.

Poleg vpliva na pravno varstvo imajo pametne pogodbe tudi globalni ekološki vpliv. Po poročilih Arvinda Narayanana iz Princetona za Odbor ameriškega senata za energijo in naravne vire verige blokov porabijo nekaj manj kot 1 odstotek vse električne energije na planetu, kar je primerljivo s porabo zveznih držav Ohio in New York skupaj. Da bi bili lahko izračuni res tako visoki, posredno potrjujejo tudi odločitve nekaterih podjetij, da gradijo lastno energetsko infrastrukturo za potrebe rudarjenja, saj se s tem izognejo stroškom omrežnine. Primer je Kanadska družba DMG Blockchain, ki širitev svojih rudarskih operacij v Britanski Kolumbiji gradi kar na postavitvi lastne transformatorske postaje[13].

Pred uporabo verig blokov in pametnih pogodb je zato treba skrbno proučiti prednosti in slabosti spremenjenega načina sklepanja in izvajanja pogodb. Predvsem pa se ne mudi. Z zlomom prenapihnjenega trga kriptovalut je odveč strah, da bomo zamudili enkratno priložnost zaslužka. Sedaj je to samo še ena od tehnologij, ki mora kot vsak drug projekt pokazati realne možnosti, da se bo vložek vanj povrnil.

7. LITERATURA IN VIRI

[1] Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY J. Transhumanist Thought, 1996 (16)*.

[2] Tar, A. (2017). Smart Contracts, Explained. *Cointelegraph*, 2017. [Online]. Najdeno 29. 4. 2018 na naslovu https://cointelegraph.com/explained/smart-contracts-explained.

[3] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[4] Lamport, L., Shostak, R., and Pease M. (1982). The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.*, 1982, (4) 3, str. 382–401.

[5] Dwork Cynthia N. M. (1992). Pricing via Processing or Combatting Junk Mail – Abstract Online]. Najdeno 29. 4. 2018 na naslovu http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp_abs.html.

[6] Back, A. (1997). A partial hash collision based postage scheme". [Online]. Najdeno 29. 4. 2018 na naslovu http://www.hashcash.org/papers/announce.txt.

[7] V. (Research fellow) Dhillon, D. (David S. Metcalf, and M. CEO of M. T. Hooper, *Blockchain enabled applications : understand the blockchain ecosystem and how to make it work for you*.

[8] Zongo, P. (2018). "The Promises and Jeopardies of Blockchain Technology," *ISACA J.*, 2018, 4, str. 28–35.

[9] Some Traders Are Talking Up Cryptocurrencies, Then Dumping Them, Costing Other Millions. (2018). *The Wall Street Journal, Europe Edition*, 2018.

[10] Bitcoin Sinks Below $6,000 as Almost Everything Crypto Tumbles – Slashdot.(2028). [Online]. Najdeno 8. 9. 2018 na naslovu https://news.slashdot.org/story/18/08/14/1353231/bitcoin-sinks-below-6000-as-almost-everything-crypto-tumbles.

[11] Cryptocurrency Market Capitalizations | CoinMarketCap. (2018). [Online]. Najdeno 8. 9. 2018 na naslovu https://coinmarketcap.com/.

[12] Lilly, P. (2018). Nvidia's outlook on cryptocurrency GPU sales is great news for gamers | PC Gamer. (2018). [Online]. Najdeno 8. 9. 2018 na naslovu https://www.pcgamer.com/nvidias-outlook-on-cryptocurrency-gpu-sales-is-great-news-for-gamers/.

[13] Corporate America Cools On Blockchain. Gartner Sees 'Disconnect Between Hype and Reality' – Slashdot. (2018). [Online]. Najdeno 8. 9. 2018 na naslovu https://it.slashdot.org/story/18/08/04/1824238/corporate-america-cools-on-blockchain-gartner-sees-disconnect-between-hype-and-reality.

Dr. Matej Kovačič*

Varnost mobilnih komunikacij

Mobile communications security

POVZETEK ● *V prispevku so predstavljeni glavni pristopi pri varovanju mobilnih komunikacij ter nekaj varnostnih izzivov, ki jih prinašajo različni možni napadi na mobilno telefonijo. Varnost mobilnih komunikacij se danes osredotoča zlasti na preprečevanje nepooblaščenega oddaljenega dostopa do podatkov, nepooblaščenega dostopa do podatkov v primeru fizičnega dostopa do mobilnega telefona ter nepooblaščenega dostopa do vsebine komunikacij in prometnih podatkov. V članku so predstavljene obstoječe varnostne rešitve in njihove omejitve. Pri tem ugotavljamo, da zagotavljanje varnosti mobilnih komunikacij ni enostavno opravilo, saj določene varnostne težave izvirajo iz same zasnove mobilnih oz. celo telefonskih omrežij v preteklosti. Odpravljanje različnih ranljivosti bo zato še dolgotrajno.*

Ključne besede ● *mobilna telefonija, informacijska varnost*

SUMMARY ● *The paper presents the main approaches for protecting mobile communications and some of the security challenges brought by various possible attacks on mobile telephony. The security of mobile communications is today focusing mainly on preventing unauthorized remote access to the device, unauthorized physical access to data, and unauthorized access to the content of communications and traffic data. The article provides an overview of existing security solutions and their limitations. We conclude that ensuring the security of mobile communications is not an easy task, since certain security problems originate from the concept of mobile telephony and/or telephony technology in the past. The elimination of various vulnerabilities will therefore be a long lasting task.*

Key words ● *mobile telephony, information security*

JEL: L 86

1. UVOD

Zgodovina šifriranja govornih komunikacij sega v obdobje 2. svetovne vojne. Prve šifrirne naprave za govorno komunikacijo so bile velike in okorne; ameriška vojska je na primer za šifriranje uporabljala napravo SIGSALY, ki je tehtala 55 ton in je napolnila srednje veliko sobo. Razvoj tehnologije je sicer prinesel tudi zmanjšanje

* Matej Kovačič, strokovni svetnik z doktoratom, Inštitut Jožef Stefan, matej.kovacic@ijs.si.

tovrstnih naprav, najpomembnejši pospešek šifriranju govornih komunikacij pa je v 90. letih prinesla digitalna tehnologija.

Ena prvih širše dostopnih aplikacij, ki je omogočala šifriranje pogovorov preko navadne telefonske (modemske) povezave ali preko interneta, je bila aplikacija PGPfone[1], ki jo je leta 1995 razvil Philip Zimmermann. Vsak izmed dveh uporabnikov je potreboval računalnik z modemom ali dostopom do interneta. S pomočjo modema ali preko interneta sta se nato uporabnika povezala drug z drugim, obe aplikaciji pa sta si nato izmenjali šifrirne ključe in preko povezave začeli prenašati digitaliziran in šifriran pogovor.

Kljub temu da je bila uporaba takšne naprave (računalnik z modemom in slušalkami) razmeroma nepraktična (ne pozabimo, da so bili tedanji računalniki precej večji in težji od današnjih), pa je napredek tehnologije od druge svetovne vojne v tem primeru lepo viden. Razvoj je šel dalje in s pojavom pametnih telefonov je šifriranje govornih komunikacij postalo še enostavnejše. Kljub temu pa varnost sodobnih mobilnih komunikacij prinaša nekaj dodatnih posebnosti. Nekatere izmed njih si bomo ogledali v nadaljevanju.

2. SODOBNI NAČINI VAROVANJA MOBILNIH KOMUNIKACIJ

Varnost mobilnih komunikacij se danes osredotoča zlasti na tri področja, katerih namen je preprečiti nepooblaščen oddaljen dostop do podatkov, nepooblaščen dostop do podatkov v primeru fizičnega dostopa do mobilnega telefona ter nepooblaščen dostop do vsebine komunikacij in prometnih podatkov.

Ključna rešitev za preprečevanje nepooblaščenega oddaljenega dostopa je uporaba t. i. okrepljenega operacijskega sistema. Običajno gre za varnostno okrepljen klon mobilnega operacijskega sistema Android, torej za operacijski sistem, ki temelji na operacijskem sistemu Android, razvijalci pa so vanj dodatno vgradili različne varnostne tehnologije ter iz njega odstranili Googlovo specifično programsko kodo, predvsem tisto, ki omogoča posredovanje različnih podatkov v Googlov podatkovni oblak. Taki operacijski sistemi so na primer Replicant, Blackphone's PrivatOS, Guardian ROM, Lineage (bivši CyanogenMod) itd., ki jih je mogoče namestiti na točno določene modele mobilnih telefonov.

V primeru varnostno okrepljenega operacijskega sistema pravzaprav ne govorimo samo o golem operacijskem sistemu, temveč o celotni distribuciji operacijskega

[1] PGPfone, najdeno na naslovu https://en.wikipedia.org/wiki/PGPfone.

sistema, v katero so že privzeto vključene (in pogosto tudi prednastavljene) različne aplikacije za zaščito zasebnosti, zlasti npr. požarni zid, podpora za šifriranje SMS-ov, VPN-odjemalec itd.

Naslednje pomembno področje je preprečevanje nepooblaščenega dostopa do podatkov, kadar ima t. i. napadalec mobilni telefon v fizični posesti. V osnovi gre pri tem za šifriranje notranjega pomnilnika, s čimer preprečimo, da bi napadalec brez gesla ali PIN-kode lahko dostopal do vsebin na telefonu oziroma mobilni telefon sploh zagnal, če je ugasnjen. Sodobni telefoni imajo šifriranje notranjega pomnilnika že privzeto vključeno, dodatna zaščita pa omogoča tudi zaklep zaslona, tako da napadalec ne more do podatkov, tudi če je telefon že zagnan, a zaklenjen.

Za odklepanje telefona se lahko uporabljajo geslo, PIN-koda ali t. i. "biometrična gesla" (npr. prstni odtis). Zadnje lahko predstavlja težavo, saj biometričnih parametrov ni mogoče zamenjati oziroma preklicati tako kot npr. geslo. Poleg tega so znani tudi primeri ponarejanja biometričnih parametrov z razmeroma preprosto tehnologijo (npr. ponarejanje prstnih odtisov)[2]. Pomembno je namreč, da identiteta ("Kdo si?") in avtentikacija ("Kako lahko to dokažeš?") uporabnika ostaneta ločeni, kar pa pri uporabi biometričnih identifikatorjev ne velja.

Pri uporabi PIN-kode ali gesla pa je težava v tem, da je dolžina teh dveh elementov v običajnih mobilnih telefonih načeloma omejena (npr. v operacijskem sistemu Android na največ 16 znakov). To je sicer razumljivo, saj si ljudje težko zapomnimo daljša gesla, a za računalniško podprte napade z grobo silo 16-mestna gesla nikakor ne nudijo ustrezne zaščite[3]. Po nekaterih ocenah bi morala biti gesla v angleškem jeziku glede na entropijo angleškega jezika v letu 2012 dolga med 32 in 54 znakov, za slovenska gesla pa je bila glede na entropijo slovenskega jezika ocena dolžine vsaj 30 znakov (Kovačič, 2012). Operacijski sistemi na mobilnih telefonih imajo zato vgrajene določene protiukrepe, s katerimi skušajo preprečiti t. i. napad z grobo silo (angl. brute force attack). Po nekaj neuspešnih poskusih odklepanja telefona namreč začnejo povečevati časovni razmik med dvema zaporednima vnosoma gesla oziroma blokirajo mobilni telefon ali celo popolnoma izbrišejo podatke na njem. Zaradi tega tudi celo sorazmerno kratko geslo (na

[2] Na tem področju so bili precej aktivni varnostni raziskovalci nemškega Computer Chaos Cluba. Tako so recimo leta 2013 uspeli zaobiti biometrično zaščito Applovega TouchID (https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid), leta 2014 so na primeru nemške obrambne ministrice pokazali, kako je mogoče zgolj iz fotografije rok pridobiti podatke o prstnih odtisih te osebe (https://www.ccc.de/en/updates/2014/ursel), leta 2017 so prikazali, kako je mogoče zaobiti biometrični identifikacijski sistem identifikacije očesne šarenice na telefonu Samsung Galaxy S8 (https://www.ccc.de/en/updates/2017/iriden), itd. ...

[3] Spletišče https://www.grc.com/haystack.htm.

primer do nekaj znakov) ponuja ustrezno zaščito, saj sistem onemogoča hitro ugibanje gesel v nedogled.

Z opisanim mehanizmom tako razmeroma dobro rešujemo problem napada z grobo silo na mehanizem za odklepanje telefona, žal pa ne tudi napada z grobo silo v primeru, ko napadalec skuša zagnati ugasnjen mobilni telefon oziroma priključiti in dešifrirati notranji pomnilnik. Običajni operacijski sistemi Android namreč uporabljajo isto geslo za zaklepanje zaslona in šifriranje notranjega pomnilnika.

Če napadalec, ki ima fizični dostop do naprave, uspe narediti kopijo (šifriranega) pomnilnika na svoj sistem, lahko s pomočjo metode grobe sile v nedogled preizkuša vsa možna gesla, ne da bi ga skrbela omejitev hitrosti preskušanja ali zaklepanje naprave. Če pri tem uporabi ustrezno hiter računalnik ali grafične kartice, lahko zaščito razbije v urah ali zgolj minutah (Schneier, 2013). Nekateri varnostno okrepljeni operacijski sistemi zato omogočajo uporabo ločenega gesla za odklepanje telefona in ločenega gesla za dešifriranje notranjega pomnilnika.

Zadnja v nizu tehnologij za zaščito mobilnih komunikacij pa so tehnologije, katerih namen je preprečiti nepooblaščen dostop do vsebine komunikacij in v nekaterih primerih tudi podatkov o prometu. Tipično gre za uporabo namenskih aplikacij, ki omogočajo šifriran prenos sporočil in govornih komunikacij, pri čemer gre za uporabo šifriranja od začetne do končne točke (t. i. end-to-end encryption).

Pri tem prenos sporočil in govora praviloma poteka preko podatkovnega prenosa, čeprav je na trgu mogoče najti tudi rešitve, ki omogočajo šifriranje govornih komunikacij od začetne do končne točke preko 2G-omrežja (npr. GSMK Cryptophone). Nekatere programske rešitve omogočajo tudi anonimizacijo (ali vsaj psevdoanonimizacijo), s čimer skrijejo podatke o prometu (kdo je klical koga in kdaj) pred mobilnim operaterjem (res pa je, da te podatke lahko vedno vidijo operaterji namenskih strežnikov, preko katerih potekajo tovrstne komunikacije).

Seveda zgolj uporaba šifriranja ni dovolj, pač pa je treba biti pozoren tudi pri sami implementaciji šifrirnih tehnologij. Pri tem nimamo v mislih zgolj uporabe ustreznih algoritmov in dovolj dolgih šifrirnih ključev, niti uporabe sodobnih šifrirnih mehanizmov, kot je na primer poudarjena zaupnost (angl. perfect forward secrecy; Helme, 2014). Pri implementaciji šifriranja so pomembne tudi na videz nerelevantne malenkosti, kot na primer izbira ustreznih kodekov za kompresijo zvoka pri govorni komunikaciji. Izbira neustreznih kodekov namreč lahko predstavlja varnostno tveganje, saj nekatere vrste kodekov, t. i. VBR-kodeki (angl. variable bit-rate), ki različno kompresirajo različne tipe zvokov, omogočajo uspešen napad na sicer šifrirane podatke. Raziskovalci iz Johns Hopkins University so leta 2008 ugotovili, da je pri uporabi VBR-kodekov mogoče z analizo sicer

šifriranih podatkov z visoko zanesljivostjo prepoznati dele besed ali celotne besede v pogovoru (Wright, Ballard, Coull, Monrose in Masson, 2008). Raziskave so pokazale, da je ob uporabi neustreznega kodeka na tak način mogoče v povprečju prepoznati 50 % besed v pogovoru, za nekatere besede pa je verjetnost prepoznave kar 90 %, kar velja ne glede na uporabljeni šifrirni algoritem (Kovačič, 2013).

3. OMEJITVE PRI VAROVANJU MOBILNIH KOMUNIKACIJ

Kljub temu da se zdi pravilna uporaba zgoraj navedenih pristopov na prvi pogled zadostna, pa to v resnici ne rešuje problema zasebnosti v celoti. Problem zasebnosti in varnosti je še vedno tukaj, le premaknil se je globlje pod površino. Dejstvo je, da mobilna telefonija v osnovi ni zasnovana tako, da bi bila lahko resnično varna, saj ima že v sami zasnovi nekaj resnih pomanjkljivosti.

Zgodovinsko gledano je bila namreč tehnologija mobilne telefonije zasnovana tako, da je bila vsa logika na strani omrežja, mobilne naprave pa so bile obravnavane le kot "neumni odjemalci". Tipični pokazatelj tega pristopa je dejstvo, da standard GSM-ja vsebuje mehanizme za overjanje mobilnih naprav, ki se povezujejo vanj, mobilni telefoni pa pristnosti omrežja, v katero se povezujejo, ne morejo overiti.

To dejstvo izkoriščajo tudi t. i. lovilci IMSI-številk (angl. IMSI Catcher; Kovačič, 2016). Gre za posebne naprave, ki se mobilnemu telefonu lažno predstavijo kot legitimna bazna postaja, v resnici pa je z njimi mogoče identificirati identiteto mobilnih telefonov v omrežju (ugotoviti t. i. IMSI-številke), izvajati prestrezanje komunikacij ter še različne druge napade na mobilne naprave. Tovrstni mehanizmi za preverjanje pristnosti so na voljo šele v omrežjih 4G (LTE), a tudi v njih so varnostni raziskovalci našli številne varnostne razpoke, s katerimi je mogoče mobilni telefon "prepričati", da se poveže z lažno bazno postajo (t. i. eNodeB) ali da ji pošlje kakšne podatke, npr. podatke o točni lokaciji (Shaik, Borgaonkar, Asokan, Niemi, Seifert, 2005).

Proti prestrezanju komunikacij s pomočjo lovilca IMSI-številk se je sicer mogoče boriti z zgoraj opisanim šifriranjem komunikacij med dvema uporabnikoma, vendar pa imajo sodobni lovilci IMSI-številk še nekatere druge neželene funkcionalnosti. Poleg tega da lovilci IMSI-številk omogočajo prestrezanje ali spreminjanje komunikacij s pomočjo napada s posrednikom (angl. man-in-the-middle attack), lahko mobilnim telefonom, ki so povezani z njim mimo omrežja, pošiljajo SMS-e ali jih kličejo. Tako je znan primer iz Ukrajine, kjer je policija januarja 2014 protestnikom s pomočjo lovilca poslala SMS, da so udeleženi pri nezakonitih demonstracijah, kriminalna združba na Kitajskem pa je lovilce

uporabljala za pošiljanje nadležnih reklamnih sporočil, s čimer so se izognili plačevanju stroškov operaterjem (Grytsenko, 2014, in Kovačič, 2016). Predvsem pa lahko lovilec mobilni telefon izolira iz omrežja (npr., da ne more več sprejemati klicev), mu izprazni baterijo ali ga do ponovnega zagona popolnoma onesposobi, s pomočjo lovilca je mogoče ugotoviti točno lokacijo mobilnega telefona, sodobnejše naprave pa znajo s pomočjo t. i. tihega klica na daljavo vklopiti mikrofon telefona in tako mobilni telefon spremeniti v pravo prisluškovalno napravo. Obstajajo pa tudi napadi, pri katerih lovilec s pomočjo napada na radijski procesor telefona nanj namesti zlonamerno kodo (virus), s katero telefon trajno okuži (Doctorow, 2016). Tako okužen telefon se nato obnaša kot prisluškovalna ali sledilna naprava, ki svojo lokacijo in neposredno na mikrofonu zajete podatke periodično sporoča v "nadzorni center".

