UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

EKONOMSKI VIDIKI INFORMACIJSKE VARNOSTI

Ljubljana, december 2014 MARKO BEKETIČ

IZJAVA O AVTORSTVU

Spodaj podpisani(-a) MARKO BEKETIČ, študent(-ka) Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor(-ica) zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije z naslovom EKONOMSKI VIDIKI INFORMACIJSKE VARNOSTI, pripravljene(-ga) v sodelovanju s svetovalcem/svetovalko prof. dr. BORKA DŽONOVA JERMAN BLAŽIČ in sosvetovalcem/sosvetovalko _/_.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbel(-a), da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v zaključni strokovni nalogi/diplomskem delu/specialističnem delu/magistrskem delu/doktorski disertaciji, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobil(-a) vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal(-a);
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predložene zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne 10.12.2014 Podpis avtorja(-ice):_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

V sodobnem in hitro razvijajočem svetu, ažurne in zanesljive informacije že dolgo niso le sredstvo za doseganje konkurenčne prednosti, ampak so življenjskega pomena za obstoj organizacij v povezanem, globaliziranem svetu. Zanesljive, točne in predvsem pravočasno pridobljene informacije so temelj za delovanje in preživetje gospodarskih subjektov v mednarodnem poslovnem okolju. Sodobna informacijska in telekomunikacijska tehnologija omogoča hitro, zanesljivo in učinkovito poslovanje s čimer odpira nove možnosti za širitev poslovanja in učinkovitejšo izrabo virov, ter nenehno ustvarja nove poslovne priložnosti. Tako v poslovnem svetu, kot v vsakdanjem življenju je uporaba informacijske tehnologije postala nepogrešljiv del vsakdanjega delovanja gospodarskih subjektov, ter s tem povzročila njihovo naraščajočo odvisnost od njene uporabe (Jahankhani, Nkhoma & Mouratidis, 2010, str. 237). Glede na to že dolgo ni več presenetljivo spoznanje, da je varnost informacij postala ena glavnih elementov pri načrtovanju letnih proračunov, ki jih podjetja namenjajo vzdrževanju, uporabi in nabavi informacijske tehnologije. Zaradi naraščajočega števila uporabnikov informacijske tehnologije v okviru neštetih omrežij in elektronskih storitev, ter njihove vse večje raznolikosti, področje informacijske varnosti postaja bolj kompleksno, posledično pa težje obvladljivo. Ker je praktično že vsak posameznik vsaj v določeni meri poklicno in osebno vpet v uporabo informacijske tehnologije, Trček (2006, str. 1) meni, da slika področja informacijske varnosti, ki je ob svojih začetkih bila bolj pregledna glede potrebnih ukrepov, sedaj postaja vse bolj zamegljena in kompleksna. Razlog je v vse večji medsebojni odvisnosti problemov, ki izhajajo iz tehnoloških, organizacijskih in zakonodajno-pravnih ved, na katerih temelji sodobno poslovanje.

Takšen razvoj dogodkov Su (2006, str. 1) pripisuje usmeritvi, ki se razvija in kaže na to, da zagotavljanje visoke ravni informacijske varnosti v zadnjih letih postaja glavni problem razvoja in množične uporabe informacijske tehnologije. Su (2006, str. 1) je ugotovil dve smeri razvoja: prva je že omenjena naraščajoča vpetost informacijske tehnologije v vse pore življenja, druga pa nakazuje v zadnjem desetletju naraščajoče[1] število varnostnih dogodkov, torej dogodkov, ki ogrozijo zaupnost, celovitost in razpoložljivost informacijskega sistema (National Institute of Standards and Technology, 2011, str. 89). Eno najpomembnejših vlog pri razvoju omenjenih usmeritev lahko pripišemo uporabi interneta, ki ga vse več gospodarskih subjektov množično uporablja zaradi globalnega dostopa do podatkov in informacij. Zaradi tega je elektronsko poslovanje postalo nepogrešljivo v sodobnem svetu, tako pri poslovanju med subjekti, kot pri poslovanju z administracijo. Njegova uporaba na eni strani prinaša številne priložnosti, na drugi pa tudi nove grožnje in nevarnosti (Slay & Koronios, 2006, str. 12). S tem se strinja tudi Cavusoglu (2004, str. 71), ki poudarja, da prav z naraščanjem elektronskega poslovanja narašča tudi število neželenih varnostnih dogodkov in napadov na informacijske sisteme ter da so prednosti elektronskega poslovanja (enostavna izmenjava informacij, nižji stroški poslovanja) hkrati največja ovira za zagotavljanje informacijske varnosti.

[1] Rezultati nekaterih novejših raziskav sicer kažejo na smer upadanja števila zaznanih varnostnih dogodkov, so pa na drugi strani njihovi stroški vedno višji in za podjetja lahko tudi usodni (podrobneje v točki 1.4.1).

Tradicionalno so podjetja na informacijsko varnost gledala kot na zavarovalno polico, ki jih ščiti pred izgubami, ki bi jih utrpeli v primeru varnostnih dogodkov (Cavusoglu, 2004, str. 73). Najvišje vodstvo podjetja informacijske varnosti v večini primerov še ni dojemalo kot nujnost, vsaj dokler ni prišlo do hujšega varnostnega dogodka (ali serije dogodkov), ki je resno ogrozil poslovanje in obstoj podjetja. S tem, ko je število varnostnih dogodkov z razvojem in množičnostjo uporabe informacijske tehnologije vztrajno naraščalo, se je spremenilo tudi dojemanje informacijske varnosti, kot temeljni pogoj, za zagotavljanje varnega poslovnega okolja v katerem podjetje ustvarja pričakovano dodano vrednost. Pregled rezultatov raziskave o informacijski varnosti »Computer Crime and Security Survey« (v nadaljevanju CCSS) v zadnjih nekaj letih potrjuje to trditev, saj se je delež proračuna, ki ga ameriška podjetja namenjajo informacijski varnosti od leta 2007 do 2011, več kot podvojil, in to kljub kriznim razmeram, v katerih so se podjetja znašla, in so zato med drugim zmanjševala tudi sredstva, namenjena naložbam v informacijsko tehnologijo. Kljub vse večjemu zavedanju o pomembnosti informacijske varnosti, ter v luči kriznih razmer, ko posamezni oddelki v podjetjih še toliko bolj tekmujejo za pridobivanje omejenih sredstev, so zahteve vrhovnega vodstva po ekonomskem upravičenju naložb vse glasnejše, pri čemer informacijska varnost ni izjema.

Lastniki podjetij od uprave, ki so ji prepustili in zaupali vodenje podjetja pričakujejo, da bo prepoznala in izpeljala tiste naložbene priložnosti, s katerimi bo povečevala vrednost podjetja (premoženja lastnikov). Če je še do nedavnega veljalo, da so bili strah, negotovost in dvom (angl. *fear, uncertainty and* doubt, v nadaljevanju FUD) glavno gonilo naložb v informacijsko varnost, pa so zlasti zaostrene gospodarske razmere v ospredje postavile potrebo po ekonomskem upravičenju le-teh. Cavusoglu (2004, str. 73) poudarja, da se v zadnjih letih pogled na naložbe v informacijsko varnost spreminja zlasti v dveh smereh. Podjetja na izdatke za informacijsko varnost ne gledajo več kot le na strošek poslovanja, temveč kot na naložbo, ki podjetju, njegovim partnerjem in kupcem ustvarja dodano vrednost. Hkrati pa se vprašanja in skrbi podjetij odmikajo od tega, kako tehnološko zagotoviti ustrezno raven informacijske varnosti, k vprašanju, ali so te naložbe ekonomsko učinkovite in s tem upravičene. Prvo in v literaturi pogosto citirano pravilo, ki ga je glede naložb v informacijsko varnost podal Crume (2001, str. 17), pravi, da podjetja za varovanje sredstev nikoli ne smejo potrošiti več, kot so ta dejansko vredna. To pomeni, da z ekonomskega vidika podjetja v informacijsko varnost vlagajo vse do točke, ko vsaka dodatna denarna enota naložbe podjetju zagotovi dodatne prihranke (izražene v denarnih enotah). Zato Gordon in Loeb (2006, str. 121) menita, da je treba izdatke za informacijsko varnost presojati z analizo stroškov in koristi (angl. *cost-benefit analysis*), saj tako lahko najdemo odgovor na eno temeljnih vprašanj s področja naložb v informacijsko varnost: Koliko izdatkov je dovolj?

Iz zapisanega tako lahko ugotovimo, da zagotavljanje ustrezne in potrebne ravni informacijske varnosti ni več skrb zgolj tistih organizacij, ki že tradicionalno veljajo za visoko tvegane (vojska, policija, vlada in drugi državni organi), temveč je nujno za vse sektorje družbe in njihove subjekte v gospodarstvu. Medtem ko organizacije višjega tveganja lahko v nekaterih primerih zagotavljajo lastno varnost za vsako ceno, morajo tržni subjekti upoštevati način z učinkovitim upravljanjem informacijske varnosti (Cavusoglu, 2004, str. 71). Pri tem vse pogosteje

uporabljajo metode s področja mikroekonomije, saj so prisiljene konstantno tehtati med stroški in koristmi, ki jih izdatki za zagotavljanje informacijske varnosti prinašajo.

Namen magistrskega dela je z uporabo strokovne literature preučiti in podati pregled področja informacijske varnosti, s poudarkom na razumevanju ekonomskega vidika naložb v informacijsko varnost. Prav ekonomski vidik informacijske varnosti je temelj razvoja številnih kazalnikov in tehnik presojanja, razumevanja ter njihovo uporabo. Le poznanje metod vrednotenja in presojanja investicijskih projektov in teoretičnih spoznaj iz mikroekonomije lahko zagotovi ustrezno presojo pri odločanju o vlaganjih v informacijsko varnost. Poleg tega je namen naloge, na podlagi teoretičnih dognanj opraviti empirično raziskavo, ki je namenjena kvantitativnemu presojanju ekonomske upravičenosti naložb v informacijsko varnost. Namen naloge je tudi zagotoviti celoviti pregled določene analitične tehnike in skupaj s primerom njene uporabe na praktičnem primeru v določeni meri prispevati k uvedbi prakse pri odločanju o ekonomsko upravičenih naložbah v informacijsko varnost.

Cilj magistrskega dela je najprej predstaviti teoretične podlage na področju ekonomike informacijske varnosti. Poleg tega je cilj naloge tudi izpostaviti naraščajoči pomen ekonomskega presojanja naložb v informacijsko varnost in umestitev področja v okvir celovitega sistema upravljanja informacijske varnosti, ki se počasi uveljavlja v naši družbi. Cilj praktičnega dela naloge je opis in prikaz uporabe kvantitativnega modela za pripravo podatkov, ki so pozneje uporabljeni kot vhodni elementi v kvantitativni model za ekonomsko presojanje naložbe v varnostni ukrep. Cilj naloge je tudi zagotoviti uspešno dopolnitev uporabljene klasične analize presojanja ekonomske upravičenosti naložb z novejšim orodjem oziroma metodo, ki na področju ekonomike informacijske varnosti še ni med pogosteje uporabljenimi.

Magistrsko delo v prvem delu z uporabo teoretičnih metod analize in študija literature podrobno predstavi obravnavano področje, skupaj s temeljnimi opredelitvami, značilnostmi in metodami, ki tvorijo celoto obravnavane teme. Ta del naloge temelji na uporabi metode kompilacije, s katero sem združil spoznanja, sklepe, stališča in izsledke znanstveno raziskovalnega dela številnih, predvsem tujih avtorjev s področja ekonomike informacijske varnosti. Omenjeno metodo sem dopolnil tudi z uporabo opisne in analitične metode, ki sta rabili predvsem za opis zakonitosti in predstavitev posameznih vsebinskih sklopov v obravnavani temi. Drugi del magistrskega dela vsebuje rezultate v obliki ocene upravičenosti naložbe v informacijsko varnost na primeru slovenskega javnega zavoda. Pri tem sem uporabil klasično metodo za kvantitativno presojanje upravičenosti naložb, sicer poznano iz splošne investicijske teorije. Metodo, ki temelji na izračunu in medsebojni primerjavi finančnih kazalnikov sem vsebinsko dopolnil z metodo vizualizacije finančnih posledic, ki se v zadnjem času čedalje bolj uveljavlja kot empirična metoda na področju ekonomike informacijske varnosti. Pri izdelavi magistrskega dela se opiram na vire, ki jih sestavljajo znanstvene monografije, prispevki na strokovnih konferencah, poročila specializiranih institucij, v največji meri pa strokovni članki o tematikah z obravnavanega področja. Ob tem sem uporabil tudi teoretično znanje, pridobljeno na dodiplomskem in podiplomskem študiju na Ekonomski fakulteti v Ljubljani ter znanje in izkušnje, pridobljene z delom v finančno-računovodski službi.

Magistrsko delo je sestavljeno iz štirih sklopov, v okviru katerih je obravnavana tematika v poglavjih podrobneje razdelana. V uvodu so predstavljeni in opredeljeni predmet obravnave, namen in cilji skupaj z načrtom vsebine naloge. V prvem poglavju obravnavam informacijsko varnost z opredelitvijo temeljnih pojmov, strnjenim pregledom kratke zgodovine področja in temeljnih principov, na katerih temelji začetek in razvoj področja informacijske varnosti. V podpoglavja prvega dela vključujem še najpogosteje uporabljene standarde in najboljše prakse pri vzpostavitvi in zagotavljanju informacijske varnosti v podjetjih. Poglavje končujem z analizo rezultatov raziskav, ki kažejo na stanje informacijske varnosti v svetu, ter z usmeritvami in pričakovanji v zvezi z razvojem dogodkov v prihodnosti. Drugo poglavje podaja celovit opis in pregled sistema upravljanja s tveganji, v okviru katerega je informacijska varnost predstavlja ena izmed podsistemov. Sistem upravljanja informacijske varnosti je po svoji vsebini program, sestavljen iz zaporednih korakov, ki skupaj tvorijo zanko ponavljajočega se procesa. Slednji se začenja z identifikacijo in oceno tveganja, ter konča z ocenjevanjem učinkovitosti, s čimer se preverja uspešnost zmanjševanja (obvladovanja) tveganj z vpeljavo varnostnih ukrepov. Tretje poglavje je namenjeno predstavitvi ekonomskih zakonitosti trga informacij, katerega vse pomembnejši del je tudi ekonomika naložb v informacijsko varnost. Cilj je določitev optimalnega obsega naložb (kjer so celotni stroški najnižji in koristi najvišje), pri čemer se uporabljajo različni kazalniki s področja, ki ga obravnava teorija vrednotenja in ocenjevanja upravičenosti naložb. Ker pa med navadnimi naložbami (npr. nakup novega stroja) in naložbami v informacijsko varnost (npr. podaljšanje licence za uporabo protivirusne zaščite) obstajajo vsebinske razlike, uporabniki kazalnike in metode temu primerno prilagajajo in razvijajo, ter s tem iščejo načine za učinkovito celovito presojanje in odločanje o naložbah v produkte in storitve za zagotavljanje informacijske varnosti. Tako je v okviru četrtega poglavja na primeru večjega slovenskega javnega zavoda prikazana uporaba klasične metode presojanja ekonomske upravičenosti naložb. Rezultate in priporočila za izbiro varnostnega ukrepa v nadaljevanju dodatno dopolnjuje še, na področju ekonomike informacijske varnosti novejša metoda vizualizacije finančnih posledic. Nalogo vsebinsko končujem s sklepom, v katerem povzemam ključne ugotovitve in spoznanja ter podajam priporočila za nadaljnjo obravnavo tematike.