Mobilni telefoni namreč za komunikacijo z omrežjem uporabljajo t. i. radijski procesor (angl. baseband processor), ki poganja t. i. real time OS in je nadrejen ostalim delom strojne opreme, vključno z aplikacijskim procesorjem. Raziskovalci so v preteklosti že našli številne varnostne ranljivosti v radijskih procesorjih (Weinmann, 2012), s pomočjo katerih je v mobilnem telefonu mogoče oddaljeno vključiti mikrofon, kamero ali dostopati do notranjega pomnilnika, in to mimo vseh zaščitnih sistemov oziroma mimo glavnega operacijskega sistema. Znan je vsaj en primer, ko so organi pregona tovrstne tehnike uspešno (in zakonito) uporabili pri svojih preiskavah. V primeru iz leta 2006 je FBI na mobilni telefon osumljenca preko omrežja namestil t. i. mehanizem za prisluškovanje (angl. roving bug), s čimer je nato na daljavo aktiviral mikrofon na mobilnem telefonu ter poslušal pogovore v njegovi bližini (Kovačič, 2006).

Poseben problem predstavljajo tudi že omenjene možnosti napadov na lokacijsko zasebnost mobilnih uporabnikov, kar je mogoče izvesti na različne načine. Omenimo lahko uporabo zlonamernih baznih postaj (tudi v LTE-omrežjih), pošiljanje t. i. tihih SMS-ov in lokacijske napade preko SS7-omrežja (Signalling System #7 je protokol za izmenjavo podatkov med telefonskimi operaterji, zaradi napak v zasnovi pa je preko njega mogoče izvajati lokacijske in tudi nekatere druge napade na mobilne telefone kar preko telefonskega omrežja (Engel, 2014)).

Tihi SMS-i so poseben tip SMS-ov, ki jih ciljni telefon sicer sprejme, vendar jih ne prikaže uporabniku. Kljub temu ob dostavi pošiljatelj lahko prejme potrdilo o dostavi, predvsem pa se njihov sprejem skupaj z lokacijo mobilnega telefona, ki je tako sporočilo prejel, zabeležijo pri mobilnem operaterju. Zato se periodično pošiljanje tihih SMS-ov pogosto uporablja za spremljanje lokacij oziroma gibanja osumljencev. Tako na primer niti ne preseneča, da so v Nemčiji v letu 2010 organi kazenskega pregona poslali skoraj pol milijona tihih SMS-ov, s katerimi so popolnoma neopazno sledili osumljencem oz. svojim tarčam (EDRI, 2012).

4. ZAKLJUČEK

Zagotavljanje varnosti mobilnih komunikacij ni preprosto opravilo. Sicer je mogoče z uporabo nekaterih zgoraj opisanih tehnologij stopnjo zaščite zasebnosti, zlasti šifriranja, precej povečati, vendar kljub temu ostaja na področju mobilne varnosti še kar precej izzivov, kar smo prikazali z opisom nekaterih bolj znanih napadov na mobilno telefonijo. Seveda zgoraj opisani seznam ranljivosti nikakor ni popoln, poleg tega varnostni raziskovalci redno odkrivajo še nove varnostne ranljivosti. Proizvajalci mobilnih naprav se v zadnjih letih čedalje bolj trudijo povečati zaščito svojih uporabnikov, toda določene težave oz. varnostne ranljivosti izvirajo še iz same zasnove mobilnih oz. celo telefonskih omrežij izpred desetletij. Odpravljanje tovrstnih ranljivosti bo zato še dolgotrajno.

5. LITERATURA IN VIRI

1. Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, Jean-Pierre Seifert. (2005). Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. Najdeno na naslovu https://arxiv.org/abs/1510.07563.
2. Bruce Schneier. (2013). A Really Good Article on How Easy it Is to Crack Passwords. Najdeno na naslovu https://www.schneier.com/blog/archives/2013/06/a_really_good_a.html.
3. Charles V. Wright, Lucas Ballard, Scott E. Coull, Fabian Monrose in Gerald M. Masson. (2008). Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversation. Najdeno na naslovu http://cs.jhu.edu/~cwright/oakland08.pdf.
4. Cory Doctorow. (2016). Baseband vulnerability could mean undetectable, unblockable attacks on mobile phones. Najdeno na naslovu https://boingboing.net/2016/07/20/baseband-vulnerability-could-m.html.
5. EDRI. (2012). Police frequently uses Silent SMS to locate suspects. Najdeno na naslovu https://edri.org/edrigramnumber10-2silent-sms-tracking-suspects/).
6. Engel, T. (2014). SS7: Locate. Track. Manipulate. Najdeno na naslovu https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf.
7. Grytsenko, W. (2014). Text messages warn Ukraine protesters they are participants in mass riot. Najdeno na naslovu http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot.
8. Karsten Nohl, Luca Melette. (2011). Defending mobile phones. Najdeno na naslovu https://events.ccc.de/congress/2011/Fahrplan/attachments/1994_111217.SRLabs-28C3-Defending_mobile_phones.pdf.
9. Kovačič M. (2016). Lovilci IMSI številk. Najdeno na naslovu https://telefoncek.si/2016/11/19/lovilci-imsi-stevilk/.
10. Kovačič, M. (2006). So mobilni telefoni prisluškovalne naprave? Najdeno na naslovu https://slo-tech.com/novice/t248422/0.
11. Kovačič, M. (2012). Gesla in varna hramba gesel (mala šola informacijske varnosti, 1. del). Najdeno na naslovu https://telefoncek.si/2012/07/30/gesla-in-varna-hramba-gesel-mala-sola-informacijske-varnosti-1-del/.

12. Kovačič, M. (2013). Varnost telefonskih komunikacij (mala šola informacijske varnosti, 14. del). Najdeno na naslovu https://telefoncek.si/2013/04/06/varnost-telefonskih-komunikacij-mala-sola-informacijske-varnosti-14-del/.
13. Scott Helme. (2014). Perfect Forward Secrecy – An Introduction. Najdeno na naslovu https://scotthelme.co.uk/perfect-forward-secrecy/.
14. Weinmann, Ralf-Philipp. (2012). Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks. Najdeno na naslovu https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf.

Matjaž Pušnik*

Strojno učenje in revizija informacijskih sistemov

Machine learning and IT audit

POVZETEK ● *Strojno učenje (angl. machine learning) je danes zelo razširjeno in se uporablja pri reševanju različnih pomembnih problemov v industriji, medicini, ekonomiji in informacijski tehnologiji. Tehnike strojnega učenja se lahko uporabljajo za prepoznavo govora, procesiranje jezikov, v bioinformatiki, za analize delniških trgov, v informacijski varnosti in tudi v reviziji. Zaradi razširjene uporabe strojnega učenja se povečuje tudi potreba za IT-revizije informacijskih sistemov, ki uporabljajo za svoje delovanje različne tehnike strojnega učenja. Po drugi strani razvoj in uporaba strojnega učenja lahko izboljšata kvaliteto revizije informacijskih sistemov in IT-revizorju pomagata pri hitrejši ter natančnejši analizi podatkov. Strojno učenje sicer odpira marsikatero vprašanje, ki ga bo treba v prihodnosti rešiti, da bo zaupanje v algoritme strojnega učenja upravičilo samostojno uporabo in zaupanje v rezultate uporabljenih algoritmov.*

Ključne besede ● *strojno učenje, umetna inteligenca, ekspertni sistemi, revizija informacijskih sistemov, IT-revizija*

SUMMARY ● *Machine learning is used to solve various important problems in industry, medicine, economics and information technology. Machine learning techniques are used for speech recognition, language processing, bioinformatics, stock market analysis, information security, audit and others. Due to the expanded use of machine learning technology the need for information systems audits, which use different machine learning techniques, is also increasing. On the other side, the development and use of machine learning in the information system audit can increase the quality of information systems audit with faster and more accurate data analysis. Machine learning opens up many questions that will need to be resolved in the future so that confidence in machine learning algorithms will justify the use of and trust in the results of the applied algorithms.*

Key words ● *machine learning, artificial intelligence, ekspert system, IT audit*

JEL: C 88 , L 86

* Matjaž Pušnik, mag. poslovodenja in organizacije, PRIS, CISA, CRISC, KPMG, matjaz.pusnik@gmail.com.

1. ZGODOVINA RAZVOJA UMETNE INTELIGENCE

Osnove umetne inteligence je postavil francoski matematik Adrien-Marie Legendre, ki je leta 1806 prvi objavil metodo najmanjših kvadratov, eno temeljnih regresijskih metod, ki jo je med opazovanjem neba uporabil za izračun orbit teles, ki potujejo okoli sonca. Metoda je bila razvita kot statistični okvir, danes se uporablja kot osnova mnogih modelov strojnega učenja.

Leonardo Torres y Quevedo je 1914 iznašel prvi avtomat za igranje šaha, ki velja za prvo računalniško igro na svetu. Warren McCulloch in Walter Pitts sta 1943 predstavila prvi model nevronske mreže v obliki logičnega kalkulatorja, katerega osnova so nevroni človeških možganov. Leta 1950 je Alan Turing postavil vprašanje, Ali lahko stroji razmišljajo.

John McCarthy, Claude Shannon in Marvin Minsky so iznašli termin umetna inteligenca na poletni šoli 1956. Oliver Selfridget je 1958 objavil članek o nevronskih mrežah, prepoznavanju vzorcev in strojnem učenju. Ameriški psiholog in računalniški znanstvenik Frank Rosenblatt je leta 1958 ustvaril perceptronski algoritem (angl. the perceptron algorithm), ki predstavlja zgodnji tip umetne nevronske mreže (angl. Artifical neural network – ANN) in je bil prvi algoritemski model, ki se uči sam. Ameriški računalniški znanstvenik Arthur Samuel si je v naslednjem letu za omenjeno vrsto samoučečih modelov izmislil izraz "strojno učenje" ter tudi razvil inovativni program Dama, ki se je zgodil kot prvi zgodnji uspeh v umetni inteligenci (angl. Artifical Inteligence – AI).

Frank Rosenblott je 1960 razvil Mark I Perceptron, prvi računalnik, ki se je učil s poskušanjem in napakami na podlagi uporabe nevronskih mrež, ki so simulirale proces razmišljanja ljudi. Leta 1961 je Marvni Minsky objavil korake, kako priti do umetne inteligence.

Ukrajinski matematik Alexey Grigorevič Ivakhnenko je 1965 razvil prvi splošno delujoč algoritem za učenje, ki nadzoruje večplastno nevronsko mrežo, kjer je več različnih nevronskih mrež medsebojno povezanih druga nad drugo. Rezultat ene nevronske mreže predstavlja vhodne podatke za drugo. Uporabljena arhitektura je zelo podobna današnji arhitekturi algoritmov za globoko učenje.

Leta 1966 je Joseph Weizenbaum objavil enostaven program ELIZA, ki je omogočal procesiranje naravnega jezika, ter tako uspešno demonstriral uporabo prvega bota.

James Lighthill je 1973 objavil tako imenovano Lighthillovo poročilo, ki je bilo zelo kritično do raziskav in osnovnih področij robotike in procesiranja naravnih jezikov. Britanska vlada je na osnovi poročila zaustavila podporo raziskavam na področju umetne inteligence.

Hans Berliner je razvil program BKG 9.8, ki je leta 1979 premagal svetovnega prvaka v Backgammonu. Računalnik je tako prvič premagal človeka v intelektualni igri.

Douglas Lenat je 1984 začel Cyc projekt, s katerim je poskusil razviti bazo znanja, ki bi omogočila samoučenje. Ernst Dieter Dickmanns je 1987 s skupino razvil VaMoRs, prvo avtonomno vozilo Mercedes kombi, opremljeno s kamerami in drugimi senzorji za vožnjo. Leta 1987 je trg umetne inteligence doživel padec. Programski jezik Lisp, optimiziran za umetno inteligenco, ne more več konkurirati s cenejšimi programskimi jeziki, ki delujejo na mikroprocesorskih računalnikih.

Računalnik IBM Deep Blue, ki je imel veliko namenskih čipov, ki so omogočali hitre izračune (do 200 milijonov potez na sekundo, ki so omogočale veliko igralno moč in iskanje potez v globino), je 1997 premagal svetovnega šahovskega prvaka Garija Kasparova v šestih partijah šaha.

Cynthia Brezeal je leta 2000 razvila socialnega robota Kismet, humanoida, ki je zmožen izkazovati čustva.

Defence Advanced Research Projects Agancy je 2004 organizirala prvo tekmovanje avtonomnih vozil, ki so prevozila puščavo Mojave v Združenih državah Amerike.

Sistem za umetno inteligenco IBM Watson, ki je sposoben odgovarjati na vprašanja, podana v naravnem jeziku, je leta 2011 premagal druge tekmovalce v kvizu Jeopardy.

Leta 2012 je Geoffrey Hintonov laboratorij zmagal na tekmovanju ImageNet Large Scale Visual Recognition Challenge z uporabo metod globokega učenja z visoko točnostjo ter prednostjo pred drugimi ekipami, z uporabo konvolucijskih nevronskih mrež. Za učenje nevronskih mrež na 1,2 milijona fotografijah so uporabili dve grafični kartici.

Google je 2012 uporabil 16.000 procesorjev za učenje globoke umetne nevronske mreže z bilijonom povezav na 10 milijonih naključno izbranih slikah storitve videov YouTube v treh dneh. Ne da bi pridobili kakršne koli podatke o slikah, je mreža začela prepoznavati slike mačk, kar so označili za začetek pomembnega razvoja na področju razpoznavanja slik.

Leta 2014 je Google kupil podjetje Deep Mind Technologies. Oktobra 2014 je GSMA Association poročal, da je na svetu v uporabi 7,22 milijarde mobilnih naprav, ameriški statistični urad poroča, da je na zemlji 7,20 milijarde ljudi.

Leta 2017 je bilo ocenjeno, da je 90 odstotkov svetovnih podatkov generiranih v zadnjih dveh letih. Vsako minuto si uporabniki storitve YouTube ogledajo več kot

štiri milijone posnetkov. Uporabniki mobilnih naprav pošljejo vsako minuto več kot 15 milijonov sporočil.

Leta 2017 je Google DeepMind naredil korak naprej z AlphaZero, ki se je naučil igrati tri računalniške igre: Go, šah in šogi. Medtem ko je AlphaGo Zero še prejel navodila človeških strokovnjakov (ekspertov), se je AlphaZero naučil igranja čisto sam ter premagal svojega predhodnika AlphaGo Zero v igri Go (po vsega osmih urah) ter najboljše računalniške programe v šahu in šogiju (prvega po štirih in drugega po dveh urah).

Konvergenca razvoja algoritmov, povečanje obsega podatkov in velika razpoložljivost računalniških zmogljivosti ter povečanje količine hrambe podatkov so v zadnjih 10 letih pripeljali umetno inteligenco iz faze navdušenja v praktično uporabo (Wilson, 2017).

2. UMETNA INTELIGENCA

Uporaba umetne inteligence spreminja naše življenje na vsakem koraku, zato jo želimo in moramo razumeti, kako vpliva na naše odločitve v vsakdanjem življenju. Danes algoritmi upravljajo, kako najdemo informacijo (na primer Google iskalnik), kako se učimo, kako potujemo, kje kupimo, kaj kupimo, kako skrbimo za svoje zdravje, kako vzpostavljamo nova prijateljstva, s kom se družimo, kako nas sprejema okolica in kako mi sprejemamo okolje. Trženje, analize podatkov, diagnosticiranje, proizvodnja, vožnja, iskanje, govor, vid, sluh se spreminjajo s pomočjo računalnikov, ki se učijo. Algoritmi obdelujejo podatke s hitrostjo in v obsegu tako hitro, kot ti podatki nastajajo, lahko bi rekli, da skoraj v realnem času.

Današnji algoritmi lahko na primer za odkrivanje goljufij prepoznajo vzorce v transakcijah v dolgih besedilih ter finančne in lokacijske informacije. Algoritmi, ki obdelujejo in analizirajo milijone podatkovnih točk iz različnih podatkovnih virov, se lahko uporabljajo za učinkovito napovedovanje vzdrževalnih del za kompleksno industrijsko opremo, na primer za letalske motorje. Analize velikih količin podatkov iz različnih socialnih omrežij, spletnih logov, transakcijskih sistemov, geolokacijskih sistemov in mobilnih naprav posameznikov se aktivno uporabljajo za trženje izdelkov in storitev (Adebayo, 2016).

Večja uporaba umetne inteligence v vsakdanjem življenju poveča vpogled v nas, naše preference, kako izbiramo, kaj želimo nadzorovati, kako nas algoritmi spreminjajo.

Kako se računalniki učijo? Za lažje razumevanje, kako deluje umetna inteligenca, je treba razumeti, kako se danes računalniki učijo. Osnovna ideja za učenje

računalnikov je uporaba nevronskih mrež, ki posnemajo delovanje človeških možganov. Zaradi boljših matematičnih formul in povečanja zmogljivosti računalnikov danes lažje modeliramo nevronske mreže. Dejansko moramo razumeti matematiko, da razumemo, kako deluje umetna inteligenca. Učenje kompleksne matematike ni ravno nekaj, kar si želi posameznik. Zakaj je pomembno, da razumemo, kako deluje umetna inteligenca? Dvomi, ki jih povzroča uporaba umetne inteligence, izhajajo iz pomanjkanja transparentnosti in nemoči, ki jo povzročajo sistemi z vgrajeno umetno inteligenco. Računalniški programi se lahko samostojno prilagajajo in delujejo na večjem obsegu uporabnikov, so vgrajeni v robote ali vozila, ki delujejo avtonomno brez pomoči človeka.

2.1. Vrste umetne inteligence

Umetno inteligenco lahko opredelimo na več načinov. Ena izmed opredelitev je delitev umetne inteligence na dve področji (Smith, 2018):

1. ekspertne sisteme,
2. strojno učenje.

2.1.1. EKSPERTNI SISTEMI

Ekspertni sistemi rešujejo probleme na "ozkem" strokovnem področju, podobno, kot to počnejo strokovnjaki (eksperti). Ekspertni sistemi omogočajo sklepanje, presojanje, delujejo z nezanesljivimi in nepopolnimi podatki ter omogočajo pojasnjevanje. Delujejo po načelu odločitvenih modelov "če to – potem to" sistema pravil in so bili prvi primeri praktične uporabe umetne inteligence.

Ekspertni sistemi so uporabni na področjih, ki niso visoko formalizirana in je potrebna intuicija. Uporabljajo se na področju inteligentnih sistemov in agentov, za poslovno odločanje (poslovna logika in pravila), vodenje procesov, za diagnosticiranje določenih bolezni, pri računalniških vmesnikih, računalniških igrah in robotiki.

2.1.2. STROJNO UČENJE

Strojno učenje je relativno novo področje v računalništvu, ki omogoča programom učenje na podlagi primerov (Clark, 2017). Umetna inteligenca vključuje prav tako strojno učenje kot tudi druge tehnike, kot sta na primer strojni vid in iskanje/pregledovanje. Umetna inteligenca pogosto deluje v ozadju računalniških programov, pogosto brez vednosti uporabnika; od prepoznavanja fotografij do priporočanja želenih oglasov prijateljem. Nad spletnimi podatki se

uporablja veliko različnih že znanih algoritmov (na primer nevronske mreže), ki oponašajo ali pa presegajo ljudi pri podobnih opravilih.