1 PODROČJE INFORMACIJSKE VARNOSTI

To je vsebinsko široko in obsežno področje, ki od poznavalca zahteva znanje iz informatike, splošne teorije in prakse varnosti ter fizičnega varovanja, poznanje zakonodaje o elektronskem poslovanju, komunikacijah in varstvu osebnih podatkov. Zahteva natančno poznanje temeljnih pojmov, principov in standardov s primeri najboljših praks, ki to področje natančno urejajo.

1.1 Opredelitve temeljnih pojmov

Po pregledu literature lahko ugotovimo, da so si opredelitve informacijske varnosti, podane od različnih avtorjev vsebinsko zelo podobne. Razlike med njimi večinoma izhajajo iz tega, da so podane v skladu z namenom raziskave in v odvisnosti od konteksta, v katerem se pojem informacijska varnost uporablja. Ta pojem sicer izhaja iz opredelitve varnosti, vsebuje pa tudi

druge elemente, ki so pomembni za razumevanje in ustrezno uporabo sredstev za zagotavljanje informacijske varnosti pri uresničevanju njenih ciljev.

1.1.1 Varnost

Ameriška organizacija National Institute of Standards and Technology (v nadaljevanju NIST) varnost opredeli kot **stanje**, ki je rezultat vzpostavitve in vzdrževanja varnostnih ukrepov. Takšno stanje podjetju omogoča uresničevanje vizije in poslanstva ter izvajanje vseh kritičnih poslovnih funkcij, in to kljub tveganjem, katerim je podjetje zaradi uporabe informacijskih sistemov izpostavljeno (National Institute of Standards and Technology, 2011, str. 167). Poenostavljeno bi varnost lahko razumeli kot stanje brez nevarnosti ali, kot pravi Canal (2005, str. 1), »Pojem varnost označuje odsotnost,« saj smo varni le, ko ni nikakršnih varnostnih dogodkov.

To opredelitev varnosti podaja kot statično kategorijo, vendar pa moramo na varnost gledati kot na **proces**, ki je močno odvisen in povezan z razvojem družbe (Sandrini, 2003, str. 5). Canal (2005, str. 1) meni, da je razumevanje varnosti odvisno od konteksta uporabe, s čimer se strinja tudi Schechter (2004, str. 9), ki podaja splošno opredelitev pojma varnosti kot »proces prepoznave dogodkov, ki imajo potencial, da povzročijo škodo in uvedba ukrepov za zmanjšanje tega potenciala«. Ta opredelitev je neodvisna od tehnološkega konteksta in konteksta uporabe ter je v zadostni meri posplošena, da je primerna za uporabo in odgovor na vprašanja, povezana z varnostjo, ki se zastavljajo s časom in razvojem.

Whitman in Mattord (2007, str. 8) ob tem še dodatno opozarjata, da je doseganje ustrezne ravni varnosti v podjetju mogoče doseči le z implementacijo večplastnega varnostnega sistema. Enako kot to velja za narodno varnost, ki je večplasten sistem varovanja suverenosti države, njenih sredstev, virov in ljudi, to velja tudi za vsako uspešno organizacijo. V takšnem večplastnem varnostnem sistemu je poleg fizičnega varovanja oseb in sredstev ter varovanja komunikacij ključen element tudi varovanje informacijskih sredstev. Temelj učinkovitega varnostnega sistema pa je jasno opredeljena varnostna politika, ki skupaj z vpeljanimi standardi in postopki tvori osnovo za vse varnostne aktivnosti, s čimer varnost postane funkcija organizacije in ne ovira pri doseganju njenih ciljev (Shaurette, 2004, str. 31).

Magistrsko delo je v nadaljevanju osredinjeno na področje informacijske varnosti s poudarkom na ekonomskem vidiku in načinih za razreševanje problematike in odgovore na vprašanja, ki se pojavljajo v okviru ekonomike informacijske varnosti.

1.1.2 Informacijska tehnologija in informacijski sistem

V slovarju izrazov organizacije NIST (2011, str. 97) je informacijska tehnologija (v nadaljevanju IT) opredeljena kot katerakoli oprema (ali medsebojno povezan sistem opreme), ki se uporablja za avtomatizirano zbiranje, hranjenje, manipulacijo, upravljanje, prikazovanje, prenos in izmenjavo podatkov in informacij. Gunasekaran, Love, Rahimi in Miele (2001, str. 350) ob tem

dodajajo, da gre za generični izraz za celoten spekter povezanih tehnologij, ki so rezultat uporabe računalnikov, strojne opreme, programske opreme, telekomunikacij interneta in elektronike.

Informacijski sistem (v nadaljevanju IS) NIST (2011, str. 94) opredeli kot skupek informacijskih virov, organiziranih za namen zbiranja, obdelave, vzdrževanja, uporabe, delitve, razširjanja in členitve informacij. Torej gre za širši pojem, saj IS ni zgolj množica povezanih računalnikov, temveč sistem, ki poleg strojne opreme (angl. *hardware*) vključuje še programsko opremo (angl. *software*), podatke, ljudi, postopke in mreže. Te kritične komponente omogočajo vhod, obdelavo, izhod in hrambo informacij, ter imajo vsaka svoje značilnosti in posledično tudi specifične varnostne zahteve (Whitman & Mattord, 2007, str. 14). Po mnenju Gunasekaran et al. (2001, str. 350) se pojem IS nanaša na način, kako so organizirani tokovi informacij, ki morajo biti organizirani tako, da zadovoljujejo potrebe po informacijah posameznika oziroma organizacije kot celote.

V opredelitvi IS sta uporabljena še pojma **podatek** in **informacija**, ki sta jedro vsakega IS in ju je treba vsebinsko ločevati. Boisot in Canals (2004, str. 15) podatke opredelita kot surova dejstva, ki predstavljajo dogodke ali fizično okolje, Losee (1997, str. 256) in standard ISO 27002 (International Organization for Standardization, 2005b, str. ix) pa informacije kot dejstva oziroma podatke, ki so preoblikovani v obliko, ki ima pomen in uporabno vrednost za prejemnika. Med podatki in informacijami mora potekati proces s katerim podatki pridobijo uporabno vrednost za uporabnika, pri čemer Harsh (2008, str. 1) posebej poudarja, da mora to preoblikovanje potekati v skladu s kontekstom odločanja.

1.2 Informacijska varnost

Potreba po varovanju informacij je stara kot človeštvo samo, saj koncept informacijske varnosti izhaja že iz prazgodovine. Takrat so imele informacije za preživetje ljudi pomembno vrednost, na primer v obliki informacije o bogatih loviščih oziroma nahajališčih hrane (Sadowsky, Dempsey, Greenberg, Mack & Schwartz, 2003, str. 18). Ne glede na čas in časovno obdobje je za človeka informacija imela določeno vrednost, s tem pa je obstajala potreba po njenem varovanju. Čeprav potreba po informacijski varnosti izhaja že iz pradavnine, pa se praksa na tem področju konstantno razvija na krilih tehnološkega napredka. Soo Hoo (2000, str. 2) poudarja, da prav tehnološki napredek po eni strani spodbuja (možnost hitre obdelave velikih količin informacij), po drugi pa zavira (nove možnosti in načini napadov na informacijska sredstva) napredek prakse informacijske varnosti.