Strojno učenje omogoča napovedovanje in predpisan pristop. Poznamo naslednje analitične tipe:

- **opisni** opisuje, kaj se je zgodilo, je zelo razširjen v vseh industrijskih panogah;
- **napovedni ali prediktivni** napoveduje z določeno stopnjo verjetnosti, kaj se bo zgodilo in je razširjen predvsem v podatkovno usmerjenih organizacijah kot ključni vir razumevanja informacij;
- **predpisani ali preskriptivni** priporoča, kaj je treba narediti, da dosežemo cilj, ki je zelo razširjen v vodilnih spletnih podjetjih.

Strojno učenje uporablja predvsem prediktivno in preskriptivno analitiko.

Obstajajo štirje načini strojnega učenja (Wilson, 2017):

- nadzorovano učenje (angl. Supervised Learning),
- nenadzorovano učenje (angl. Unsupervised learning),
- delno nadzorovano učenje (angl. Semi supervised learning),
- spodbujevalno učenje (angl. Reinforcement learning).

2.1.2.1. Nadzorovano učenje

Nadzorovano učenje je danes ena izmed najbolj uporabljenih metod med algoritmi strojnega učenja. Nadzorovano učenje se uporablja pri učenju na primerih, kjer že poznamo končen pravilni odgovor. Nadzorovano učenje temelji na učenju iz niza primerov, ki jih zagotovimo in primerno kategoriziramo oziroma označimo ljudje. Človek se odloči, katere podatke je treba uporabiti (imenujemo priprava), zagotovi učne podatke (primerne podatke za učenje izbranega modela) in podatke za testiranje izbranega modela (testni podatki).

Na primer, nadzorovano strojno učenje se danes v praksi uporablja pri pregledovanju slik (Ribeiro, Singh, Guestrin, 2016), iz katerih želimo prepoznati določeno osebo (na primer, Janez Novak, pri uporabi nadzora nad dostopom do varovanih prostorov).

Potrebni koraki za zgoraj navedeni primer so:

1. Priprava podatkov in kategorizacija

   Najprej pregledamo vse fotografije, ki jih hranimo v organizaciji (množica podatkov, angl. The data set), in označimo vse tiste, na katerih je Janez Novak. Vzeli bi vse fotografije in jih razdelili na dva kupa. Prvo množico fotografij bi uporabili za učenje (učni podatki), drugo množico pa za testiranje modela. Z drugim kupom fotografij bi preverili, kako natančen je naš model, koliko fotografij z Janezom Novakom najde.

Ko je model pripravljen, mu damo na voljo podatke (mu posredujemo fotografije za preverjanje). Matematično gledano je naš cilj poiskati funkcijo, ki na vhodu dobi fotografijo, rezultat funkcije je 0, kadar na fotografiji ni Janeza Novaka, in 1, če je na njej Janez Novak.

Ta korak imenujemo označevanje oziroma kategorizacija. V našem primeru je rezultat učenja tipa DA/NE, rezultat nadzorovanega učenja je lahko tudi drugačen, kot samo vrednost 0 in 1. Zgradimo lahko na primer model, ki vrne kot rezultat oceno verjetnosti poplačila kredita kreditne kartice, v tem primeru je lahko rezultat vrednost med 0 in 100 %, kar imenujemo regresija (Sculley, Holt, Golovin, 2014).

2. Učenje

   V koraku učenja model naredi predvidevanje za vsako fotografijo s sledenjem pravilom, na poti se odloča, ali bo upošteval izbrano vozlišče. Model deluje od leve proti desni, nivo za nivojem. Za trenutek bomo pozabili na bolj zapletena omrežja. Ko omrežje izračuna za vsako vozlišče v omrežju, pridemo do najbolj desnega vozlišča (končno vozlišče), ki zasveti ali ne, ko ga dosežemo.

   Ker že vemo, na katerih fotografijah je Janez Novak, lahko modelu povemo, ali je njegova napoved pravilna ali nepravilna. Nato dodamo te informacije v omrežje.

   Funkcija, ki določa, "kako daleč od pravilnega odgovora je napoved modela", algoritem uporabi kot povratno informacijo. Imenujemo jo stroškovna funkcija, ki je znana tudi kot funkcija cilja, funkcija koristnosti ali izhodna funkcija. Izhodni rezultati se nato uporabijo za računanje vpliva sprememb vhodnih parametrov (spreminjanje moči povezav in pristranskosti med vozlišči v procesu), ki se v angl. imenuje backpropagation, saj informacije potujejo "nazaj" iz vozlišč rezultatov.

2.1.2.2. Delno nadzorovano učenje

Delno nadzorovano učenje kombinira uporabo nekategoriziranih podatkov z majhno množico kategoriziranih podatkov v fazi učenja. Učni modeli so lahko zelo natančni in ugodnejši za učenje v primerjavi z modeli, kjer uporabljamo popolnoma kategorizirane podatke. Znani so primeri, kjer so pri delno nadzorovanem učenju uporabili samo 30 značilk za posamezni razred, pri tem pa so dosegli enako učinkovitost kot pri nadzorovanem učenju, ki je uporabil 1360 značilk za posamezni razred. Tako so zelo hitro prilagodili zmožnost napovedovanja z 20 kategorij na 110. Uporaba nekategoriziranih podatkov lahko včasih pomaga izboljšati model, čeprav ne poznamo odgovora, se naučimo nekaj, kar je verjetno in kako pogosto se pojavi (Wilson, 2017).

Primeri poslovne uporabe nadzorovanega in delno nadzorovanega učenja:

- razumevanje pospeševanja prodaje izdelkov, kot so cene konkurentov, dostava, oglaševanje in podobno, ter za optimizacijo cen in ocenjevanje cenovne elastičnosti izdelkov;
- razvrščanje strank na podlagi verjetnosti za poplačilo kredita;
- predvidevanja, ali so kožna znamenja glede na njihove značilnosti (oblika, velikost, barva ipd.) rakava ali ne;
- predvidevanje obnašanja kupcev;
- predvidevanje verjetnosti izpeljave prodaje;
- razumevanje lastnosti izdelkov, ki povečajo verjetnost prodaje;
- vzpostavitev okvira za odločanje pri zaposlovanju novih kadrov;
- analiza sentimenta proizvodov glede na percepcijo trga;
- kreiranje klasifikatorjev za filtriranje neželene pošte;
- predvidevanje, koliko bolnikov bo obravnavanih v določenem času;
- predvidevanje, kako pogosto bo posameznik izbral spletni oglas;
- predvidevanje števila klicev v klicnem centru za ustrezno kadrovanje;
- predvidevanje porabe elektrike v elektrodistribucijskem centru;
- pravočasno odkrivanje goljufij pri transakcijah s kreditnimi karticami; uporaba tehnologije globokega učenja da boljše rezultate;
- enostaven, poceni način za klasifikacijo fotografij (na podlagi satelitskih slik podnebnih sprememb spremljanje zmanjšanja kmetijskih površin);
- napovedovanje povpraševanja po izdelkih in zagotavljanje ustreznih varnostnih zalog;
- predvidevanje cen avtomobilov na podlagi njihovih lastnosti (starost, prevoženi kilometri ipd.);
- predvidevanje verjetnosti vključitve bolnikov v programe zdravljenja;
- predvidevanje, ali so registrirani uporabniki pripravljeni plačati določeno ceno za izbrani izdelek.

2.1.2.3. Nenadzorovano učenje

Nenadzorovano učenje temelji na učenju iz niza primerov, ki jih zagotovimo, vendar jih ne označimo oziroma kategoriziramo. Pri nenadzorovanem učenju na vhodu damo podatke in skušamo v podatkih poiskati določene vzorce, tako da jih združujemo v skupine (angl. Clustering) ali poiščemo odstopanja (prepoznavanje anomalij). Na primer (Upadhyay, McCormick, 2018):

1. Ste proizvajalec majic, ki ima izmerjenih veliko različnih velikosti ljudi. Algoritem za razvrščanje skupin grupira meritve v različne množice tako, da se lahko odločamo med majicami velikosti XS, S, M, L, XL in XXL.

2. Vodja IT-zagonskega podjetja, ki se ukvarja z varnostjo, želi iz prometnih logov povezav v omrežju poiskati odstopanja. Omrežni promet, ki odstopa od tipične uporabe, omogoča identificiranje zaposlenih, ki so si prenesli celotno bazo strank (CRM), ker načrtujejo odhod, ali pa odstopanja pri nakazilih denarja na nov bančni račun.
3. Razvojno skupino Google Brain zanima, kaj so uporabniki naložili na YouTube. Resnična zgodba (YouTube Cat finder) razkriva, kako je razvojna skupina Google Brain skupaj z raziskovalci s Stanforda razvila algoritem, ki posnetke stortive YouTube razvrsti v različne skupine po različnih kategorijah, vključno s skupino, ki vsebuje muce. Algoritem ni bil nastavljen, da bi poiskal muce, algoritem je avtomatsko razvrstil posnetke muc v svojo skupino (in tisoč drugih objektov, od 22.000 kategorizirano opredeljenih, v ImageNet) skupaj brez kakršnihkoli podatkov za učenje.

Ena izmed obetavnih idej nenadzorovanega učenja je tako imenovani generative adversarial networks, kjer tekmujeta dve nevronski mreži druga poti drugi. Eno mrežo imenujemo generator in je odgovorna za generiranje podatkov, ki poskušajo zavesti drugo mrežo, ki se imenuje diskriminator.

Primeri poslovne uporabe nenadzorovanega učenja:

- segmentiranje strank v različne skupine glede na različne karakteristike (na primer v starostne skupine) za učinkovitejše izvajanje marketinških akcij in preprečevanje odhajanja strank;
- segmentiranje zaposlenih na podlagi verjetnosti za odhod iz podjetja;
- segmentiranje strank za učinkovitejše izvajanje marketinških akcij z manjšim naborom značilnosti strank (na primer priljubljenost izdelkov);
- segmentiranje kartic zvestobe progresivno na manjše segmente skupin strank;
- informiranje o uporabi oziroma razvoju izdelkov določenim skupinam strank z uporabo ključnih besed na podlagi podatkov iz socialnih omrežij;
- priporočanje strankam, kateri film naj si ogledajo na podlagi priljubljenosti pri drugih strankah s podobnimi značilnostmi. Priporočanje časopisnih novic bralcem, ki želijo prebrati novice na podlagi, ki jih priporočajo prijatelji.

2.1.2.4. Spodbujevalno učenje

Pri spodbujevalnem učenju nimamo kategoriziranih množic podatkov, vendar znamo povedati, ali se bližamo cilju (funkcija nagrajevanja). Otroška igra vroče-hladno je dober primer tega koncepta. Cilj je, da poiščemo skriti objekt, pri tem pa nas prijatelj usmerja proti cilju, "vroče", bližje smo cilju, "hladno", oddaljujemo se od njega. Vroče-hladno je funkcija nagrade, cilj algoritma je maksimizacija funkcije nagrade. Funkcija nagrade je zapoznela in redka oblika kategoriziranih

podatkov. Namesto da dobimo specifičen "pravilen/napačen" odgovor za vsako podatkovno točko, dobimo zapoznelo reakcijo in usmeritev, ali se bližamo cilju (Wilson, 2017).

Primeri:

- Deepmind je opisal sistem, ki uporablja spodbujevalno učenje skupaj z globokim učenjem za igranje različnih Atari video igric, nekatere zelo uspešno (Brakeout) in druge zelo slabo (Montezumas revenge).
- Študenti na Stanfordu so prikazali izboljšano uporabo spodbujevalnega učenja. Pri Deepmindu se nekateri algoritmi niso bili zmožni naučiti, kako igrati Montezumas revenge. Študenti so to opisali: "Agenti spodbujevalnega učenja se mučijo pri učenju v okolju z redkimi nagradami. Če nimamo dovolj vroče-hladnih usmeritev, je težko poiskati cilj. Zato so študenti naučili sistem, da razume in se odziva na usmeritve, podane v naravnem jeziku, kot so "splezaj po lestvi dol" ali "vzemi ključ", in tako zagotovili večjo točnost algoritma.

Primeri poslovne uporabe spodbujevalnega učenja:

- optimizacija trgovalnih strategij pri opcijskih trgovalnih portfeljih;
- optimizacija logistike v skladiščih z uporabo robotov;
- optimizacija cen v realnem času pri spretnih avkcijah izdelkov z omejeno zalogo;
- uravnavanje obremenitev električnih omrežij na podlagi povpraševanja;
- optimizacija vožnje avtonomnih vozil.

V IT-reviziji umetna inteligenca nadomešča prediktivno revizijo in programe za vzorčenje (na primer IDEA, ACL, Microsoft Excel), predvsem za iskanje kritičnih točk, ki so lahko večja tveganja, in izvajanje optimalnih revizijskih aktivnosti, in tako nadomešča napor IT-revizorjev in revizorjev računovodskih izkazov.

3. IT-REVIZIJA STROJNEGA UČENJA

Na voljo je več različnih načinov revizije strojnega učenja, od revizije razvoja programske opreme do revizije programske kode. Revizorji lahko zagotovimo učinkovitost izbranega algoritma za strojno učenje tako, da opravimo revizijo celotnega procesa razvoja programske opreme, ki ima vgrajeno strojno učenje, to je od faze načrtovanja do faze implementacije pri tradicionalnem razvoju programske opreme. Zrelostni nivo programske kode, ki podpira strojno učenje, je največkrat pod nivojem standardnega programskega razvoja, vendar bi moral večji del pregleda same programske kode pokriti vse potrebe in cilje revizije (Clark, 2016).

Odprti standard za podatkovno rudarjenje (angl. Cross-industry standard process for data mining – CRISP-DM), ki se uporablja za standardiziran proces razvoja za podatkovno rudarjenje, je lahko uporabno orodje, ki pomaga revizorju pri izvajanju revizije strojnega učenja. CRISP-DM uporabljajo razvijalci pri razvoju aplikacij strojnega učenja, ki temelji na enakih načelih kot razvoj standardne programske opreme in ga je možno prilagoditi procesu razvoja strojnega učenja.

Koraki razvoja algoritma strojnega učenja so (Marbán, Segovia, 2009):

1. razumevanje poslovnega primera,
2. razumevanje podatkov,
3. priprava podatkov,
4. modeliranje,
5. ocenjevanje/preverjanje,
6. produkcija.

Revizija aplikacij, ki uporabljajo strojno učenje, omogoča doseganje visokega nivoja zagotovil z uporabo CRISP-DM. Če strokovnjaki natančno pregledajo vsak korak algoritma, lahko dajo večje zagotovilo. Okvir CRISP-DM je treba prilagoditi glede na cilj revizije, poleg tega pa je treba vsak korak revizije ustrezno in natančno dokumentirati. Ključni korak revizije strojnega učenja pri pripravi podatkov, modeliranju in ocenjevanju, ki običajno zahteva znanje o programiranju, podatkovnih bazah, linearni algebri, teoriji verjetnosti in statistiki, se lahko izvede tudi brez teh znanj, če se pri reviziji zanašamo na tradicionalne tehnike vzorčenja. Interes skupnosti razvoja strojnega učenja je razvoj modelov, ki jih lahko razume vsak. To je zelo pomembno, predvsem na področju medicine, kjer posamezniki ne zaupajo algoritmom, razen če razumejo, kako smo prišli do rezultatov. Za revizijo algoritmov strojnega učenja se uporabljata tudi revizijska okvira LIME in FairML, ki omogočata le interpretacijo vpliva posameznih karakteristik na model in ne upoštevata tveganj, povezanih s procesom strojnega učenja. Za ta del je uporaben okvir CRISP-DM. Poudariti je treba, da so LIME in FairML skupaj s CRISP-DM uporabni v fazi ocenjevanja za razumevanje delovanja modela (Clark, 2018).

Ko model strojnega učenja naučimo in damo v produkcijo, le-ta uporabi na vhodu podatke iz ene množice hkrati, lahko pa tudi v obliki podatkovnega toka (*angl. data stream*), seveda odvisno od uporabe. To je diskretni model, ki uporablja na vhodu hkrati samo eno množico podatkov. V vsakem primeru mora revizor pregledati, kaj so vhodni parametri, pregledati nabor psevdopodatkov za vhod v algoritem in pregledati rezultate za lastnosti, ki bi omogočile morebitno pristranskost algoritma. Na primer model za dajanje posojil, ki izloča rasne skupine glede na poštne številke. S polnjenjem modela z robnimi podatki lahko

potrdimo potencialno pristranskost modela, ne da bi delovanje algoritma v celoti preverili, kako in zakaj algoritem pride do določenega rezultata. V nekaterih primerih nam tudi pomoč strokovnjakov za strojno učenje ne pomaga, ker ni možno podrobno pregledati oziroma ovrednotiti nekaterih modelov (na primer podpornih vektorskih strojev in nevronske mreže). S pregledom rezultatov različnih skupin vhodnih vzorcev podatkov lahko ocenimo praktično natančnost algoritma v primerjavi z matematično, ki se uporablja v fazi modeliranja (uspešnost oziroma natančnost modela in njegova zmožnost doseganja poslovnih ciljev je enostavnejša za revizijo).

4. ZAKLJUČEK

Umetna inteligenca in strojno učenje sta v zadnjem desetletju zelo napredovala, in čeprav naj bi bili še na začetku, narašča tudi potreba po IT-reviziji informacijskih sistemov, ki uporabljajo strojno učenje.

Trenutni "IT-revizijski" okviri revizorje predvsem usmerjajo, kako izvesti revizijo strojnega učenja z vidika razvoja algoritmov strojnega učenja in ne namenskih kontrolnih ciljev, ki so osredotočeni na tveganja, povezana z uporabo tehnik strojnega učenja. Za podrobno revizijo algoritmov strojnega učenja je potrebna pomoč strokovnjakov s področja strojnega učenja. Upravičeno lahko pričakujemo, da bo uporaba revizijskega okvira CRISP-DM in podobnih povečala število revizij strojnega učenja, ki se uporablja v praksi, in počasi povečala zaupanje v umetno inteligenco ter zagotovila ustrezne odgovore na vsa vprašanja.

Razvoj in uporaba orodij za IT-revizijo, ki uporabljajo strojno učenje, lahko izboljšajo kvaliteto revizije informacijskih sistemov, tako da IT-revizorju pomaga pri hitrejši in natančnejši analizi podatkov za dajanje ustreznih zagotovil za točnost in pravilnost delovanja informacijskih sistemov.

5. LITERATURA IN VIRI

5.1. Literatura

1. Machine Learning for Complete Beginners: A Visual Guide to Machine Learning with Python, Data Science, TensorFlow, Artificial Intelligence, Random Forests and Decision Trees, Robert Wilson, 2017.
2. Machine Learning System, Jeff Smith, Manning Publications Co., 2018.
3. The Revenue Acceleration Rules: Supercharge Sales and Marketing Through Artificial Intelligence, Predictive Technologies and Account-Based Strategie, Shashi Upadhyay in Kent McCormick, Willey, 2018.

5.2. Viri

1. Adebayo, J. A. (2016). "FairML: ToolBox for Diagnosing Bias in Predictive Modeling," DSpace@MIT, 2016. Najdeno na naslovu http://hdl.handle.net/1721.1/108212.
2. Clark, A. (2016). "Focusing IT Audit on Machine Learning Algorithms," MISTI Training Institute. Najdeno na naslovu http://misti.com/internal-audit-insights/focusing-it-audit-on-machine-learning-algorithms.
3. Clark, A. (2017). "Machine Learning Audits in the 'Big Data Age'," CIO Insights, 19 April 2017. Najdeno na naslovu www.cioinsight.com/it-management/innovation/machine-learning-audits-in-the-big-data-age.html.
4. Clark, A. (2018). "The Machine Learning Audit—CRISP-DM Framework", ISACA Journal, 2018, 1.
5. Kaur, S. (2015). "A Review of Software Development Life Cycle Models," International Journal of Advanced Research in Computer Science and Software Engineering, 2015, (11), 5, str. 354–60. Najdeno na naslovu http://ijarcsse.com/Before_August_2017/docs/papers/Volume_5/11_November2015/V5I11-0234.pdf.
6. Marbán, G. M., J. Segovia. (2009). "A Data Mining and Knowledge Discovery Process Model, Data Mining and Knowledge Discovery in Real Life Applications," Intech.com, 2009 Najdeno na naslovu http://cdn.intechopen.com/pdfs/5937/InTech-A_data_mining_amp_knowledge_discovery_process_model.pdf.
7. Ribeiro, M. T., Singh, S., Guestrin, C. (2016). "Why Should I Trust You?," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining – KDD '16, 13 August 2016.
8. Sculley, D., G. Holt, D. Golovin; E. Davydov, Phillips, T., Ebner, D, Chaudhary, V., Young, M. (2014). "Machine Learning: The High Interest Credit Card of Technical Debt," SE4ML: Software Engineering 4 Machine Learning (NIPS 2014 Workshop), November 2014. Najdeno na naslovu http://www.eecs.tufts.edu/~dsculley/papers/technical-debt.pdf.

Mag. Robert Horvat*

Računovodenje popustov po novem MSRP 15 (2. del)

Accounting for discounts and price concessions using new IFRS 15 (2nd part)

POVZETEK ● *Prvega januarja letos je začel veljati novi Mednarodni standard računovodskega poročanja MSRP 15 – Prihodki iz pogodb s kupci, ki v računovodenje prihodkov prinaša precej pomembnih novosti. Ker se nekaj novosti nanaša tudi na računovodenje popustov, ki jih podjetja odobravajo svojim kupcem, v prispevku podrobno in s praktičnimi primeri predstavljamo, kako je treba po novem računovoditi popuste, da bo to skladno z zahtevami novega standarda. V prvem delu smo se ukvarjali predvsem s problematiko računovodenja pogodb s tako imenovanimi sprotnimi/tekočimi in (pričakovanimi/načrtovanimi) naknadnimi popusti, drugi del pa je v celoti namenjen predstavitvi postopkov in metod računovodenja pogodb z vključenimi obljubami popustov za dodatno blago in/ali storitve, kot so opredeljene v MSRP 15.B39–15.B41.*

Ključne besede ● *prihodki, popusti, MSRP 15*

SUMMARY ● *On 1 January this year, the new International Financial Reporting Standard IFRS 15 – Revenue from Contracts with Customers, came into use, introducing many important changes into the existing practices of revenue recognition and accounting. Many important changes relate to the accounting of discounts and price concessions that companies frequently grant to their customers. In the paper, we systematically and in detail explain the main changes in this respect, including practical examples how to correctly account for discounts and price concessions according to the new standard. Because of the extensiveness of the topic, it is presented in two parts. While the first part's focus was mainly on the methods and procedures of accounting for contracts with present/current and (expected/planned) subsequent discounts and price concessions, this second part is completely dedicated to the methods and procedures of accounting for contracts with promises of discounts for additional goods and/or services as defined in IFRS 15.B39 – 15.B41.*

Key words ● *revenue, discounts, price concessions, IFRS 15*

JEL: M 41

* Robert Horvat, mag., univ. dipl. ekon., Univerza v Mariboru, Ekonomsko-poslovna fakulteta, robert.horvat@um.si.

1. UVOD

1. januarja letos je začel veljati novi Mednarodni standard računovodskega poročanja MSRP 15 – Prihodki iz pogodb s kupci.[1] Standard se v več pogledih pomembno odmika od dosedanjih rešitev računovodenja prihodkov, pri čemer se veliko novosti nanaša tudi na računovodenje popustov, ki jih podjetja odobravajo svojim kupcem. Glavnina sprememb, ki jih MSRP 15 prinaša v tej zvezi, je povezana s spremembami pravil za pogodbe, v katerih dogovorjena kupnina (nadomestilo) ni opredeljena fiksno, in s spremembami pravil za pogodbe, ki poleg prodanega blaga in/ali storitev vključujejo tudi obljube (možnost) popustov za dodatno blago in/ali storitve. Medtem ko smo v prvem delu prispevka obravnavali računovodenje sprotnih/tekočih in naknadnih popustov, v drugem delu prispevka prikazujemo računovodenje popustov za dodatno blago in/ali storitve, kot so opredeljeni v MSRP 15.B39 do 15.B41.

2. RAČUNOVODENJE POPUSTOV ZA DODATNO BLAGO IN/ALI STORITVE

Popusti za dodatno blago in/ali storitve so popusti, pri katerih se pravica do popusta, ki jo kupec pridobi oziroma pridobiva s sklenitvijo pogodbe, ne nanaša na blago in/ali storitve v tej pogodbi, ampak na blago in/ali storitve, ki ga/jih bo kupec šele (morda) kupil (tako imenovano dodatno blago in/ali storitve). Gre za popuste z veljavnostjo za prihodnje nakupe/pogodbe, zato jih lahko označimo tudi kot prospektivne popuste.

MSRP 15.B40 določa, da se ob sklenitvi prodajne pogodbe kupcu dana možnost pridobitve dodatnega blaga in/ali storitev po znižani ceni ali brezplačno pripozna kot posebna, torej ločena izvršitvena obveza takšne pogodbe, kadar kupcu daje stvarno pravico, ki je brez njene sklenitve ne bi prejel. Ker menimo, da je za pravilno interpretacijo in uporabo tega določila ključno pravilno razumevanje pojma *stvarna pravica*, prvi del razlage namenjamo razčiščevanju tega vprašanja. V izvirniku standarda v angleškem jeziku se namreč namesto pojma *stvarna pravica* uporablja pojem *materialna pravica* (angl. *material right*), ki ima po našem mnenju širši pomen. Pridevnik *materialen* se namreč lahko razlaga tudi kot *pomemben*/*relevanten*. V angleškem jeziku tako "*material right*" ne pomeni samo

[1] 11. junija je Strokovni svet Slovenskega inštituta za revizijo sprejel prenovljeni SRS 15 (2019) – Prihodki, ki glede računovodenja prihodkov od prodaje, vključno z računovodenjem popustov, ki ga predstavljamo v tem prispevku, v vseh pomembnih pogledih sledi rešitvam iz MSRP 15 – Prihodki iz pogodb s kupci.

stvarne, ampak tudi pomembno/relevantno pravico. Če to sprejmemo, pomeni, da se ob sklenitvi prodajne pogodbe kupcu dana možnost pridobitve dodatnega blaga in/ali storitev po znižani ceni ali brezplačno pripozna kot posebna, torej ločena izvršitvena obveza te pogodbe, kadar kupcu daje ne le *stvarno*, ampak tudi *pomembno/relevantno* pravico, ki je (ceteris paribus) ne bi prejel brez sklenitve te pogodbe. Iz strokovnih gradiv, ki jih na temo "*material right*" v povezavi z MSRP 15.B40 najdemo na spletu[2], lahko razberemo, da se presoja, ali je neka pogodbena pravica kupca do pridobitve dodatnega blaga in/ali storitev po znižani ceni pomembna/relevantna ("materialna"), povezuje predvsem z oceno njenega vpliva na nakupno obnašanje tega kupca. Če lahko utemeljeno pričakujemo, da je zaradi nje verjetnost njegovih dodatnih nakupov večja, potem velja, da je kriterij pomembnosti/relevantnosti ("materialnosti") izpolnjen. Če ne, potem ne gre za pomembno/relevantno ("materialno") pravico, in se zato zanjo ne pripozna samostojna oziroma ločena izvršitvena obveza.

Čeprav na prvi pogled majhna, menimo, da je za pravilno razumevanje in uporabo MSRP 15.B40 takšna dopolnitev še kako pomembna. Pomeni namreč, da ob sklenitvi pogodbe kupcu dana možnost pridobitve dodatnega blaga in/ali storitev po znižani ceni velja kot stvarna/materialna pravica samo takrat, ko je zaradi nje verjetnost, da bo do dodatnih nakupov dejansko prišlo, večja, kot bi bila, če kupec te pogodbe (ceteris paribus) ne bi sklenil, zaradi česar ne bi dobil takšne možnosti za nakup dodatnega blaga in/ali storitev s popustom. Da bi bil ta pogoj lahko izpolnjen, mora biti kupcu dana ugodnost ob nakupu dodatnega blaga in/ali storitev večja, kot bi jo imel, če pogodbe, s katero je takšno ugodnost pridobil, ne bi sklenil. Podjetje mora zato pri svoji presoji pomembnosti/relevantnosti takšne pravice/ugodnosti upoštevati tudi vse ostale popuste, ki so kupcu na voljo neodvisno od sklenitve navedene pogodbe. Prav tako mora podjetje pri tovrstni presoji upoštevati tudi predhodne posle z istim kupcem, s katerimi je ta morebiti že pridobil enako ali podobno pravico/ugodnost za nakupe dodatnega blaga in/ali storitev. Že pridobljena pravica se namreč ne more še enkrat upoštevati kot stvarna/materialna pravica v kasnejših pogodbah. Pa si poglejmo, kaj to pomeni v praksi.

[2] Glej na primer KPMG, 2016, str. 276: *"Če podjetje oceni, da pravica pomembno vpliva na obnašanje kupca, potem je nanjo potrebno razporediti del transakcijske cene, tudi če je takšna razporeditev kvantitativno zanemarljiva."* Ali pa KPMG, 2016, str. 287: *"Če je spodbuda pomembna za odločitev stranke, da vstopi v pogodbo, potem gre za stvarno/materialno pravico."* https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/IFRS-practice-issues-revenue.pdf.

Primer 9

Podjetje sklene s kupcem pogodbo o prodaji izdelka A, katerega prodajna cena znaša 100.000 evrov. Kupec hkrati s to pogodbo pridobi tudi možnost kasnejšega nakupa izdelka B s 50-odstotnim popustom, veljavnega en mesec. Podjetje sicer izdelek B redno prodaja po prodajni ceni 50.000 evrov. Upoštevaje MSRP 15.B40, možnost za kasnejši nakup izdelka B s popustom šteje kot stvarna/materialna pravica samo, če je ugodnost v višini 50-odstotnega popusta večja, kot bi jo kupec imel za nakup izdelka B, če ne bi pred tem sklenil pogodbe za nakup izdelka A. Če bi tako na primer podjetje za izdelek B v obdobju veljavnosti popusta vsem kupcem ponujalo enak, torej 50-odstotni popust, neodvisno od tega, ali so pred tem kupili izdelek A ali ne, to pomeni, da pogodba za izdelek A ne vsebuje stvarne/materialne pravice za nakup izdelka B, saj je popust, ki ga s takšno pogodbo prejme kupec, enak popustu, ki ga za izdelek B dobi vsak kupec, tudi če pred tem s podjetjem ni sklenil nobene pogodbe.

Pomembno drugačna pa je situacija, ko je 50-odstotni popust za nakup izdelka B na voljo samo kupcem, ki so pred tem s podjetjem sklenili pogodbo za nakup izdelka A ali kak drug enakovreden nakupni posel[3]. V tem primeru je namreč ugodnost v višini 50-odstotnega popusta za izdelek B bistveno večja, kot bi jo kupec imel, če ne bi prej sklenil pogodbe za nakup izdelka A. Tako je izpolnjen osnovni pogoj za pripoznanje popusta kot stvarne/materialne pravice, s tem pa tudi kot ločene izvršitvene obveze znotraj pogodbe za nakup izdelka A.

Tako kot na vse druge ugotovljene izvršitvene obveze posamezne pogodbe je po določilih MSRP 15 tudi na takšno obvezo treba razporediti del skupne transakcijske cene sklenjene pogodbe. Standard v tej zvezi predpisuje metodo samostojnih prodajnih cen, kar pomeni, da mora podjetje najprej oceniti samostojno prodajno ceno ugotovljene stvarne/materialne pravice, nato pa na njeni osnovi na izvršitveno obvezo razporediti sorazmeren del skupne transakcijske cene pogodbe. Pri tem mora podjetje iz ocene samostojne prodajne cene stvarne/materialne pravice izločiti učinke vseh popustov, ki jih kupec izdelka B lahko dobi, tudi če prej ne sklene pogodbe za nakup izdelka A.[4]

V konkretnem primeru podjetje vsem kupcem v opazovanem obdobju nudi 20-odstotni popust na izdelek B, neodvisno od tega, ali so pred tem sklenili s podjetjem kakšno pogodbo ali ne. Kot stvarna/materialna pravica v tem primeru

---

3 Ta pa mora biti kot pogoj za pridobitev stvarne/materialne pravice ekonomsko relevanten (glej primer 10).

4 Upoštevajoč predpostavko ceteris paribus.

velja zgolj popust v višini 30 odstotkov. To pa zato, ker je samo 30 odstotkov popusta tisti popust, za katerega lahko trdimo, da ga kupec ne bi prejel, če pred tem ne bi sklenil pogodbe za nakup izdelka A. Popust v višini 20 odstotkov je namreč kupcu na voljo neodvisno od sklenitve predhodne pogodbe za izdelek A. Podjetje mora pri oceni samostojne prodajne cene ugotovljene stvarne/ materialne pravice upoštevati tudi, kakšna je verjetnost, da bo kupec možnost za nakup izdelka B dejansko izkoristil.

Podjetje npr. to verjetnost ocenjuje na 50 odstotkov. Samostojna prodajna cena stvarne/materialne pravice se potem na podlagi navedenih predpostavk oceni v znesku 7.500 evrov (= 0,5 × 0,3 × 50.000 € = verjetnost, da bo kupec izdelek B kupil × 30-odstotni popust, ki velja kot stvarna pravica × redna prodajna cena izdelka B) in uporabi pri razdelitvi transakcijske cene pogodbe, kot je to prikazano v tabeli 14.[5]

Tabela 14: Razdelitev transakcijske cene med prodano blago in stvarno pravico iz naslova obljube popusta za dodatno blago in/ali storitve

Izvršitvena obveza	Zaračunana vrednost	Samostojna prodajna cena	Delež samostojne prodajne cene	Razdelitev transakcijske cene
Izdelek A	100.000 €	100.000 €	100.000 / 107.500 = 0,9302	0,9302 × 100.000 € = 93.020 €
Stvarna pravica	–	7.500 €	7.500 / 107.500 = 0,0698	0,0698 × 100.000 € = 6.980 €
SKUPAJ	100.000 €	107.500 €	1	100.000 €

Podjetje ob izdaji računa in prenosu obvladovanja izdelka A na kupca pripozna prihodke v višini 93.020 evrov, medtem ko za znesek 6.980 evrov iz naslova stvarne pravice pripozna pogodbeno obveznost, ki jo med prihodke prenese šele, ko je možnost za nakup izdelka B s popustom izkoriščena (a) ali pa poteče (b).

[5] Podjetju samostojne prodajne cene, ko je enkrat ocenjena, ni treba več ponovno ocenjevati (MSRP 15.88).

Tabela 15: Knjiženje popusta za dodatno blago in/ali storitve[6]

	Debet	**Kredit**
Kupec kupi izdelek A		
Terjatve do kupcev za izdelek A	100.000	
Prihodki od prodaje izdelka A		93.020
Pogodbena obveznost		6.980
a) Kupec kupi izdelek B s popustom		
Terjatve do kupcev za izdelek B	25.000	
Pogodbena obveznost	6.980	
Prihodki od prodaje izdelka B		31.980
b) Možnost nakupa izdelka B s popustom poteče		
Pogodbena obveznost	6.980	
Prihodki od prodaje izdelka A		6.980

Primer 10

Prejšnjemu primeru so vsebinsko podobni primeri, ko trgovci kupcem na blagajni poleg računa podarijo še kupon za popust ob naslednjem nakupu[7]. Če tak kupon prejmejo vsi kupci, neodvisno od vrednosti nakupa, potem ta po naši oceni ne predstavlja stvarne/materialne pravice. V takem primeru kupec, ki je na primer kupil za 1.000 evrov različnega blaga in prejel kupon za popust, s svojim nakupom ni pridobil nič večje ugodnosti ob prihodnjem nakupu kot kupec, ki je na primer kupil samo žvečilko za 50 centov in prejel enak kupon za popust ob prihodnjem nakupu. Ker sta oba pridobila enako ugodnost, to pomeni, da gre zgolj za formalno pogojenost popusta s sklenitvijo predhodnega posla, ne pa tudi stvarno. Popust je namreč na voljo tudi kupcem, ki pred tem s podjetjem sklenejo zgolj po obsegu ekonomsko zanemarljivo pogodbo, kar pomeni praktično vsem, ki to želijo. Kot pogoj za pridobitev pravice do popusta ob naslednjem nakupu je zato tak predhodni nakup ekonomsko nebistven in posledično na njegovi osnovi izdan kupon po naši oceni ne izpolnjuje pogojev MSRP 15.B40 za pripoznanje kot stvarna/materialna pravica.

---

6 Vsi primeri knjiženja v prispevku so zaradi večje preglednosti prikazani brez upoštevanja DDV-ja.

7 Odvisno od odločitve podjetja je tak popust lahko omejen samo na specificirano blago v pogodbi, ali pa ga kupec lahko uveljavi za katerokoli blago, ki ga podjetje prodaja. Takšni kuponi so običajno tudi časovno in/ali vrednostno omejeni, vendar to na ugotavljanje, ali jih pripoznamo kot stvarno/materialno pravico ali ne, nima vpliva. Na primer, kadar kupec na blagajni prejme kupon za 15-odstotni popust ob prihodnjem nakupu ali za vse prihodnje nakupe v obdobju enega meseca do njihove skupne vrednosti 1.000 evrov.

Pomembno drugačna pa je situacija, ko je podelitev kupona za popust neposredno odvisna od zneska kupčevega nakupa. Na primer, kadar ima podjetje vzpostavljen sistem, po katerem vsakemu kupcu, s katerim sklene pogodbo v vrednosti vsaj 100 evrov, pripada kupon za 15-odstotni popust ob naslednjem nakupu. Ker je ugodnost 15-odstotnega popusta omejena samo na kupce, ki s podjetjem pred tem sklenejo pogodbo v vrednosti vsaj 100 evrov, to pomeni, da vsak nakup v vrednosti vsaj 100 evrov vključuje tudi stvarno/materialno pravico iz naslova možnosti dodatnih nakupov po znižani ceni, za katero je po MSRP 15.B40 treba pripoznati ločeno izvršitveno obvezo in nanjo razporediti tudi del transakcijske cene takega nakupa. Da bi to naredili, mora podjetje najprej oceniti samostojno prodajno ceno stvarne/materialne pravice, pri tem pa upoštevati tako verjetnost, da bo kupec to pravico izkoristil, kakor tudi pričakovani znesek njene realizacije.