Informacije imajo v poslovnem svetu zelo pomembno mesto. V mednarodnem poslovnem okolju, ko je medsebojna povezanost in sodelovanje podjetij na mednarodni ravni vsakdanja realnost, je pravočasen dostop do ključnih informacij lahko temeljna prvina doseganja konkurenčne prednosti. Za podjetje ima informacija različne vrednosti, od tega, da zagotavlja navadne dnevne transakcije, do tega, da omogoča sprejemanje strateških odločitev. Je pa vrednost informacije odvisna predvsem od njenih lastnosti (Whitman & Mattord, 2007, str. 9), saj se s spreminjanjem slednjih glede na okoliščine spremeni tudi vrednost informacije za

različne uporabnike. Na primer čas, v katerem je informacija uporabniku na voljo, je ključnega pomena za njeno vrednost, saj prepozno pridobljene informacije ne omogočajo pravočasnega reagiranja in s tem uresničevanja zastavljenih ciljev.

1.2.1 Kratek pregled zgodovine razvoja informacijske varnosti

Whitman in Mattord (2007, str. 3–4) menita, da se zgodovina informacijske varnosti začne z zgodovino računalniške varnosti. Potreba po računalniški varnosti, torej varovanju fizičnih lokacij, strojne in programske opreme pred zunanjimi grožnjami, se je močno povečala zlasti med drugo svetovno vojno. Sprva so bili varnostni ukrepi šifrirano komuniciranje, uporaba posebnih ključev, obrazno prepoznavanje pooblaščenih oseb od varnostnikov in podobno. V teh prvih obdobjih, ko so bili računalniki še izključno samostojni sistemi, brez povezav z drugimi računalniki in napravami, je bila informacijska varnost povsem neposreden proces v obliki fizičnega varovanja pred krajami oziroma uničenjem teh sistemov. Naraščajoča potreba po zagotavljanju nacionalne varnosti je razvoj peljala v smeri tehnološko bolj sofisticiranih in izpopolnjenih računalniških varnostnih ukrepov. V devetdesetih letih prejšnjega stoletja, ko so računalniki postali dostopni širši javnosti in s tem prešli tudi v množično domačo uporabo, se je povečala potreba po povezovanju računalnikov in prej zaprtih računalniških mrež v skupno svetovno mrežo. Ob koncu dvajsetega stoletja, ko je internet prestopil meje vladnih, šolskih in industrijskih organizacij, je postal svetovna mreža in s tem medsebojno povezal milijone računalniških mrež in še veliko več uporabnikov. Razvijalci in uporabniki IS so hitro spoznali, da zgolj fizično varovanje ne zadošča potrebam po informacijski varnosti, s čimer so se začele razvijati naprednejše računalniško podprte rešitve, kot so sistemi za nadzor dostopa, mehanizmi za overjanje pristnosti in podobno. Zlasti dejstvo, da zagotavljanje informacijske varnosti ob začetnem razvoju in uporabi interneta na listah prioritet ni spadalo v sam vrh, je omogočilo razmah in povečanje števila varnostnih dogodkov.

V obdobju zadnjih nekaj let je bliskovit tehnološki napredek na področju IS in postopen prehod v smeri razvoja odprtih avtonomnih sistemov odprl nova vprašanja in potrebe po razvoju varnih IS. Mouratidis (2010, str. 117) poudarja, da je že od začetnih faz in v celotnem procesu razvoja programske opreme potreben vzporeden razvoj varnostnih rešitev in ne zgolj izpopolnjevanje funkcionalnosti programa. Po njegovem mnenju je treba varnostne rešitve integrirati v programske jezike in metodologije v celotnem ciklu razvoja programske opreme, ker se tako potencialni varnostni dogodki omejijo in izolirajo že v zgodnjih fazah razvoja.

1.2.2 Opredelitev in temeljni principi informacijske varnosti

Različne opredelitve pojma informacijska varnost v strokovni literaturi so si po vsebini zelo podobne, saj v osnovi izhajajo iz opredelitev varnosti, kot je opredeljena v prejšnjem podpoglavju. Poenostavljeno lahko rečemo, da je varnost proces varovanja pred (namerno ali nenamerno) poškodbo ali uničenjem. Za varovanje informacij pa se je s časoma uveljavil izraz informacijska varnost (angl. *information security*), ki jo standardi ameriškega komiteja za nacionalne varnostne sisteme opredelijo kot varovanje informacij in njihovih kritičnih

elementov, vključujoč sisteme in strojno opremo, s katerimi se uporabljajo, shranjujejo in posredujejo informacije (Whitman & Mattord, 2007, str. 8). Na osnovi te opredelitve Grobler (2003, str. 16) poda široko in izčrpno opredelitev informacijske varnosti, ki pravi: »*Informacijska varnost je proces varovanja informacij, sistemov in strojne opreme, ki uporabljajo, shranjujejo in posredujejo informacije pred širokim naborom groženj, za zagotavljanje kontinuitete poslovanja, minimiziranja poslovne škode in maksimiziranja donosov z ohranjanjem zaupnosti, celovitosti in razpoložljivosti informacij in informacijskih sredstev.*« S to opredelitvijo je po mnenju Tryfonasa (2010, str. 208) informacijsko varnost mogoče razumeti iz treh različnih perspektiv: varovanje poslovanja pred grožnjami s ciljem minimiziranja poslovne škode, maksimiziranje donosa naložb in kot varovanje informacijskih sredstev.

V strokovni literaturi pa se poleg termina informacijska varnost izmenično uporablja tudi termin računalniška varnost (angl. *computer security*). Čeprav imata oba termina skupen cilj v zagotavljanju zaupnosti, celovitosti in razpoložljivosti, pa ju ne smemo uporabljati kot sinonima. Informacijska varnost je osredinjena na informacije, računalniška varnost pa na delovanje računalniškega sistema in virov informacij (National Institute of Standards and Technology, 1995, str. 5), kot so strojna, programska oprema in podatki, ne osredinja pa se na informacije, shranjene v njem. Trček (2006, str. 3) opozarja še na medsebojno nezamenljivost terminov varnost informacijske tehnologije (angl. *information technology security*), ki pomeni zagotavljanje varnosti računalniških sistemov s tehnološkega vidika, in varnost informacijskih sistemov (angl. *information systems security*), ki pa pomeni zagotavljanje varnosti računalniških sistemov z upoštevanjem človeškega faktorja.

Od samih začetkov razvoj področja informacijske varnosti temelji na konceptu, ki je v industriji med poznavalci informacijske varnosti poznan kot »CIA-tirada« ali »CIA-trikotnik«. Gre za temeljni koncept, ki je kot standard informacijske varnosti v uporabi že več kot dvajset let (Puangsri, 2009, str. 17). Osnovni principi informacijske varnosti CIA-triade s slike 1 so zaupnost (angl. *confidentiality*), celovitost (angl. *integrity*) in razpoložljivost (angl. *availability*), pri čemer kratica *CIA* izhaja iz začetnic teh principov v angleščini.

Večina opredelitev informacijske varnosti iz strokovne literature temelji na konceptu CIA-trikotnika. Podobno velja tudi za mednarodne standarde, med katerimi je s področja informacijske varnosti najpogosteje citiran ISO/IEC 27002 (International Organization for Standardization, 2005b, str. 1), ki informacijsko varnost opredeljuje kot »ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij; poleg tega pa tudi ohranjanje drugih lastnosti, kot so verodostojnost, odgovornost, neovrgljivost in zanesljivost«. Standard s tem potrjuje, da je varovanje informacij temeljna skrb informacijske varnosti in temeljna disciplina za zagotavljanje osnovnih principov. Aoufi (2009, str. 4–5) dodaja, da glede pomembnosti principov hierarhija med njimi ne obstaja. Pomembnost posameznega principa je odvisna od konteksta uporabe, pri čemer velja, da v vseh primerih za zagotavljanje ustrezne ravni informacijske varnosti ni treba zagotoviti vseh treh principov hkrati. Na primer za informacije javnega značaja je pomembno, da so celovite in razpoložljive, medtem ko zaupnosti zaradi njihove narave in ciljnega občinstva ni treba zagotoviti. Razlaga posameznih principov s primeri je podana v nadaljevnju:

Slika 1: CIA-triada

Vir: Prirejeno po P. Puangsri, Quantified Return On Information Security Investment – A Model for Cost–Benefit Analysis, 2009, str. 18.