V konkretnem primeru sklene podjetje s kupcem pogodbo v vrednosti 130 evrov, na podlagi katere ta pridobi tudi kupon za 15-odstotni popust ob naslednjem nakupu. Na podlagi preteklih izkušenj podjetje ugotavlja, da je unovčenih približno 75 odstotkov vseh izdanih kuponov in da povprečna pogodba s kupcem znaša 50 evrov. Ker je kupec na podlagi svojega nakupa pridobil samo en kupon, to pomeni oceno pričakovanega popusta ob njegovem naslednjem nakupu v višini 5,63 evra (= 1 × 0,75 × 50 € × 0,15 = en kupon × 75-odstotna verjetnost njegove unovčitve × 50 € povprečnega nakupa × 15-odstotni popust). Ta vrednost se nato uporabi kot podlaga za razdelitev transakcijske cene pogodbe, kot je to prikazano v tabeli 16.[8]

Podjetje ob izdaji računa in prenosu pogodbenega blaga na kupca pripozna prihodke v višini 124,61 evra, medtem ko za znesek 5,39 evra iz naslova stvarne pravice pripozna pogodbeno obveznost, ki jo med prihodke prenese šele ob kupčevem naslednjem nakupu (a) ali ko poteče rok za njeno uveljavitev (b) (tabela 17).

[8] Podobno bi ravnali, če bi kupcu na podlagi sklenjene pogodbe pripadal 15-odstotni popust na vse prihodnje nakupe v določenem roku, navzgor omejeno do neke njihove izbrane maksimalne vrednosti. Razlika je le, da je v tem primeru kupon za 15-odstotni popust mogoče uporabiti za več prihodnjih nakupov, vendar največ do določenega maksimuma v enem mesecu. V takšnem primeru bi zato podjetje moralo oceniti skupno pričakovano vrednost kupčevih nakupov v obdobju veljavnosti kupona, vendar ne več od določenega maksimuma. Če podjetje to vrednost oceni na primer na 100 €, potem samostojna prodajna cena v pogodbi zajete stvarne pravice znaša 15 € (= 100 € × 0,15). Transakcijska cena pogodbe se razdeli na enak način, kot je prikazano v tabelah 14 in 16.

Tabela 16: Razdelitev transakcijske cene med prodano blago in stvarno pravico iz naslova obljube popusta za dodatno blago in/ali storitve

Izvršitvena obveza	Zaračunana vrednost	Samostojna prodajna cena	Delež samostojne prodajne cene	Razdelitev transakcijske cene
Blago	130 €	130 €	130 / 135,63 = 0,9585	0,9585 × 130 € = 124,61 €
Stvarna pravica	-	5,63 €	5,63 / 135,63 = 0,0415	0,0415 × 130 € = 5,39 €
SKUPAJ	130 €	135,63 €	1	130 €

Tabela 17: Knjiženje kupona za popust ob naslednjem nakupu

	Debet	Kredit
Kupec kupi blago v vrednosti 130 € in prejme kupon		
Denar v blagajni	130,00	
Prihodki od prodaje		124,61
Pogodbena obveznost		5,39
a) Kupec ob naslednjem nakupu v višini 50 € unovči kupon		
Denar v blagajni	42,50	
Pogodbena obveznost	5,39	
Prihodki od prodaje		47,89
b) Kupon poteče		
Pogodbena obveznost	5,39	
Prihodki od prodaje		5,39

V praksi so pogosti tudi primeri, ko podjetja kupcem namesto kuponov, kjer je popust opredeljen v odstotku od vrednosti prihodnjega nakupa (torej variabilno), podarijo vrednostni bon, kjer je popust opredeljen v fiksnem znesku. Na primer, ko na vsakih 100 evrov vrednosti nakupa kupec prejme bon v znesku 10 evrov, ki ga lahko porabi ob svojem naslednjem nakupu. Kar se tiče računovodenja takšnih pogodb, je to v celoti enako kot pri kuponih, le da je ocenjevanje njihove samostojne prodajne cene nekoliko lažje, saj je znesek realizacije fiksen, zato je treba oceniti samo še verjetnost, da bo kupec bon unovčil. Če tako na primer podjetje ob sklenitvi pogodbe kupcu podari bon za 10 evrov in ocenjuje, da je verjetnost njegove unovčitve 50-odstotna, to pomeni, da samostojna prodajna cena takšnega bona znaša 5 evrov (= 0,5 × 50 € = 50-odstotna verjetnost

unovčitve × nominalna vrednost bona). Vsi nadaljnji postopki računovodenja so enaki kot pri popustih v obliki kuponov.[9]

Posebna vrsta pogodb z možnostjo pridobitve dodatnega blaga in/ali storitev so tudi pogodbe s kupci, v katerih je popust kupca na dodatno blago in/ali storitve vezan na določeno minimalno vrednost njegovih prejšnjih nakupov. Tak je primer, ko podjetje vsem kupcem, ki v tekočem letu dosežejo neko vnaprej opredeljeno vrednost nakupov (tako imenovani mejnik), na vse njihove nadaljnje nakupe v istem letu odobri popust. Ker brez prejšnjih nakupov do določene vrednosti kupec popusta za dodatno blago in/ali storitve ne more prejeti, to pomeni, da vse pogodbe do tako določene (mejne) vrednosti nakupov vsebujejo tudi stvarno/materialno pravico za dodatne nakupe po znižani ceni, ki jo je treba za potrebe računovodenja prihodkov pripoznati kot ločeno izvršitveno obvezo teh pogodb in nanjo razporediti tudi del njihove transakcijske cene. Posebnost takega primera v primerjavi s predhodnimi je, da je tukaj pogoj za stvarno/materialno pravico določen kumulativno. Nakupi se seštevajo, dokler ne dosežejo vrednosti, od katere naprej kupcu pripada popust. Pa si to poglejmo na praktičnem primeru.

Primer 11

Podjetje vsem kupcem, ki v tekočem letu sklenejo več kot za 100.000 evrov pogodb, na vse dodatne pogodbe nudi popust v višini 10 odstotkov. Podjetje mora v takšnem primeru za vsakega posameznega kupca najprej oceniti skupno vrednost pogodb, ki naj bi jih po pričakovanjih z njim v tekočem letu sklenilo (na primer na podlagi svojih preteklih izkušenj s kupcem, informacij o načrtih kupca itd.). Brez tega namreč ni mogoče izračunati vrednosti popustov, ki naj bi mu po pričakovanjih pripadli.

Podjetje npr. za konkretnega kupca ocenjuje, da bo v tekočem letu z njim sklenilo skupaj za okoli 150.000 evrov prodajnih pogodb. Na tej osnovi lahko ugotovimo, da bo ta kupec, če se predpostavka o skupni vrednosti sklenjenih pogodb uresniči, v tekočem letu od podjetja dobil skupaj za 5.000 evrov popustov (= 0,1 × 50.000 € = 10-odstotni popust × vrednost pogodb preko 100.000 €). Tako izračunana samostojna prodajna cena stvarne/materialne pravice do dodatnega blaga in/ali

[9] Posebna različica pogodb s popusti v obliki bonov so tudi pogodbe, kjer kupci bonov na osnovi svojih nakupov ne prejemajo sproti, torej ob sklenitvi pogodbe, ampak jim podjetje tak bon podari na koncu nekega določenega obračunskega obdobja, na primer na koncu leta za preteklo leto. Če je znesek v fiksnem razmerju z vrednostjo sklenjene pogodbe, potem to, ali dobi bon na koncu ali sproti, ne vpliva na računovodenje. Če pa je znesek bona progresiven glede na obseg nakupov – več nakupov, večji odstotek popusta v obliki bona, potem mora podjetje ob sklenitvi vsake pogodbe za vsakega kupca posebej oceniti pričakovani obseg nakupov v obračunskem obdobju in na njegovi osnovi pričakovani skupni obseg popustov v obliki bonov (enako kot pri kuponih).

storitev po znižani ceni se nato uporabi kot osnova za razdelitev transakcijske cene začetnih 100.000 evrov pogodb, kot je to prikazano v tabeli 18.

Tabela 18: Razdelitev transakcijske cene med pogodbeno blago in/ali storitve in stvarno pravico iz naslova obljube popusta za dodatno blago in/ali storitve

Izvršitvena obveza	Zaračunana vrednost	Samostojna prodajna cena	Delež samostojne prodajne cene	Razdelitev transakcijske cene
Blago in/ali storitve	100.000 €	100.000 €	100.000 / 105.000 = 0,9524	0,9524 × 100.000 € = 95.240 €
Stvarna pravica	–	5.000 €	5.000 / 105.000 = 0,0476	0,0476 × 100.000 € = 4.760 €
SKUPAJ	100.000 €	105.000 €	1	100.000 €

Npr., prva pogodba, ki jo kupec sklene s podjetjem v tekočem letu, znaša 50.000 evrov. Ker to predstavlja natanko polovico vrednosti, potrebne za pridobitev popusta za dodatno blago in/ali storitve, bo v tem primeru podjetje na stvarno pravico razporedilo tudi polovico njene skupne ocenjene transakcijske cene za začetnih 100.000 evrov pogodb, kar znaša 2.380 evrov (= 0,5 × 4.760 € = 50 odstotkov izpolnjenega pogoja za pridobitev popusta × 4.760 € skupne ocenjene transakcijske cene stvarne pravice za začetnih 100.000 € pogodb). Preostanek transakcijske cene sklenjene pogodbe v višini 47.620 evrov odpade na prodano blago in/ali storitve (= 50.000 € – 2.380 €).

Podjetje ob izdaji računa in prenosu pogodbenega blaga in/ali storitev na kupca pripozna prihodke v višini 47.620 evrov, medtem ko za 2.380 evrov iz naslova stvarne pravice pripozna pogodbeno obveznost, ki jo med prihodke prenese šele ob sklenitvi pogodb s kupcem, ki presegajo njihovo kumulativno vrednost 100.000 evrov, določeno kot mejnik za pridobitev popustov. Ko kumulativna vrednost sklenjenih pogodb preseže mejo 100.000 evrov, se do takrat pripoznana pogodbena obveznost začne postopoma prenašati med prihodke, in sicer sorazmerno z napredovanjem kumulativne vrednosti realiziranih popustov do njihove celotne izhodiščno ocenjene vrednosti (tabela 19).

Tabela 19: Knjiženje količinskega popusta za dodatno blago in/ali storitve

	Debet	Kredit
Kupec sklene prvo pogodbo v vrednosti 50.000 €		
Terjatve do kupcev	50.000	
Pogodbena obveznost		2.380
Prihodki od prodaje		47.620
Kupec sklene drugo pogodbo v vrednosti 70.000 €		
Terjatve do kupcev (upoštevani popusti)	[a]68.000	
Pogodbena obveznost		[b]476 €
Prihodki od prodaje		68.476
Kupec sklene tretjo pogodbo v vrednosti 15.000 €		
Terjatve do kupcev (upoštevani popusti)	13.500	
Pogodbena obveznost	[c]1.428	
Prihodki od prodaje		14.928
Kupec sklene četrto pogodbo v vrednosti 30.000 €[10]		
Terjatve do kupcev (upoštevani popusti)	27.000	
Pogodbena obveznost	[d]1.428 €	
Prihodki od prodaje		28.428

[a] 50.000 € blaga in/ali storitev se zaračuna po polni ceni, preostalih 20.000 € pa z 10 odstotki popusta (= 18.000 €), saj je podjetje doseglo mejo 100.000 €, po kateri mu ta popust pripada.

[b] Kupec je s sklenitvijo druge pogodbe v znesku 70.000 € v celoti izpolnil pogoj kumulativno 100.000 € nakupov za pridobitev popustov na dodatno blago in/ali storitve (50.000 € + 70.000 € = 120.000 €). Posledično se na izvršitveno obvezo iz naslova te stvarne pravice razporedi še preostanek njene skupne ocenjene transakcijske cene v višini 2.380 € (glej tabelo 18). Vendar pa kupec s sklenitvijo druge pogodbe ni le izpolnil pogoja za pridobitev popustov, pač pa je za presežek te pogodbe preko postavljene meje 100.000 € že bil tudi upravičen do 10-odstotnega popusta. Pomeni, da je za 20.000 € svojih nakupov pravico že izkoristil in na tej osnovi pridobil 2.000 € popustov. Ker 2.000 € popustov predstavlja 40 odstotkov celotne izhodiščno ocenjene vrednosti popustov za tega kupca (= 2.000 € × 100 / 5.000 €), to pomeni, da je med prihodke treba prenesti tudi 40 odstotkov celotne pripoznane pogodbene obveznosti za te popuste, kar znese 1.904 € (= 0,4 × 4.760 €). Skupen učinek obeh vplivov na pogodbeno obveznost se kaže kot njeno povečanje za 476 € (= 2.380 € − 1.904 €).

[10] Če kupec do konca leta ne bi sklenil nobene pogodbe več, potem bi se ves preostanek pripoznane pogodbene obveznosti iz naslova te pogodbe v višini 1.428 € (= 2.380 € + 476 € − 1.428 €) v celoti prenesel med prihodke.

[c] 1.500 € popusta, ki ga je kupec dobil s sklenitvijo te pogodbe, predstavlja 30 odstotkov celotne izhodiščno ocenjene skupne vrednosti popustov za tega kupca (= 1.500 € × 100 / 5.000 €). Posledično se med prihodke prenese tudi 30 odstotkov celotne pripoznane obveznosti za te popuste, kar znese 1.428 € (= 0,3 × 4.760 €).

[d] 3.000 € popusta iz te pogodbe predstavlja 60 odstotkov celotne izhodiščno ocenjene vrednosti popustov za tega kupca (= 3.000 € / 5.000 €). Ker je kupec 70 odstotkov izhodiščno ocenjene vrednosti popustov že izkoristil (40 odstotkov s prvo pogodbo in 30 odstotkov z drugo), se med prihodke lahko prenese samo še preostanek pripoznane pogodbene obveznosti za te popuste (30 odstotkov), kar znaša 1.428 €.

Posebna različica prejšnjega primera so tudi tako imenovani količinski popusti, ko podjetja s kupci sklepajo pogodbe, v katerih je prodajna cena na enoto blaga ali storitve opredeljena variabilno. To pomeni, da velja osnovna cena do določene količine, ko pa kupec to količino preseže, je za vse nadaljnje nakupe upravičen do popusta. Računovodenje takšnih pogodb je načeloma enako kot v prejšnjem primeru, vendar z določenimi posebnostmi. Pa si to poglejmo na praktičnem primeru.

Primer 12

Podjetje ima npr. s kupcem sklenjeno pogodbo, po kateri znaša cena za prvih 1000 kosov izdelka v koledarskem letu 500 evrov za kos, za naslednjih 1000 kosov 480 evrov za kos in za vse nadaljnje kose 450 evrov za kos. Ker v pogodbi določen popust v višini 20 evrov za kos kupcu pripada le za več kot 1000 kosov, popust v višini dodatnih 30 evrov za kos pa za količine čez 2000 kosov, to pomeni, da vse pogodbe do kumulativno 2000 kosov predmetnega izdelka poleg kupljenega blaga vsebujejo tudi stvarno/materialno pravico za nakupe dodatnih enot enakega blaga po znižani ceni. Posledično je za vsako pogodbo do kumulativno 2000 kosov predmetnega izdelka poleg izvršitvene obveze za prodano blago treba pripoznati tudi ločeno izvršitveno obvezo za v pogodbi vsebovano stvarno/materialno pravico. Tudi tukaj je za pravilno računovodenje tako ugotovljene stvarne/materialne pravice treba najprej oceniti njeno samostojno prodajno ceno, vendar v primerjavi s predhodnimi primeri takšna pogodba vsebuje nekaj posebnosti, ki jih je pri tem treba upoštevati.

Podjetje npr. za konkretnega kupca ocenjuje, da bo v koledarskem letu kupil skupaj 3000 kosov navedenega izdelka. Iz tega lahko izračunamo, da bo skupaj po pričakovanjih od podjetja prejel za 70.000 evrov količinskih popustov; za prvih 1000 kosov nič, za drugih 1000 kosov 20.000 evrov (= 1000 × 20 €) in za zadnjih 1000 kosov 50.000 evrov (= 1000 × 50 €). Standard za primere, ko je dodatno blago enako ali podobno blagu iz pogodbe, dovoljuje dva alternativna pristopa

računovodenja. Poleg že predstavljenega splošnega modela (ocena samostojne prodajne cene stvarne pravice) še alternativnega (tako imenovano dovoljeno alternativo iz MSRP 15.B43), po katerem podjetje prihodke za vse pričakovane enote prodanega izdelka pripozna po enaki (povprečni) ceni. V nadaljevanju podrobneje prikazujemo računovodenje za obe alternativni možnosti. Knjigovodenje je za obe alternativi prikazano skupaj v tabeli 22.

a) Splošni model

Ker konkretna pogodba popuste povezuje s količino, in sicer popust 20 evrov za kos, ko je dosežena količinska meja 1000 kosov, in popust dodatnih 30 evrov za kos, ko je dosežena količina 2000 kosov, to pomeni, da samostojna prodajna cena stvarne/materialne pravice v pogodbah za prvih 1000 kosov izdelka (prvi količinski mejnik) ni enaka samostojni prodajni ceni stvarne/materialne pravice v pogodbah za drugih 1000 kosov izdelka (druga količinska meja). Posledično je zato treba ti dve samostojni prodajni ceni oceniti ločeno.[11]

Ker kupcu, ko je dosežena prva količinska meja 1000 kosov izdelka, pripada zgolj popust v višini 20 evrov za vse nadaljnje kose, pomeni, da od skupaj pričakovanih popustov v višini 70.000 evrov samo 40.000 evrov (= 2000 kosov izdelka s popustom × 20 € popusta za kos) odpade na stvarno/materialno pravico v pogodbah za prvih 1000 kosov izdelka, preostanek v višini 30.000 evrov pa se nanaša na stvarno/materialno pravico v pogodbah tega izdelka za drugih 1000 kosov. Posledično to pomeni tudi ločeno razdelitev transakcijske cene za ene in druge, kot je to prikazano v tabelah 20 in 21.

Tabela 20: Razdelitev transakcijske cene med pogodbeno blago in stvarno pravico za prvih 1000 kosov sklenjenih pogodb

Izvršitvena obveza	Zaračunana vrednost	Samostojna prodajna cena	Delež samostojne prodajne cene	Razdelitev transakcijske cene
Blago	500.000 €	500.000 €	500.000/540.000 = 0,9259	0,9259 × 500.000 € = 462.950 €
Stvarna pravica	–	40.000 €	40.000/540.000 = 0,0741	0,0741 × 500.000 € = 37.050 €
SKUPAJ	500.000 €	540.000 €	1	500.000 €

[11] Če bi bilo še več takih količinskih mej, bi bilo potrebnih še več ločenih ocen samostojnih prodajnih cen ugotovljene stvarne/materialne pravice, in sicer za vsako količinsko mejo posebej.

Tabela 21: Razdelitev transakcijske cene med pogodbeno blago in stvarno pravico za drugih 1000 kosov sklenjenih pogodb

Izvršitvena obveza	Zaračunana vrednost	Samostojna prodajna cena	Delež samostojne prodajne cene	Razdelitev transakcijske cene
Blago	480.000 €[12]	480.000 €	480.000 / 510.000 = 0,9412	0,9412 × 480.000 € = 451.776 €
Stvarna pravica	-	30.000 €	30.000 / 510.000 = 0,0588	0,0588 × 480.000 € = 28.225 €
SKUPAJ	480.000 €	510.000 €	1	480.000 €

Kupec npr. prvo pogodbo v tekočem letu sklene za 600 kosov predmetnega izdelka. Ker s tem meja za količinski popust še ni dosežena, kupcu ne pripada še noben popust. Transakcijska cena te pogodbe zato znaša 300.000 evrov (= 600 kosov × 500 € za kos). Vendar pa pogodba že vsebuje stvarno/materialno pravico iz naslova možnosti za dodatne izdelke po znižani ceni, saj podjetje ocenjuje, da bo kupec kumulativno v koledarskem letu presegel mejo, postavljeno za pridobitev količinskih popustov. S sklenitvijo konkretne pogodbe za 600 kosov je tako kupec izpolnil 60 odstotkov (= 600 kosov/1000 kosov) količinske meje za pridobitev popusta v višini 20 evrov za kos. Zato se del transakcijske cene te pogodbe v višini 22.230 evrov (= 0,6 × 37.050 €[13]) razporedi na stvarno/materialno pravico za dodatne izdelke po znižani ceni, medtem ko se na prodane izdelke razporedi ves preostanek v višini 277.770 evrov (= 300.000 € − 22.230 €). Prihodki za prodane izdelke se v višini 277.770 evrov pripoznajo, ko so ti preneseni na kupca, medtem ko se prihodki iz naslova stvarne/materialne pravice pripoznajo, ko je ta s prihodnjimi nakupi čez 1000 kosov realizirana ali pa poteče.