- **Zaupnost informacij**

  Po standardu ISO 27001 (International Organization for Standardization, 2005a, str. 2) zaupnost informacij pomeni zagotavljanje dostopnosti informacije samo pooblaščenim osebam. Zaupnost informacije je zagotovljena, kadar do nje lahko dostopajo izključno tiste osebe, ki imajo vnaprej odobren dostop oziroma podeljene pravice, ne glede na to, kje in v kakšni obliki je informacija shranjena. Kadar se zgodi, da nepooblaščena oseba (ali sistem) zaupno informacijo vidi oziroma do nje dostopi, govorimo o varnostnem dogodku kršitve zaupnosti. Na primer pri plačevanju s kreditno kartico preko interneta se s transakcijo prenašajo tudi informacije o številki kreditne kartice in njeni varnostni kodi. Plačilni sistem zaupnost zagotavlja s šifriranjem teh prenesenih podatkov, z omejevanjem lokacij, kjer se informacija shranjuje (podatkovne baze, strežniški dnevniki, varnostne kopije,…) in z omejevanjem dostopa do teh lokacij (Feruza & Kim, 2007, str. 19). Torej varnostni dogodek nastopi, če je na primer informacija o številki kartice in/ali varnostni kodi kadarkoli v tem procesu dostopna nepooblaščeni osebi ali sistemu. Do dogodka glede kršitve zaupnosti lahko pride namerno ali nenamerno ter na več različnih načinov[2]: fizična kraja prenosnega računalnika, na katerem so zaupne informacije; vdor hekerja v bazo podatkov spletnega podjetja, kjer so shranjeni osebni podatki kupcev in poslovnih partnerjev; kadar zaposleni zavrže papirni dokument z zaupnimi podatki, ne da bi ga uničil; kadar je elektronska pošta pomotoma poslana nepooblaščenim prejemnikom zunaj podjetja in podobno. Whitman in Mattord (2007, str. 11) ter Tipton (2004, str. 18) opozarjajo, da je vrednost zagotavljanja zaupnosti informacij še posebej visoka, kadar gre za osebne podatke ljudi (zaposlenih, kupcev, pacientov, …), saj ti posamezniki pričakujejo, da bodo njihovi osebni podatki ostali zaupni, ne glede na to, kdo jih hrani. Za zagotavljanje zaupnosti informacij so na voljo

[2] Podrobnejši opis s primeri najpogostejših načinov kršitve zaupnosti je podan v članku Tiptona (2004, str. 19).

različne metode, kamor prištevamo (Whitman & Mattord, 2007, str. 11): klasifikacijo informacij, varno shranjevanje dokumentov, apliciranje splošnih varnostnih politik in izobraževanje varuhov informacij ter končnih uporabnikov. Poleg navedenih metod so se v stroki razvili tudi posebni modeli[3] za zagotavljanje zaupnosti informacij, ki natančno opisujejo ukrepe in specificirajo način uporabe varnostnih orodij za dosego želene ravni zaupnosti informacij (Tipton, 2004, str. 20).

- **Celovitost informacij**
  Standard ISO 27001 (International Organization for Standardization, 2005a, str. 2) celovitost informacij opredeli kot varovanje pravilnosti in popolnosti informacije. S celovitostjo je zagotovljeno, da podatki pravilno in nespremenjeno predstavljajo originalno varovano informacijo ter da so zaščiteni pred namernimi in nenamernimi nepooblaščenimi spremembami. Primeri kršenja celovitosti informacij (Feruza & Kim, 2007, str. 19) so lahko povsem nedolžne in nenamerne narave, denimo, ko zaposleni pomotoma izbriše datoteke, ki niso ključnega pomena za podjetje, ali če pomotoma napačno vtipka naslov stranke v podatkovno bazo. Kršenje je lahko tudi namerno v obliki načrtnega izbrisa strateških podatkov podjetja, nepooblaščenega spreminjanja podatkov na spletni strani podjetja, oddajanja velikega števila odgovorov v spletnih nagradnih igrah in podobno. Primeri, ko je zagotavljanje celovitosti informacij kritičnega pomena za uporabnike (Tipton, 2004, str. 21), so npr. pri nadzoru zračnega prometa, pri vojaških obrambnih sistemih, pri sistemih socialnega varstva, plačni sistemi in podobno.

- **Razpoložljivost informacij**
  Razpoložljivost informacij po opredelitvi ISO 27001 (International Organization for Standardization, 2005a, str. 2) pomeni vzpostavitev in vzdrževanje nemotenega dostopa do informacij pooblaščenim osebam vsakič, ko jih potrebujejo. Torej gre za stanje, v katerem ne pride do onemogočenega dostopa do informacij zaradi naravnih nesreč (npr. potres, poplave), človeških dejanj (npr. stavka zaposlenih), izpada dobave elektrike ali pa namerne ohromitve razpoložljivosti sistema – DoS-napad (angl. *denial of service attack*), napad računalniškega črva, ki ohromi ali celo povsem onemogoči uporabo računalnikov v mreži.

Zagotavljanje teh temeljnih principov informacijske varnosti je enako pomembno od samega začetka razvoja področja pa vse do danes (in bo ostalo tudi v prihodnosti). V začetnih fazah razvoja, ko so bila računalniška okolja še relativno enostavna, so ti trije principi zadostovali za zagotavljanje ustrezne ravni informacijske varnosti. Vendar pa CIA-trikotnik z razvojem računalniške industrije in mnogo večje kompleksnosti okolja ne zadošča več. Tako je zaradi omejitev načina CIA-trikotnika Donn B. Parker predstavil alternativni model (Wu, 2009, str. 92). Z njim je dodal še tri principe in tako razširil CIA-triado, model pa poimenoval »Šest atomskih elementov informacije« (angl. *Parkerian Hexad*):

[3] Na primer model Bell–LaPadula, modeli za nadzor dostopa – glej Tipton (2004, str. 20) in Slay in Koronios (2006, str. 52).

- **Posest ali nadzor informacij**
  To pomeni ohranjanje nadzora (angl. *control*) in zmožnosti uporabe informacije (Wu, 2009, str. 92). Primer je lahko izguba ali kraja ovojnice z zaupnimi podatki (npr. zdravniški izvid), s čimer je prišlo zgolj do kršenja posesti (angl. *possession*) oziroma nadzora nad informacijo v primeru, da nepooblaščena oseba ovojnice ne najde oziroma ne odpre. Vendar pa, ker lastnik informacije nad tem nima nadzora, ga lahko povsem upravičeno skrbi kršitev zaupnosti.

- **Originalnost ali pristnost informacij**
  Standard ISO/IEC 13335-1 originalnost oziroma pristnost (angl. *authenticity*) opredeli kot lastnost, ki zagotavlja, da je identiteta osebe ali sredstva natančno tista, za katero se izdaja (Steichen, b.l., str. 7). Informacija je originalna, ko je na primer shranjena ali posredovana v enakem stanju kot takrat, ko je bila ustvarjena. Pogost primer kršenja je ponarejanje podatka o naslovu pošiljatelja elektronske pošte (angl. *E-mail spoofing*), s čimer prejemnika pretenta, da odpre elektronsko pošto, kar sicer zelo verjetno ne bi storil.

- **Uporabnost informacij**
  Uporabnost (angl. *utility*) pomeni zagotavljanje oblike informacij, ki imajo za uporabnika določeno vrednost, ki se uporablja za točno določen namen oziroma izpolnitev cilja (Whitman & Mattord, 2007, str. 12). Primer kršenja uporabnosti je sprememba formata shranjenih podatkov, ki v obstoječi informacijski arhitekturi zato ne bi bili več uporabni (bi pa bili zaupni, celoviti, razpoložljivi v posesti in originalni).

Čeprav ta model dopolni CIA-trikotnik, pa glede na razvoj informatike še ne zadosti vsem potrebam po zagotavljanju informacijske varnosti. Wu (2009, str. 93) meni, da sta še dva principa informacij, ki ju ta model ne vključuje in ki sta ključnega pomena za zagotavljanje ustrezne ravni informacijske varnosti glede na potrebe in kompleksnost okolja:

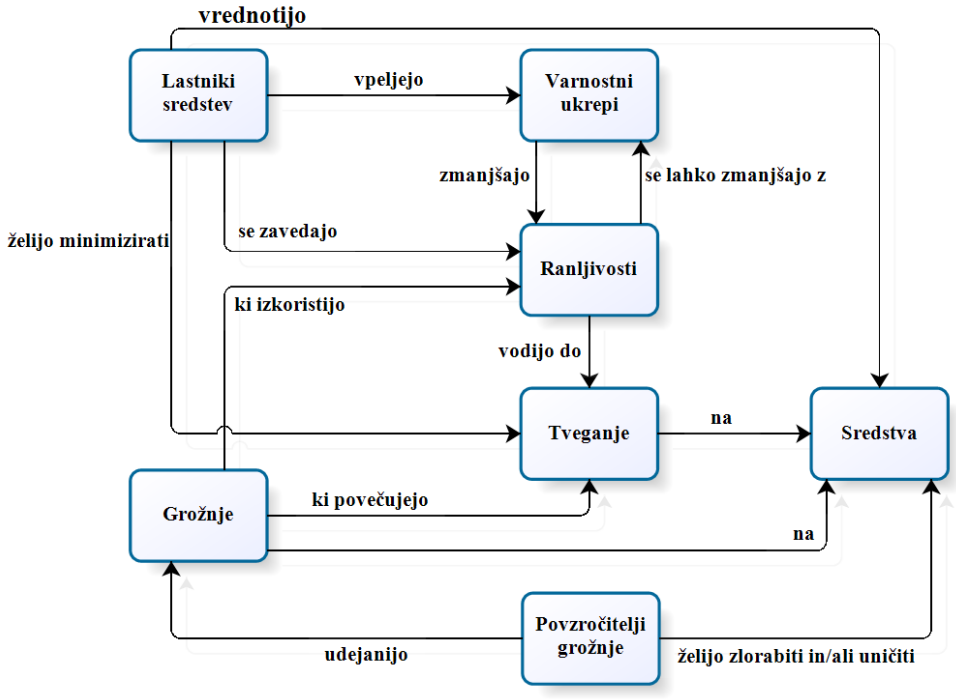
- **Neovrgljivost informacij**
  Standard ISO/IEC 13335-1 jo opredeli kot zmožnost dokazovanja dogodka, ki se je zgodil na način, da ga kasneje ni mogoče zanikati (Steichen, b.l., str. 7). Torej, tako kot pošiljatelj ne more zanikati, da informacije ni poslal, tudi prejemnik ne more zanikati, da jo je prejel. Uporaba metod za zaščito neovrgljivosti (angl. *non-repudiation*) je pri elektronskem poslovanju (Feruza & Kim, 2007, str. 20), kjer se uporabljajo orodja, kot je digitalni podpis in šifriranje.

- **Zasebnost informacij**
  Zasebnost (angl. *privacy*) se nanaša na medsebojno povezavo med tehnologijo in pravno pravico zbiranja, hranjenja in posredovanja osebnih podatkov (Feruza & Kim, 2007, str. 23). Tehnologija za zagotavljanje zasebnosti na eni strani podatke in informacije ščiti pred nepooblaščenim dostopom, po drugi pa mora lastniku omogočiti upravljanje z njimi (npr. da lahko sam podeljuje pravice posameznikom in/ali sistemom za dostop do podatkov).

1.2.3 Shema povezave pojmov

Za boljše razumevanje in učinkovitejšo uporabo konceptov informacijske varnosti je potrebno poznanje povezav med temeljnimi komponentami. Pri tem je uporaba vizualne predstavitve (slika 2) uporabno orodje, vendar ne smemo pozabiti, da gre za splošen prikaz, ki se uporablja kot vodilo za preprečevanje in/ali reševanje varnostnih dogodkov.

Slika 2: Povezava med temeljnimi komponentami informacijske varnosti



Vir: E.S. Aoufi, Economic Evaluation of Information Security, 2009, str. 5.

Standard ISO 27001 (International Organization for Standardization, 2005a, str. 2), ki po standardu ISO 13335-1 povzema definicijo, **sredstvo** (angl. *asset*) opredeli kot »vse, kar ima določeno vrednost za podjetje«. Tsiakis (2010, str. 8) sredstva deli na otipljiva ali materialna (strojna in programska oprema, človeški viri, …) in neotipljiva ali nematerialna (blagovna znamka, ugled podjetja, zunanji dejavniki, …). Številna sredstva v podjetju so v obliki informacij, ki se hranijo, obdelujejo in posredujejo z uporabo IT za izpolnjevanje varnostnih zahtev. **Lastnik sredstva** (angl. *asset owner*) je tisti (podjetje, skupina ljudi, posameznik), ki sredstvo ovrednoti oziroma mu pripisuje vrednost, ima pa tudi od vodstva dodeljeno odgovornost za vzpostavitev kontrole in mehanizmov za njegovo varovanje (National Institute of Standards and Technology, 2011, str. 92). Na drugi strani tudi **povzročitelj grožnje** (angl. *threat agent*) sredstvo ovrednoti in ga za doseganje lastne koristi zlorabi oziroma uporabi v nasprotju z interesi lastnika. Vidalis in Jones (2005, str. 371) povzročitelje groženj opredelita kot posameznika ali skupino ljudi, ki ima interes (korist) za izvedbo napada na informacijsko infrastrukturo. V osnovni delitvi[4] bi za povzročitelje groženj razlikovali med naravnimi pojavi (požar, poplava,

[4] Podrobnejša delitev je podana v člankih Vidalisa in Jonesa (2005) ter Vidalisa (2003).

potres) in človeškim faktorjem (zlonamerni uporabniki, nenamerne napake uporabnikov), sicer pa so glede na literaturo in standarde mogoče različne delitve.

Različni povzročitelji so tako vir **grožnje** (angl. *threat*), ki jih standard ISO 27002 (International Organization for Standardization, 2005b, str. 3) povzeto po standardu ISO 13335-1 enostavno opredeli kot »potencialni vzrok neželenega dogodka, ki lahko povzroči škodo sistemu ali podjetju«. Lastniki sredstev v podjetju imajo grožnje za potencialno škodo na sredstvu, zaradi česar se njegova vrednost zmanjša. Chen (2009, str. 6) dodaja, da je grožnje potrebno razumeti v kontekstu obstoječe **ranljivosti** (angl. *vulnerability*), ki jo standard ISO 27002 (International Organization for Standardization, 2005b, str. 3) opredeljuje kot »šibkost sredstva, ki jo grožnja lahko izrabi«. Ranljivost je lahko tehnična napaka (Chen, 2009, str. 6), ki se na primer rešuje z uporabo specializiranih programskih orodij, lahko pa je vezana na človeški faktor (premalo osebja za pokrivanje vseh varnostnih vidikov, pomanjkljiva izobrazba osebja, neupoštevanje varnostnih politik, …). Tako lastnik sredstva na osnovi zaznanih groženj in poznanja ranljivosti ocenjuje **tveganje** (angl. *risk*) za nastanek škode. Ker se opredelitve tveganja v literaturi razlikujejo, jih Aoufi (2009, str. 8) v kontekstu informacijske varnosti povzame in tveganje opredeli kot »*verjetnost, da bo povzročitelj grožnje izkoristil ranljivosti za povzročitev škode oziroma izgube zaradi kršenja zaupnosti, celovitosti in razpoložljivosti sredstva*«. Iz opredelitve izhaja, da je tveganje funkcija verjetnosti nastanka grožnje, ranljivosti in učinka na vrednost sredstva, ki ga povzroči uresničena grožnja. Ker je lastnik sredstva v podjetju odgovoren za njegovo varovanje, je motiviran, da z vpeljavo **varnostnih ukrepov** (angl. *countermeasures*) zmanjšuje (minimizira) tveganje zanj. Varnostni ukrep je torej delovanje, naprava ali postopek, ki zmanjšuje ranljivosti, grožnje ali prepreči oziroma omejuje napade in škodo, ki jo povzročijo (National Institute of Standards and Technology, 2011, str. 49).