Denimo, da kmalu za prvo kupec sklene še drugo pogodbo v tekočem letu, in sicer tokrat za 700 kosov. V tem primeru je transakcijska cena pogodbe sestavljena iz 400 kosov po polni ceni 500 evrov za kos in preostalih 300 kosov po znižani ceni 480 evrov za kos, saj ti kosi že presegajo količinsko mejo 1000 kosov, pogodbeno določeno kot pogoj za pridobitev popusta 20 evrov za kos. Skupaj torej transakcijska cena pogodbe znaša 344.000 evrov (= 400 kosov × 500 € za kos + 300 kosov × 480 € za kos). Tudi ta pogodba vsebuje stvarno/materialno pravico, saj je kupec z njo izpolnil preostalih 40 odstotkov (= 400 kosov/1000 kosov) meje za količinski popust v višini 20 evrov za kos, in dodatno še 30 odstotkov (= 300

[12] Transakcijska cena za drugih 1000 kosov je zaradi popusta 20 € za kos nižja kot za prvih 1000 kosov.

[13] Skupna ocenjena transakcijska cena stvarne pravice v pogodbah za prvih 1000 kosov izdelka (prva količinska meja).

kosov/ 1000 kosov) meje za dodatni količinski popust 30 evrov za kos. Posledično se del transakcijske cene te pogodbe v višini 23.287,50 evrov (= 0,4 × 37.050 € + 0,3 × 28.225 €) razporedi na stvarno/materialno pravico za popuste, medtem ko se na prodane izdelke razporedi ves preostanek v višini 320.712,50 € (= 344.000 € – 23.287,50 €). Prihodki za prodane izdelke se v višini 320.712,50 evrov pripoznajo, ko so ti preneseni na kupca, medtem ko se prihodki iz naslova stvarne/materialne pravice pripoznajo, ko je ta s prihodnjimi nakupi realizirana ali pa poteče.

Poleg tega se ob prenosu obvladovanja zadnjih 300 kosov izdelka na kupca[14] pripoznajo še prihodki iz naslova delne realizacije stvarne/materialne pravice za popust 20 evrov za kos, saj je teh 300 kosov kupec že prejel po znižani ceni 480 evrov namesto prvotnih 500 evrov. To pomeni, da je bila stvarna pravica do tega popusta že realizirana v obsegu 15 odstotkov (= 300 kosov / 2000[15] kosov), kar znese 5.557,50 evra (= 0,15 × 37.050 €), ki se iz pogodbene obveznosti prenesejo med prihodke. Smiselno enako se računovodijo tudi vse nadaljnje pogodbe, dokler ni stvarna/materialna pravica ali v celoti realizirana ali poteče. Knjiženje celotnega primera je prikazano v tabeli 22.

Kot se iz primera lepo vidi, je lahko računovodenje prospektivnih količinskih popustov po splošnem modelu precej zapleteno, kadar obstaja več možnih višin popusta. MSRP 15 zato dopušča tudi alternativno možnost, ki je v osnovi precej preprostejša, vendar pa omejena samo na določene primere. MSRP 15.B43 določa naslednje: *"Če ima kupec stvarno pravico do pridobitve prihodnjega blaga ali storitev ter so to blago ali storitve podobni prvotnemu blagu ali storitvam iz pogodbe ter se zagotavljajo v skladu s pogoji prvotne pogodbe, lahko podjetje kot praktično alternativo ocenjevanju samostojne prodajne cene opcije dodeli transakcijsko ceno blagu ali storitvam iz možnosti na podlagi blaga ali storitve, ki naj bi se zagotovile, in pričakovanega nadomestila. Običajno tovrstne možnosti veljajo za obnavljanje pogodbe."* Pa si poglejmo na praktičnem primeru, kaj konkretno to pomeni.

[14] To so tisti, ki v drugi pogodbi že presegajo prvo količinsko mejo 1000 kosov.

[15] Stvarna/materialna pravica, vsebovana v pogodbah za prvih 1000 kosov izdelka (20 € popusta na enoto), se nanaša na vseh preostalih 2000 kosov, ki naj bi jih kupec po pričakovanju še kupil v tekočem letu.

b) Dovoljena alternativa

Uporaba dovoljene alternative iz MSRP 15.B43 pomeni, da podjetje prihodke za vse pričakovane enote prodanega izdelka pripozna po enaki (povprečni) ceni. Ker podjetje pričakuje, da bo skupaj prodalo 3000 kosov izdelkov, pri čemer bo kupcu obračunalo skupaj za 70.000 evrov količinskih popustov, to pomeni, da pričakovani povprečni popust na enoto izdelka znaša 4,67 odstotka (= 70.000 € × 100 / 1,500.000 €). Ocenjena povprečna prodajna cena za izdelek tako znaša 476,67 evra (= 500 € − 0,0467 × 500 €).[16]

Ob sklenitvi prve pogodbe za 600 kosov izdelkov to pomeni pripoznanje 286.000 evrov prihodkov (= 600 kosov × 476,67 €). Ker ob sklenitvi te pogodbe kupec še ni upravičen do nobenega popusta, se transakcijska cena te pogodbe pripozna v polni vrednosti, torej brez popustov, kar znaša 300.000 evrov (= 600 kosov × 500 €). Presežek transakcijske cene nad pripoznanimi prihodki v višini 14.000 evrov se pripozna kot pogodbena obveznost iz naslova stvarne/materialne pravice kupca do dodatnih izdelkov po znižani ceni, ko bo dosegel za to postavljeno količinsko mejo.

Ob sklenitvi naslednje pogodbe za 700 kosov bo podjetje ravnalo enako in prihodke pripoznalo v višini 333.667 evrov (= 700 kosov × 476,67 €). Transakcijska cena pogodbe v tem primeru znaša 344.000 evrov (= 400 kosov × 500 € + 300 kosov × 480 €). Presežek transakcijske cene nad pripoznanimi prihodki sedaj znaša 10.333 evrov (= 344.000 € − 333.667 €) in se prav tako pripozna kot povečanje pogodbene obveznosti iz naslova stvarne/materialne pravice kupca do dodatnih izdelkov po znižani ceni.

Ko podjetje sklene tretjo pogodbo za 1000 kosov, ponovno pripozna prihodke po ceni 476,67 evra za kos, kar znese 476.667 evrov. Transakcijska cena tretje pogodbe je tokrat nižja od pripoznanih prihodkov in znaša 471.000 evrov (= 700 kosov × 480 € + 300 kosov × 450 €). Presežek pripoznanih prihodkov nad transakcijsko ceno v višini 5.667 evrov (= 476.667 € − 471.000 €) se zato pripozna kot zmanjšanje pogodbene obveznosti iz naslova stvarne/materialne pravice kupca do dodatnih izdelkov po znižani ceni.

Ko podjetje sklene četrto pogodbo za 1000 kosov, je z njo preseglo izhodiščno ocenjeni obseg prodaje temu kupcu, s tem pa tudi izhodiščno ocenjeno skupno transakcijsko ceno za ta obseg; za 3000 kosov je bila ocenjena na 1.430.000

[16] Do enakega rezultata pridemo tudi, če celotno ocenjeno transakcijsko ceno za 3000 kosov v višini 1.430.000 € preračunamo na enoto izdelka (= 1.430.000 € / 3000 kosov).

evrov, medtem ko sklenitev četrte pogodbe za 1000 kosov pomeni 300 kosov oziroma 135.000 evrov več od izhodiščno predvidenih. To posledično pomeni, da začetna ocena povprečne prodajne cene za obravnavane izdelke za obravnavanega kupca ni bila prava, zato jo je treba izračunati na novo, hkrati pa ustrezno popraviti tudi že pripoznane prihodke. Podjetje mora pri tem na novo oceniti pričakovani obseg prodaje kupcu za tekoče leto. Denimo, da ga oceni na skupaj 4000 kosov. Ocenjena transakcijska cena za teh 4000 kosov znaša 1.880.000 evrov (1.430.000 € za izhodiščno predvidenih 3000 kosov plus 450.000 € za dodatnih 1000 kosov po novi oceni). Povprečna prodajna cena na tej osnovi znaša 470 evrov (= 1,880.000 € / 4000 kosov).

Podjetje prihodke za četrto pogodbo pripozna v višini 470.000 evrov. Vendar pa mora ta znesek popraviti še za preveč pripoznane prihodke iz predhodnih pogodb. Pred spremembo ocenjene povprečne cene je bilo obračunanih za 2300 kosov prihodkov po povprečni ceni 476,67 evra, kar pomeni 1.096.333 evrov prihodkov. Ker je na novo ocenjena povprečna cena nižja, to pomeni za 15.333 evrov preveč pripoznanih prihodkov (= 1.096.333 – 2300 kosov $\times$ 470 €). Podjetje bo zato za četrto pogodbo pripoznalo za toliko manj prihodkov, kar znese 454.667 evrov (= 470.000 € $-$ 15.333 €).[17] Ker pripoznani prihodki presegajo transakcijsko ceno pogodbe, se ta razlika v višini 4.667 evrov pripozna kot zmanjšanje pogodbene obveznosti.

Če kupec s podjetjem do konca leta ne sklene več nobene pogodbe, potem se preostanek pogodbene obveznosti iz naslova te pogodbe v višini 14.000 evrov (= 14.000 € + 10.333 € $-$ 5.667 € $-$ 4.667 €) v celoti prenese med prihodke.

[17] Podjetje mora, če uporablja takšno alternativno rešitev, na vsak datum poročanja preveriti, ali izhodiščne predpostavke, na katerih temelji izračunana povprečna cena, še držijo, in po potrebi svoje izračune ter na njihovi osnovi pripoznane prihodke in pogodbeno obveznost ustrezno popraviti (navzgor ali navzdol).

Tabela 22: Knjiženje količinskega popusta za dodatno blago in/ali storitve

	Splošni model		Dovoljena alternativa	
	Debet	**Kredit**	**Debet**	**Kredit**
Kupec sklene 1. pogodbo za 600 kosov				
Terjatve do kupcev	300.000		300.000	
Pogodbena obveznost		22.230		14.000
Prihodki od prodaje		277.770		286.000
Kupec sklene 2. pogodbo za 700 kosov				
Terjatve do kupcev	344.000		344.000	
Pogodbena obveznost		[a]22.730 €		10.333
Prihodki od prodaje		321.270		333.667
Kupec sklene 3. pogodbo za 1000 kosov				
Terjatve do kupcev	[b]471.000		471.000	
Pogodbena obveznost	[c]7.235		5.667	
Prihodki od prodaje		478.235		476.667
Kupec sklene 4. pogodbo za 1000 kosov				
Terjatve do kupcev	450.000		450.000	
Pogodbena obveznost	[d]37.725 €		4.667	
Prihodki od prodaje		487.725		454.667
Zaključek koledarskega leta (potek obdobja veljavnosti popustov)				
Pogodbena obveznost			14.000	
Prihodki od prodaje				14.000

[a] Ob sklenitvi druge pogodbe je bilo pripoznano za 23.287,50 € dodatne pogodbene obveznosti. Hkrati je bilo zaradi delne realizacije stvarne pravice med prihodke preneseno za 5.557,50 € te obveznosti. Skupni učinek je torej povečanje pogodbene obveznosti za 22.730 € (= 23.287,50 € − 5.557,50 €).

[b] 700 kosov × 480 € + 300 kosov × 450 €.

[c] Ob sklenitvi tretje pogodbe podjetje izpolni preostalih 70 odstotkov količinske meje za dodatni popust 30 € za kos, kar pomeni pripoznanje dodatnih 19.757,50 € pogodbene obveznosti (= 0,7 × 28.225 €). Hkrati zaradi delne realizacije stvarne pravice za popuste med prihodke prenese 26.992,50 € te obveznosti. In sicer 18.525 € iz naslova delne realizacije popustov 20 € za kos (= 50-odstotna realizacija stvarne pravice × 37.050 €) in 8.467,50 € iz naslova delne realizacije popustov za dodatnih 30 € za kos (= 30-odstotna realizacija stvarne pravice × 28.225 €). Skupni učinek obeh vplivov je torej zmanjšanje pogodbene obveznosti za 7.235 € (= 19.757,50 € − 26.992,50 €).

[d] Ker je kupec s sklenitvijo četrte pogodbe presegel 3000 kosov izhodiščno ocenjenega skupnega obsega pogodb (prva pogodba 600 kosov + druga pogodba 700 kosov + tretja pogodba 1000 kosov + četrta pogodba 1000 kosov = 3300 kosov), to pomeni, da je v celoti izkoristil tudi pripoznane stvarne pravice za količinske popuste. Posledično se zato preostanek iz tega naslova pripoznane pogodbene obveznosti v celoti prenese med prihodke.

3. ZAKLJUČEK

Ena večjih novosti, ki jih v računovodenje prihodkov prinaša novi MSRP 15 v primerjavi s prejšnjim, se nanaša na računovodenje pogodb, ki poleg blaga in/ali storitev, ki so predmet kupčevega nakupa, vsebujejo še obljube podjetja kupcu, da lahko pridobi dodatno blago in/ali storitve s popustom. Kadar takšne obljube kupcu dajejo stvarno/materialno pravico, jih je treba po določilih novega standarda pripoznati kot ločene izvršitvene obveze in nanje razporediti tudi del skupne transakcijske cene takšne pogodbe. MRS 18 podobnih določil/zahtev ni imel, zato menimo, da gre za veliko novost, ki bo v več pogledih pomembno vplivala tako na obstoječe prakse podjetij v zvezi z računovodenjem prihodkov kakor tudi na njihove izide. Vsekakor pričakujemo, da bo računovodenje pogodb s tovrstnimi obljubami postalo bistveno bolj zapleteno, kot je bilo doslej.

Glavne izvedbene izzive novega standarda vidimo predvsem v ugotavljanju, ali neka obljuba za pridobitev dodatnega blaga in/ali storitev s popustom predstavlja stvarno/materialno pravico, za katero je treba pripoznati ločeno izvršitveno obvezo, ali ne. V marsikaterem primeru bo izziv ugotoviti, kakšna je prava samostojna prodajna cena takšne izvršitvene obveze, kakor tudi, kdaj pripoznati prihodke iz njenega naslova. Glede vpliva na izide lahko pričakujemo, da bo v prihodnje del transakcijske cene, ki se nanaša na ugotovljeno stvarno/materialno pravico kupca do popusta za dodatno blago in/ali storitve, med prihodki pripoznan kasneje kot doslej.

Glavna prednost, ki jo v zvezi z računovodenjem popustov vidimo v novem standardu, je, da njegove rešitve puščajo manj prostora za manipulacije v obliki sklepanja pogodb s povišanimi cenami pred datumom poročanja in vnaprej dogovorjenimi popusti po tem datumu (zaradi načrtnega/ciljnega uravnavanja poslovnega izida).

4. LITERATURA IN VIRI

1. Accounting Judgments on Terms of Likelihood in IFRS: Korea and Australia: KASB Research Report No.39 / AASB Research Report No.2. (2016). Najdeno na naslovu http://www.aasb.gov.au/admin/file/content102/c3/July_2016_(KASB-AASB)%20Accounting%20Judgments%20on%20Terms%20of%20Likelihood%20in%20IFR....pdf.

2. IFRS 15 Revenue from Contracts with Customers: A closer look at the new revenue recognition standard. Ernst & Young. (2016). Najdeno na naslovu http://www.ey.com/Publication/vwLUAssets/EY-Apply-RevRec-Update-Sept2016/$File/EY-Apply-RevRec-Update-Sept2016.pdf.
3. MSRP 15 (2016). Najdeno na naslovu http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R1905.
4. Revenue from contracts with customers. PricewaterhouseCoopers. (2017). Najdeno na naslovu https://www.pwc.com/us/en/cfodirect/assets/pdf/accounting-guides/pwc-revenue-recognition-global-guide.pdf.
5. Revenue Issues In-Depth. KPMG. (2016). Najdeno na naslovu https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/IFRS-practice-issues-revenue.pdf.

Skladnost pogodbe o revidiranju z določbami uredbe GDPR

IZ PRAKSE ZA PRAKSO (PR-REV 5-5/18)

Revizijski svet je na svoji seji pojasnil stališče glede skladnosti pogodbe o revidiranju z določbami uredbe GDPR.

IZHODIŠČE

Revizijska družba mora v skladu z zahtevami ZRev-2 kot zaupne varovati vse podatke, dejstva in okoliščine, za katere je izvedela pri opravljanju revidiranja, razen v primerih, kjer zakon določa drugače. Varovanje zaupnosti podatkov se nanaša tudi na vse osebne podatke, s katerimi se seznani med revidiranjem. Revizijska družba ni zavezana k dolžnosti varovanja zaupnih podatkov zgolj v primerih iz 4. odst. 38. člena ZRev-2.

Ne glede na to določbo pa je treba v zvezi z varovanjem in predvsem ravnanjem z osebnimi podatki pri revizijski družbi spoštovati tudi uredbo GDPR in drugo zakonodajo, ki se nanaša na varovanje osebnih podatkov.

Revizijska družba v skladu z zakonskimi pooblastili pri revidiranju računovodskih izkazov deluje kot upravljavec osebnih podatkov, saj:

- pridobiva in uporablja osebne podatke v svojem imenu in za svoj račun;
- izhaja podlaga za obdelavo osebnih podatkov, pridobljenih pri naročniku revidiranja, iz Zakona o revidiranju;
- pri opravljanju revidiranja ni odvisna od navodil naročnika revidiranja.

Zaradi narave dela ima vpogled oziroma zbira osebne podatke fizičnih oseb, ki so zaposlene pri naročniku revidiranja (revidirancu) ali druge z njim povezane fizične osebe, na primer člani organov upravljanja, kupci proizvodov in storitev, zato mora pri opravljanju revizije upoštevati vse zahteve zakonodaje, ki se nanašajo na upravljavca osebnih podatkov.

V skladu z uredbo GDPR imajo posamezniki v zvezi z zbranimi osebnimi podatki posamezne pravice, ki so jih dolžni zagotavljati upravljavci osebnih podatkov (torej tudi revizijske družbe). Ključne pravice posameznikov po uredbi so:

- pravica do dostopa do njegovih osebnih podatkov,
- pravica do popravka,
- pravica do izbrisa,
- pravica do omejitve uporabe,
- pravica do prenosljivosti podatkov,
- pravica do ugovora,
- pravica do pritožbe nadzornemu organu.

Revizijska družba zagotavlja te pravice, upoštevajoč značilnosti in namen izvajanja revidiranja, zato v posameznih primerih posameznik ni upravičen do uveljavljanja vseh navedenih pravic.

Dolžnost revizijske družbe je, da pri obdelavi osebnih podatkov zagotovi ustrezne tehnične in organizacijske ukrepe ter nemudoma obvesti posameznika in nadzorni organ o vseh varnostnih incidentih, ki so se pri tem zgodili.