1.2.4 Implementacija informacijske varnosti

Implementacija informacijske varnosti je postopen proces, ki zahteva usklajevanje, čas in napore, ter lahko poteka v dveh smereh: od spodaj navzgor ali od zgoraj navzdol.

Način implementacije od spodaj navzgor (angl. *bottom–up approach*) pomeni, da posamezni tehniki in sistemski administratorji sami poskušajo zagotoviti in povečati informacijsko varnost sistemov, ki jih upravljajo (Whitman & Mattord, 2007, str. 18). Caballero (2010, str. 16) ob tem dodaja, da medsebojno povezana področja oziroma nivoji informacijske varnosti kot celota ne delujejo, če na najnižjem nivoju (fizično varovanje) varovanje ni ustrezno zagotovljeno. Prednost tega načina je, da temelji na strokovnem znanju posameznih tehnikov in administratorjev, njihovem poznanju groženj in ranljivosti sistema, s katerimi se pri svojem delu vsak dan srečujejo. Slabost in razlog, da tovrsten način le redko vodi v celovito in uspešno zagotavljanje varnosti sistema celotne organizacije, je pomanjkanje podpore vodstva projektu, posledično pa tudi pomanjkljivo sodelovanje zaposlenih.

Pri načinu od zgoraj navzdol (angl. *top–down approach*) je projekt implementacije informacijske varnosti sprožen od najvišjega vodstva, ki se ravna po pravilih varnostne politike organizacije in

ima jasno zastavljene cilje projekta (Whitman & Mattord, 2007, str. 19). Projekti za zagotavljanje informacijske varnosti so s tem načinom praviloma uspešnejši zaradi popolne podpore vodstva, zagotovljenih finančnih sredstev in moči vodstva, da vpliva na organizacijsko kulturo. Kot to velja za vse večje projekte v organizacijah, je podpora vodstva ključni dejavnik uspeha tudi pri projektih informacijske varnosti. Vodstvo mora nadzirati in pospeševati potek projekta ter zagotavljati sodelovanje vseh zaposlenih. Pomembno vlogo ima tudi dokumentiranje vseh procesov in postopkov, ki morajo biti integrirani v organizacijsko kulturo, zato da fluktuacija zaposlenih nebi bila razlog za neuspeh projekta.

1.2.5 Vpliv človeških virov na informacijsko varnost

Pregled rezultatov raziskav s področja informacijske varnosti (podrobneje v nadaljevanju) podaja dejstvo, da kljub številnim raziskavam in razvoju še zdaleč nismo na točki, ko bi lahko trdili, da je mogoče zagotoviti in vzpostaviti popolno varen IS. Mouratidis (2010, str. 115) razlog vidi v tem, da se zagotavljanje varnosti pogosto razume zgolj kot tehnični problem, ki se rešuje s standardnimi varnostnimi mehanizmi (npr. sistem avtentikacije). Tako se rešuje tehnična plat problema, zapostavlja pa se socialno dimenzijo varnosti in dejstvo, da je človeški faktor razlog za številne varnostne dogodke. V literaturi je človeški faktor pogosto označen kot najšibkejši člen varnosti IS (Henry, 2004, str. 51; Trček, 2006, str. 8; Whitman & Mattord, 2007, str. 16), zato tudi mednarodni standardi, točneje, osmo poglavje standarda ISO 27002 (International Organization for Standardization, 2005b, str. 23–28) podajajo postopke ravnanja s človeškimi viri za zagotavljanje informacijske varnosti.

Zato je toliko bolj pomembno, da ima podjetje za zagotavljanje varnosti jasno opredeljeno varnostno politiko in enako kot pri implementaciji informacijske varnosti predano vodstvo, ki projektom daje popolno podporo. Vendar pa varnostna politika sama po sebi še ne prinaša rezultatov, če ozaveščenost in znanje zaposlenih nista na ravni, ki bi zagotavljala pravilno uporabo tehnologije in spoštovanje predpisanih postopkov. Zato je pomembno, da vodstvo zaposlene motivira ter zagotavlja njihovo konstantno izobraževanje in ozaveščanje. Henry (2004, str. 54) ob tem poudarja, da mora biti izobraževanje prilagojeno funkcijam in tveganjem, ki so jim posamezni profili zaposlenih izpostavljeni. Predvsem pa mora biti povezano s konkretnimi primeri iz prakse ter dovolj pogosto (v okviru rednih sestankov), da so zaposleni seznanjeni z aktualnimi grožnjami in primeri varnostnih dogodkov. Med slednjimi se v zadnjem času[5] pogosto omenjajo tehnike za pridobivanje zaupnih podatkov od zaposlenih, imenovane socialni inženiring (angl. *social engineering*), ki nato zlonamernim uporabnikom omogočajo vdor v sistem (Duff, 2005, str. 68).

[5] Po raziskavi podjetja Dimensional Research (2011) iz septembra 2011 se 97% varnostnih strokovnjakov zaveda groženj socialnega inženiringa, 43% vprašanih je že bilo tarča tovrstnih napadov, 41% pa jih tega nedvomno ne more zanikati.

1.2.6 Tehtanje med varnostjo in uporabnostjo

Glede na ugotovitve iz prejšnjega podpoglavja izhaja dejstvo, da je popolno informacijsko varnost nemogoče zagotoviti. V tem leži temeljni konflikt med varnostjo in uporabnostjo. Na eni strani dopuščanje povsem prostega pretoka informacij kot glavne prednosti in uporabnosti IT ogroža celovitost informacij, po drugi pa močno zavarovan IS prekomerno omejuje uporabnike pri uporabi vseh funkcionalnosti IT. Zato Whitman in Mattord (2007, str. 17) poudarjata, da je treba doseči uravnotežen nivo med varnostjo in uporabnostjo IS. V praksi pa se po navedbah Soo Hoo (2000, str. 3) pogosto dogaja, da podjetja uporabnost postavljajo pred varnost. Zato je za doseganje tega nivoja ključnega pomena, da se vsi deležniki v podjetjih in organizacijah zavedajo skupnega cilja – da so podatki dostopni v času in v obliki, kot se potrebujejo (Whitman & Mattord, 2007, str. 18).

1.3 Standardi področja informacijske varnosti

Standard je v splošnem pomenu sestav zahtev, ki jih material, izdelek, storitev ali sistem mora izpolnjevati. Če imamo opravka s standardiziranim sistemom, smo lahko prepričani, da gre za sistem, ki v celoti izpolnjuje vse zahteve standarda, za katerega je pridobil ustrezen certifikat. Tofan (2011, str. 128) navaja, da uporaba standardov zagotavlja želene in/ali pričakovane lastnosti izdelkov in storitev, kot so kvaliteta, varnost uporabe, zanesljivost, učinkovitost in izmenljivost ob stroškovni učinkovitosti. Čeprav so standardi napisani za potrebe posameznih industrij, pa sta Bhasker in Kapoor (2010, str. 55) mnenja, da so standardi informacijske varnosti lahko uporabni za različna področja, če jih uporabniki prilagodijo svojim potrebam in ciljem.