Na podlagi predstavljenega izhodišča je bila sprejeta naslednja strokovna razlaga.

STROKOVNA RAZLAGA

Upoštevaje dejstvo, da je revizijska družba, ko izvaja revidiranje računovodskih izkazov, upravljavec osebnih podatkov in osebne podatke obdeluje pri izpolnjevanju zakonskih in pogodbenih obveznosti, Revizijski svet Slovenskega inštituta za revizijo meni, da je v pogodbe o revidiranju računovodskih izkazov koristno vključiti naslednje določbe:

"Naročnik bo revizijski družbi posredoval vse podatke in informacije, ki jih bo ta zahtevala za izvedbo revidiranja, vključno z osebnimi podatki posameznikov, s katerimi razpolaga."

"Pri ravnanju z osebnimi podatki posameznikov bo revizijska družba ravnala v skladu z uredbo GDPR in drugo veljavno zakonodajo s področja varstva osebnih podatkov in izpolnjevala vse svoje obveznosti kot samostojni upravljavec osebnih podatkov."

Razmerje med investicijami in amortizacijo v Gordonovem modelu rasti

IZ PRAKSE ZA PRAKSO (PR-OV 5-5/18)

Problematiko razmerja med investicijami in amortizacijo v izračunu preostale vrednosti s pomočjo Gordonovega modela je obravnaval Odbor sekcije pooblaščenih ocenjevalcev vrednosti in v tej zvezi sprejel naslednjo strokovno razlago.

IZHODIŠČE

Pooblaščeni ocenjevalci vrednosti podjetij se pri svojem delu pogosto srečujejo z dilemo, povezano z razmerjem med investicijami in amortizacijo pri oceni preostale (rezidualne) vrednosti podjetja s pomočjo Gordonovega modela rasti. Najpogosteje pri tem ocenjevalci vrednosti ocenijo normalizirani prosti denarni tok, ki ga vključijo v izračun preostanka vrednosti tako, da izenačijo vrednost amortizacije in investicij. Na odbor sekcije pooblaščenih ocenjevalcev vrednosti je bilo naslovljeno vprašanje, ali je pri izračunu preostale vrednosti primerno, da pri oceni normaliziranega prostega denarnega toka v preostanku vedno izenačimo vrednost investicij in amortizacije.

Na podlagi zastavljenega vprašanja je bila sprejeta naslednja strokovna razlaga.

STROKOVNA RAZLAGA

Pri ocenjevanju vrednosti podjetij po metodi pričakovanih prostih neto denarnih tokov je ustreznost ocene vrednosti močno odvisna od ustreznosti ocene preostale vrednosti podjetja, ki jo najpogosteje ocenjujemo s pomočjo Gordonovega modela rasti. Preostala vrednost v večini primerov predstavlja pomemben delež celotne ocenjene vrednosti (v povprečju dosega okoli 70 % (ali več) celotne ocenjene vrednosti kapitala podjetij), zato je za ustreznost ocene vrednosti pomembno, da so finančni parametri, ki vstopajo v Gordonov model rasti, ustrezno ocenjeni, vsebinsko povezani in v medsebojnih ustreznih razmerjih. Pri določanju teh parametrov se zelo pogosto pojavljata napaki, ki lahko pomembno vplivata na ocenjeno vrednost:

- *ocenjevalci določijo neustrezno razmerje med rastjo normaliziranega prostega denarnega toka ter amortizacijo in investicijami;*
- *ocenjevalci v preostanek neustrezno vključijo amortizacijo, ki izhaja iz neopredmetenih sredstev z omejeno dobo koristnosti.*

Razmerje med amortizacijo in investicijami

Ocena vrednosti preostanka, ki temelji na predpostavki, da je v okviru normaliziranega denarnega toka amortizacija enaka investicijam, lahko velja samo v razmerah, v katerih ni inflacije (če načrtujemo v nominalnih kategorijah), ter v razmerah, v katerih ne načrtujemo rasti (g) normaliziranega prostega denarnega toka.

Pri ocenjevanju vrednosti podjetij se v praksi zelo pogosto uporablja poenostavljena predpostavka, da je projicirana amortizacija v preostanku enaka amortizaciji iz zadnjega leta natančnega načrtovanja, tej pa je enaka tudi normalizirana vrednost investicijskih vlaganj (CAPEX). Takšna predpostavka je teoretično sporna že zaradi različnega vpliva, ki ga ima inflacija na oba parametra. Investicije v opredmetena sredstva se v računovodske izkaze knjižijo po nabavni vrednosti in se v času dobe koristnosti praviloma ne prilagajajo (prevrednotujejo) inflaciji, kar pomeni, da amortizacija, ki jo za ta sredstva skozi leta obračunavamo, praviloma ne vključuje inflacijskih učinkov. Po drugi strani se investicije v opredmetena osnovna sredstva izvajajo v časovni kontinuiteti in je njihova višina (tudi) pod vplivom inflacijskih gibanj na trgu opredmetenih osnovnih sredstev. Skozi leta se dispariteta med investicijami in amortizacijo zaradi neenakega vpliva inflacije poveča, in to praviloma tako, da so investicijska vlaganja višja od obračunane amortizacije. Ta dispariteta vpliva na davčni ščit, preko njega na prosti denarni tok in s tem na vrednost podjetja.

Višina investicij v opredmetena osnovna sredstva mora biti v neposredni povezavi z rastjo podjetja. Rast podjetja je odvisna od več dejavnikov: od dejavnosti, v kateri podjetje posluje, ter razvojne faze, v kateri se podjetje nahaja. V splošnem velja, da so projicirane investicije višje od amortizacije v hitro rastočih dejavnostih ter v podjetjih, ki se nahajajo v fazi hitre rasti poslovanja. Razlika med potrebnimi investicijami, ki podpirajo pričakovano rast, ter obračunano amortizacijo se praviloma začne zmanjševati, ko podjetje vstopi v zrelo fazo razvoja, ali pa, ko se umiri rast dejavnosti, v kateri podjetje deluje. V tovrstnih primerih je neustrezno predpostavljati, da bodo investicije v preostanku poenostavljeno enake višini obračunane amortizacije.

Razlike med višino investicij in amortizacijo se pojavljajo tudi pri podjetjih, ki imajo dolgotrajne investicijske cikluse. V takšnih primerih obdobjem pospešenega

investiranja, ko vrednost investicij močno presega vrednost amortizacije, sledijo obdobja, ko vrednost amortizacije močno presega vrednost investicij. V takih primerih je priporočljivo, da ocenjevalci vrednosti pri svojem delu uporabijo večfazne modele rasti, ali pa obdobje podrobnejšega načrtovanja podaljšajo, tako da zajamejo celoten investicijski ciklus podjetja, kar jim tudi omogoči, da v oceno preostanka lahko vključijo normirane vrednosti obeh omenjenih elementov prostega denarnega toka.

Ko imamo opravka z ocenjevanjem preostale vrednosti s pomočjo Gordonovega modela rasti, je ena izmed ključnih predpostavk, o katerih se moramo ocenjevalci opredeliti, višina rasti prostega denarnega toka (g), ki jo v Gordonovem modelu projiciramo v neskončnost. Prosti denarni tok podjetja lahko v večini primerov v neskončnost raste samo pod predpostavko, da so načrtovane investicije v opredmetena sredstva višje od amortizacije.

Formula za Gordonov model je:

$$TV = FCF\,(1 + g) / (r - g)$$

Kjer je:

TV = preostala vrednost
FCF = prosti denarni tok
g = stopnja rasti FCF
r = diskontna stopnja

Poglejmo si primer razmerja med investicijami in amortizacijo ob predpostavki, da bodo podjetje in investicije rastle po stopnji 5 % letno.

Slika 1: Razmerje med investicijami in amortizacijo ob predpostavki 5-% letne rasti

Leto	*Investicije 5-% rast*	*Am stopnja v %*	*Obračun Am v l. 2018*
2013	*1.000*	*10 %*	*100*
2014	*1.050*	*20 %*	*210*
2015	*1.103*	*20 %*	*221*
2016	*1.158*	*20 %*	*232*
2017	*1.216*	*20 %*	*243*
2018	***1.276***	*10 %*	*128*
		Skupaj	***1.133***

$I_{2018} = 1.276 > Am_{2018} = 1.133$

$\$ (Am_{2018} / I_{2018}) = -11{,}2\ \%$

Iz prikazanega primera je razvidno, da je ob predpostavki 5-% rasti obračunana amortizacija v 6. letu za 11,2 % nižja od vrednosti investicij. Razlika narašča z dolžino obdobja in naraščanjem pričakovane rasti. Če bi raziskovali razmerje med investicijami in obračunano amortizacijo ob predpostavki 15-letne pričakovane življenjske dobe opredmetenih osnovnih sredstev ter pričakovani 2-% stopnji rasti denarnega toka in investicij, bi razlika med investicijami in amortizacijo po 15 letih znašala 14 %, če pa bi bila pričakovana rast 5-%, bi razlika narastla na 38 %.

Iz prikazanega je razvidno, da morajo ocenjevalci vrednosti, ki svoje ocene vrednosti utemeljujejo na Gordonovem model rasti, razmerju med investicijami in amortizacijo v preostalem normiranem prostem denarnem toku posvetiti bistveno več pozornosti. Hkrati morajo svoje izbrane predpostavke ustrezno utemeljiti, predvsem pa morajo ohraniti ekonomsko logična razmerja med parametri, ki vstopajo v izračun preostanka.

Neustrezno načrtovanje amortizacije, ki izhaja iz neopredmetenih sredstev z omejeno končno dobo koristnosti

Kadar ocenjujemo podjetja, kjer pomemben del amortizacije izhaja iz neopredmetenih sredstev, lahko ta del amortizacije pomembno vpliva na izračun normaliziranega denarnega toka ter s tem neposredno na samo višino ocenjene vrednosti. Glede na to, da se amortizacija, ki izhaja iz neopredmetenih sredstev (po davčnem statusu, dobi koristnosti, potrebi po reinvestiranju ipd.), pomembno razlikuje od amortizacije opredmetenih sredstev, je smiselno in priporočljivo, da se obračun amortizacije neopredmetenih sredstev izvede ločeno od obračuna preostale amortizacije. Pri tem se ga pri izračunu preostale vrednosti izloči iz ocene normaliziranega denarnega toka in se ga k vrednosti podjetja doda kot ločeno ocenjeno postavko vrednosti. To je smiselno, ker so nekatera neopredmetena sredstva pogosto enkratnega značaja, iz česar izhaja, da reinvestiranje v njihovo obnovo praviloma ni potrebno.

Amortizacije neopredmetenih sredstev zaradi omenjenih razlogov praviloma ne moremo normalizirati in je zato ne moremo vključiti v izračun preostanka s pomočjo Gordonovega modela rasti. Amortizacija neopredmetenih sredstev tudi ne vključuje vpliva inflacijskih gibanj. Priporočljivo je, da tovrstno amortizacijo izključimo iz izračuna preostale vrednosti ter ločeno ocenimo vse njene morebitne vplive na denarni tok podjetja (davčni ščit) ter te vplive kot samostojno postavko vključimo v oceno vrednosti podjetja. Podobno velja za vse postavke denarnega toka, ki imajo podobne značilnosti kot amortizacija neopredmetenih sredstev, tj., da ne rastejo v času, da so enkratne narave in da imajo omejeno življenjsko dobo

(npr. prenesena davčna izguba). Vrednost podjetja je v tem primeru sestavljena iz naslednjih elementov:

$$EV = PV_f + PV_{tv} + PV_{a,}$$

pri čemer je:

EV = vrednost podjetja,

PV_f = sedanja vrednost denarnih tokov v obdobju natančnega načrtovanja,

PV_{tv} = sedanja vrednost preostale vrednosti, izhajajoče iz normaliziranih prostih denarnih tokov,

PV_a = sedanja vrednost denarnih tokov, ki so posledica amortizacije neopredmetenih sredstev, prenesenih davčnih izgub ipd., ki nastanejo po obdobju natančnega načrtovanja (npr. davčni ščit).

Ocenjevalec vrednosti lahko kontrolo ustreznosti opisanega načina ocenjevanja preostale vrednosti izvede s pomočjo implicitno izhajajočih mnogokratnikov iz preostale vrednosti (npr. mnogokratniki vrednost/EBITDA ipd.), ki jih lahko primerja z načrtovanimi mnogokratniki primerljivih podjetij, če ima te podatke.

Vloga revizijske komisije glede notranje revizije

IZ PRAKSE ZA PRAKSO (PR-NR 7-5/18)

IZHODIŠČE

Revizijska komisija[1] ima pomembno vlogo pri spremljanju notranje revizije in podpori za kakovostno delovanje. S spremembo Zakona o gospodarskih družbah (odslej ZGD-1)[2] leta 2015 je bila z novim 281.a členom dana notranji reviziji dodatna veljava in s tem dodatni pomen tudi revizijski komisiji pri spremljanju njenega delovanja in predlaganju potrebnih soglasij (odobritev) in drugih sklepov nadzornemu svetu.

ZGD-1 zahteva, da mora revizijska komisija spremljati učinkovitost in uspešnost notranje revizije (če notranja revizija obstaja[3]) ter sodelovati z notranjim revizorjem, zlasti z medsebojnim obveščanjem o glavnih zadevah v zvezi z notranjo revizijo[4]. S tem je dan notranji reviziji poseben status med dejavnostmi družbe, saj lahko sicer pridobiva revizijska komisija (enako velja za nadzorni svet[5]) informacije o družbi le od uprave.

Zakonsko določena so soglasja nadzornega sveta do ključnih zadev in dokumentov notranje revizije: aktu, ki določa njen namen, pomen, naloge, pristojnosti in pooblastila (in s katerim se vzpostavi dejavnost notranje revizije) k

---

1 RPo ZGD-1 je revizijska komisija delovno telo/organ nadzornega sveta gospodarske družbe v dvotirnem sistemu upravljanja družbe in prav tako delovno telo/organ upravnega odbora v enotirnem sistemu upravljanja družbe (za družbo je sicer uporabljen izraz organizacija po Standardih; odslej tudi družba).

2 Zakon o gospodarskih družbah (ZGD-1, Uradni list RS, št. 65/09 – uradno prečiščeno besedilo, 33/11, 91/11, 32/12, 57/12, 44/13 – odl. US, 82/13, 55/15 in 15/17).

3 Združenje nadzornikov Slovenije priporoča revizijski komisiji družbe, v kateri notranja revizija še ni vzpostavljena, da vsaj enkrat letno presodi, ali je potrebna, ter navaja, katere okoliščine in dejavnike naj pri presoji upošteva.

4 Z 281.a členom ZGD-1 je nadzornemu svetu omogočeno, da lahko od notranjega revizorja zahteva dodatne informacije. Če ima družba revizijsko komisijo, izvršuje to pravico revizijska komisija. (Opomba: v prispevku nista obravnavana način in okoliščine v zvezi s to aktivnostjo.)

5 V družbi, kjer revizijska komisija ni imenovana, velja predstavljeno neposredno za nadzorni svet.

imenovanju in prejemkom vodje notranje revizije (in njegovi razrešitvi), k pogodbi z zunanjim izvajalcem (in njegovi spremembi in odpovedi) ter k letnim in večletnim načrtom dela notranje revizije. Nadzorni svet ta soglasja sprejema na podlagi predhodne obravnave revizijske komisije in njenih predlogov.

Način izvajanja predpisanih nalog se v določeni meri razlikuje med revizijskimi komisijami (glede na njihovo sestavo in pristop, kot velja tudi za druge naloge). Pomagajo jim priporočila strokovnih organizacij, pri nas predvsem Priporočila za revizijske komisije, ki jih je izdalo Združenje nadzornikov Slovenije (odslej Priporočila)[6]. Z revizijsko komisijo komunicira vodja notranje revizije, ki naj pozna priporočene pristope ter spozna njena specifična pričakovanja. Vse z namenom, da se lahko notranja revizija ustrezno in proaktivno odziva v skupnem prizadevanju za uspešno doseganje ciljev družbe.

STROKOVNA RAZLAGA

Revizijska komisija lahko nudi ključno pomoč notranji reviziji, tako da

- *zagotavlja neodvisnost notranje revizije,*
- *preverja, če ima notranja revizija potrebne kadre in sredstva za svoje delovanje,*
- *obravnava ključne zadeve notranje revizije in predlaga nadzornemu svetu, da sprejme predpisana soglasja,*
- *zahteva uresničevanje priporočil notranje revizije v dogovorjenih rokih.*

Tudi vodja notranje revizije naj bo proaktiven pri sodelovanju z revizijsko komisijo. Z njenim predsednikom naj naveže in vzdržuje stik, po potrebi naj ga seznanja z delom notranje revizije in pričakovanji za pomoč pri krepitvi njene vloge tudi izven terminov sej.

Priporočila ob obravnavi zadev, h katerim daje revizijska komisija nadzornemu svetu predloge za soglasja, dajejo še nekaj dodatnih napotkov revizijski komisiji. V nadaljevanju jih predstavljamo in dodajamo nekaj primerov iz prakse, ki bi morala zagotoviti:

- *upoštevanje Hierarhije pravil notranjega revidiranja (kar se opredeli tudi v notranjerevizijski temeljni listini):*
  - *revizijska komisija zahteva uporabo mednarodnih standardov in drugih pravil notranjega revidiranja, sicer pa nameni vsebinsko pozornost namenu notranje revizije v konkretni družbi in področjem njenega delovanja, kjer bo lahko največ prispevala;*

[6] Priporočila za revizijske komisije, Združenje nadzornikov Slovenije, četrta dopolnjena izdaja, december 2017.

- *ustrezno usposobljene notranje revizorje in zadostna sredstva za njihovo delovanje, vključno s predlogom nadzornemu svetu glede povečanja oddelka notranje revizije (smiselno enako velja v primeru opravljanja dejavnosti z najemom zunanjih izvajalcev):*
  - *revizijska komisija se zaveda, da brez kakovostnega in številčno zadostnega kadra notranja revizija ne more uspešno izvajati svojih nalog in prispevati k uspešnosti družbe; zato preverja, kako notranji revizorji skrbijo za izboljševanje svojih znanj in veščin (dejansko, ne le zaradi podaljševanja veljavnosti strokovnih nazivov), jih dopolnjujejo z delom zunanjih izvajalcev, ko gre za posebna, specialistična znanja in izkušnje in s tem tudi prenos dobre prakse, ter podpira nadzorni svet s predlogi, da preskrbi zadostna sredstva za te namene;*
- *mandat vodji notranje revizije za večletno obdobje, na primer za vsaj 4 ali 5 let:*
  - *revizijska komisija se zaveda, da bi kratek mandat vodje potencialno ogrožal neodvisnost notranje revizije, zato poskrbi, da je imenovanje za večletno obdobje;*
- *redno neposredno sodelovanje z vodjo notranje revizije in se najmanj enkrat letno z njim sestane na uradnem sestanku brez navzočnosti kateregakoli člana uprave:*
  - *revizijska komisija se želi občasno temeljito pogovoriti z vodjo notranje revizije kot s partnerjem pri nadzoru družbe, z izmenjavo pogledov in informacij, brez drugih udeleženih, ne zaradi morebitnega nezaupanja v upravo, temveč ker je takšen pogovor temeljitejši in bolj osredotočen na videnje tveganj v družbi in možnosti njihovega upravljanja;*
- *redno obravnavo poročil o delu notranje revizije in uresničevanju njenih priporočil, vključno s proučitvijo ustreznosti in pravočasnosti odzivov nanje:*
  - *revizijska komisija se osredotoča na bistvene ugotovitve in razloge zanje ter predvsem, kako se uvajajo predlagane izboljšave;*
- *obravnavo letnega poročila o delu notranje revizije pred njegovo predajo nadzornemu svetu (zakonsko predpisana najpozneje v treh mesecih po zaključku poslovnega leta);*
- *seznanjanje z obdobnimi samoocenitvami in zunanjo presojo kakovosti notranje revizije ter spremljanje izboljševanja notranje revizije:*
  - *revizijska komisija povabi zunanjega presojevalca, da ji osebno predstavi svojo oceno delovanja notranje revizije in njegovega videnja nadaljnjih potrebnih izboljšav, sicer pa se osredotoča vsaj na njihovo letno spremljanje;*
- *presojo, ali je petletni razmik med zunanjimi presojami primeren ali je potreben krajši:*

- *revizijska komisija se zaveda, da je v hitro se spreminjajočem okolju petletni razmik morebiti predolg in o tem presodi glede na razvitost upravljanja in notranje revizije;*
- *opredelitev kriterijev za izbor zunanjega presojevalca in vnaprejšnjo seznanitev s ponudbami in predlogom uprave za izbor ponudnika ter v primeru nestrinjanja nadzornemu svetu predlaga proučitev ali njegovo soglasje h končnemu izboru.*

V nadaljevanju predstavljamo priporočene pristope vodje notranje revizije k zgoraj izpostavljenim priporočenim vsebinam dela revizijske komisije:

- *predstaviti bistvo Hierarhije pravil notranjega revidiranja in pomena uporabe Standardov za družbo ter seveda zagotoviti, da so zahtevana za notranjerevizijsko delovanje v organizaciji;*
- *poskrbeti, da metodologija načrtovanja na podlagi ključnih tveganj vključuje tudi meje, do katere višine ocenjenih tveganj se morajo izvesti posli dajanja zagotovil (revizije) in do kje le v primeru presežnih virov, ter dati realno oceno potrebnega osebja tako z vidika usposobljenosti kot potrebnega časa za izvedbo poslov na področjih ključnih tveganj (ob drugih v zunanjih in notranjih predpisih ter Standardih določenih nalogah), ne glede na trenutne ali možne zaposlitve ali najem zunanjih izvajalcev, ter načrtovati kakovostna potrebna usposabljanja (vključno s samoizobraževanjem);*
- *poskrbeti, da je prepoznan kot strokovna avtoriteta s pokončno držo;*
- *poskrbeti z vsem svojim delovanjem za zaupanja vreden in strokoven odnos, ki pomaga revizijski komisiji pri delovanju;*
- *pripraviti jasno zasnovana, jedrnata poročila notranje revizije z navedbo ključnih ugotovitev in priporočil; na sejah revizijske komisije pa izpostaviti bistveno z vidika upravljanja tveganj in koristi za organizacijo, in ne povzemati zapisanega (odgovornost članov revizijske komisije vključuje temeljit pregled gradiva pred sejo), ter pri predstavitvah uresničevanja priporočil v primeru prekoračitev rokov poudariti s tem povezana tveganja;*
- *poskrbeti, da bo letno poročilo o delu notranje revizije pravočasno predano revizijski komisiji, še pred predajo nadzornemu svetu v zakonskem roku, sicer pa preveriti pričakovanja glede celovitih mnenj in se na njihovo izdajanje metodološko pravočasno pripraviti;*
- *poskrbeti, da bo revizijska komisija seznanjena z akcijskimi načrti na podlagi notranjih in zunanjih presoj kakovosti notranje revizije ter z njihovim izpolnjevanjem v zadanih rokih, z vidnimi kakovostnimi premiki naprej;*
- *opozoriti revizijsko komisijo, da bi bil potreben krajši razmik med zunanjimi presojami kakovosti, ali vsaj proučiti primernost petletnega razmika;*

- *pripraviti predlog kakovostnih kriterijev za izbor zunanjega presojevalca kakovosti notranje revizije in jih dati revizijski komisiji, da se o njih opredeli.*

Ena od prednosti za delo revizijskih komisij[7] *je tudi krepitev vloge notranje revizije. Med drugim je poudarjeno preverjanje revizijske komisije, če se načrti dela notranje revizije (in njihovo izvajanje) osredotočajo na upravljanje ključnih poslovnih tveganj ter če področja notranjega revidiranja, vključno z upravljanjem in cilji notranjih revizij, izhajajo iz teh ključnih tveganj. Ob tem si tudi postavlja vprašanja, kot so: ali notranja revizija pomaga revizijski komisiji razumeti kakovost kontrolnega okolja, poslovnih procesov in zaposlenih? Ali je notranja revizija dovolj cenjena in upoštevana?*

Vodja notranje revizije naj poskrbi, da bo revizijska komisija na ta in podobna vprašanja lahko odgovorila pritrdilno.

7 Prioritete za delo revizijskih komisij v letu 2017/2018, Združenje nadzornikov Slovenije, maj 2017.

Izrazna vrednost kazalnika čista donosnost kapitala

IZ PRAKSE ZA PRAKSO (PR-RAC 5-5/18)

Izrazno vrednost kazalnika čista donosnost kapitala je obravnaval Odbor sekcije preizkušenih računovodij in računovodij in pripravil naslednjo strokovno razlago.

IZHODIŠČE

Kazalnik čista donosnost kapitala je v 8.31. členu Pravil skrbnega računovodenja 8 (2016) opredeljen kot razmerje med čistim poslovnim izidom obračunskega obdobja in povprečnim kapitalom (brez čistega poslovnega izida obračunskega obdobja). Pove nam, kolikšna je donosnost kapitala, to je, koliko je vložena enota kapitala prinesla v obdobju, za katero smo izračunavali donosnost. Če je organizacija dosegla pozitiven čisti poslovni izid, se je premoženje, ki so ga lastniki kapitala vanjo vložili, povečalo, če je dosegla negativen poslovni izid, pa zmanjšalo.

Donosnost izračunavamo za obdobja, za katera sestavljamo računovodske izkaze, torej za poslovna leta, lahko pa tudi za drugačna obračunska obdobja.

Navadno ima organizacija, za katero izračunavamo čisto donosnost kapitala, pozitivni povprečni kapital (brez čistega poslovnega izida obračunskega obdobja). Lahko pa se zgodi, da je znesek povprečnega kapitala (brez čistega poslovnega izida) enak nič oz. je celo negativen, ker dolgovi organizacije presegajo znesek njenih sredstev. V takih okoliščinah tega kazalnika ni mogoče izračunati[1], saj vloženega kapitala ni: kapital, ki so ga nekoč lastniki v organizacijo vložili, je namreč izgubljen.

Velja tudi, da je vrednost kazalnika izredno občutljiva za višino zneska pozitivnega povprečnega kapitala (brez čistega poslovnega izida obračunskega obdobja): pri nizkem povprečnem kapitalu že majhna sprememba v znesku čistega poslovnega izida močno vpliva na velikost izračunane čiste donosnosti kapitala.

[1] Tehnično je (razen če je povprečni kapital enak nič) izračun mogoč, a ni smiseln.

Na tej osnovi objavljamo naslednjo strokovno razlago.

STROKOVNA RAZLAGA

Kazalnik čista donosnost kapitala je temeljni kazalnik donosnosti, ki pove, koliko je prinesla vložena enota kapitala v obdobju, za katero se izračunava kazalnik. Če je znesek povprečnega kapitala organizacije (brez čistega poslovnega izida tekočega leta) enak nič ali negativen, tega kazalnika ni mogoče izračunati. Da bi dobili boljšo sliko o poslovanju organizacije, je primerno upoštevati vsaj še kazalnik čista donosnost sredstev, ki je razmerje med čistim poslovnim izidom obračunskega obdobja in povprečnimi sredstvi, saj povprečna vrednost sredstev ne more biti negativna.

Pravnomočnost odmerne odločbe in naknadno ugotovljena kršitev materialnega zakona

IZ PRAKSE ZA PRAKSO (PR-DAV 4-5/18)

Problematiko, povezano z uporabo pravnih sredstev po pravnomočnosti odmernih odločb organov prve stopnje Finančne uprave RS, je obravnaval Odbor sekcije preizkušenih davčnikov. Pri tem je posebej izpostavljeno vprašanje, katero pravno sredstvo je dopustno uporabiti in kdo ga lahko uporabi. V tej zvezi je odbor pripravil naslednjo strokovno razlago.

IZHODIŠČE

Zakon o dohodnini (ZDoh-2) in Zakon o davku od dohodkov pravnih oseb (ZDDPO-2) vsebujeta vrsto vsebinskih določb, s katerimi se določijo posamezne vrste obdavčenih dohodkov, vendar je njihova uporaba v konkretnih davčnih zadevah pogosto povezana z uporabo določb drugih materialnih zakonov. Težave z uporabo materialnih zakonov v praksi nastajajo zaradi nejasnih, pomanjkljivih, nekonsistentnih ali ohlapnih zakonskih dikcij. Temu prispeva vedno več materialnih zakonov in njihovih novel. Zato je pri reševanju določenih konkretnih vprašanj ugotavljanja zakonskega stanu na podlagi posamezne materialne norme, ki vpliva na davčno obravnavo posameznega dohodka (kakor tudi priznanega odhodka), odločilna pravilna in zakonita razlaga konkretne materialne norme. Zlasti je v posameznih primerih težko reševanje vprašanja, ali je v obrazložitvi davčne odmerne odločbe prišlo do nedopustne ekstenzivne razlage posameznega materialnega zakona, kar pomeni izven obsega in v neskladju z namenom zakona.

V primerjavi s fizičnimi osebami imajo pravne osebe praviloma večje možnosti dobiti potrebno pomoč oziroma podporo davčnih in pravnih strokovnjakov v zvezi s prejetimi odmernimi davčnimi odločbami. Na tej podlagi lahko vlagajo pritožbe zoper konkretne odmerne odločbe v davčnem postopku kakor tudi tožbe v upravnem sporu. Odsotnost ustrezne strokovne pomoči pogosto davčnim zavezancem, zlasti pa fizičnim osebam, onemogoči uporabo pritožbe kot rednega pravnega sredstva.

Na podlagi navedene problematike je ključno vprašanje, kaj na podlagi veljavne postopkovne zakonodaje lahko stori davčni zavezanec za vzpostavitev zakonitega stanja, kateremu je bila izdana in vročena davčna odmerna odločba, zoper katero ni vložil pritožbe, po pravnomočnosti te odločbe pa je izvedel, da obstajajo znaki kršitve materialnega zakona v tej odločbi.

Na podlagi predstavljenih strokovnih izhodišč objavljamo naslednjo strokovno razlago.

STROKOVNA RAZLAGA

Zakon o davčnem postopku (ZDavP-2) vsebuje v 2. podpoglavju o izrednih pravnih sredstvih VI. poglavja (pravna sredstva) postopkovni institut odprave in razveljavitve oziroma spremembe odločbe po nadzorstveni pravici. V drugem odstavku 88. člena ZDavP-2 je določeno, da v primeru kršitve materialnega zakona lahko davčni organ po nadzorstveni pravici odpravi, razveljavi ali spremeni odmerno odločbo v petih letih od dneva, ko je bila odločba vročena zavezancu za davek.

Prvi odstavek 276. člena Zakona o splošnem upravnem postopku (ZUP) določa, da odločbo lahko odpravi ali razveljavi po nadzorstveni pravici organ druge stopnje, to pa je v davčnem postopku Ministrstvo za finance (drugi odstavek 70. člena ZDavP-2).

Ministrstvo za finance v skladu z določbami prvega odstavka 275. člena ZUP-a kot pristojni organ po nadzorstveni pravici odpravi oziroma razveljavi odločbo po uradni dolžnosti, če izve oziroma sam ugotovi, da so podani razlogi za odpravo ali razveljavitev. Ker je Ministrstvo za finance kot drugostopenjski organ tudi pritožbeni organ (enako funkcijo imajo drugostopenjski organi v drugih upravnih postopkih), ZUP v navedenem odstavku 275. člena dopušča stranki (davčnemu zavezancu), da od Ministrstva za finance kot nadzorstvenega organa zahteva, da odmerno odločbo odpravi, razveljavi oziroma jo spremeni. Takšno zahtevo lahko poleg davčnega zavezanca vloži inšpektor, državni pravobranilec ali državni tožilec.

Če je bila zoper odmerno odločbo vložena pritožba oziroma kakšno drugo pravno sredstvo, Ministrstvo za finance zahtevo za odpravo, razveljavitev ali spremembo odločbe po nadzorstveni pravici zavrže kot nedopustno (drugi odstavek 275. člena ZUP-a).

Uporabo instituta odprave, razveljavitve oziroma spremembe po nadzorstveni pravici posebej izpostavljamo v primerih precedenčnih sodb Vrhovnega sodišča o vprašanjih pravilne uporabe materialnega zakona v davčnih zadevah, ki bi po presoji pristojnega organa narekovale uporabo navedenega instituta.

Dokazi pri poslih dajanja zagotovil in revidiranja informacijskih sistemov

IZ PRAKSE ZA PRAKSO (PR-RIS 5-5/18)

Problematiko revizijskih dokazov pri poslih dajanja zagotovil in revidiranja IS-jev je obravnaval Odbor sekcije preizkušenih revizorjev informacijskih sistemov (v nadaljevanju: PRIS) in pripravil naslednjo strokovno razlago.

IZHODIŠČE

ITAF™: Okvir strokovnega ravnanja za dajanje zagotovil/revidiranje IS-jev (v nadaljevanju tudi: okvir ITAF), 3. izdaja, v povezavi z revizijskimi dokazi pri poslih dajanja zagotovil in revidiranja IS-jev zahteva, da morajo strokovnjaki dajanja zagotovil in revidiranja IS-jev pridobiti zadostne in ustrezne dokaze, da lahko sprejmejo primerne sklepe, s katerimi utemeljijo izide posla in potrdijo ugotovitve (ITAF, standard 1205.1).

Na podlagi predstavljenega izhodišča je bila sprejeta naslednja strokovna razlaga.

STROKOVNA RAZLAGA

Okvir ITAF v standardu 1205 in izvedbeni smernici 2205 opredeljuje vrste in načine zbiranja ustreznih in zadostnih revizijskih dokazov, s katerimi PRIS in njegovi sodelavci (v nadaljevanju tudi revizijska skupina) zagotovijo, da lahko sprejmejo ustrezne ugotovitve. Ta razlaga je umerjena na izvedbeni proces zbiranja, hranjenja in uničenja revizijskih dokazov, ki temelji na okviru ITAF, zato je prav, da bralec pred tem člankom prebere tudi navedeni standard in smernico okvira ITAF.

*Tako okvir ITAF kot ta prispevek večkrat uporabljata besedni zvezi **ustrezni in zadostni** revizijski dokazi. Revizijski dokazi izpolnjujejo zgornji dve zahtevi, če:*

- *za vsako odločitvijo stoji revizijski dokaz, npr.: dokumentacija, iz katere so razvidna testiranja – ni nujno, da za vsako enoto v vzorcu obstaja optični*

zajem[1]*, računalniški izpis, kopija izvirnih dokumentov (več o tem v nadaljevanju);*
- *lahko v vsakem trenutku primerno usposobljena oseba na osnovi revizijskih dokazov – dokumentacije, brez prisotnosti članov revizijske skupine, ki je izvajala postopke, ponovi revizijo in pride do enakih zaključkov.*

Poznamo različne vrste in oblike revizijskih dokazov:
- *listinski dokazi (pogodbe, pisne usmeritve in postopki, računalniški izpisi, izidi izvlečkov podatkov, zapisi transakcij, izpisi programov in podobno);*
- *t. i. tiskalka*[2]*, ki dokazuje obstoj posameznih notranjih kontrol oziroma aktivnosti;*
- *pisne in ustne navedbe revidirancev;*
- *zapisi revizorja (zapiski sestankov, zapisi opazovanj različnih procesov, opisi in izidi testiranj in analiz ...).*

Iz zgornjih alinej je razvidno, da revizijske dokaze pogosto predstavljajo zapisi revizorja. Razlog je predvsem v učinkovitosti izvajanja postopkov revizije. Pridobivanje dokumentacije, ki izkazuje revizijske sledi o izvedenih notranjih kontrolah za vsako izbrano enoto v vzorcu, lahko na primer od naročnika revizijske storitve terja precej časa in napora. Prav tako takšen način pogosto ni učinkovit z vidika hrambe revizijske dokumentacije. Ker se vsi izvirni dokumenti nahajajo pri naročniku, je praviloma mogoč njihov ponovni pregled (na primer pri nadzoru), pri čemer je smiselno, da revizor za vsak primer preveri notranje postopke za uničevanje dokumentacije in brisanje zapisov, ki jih organizacija ne potrebuje več (kar je za določene vrste dokumentov in zapisov celo zakonsko zahtevano). Vsekakor pa je prav, da se pridobi vsaj en primer dokumentov ter razvidov notranjih kontrol in aktivnosti za vsak proces, ki je predmet revizije (t. i. sprehajalno preizkušanje). Razloga za to sta dva:
1. *da se revizor prepriča, ali je aktivnosti znotraj procesa in ustroj notranjih kontrol pravilno razumel;*
2. *da se evidentira, kateri dokumenti oz. drugi razvidi dokazujejo obstoj notranjih kontrol, ki so predmet revidiranja na izbranem vzorcu.*

Tudi dokumente, pri katerih revizor odkrije izjeme, odstopanja od napake ali celo namerne nepravilnosti, naj revizor kot izvirnik ali kot kopijo vključi v revizijsko dokumentacijo, saj so tovrstni dokumenti posebej izpostavljeni nevarnostim izgube ali uničenja.

---

1 Angl: scan, [URL: http://www.islovar.org/islovar].

2 Angl: print screen, [URL: http://www.islovar.org/islovar].

*Pri revizijah informacijskih sistemov je pomembna komponenta pri zbiranju revizijskih dokazov tudi **čas**. Določena (aplikativna) kontrola, ki je obstajala in delovala v nekem trenutku, lahko v drugem trenutku deluje drugače ali sploh ne deluje. Zato je treba v revizijski dokumentaciji (dokazih) natančno navesti, kdaj je bila takšna kontrola testirana oz. kako smo se prepričali, da je obstajala in delovala v celotnem obdobju revidiranja.*

Pri revizijskih dokazih gre velikokrat za neko obliko kopij izvirnikov dokumentacije naročnika, zato je prav, da jo revizor varuje skladno z dobrimi praksami na tem področju. Zaradi revizorjeve narave dela (terensko delo) je običajno še posebej veliko tveganje nepooblaščene izgube revizijskih dokazov v elektronski obliki. Varstvo podatkov in informacij – vse od pridobitve do uničenja, vključno z uničenjem, mora biti pri revizorjih na nivoju splošno znanih standardov na tem področju.

KANDIDATI, KI SO USPEŠNO ZAKLJUČILI IZOBRAŽEVANJE PRI INŠTITUTU

V okviru izobraževanja je Slovenski inštitut za revizijo organiziral zaključne izpite za kandidate, vpisane v izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor.

Po uspešni izdelavi in zagovoru zaključnega dela je Slovenski inštitut za revizijo izdal potrdilo (certifikat) za strokovni naziv preizkušeni notranji revizor/ preizkušena notranja revizorka:

- **Simoni Okorn**.

Čestitkam se v imenu vseh imetnikov nazivov, vpisanih v registre pri Inštitutu, pridružuje tudi Slovenski inštitut za revizijo.