Uporaba standardov omogoča primerjave uspešnosti med podjetji v panogi (angl. *benchmarking*), kar velja tudi za področje informacijske varnosti, v okviru katerega podjetja z uporabo tovrstnih primerjav ocenjujejo lastne sisteme upravljanja informacijske varnosti (Humphreys, 2007, str. 8). Za doseganje ustrezne ravni informacijske varnosti različne organizacije izdajajo standarde, vodstva držav pa sprejemajo zakonodajo, s čimer zagotavljajo učinkovito uporabo sredstev in množično uporabo dobrih praks v gospodarstvu. Tofan (2011, str. 129) pojasnjuje, da standardi informacijske varnosti, podobno kot standardi za druga področja, vsem deležnikom (zaposlenim, dobaviteljem, kupcem, ...) dajejo zagotovilo, da podjetje na certificiran način zagotavlja varnost svojih poslovnih procesov in aktivnosti. Standardi in primeri dobrih praks s področja informacijske varnosti, za katere je pregled literature pokazal, da se uporabljajo najpogosteje, so predstavljeni v nadaljevanju.

1.3.1 Serija standardov ISO/IEC 27000

Standardi serije ISO/IEC 27000, poznani tudi kot družina standardov sistema za upravljanje informacijske varnosti (angl. *Information Security Management System*) ali na kratko ISO27k (angl. *ISO27k Family*), vključujejo standarde s področja informacijske varnosti, ki jih skupaj objavljata organizaciji International Organization for standardization (v nadaljevanju ISO) in International Electrotechnical Commission (v nadaljevanju IEC). Serija teh standardov podaja

priporočila najboljše prakse za upravljanje informacijske varnosti, tveganj in vpeljave varnostnih kontrol v okviru sistema za upravljanje informacijske varnosti (v nadaljevanju SUIV). Serija je namenjena širokemu področju uporabe ter podjetjem različnih oblik in velikosti, saj zajema širše področje varnosti kot samo zagotavljanje zasebnosti, zaupnosti in tehnično-varnostne rešitve (Tofan, 2011, str. 128).

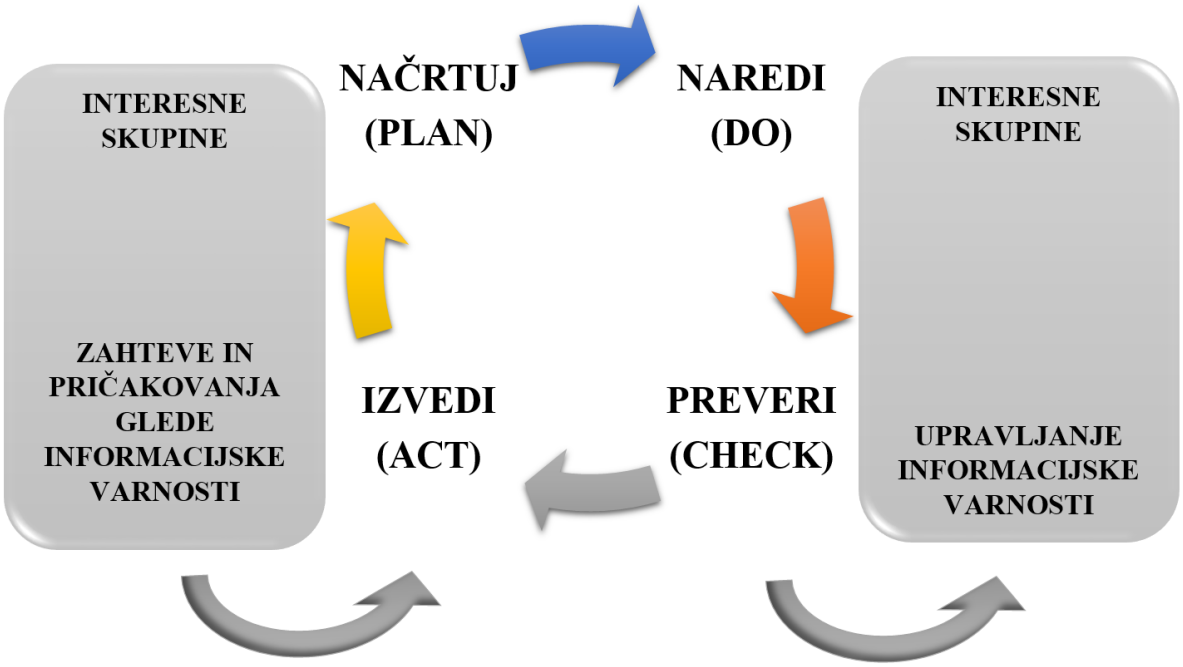
Prvi izmed standardov te serije (ISO27001) je bil objavljen leta 2005[6] po reviziji standarda ISO/IEC17799, objavljenega leta 2000. Prav ISO/IEC17799 velja za predhodnika[7] standardov družine ISO27k, saj izhaja iz drugega dela britanskega standarda BS7799, ki z vsebinskega vidika predstavlja specifikacijo SUIV (Humphreys, 2007, str. 20). V nadaljevanju so na kratko predstavljeni najpomembnejši izdani[8] standardi družine ISO27k (Humphreys, 2007; Tofan, 2011; Plate, 2011; Clinch 2009):

- **ISO/IEC 27000 – Pregled in izrazje**
  Ta standard opisuje temeljne principe, koncepte in izrazoslovje za celotno serijo ISO27k standardov. Poleg tega podaja pregled in medsebojne povezave med standardi in je namenjen uporabnikom vseh preostalih standardov te serije, saj pomeni enotno skupno točko za začetno razumevanje.

- **ISO/IEC 27001 – Sistemi upravljanja informacijske varnosti – zahteve**
  Standard opredeli sedem ključnih elementov za oblikovanje in vzpostavitev certificiranega SUIV v vseh vrstah podjetij in organizacij. Torej natančno opredeli zahteve za vzpostavitev, implementacijo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje dokumentiranega SUIV. Pri tem ne zahteva uporabe točno določenih varnostnih kontrol, temveč določa postopke in zahteve, potrebne za identificiranje kontrol, ki so primerne glede na specifike posameznega podjetja. Standard po reviziji leta 2002 uvaja uporabo cikličnega modela »Plan–Do–Check–Act« (v nadaljevanju PDCA-model), na osnovi katerega podjetja vzpostavijo zanje ustrezno raven informacijske varnosti, ki jo z rednim spremljanjem in pregledovanjem učinkovitosti vpeljanega SUIV zagotavljajo tudi v prihodnosti. Omenjeni PDCA-model (slika 3) je sestavljen iz štirih faz, kjer faza »načrtuj« (angl. *plan*) pomeni oblikovanje SUIV z oceno tveganj informacijske varnosti in izborom ustreznih varnostnih kontrol glede na politiko podjetja. Faza »naredi« (angl. *do*) zahteva implementiranje in delovanje oblikovanega SUIV, faza »preveri« (angl. *check*) pa pregledovanje in ocenjevanje uspešnosti SUIV ter poročanje rezultatov vodstvu. Četrta faza »izvedi« (angl. *act*) zahteva izvedbo ugotovljenih potrebnih (preventivnih in kurativnih) sprememb in izboljšav v praksi za izboljšanje vzpostavljenega SUIV. Slika 3 tako ilustrativno prikazuje, da se vhodni elementi, torej varnostne zahteve in pričakovanja interesnih skupin glede informacijske varnosti v SUIV, v procesih in aktivnostih preoblikujejo v izhodne elemente, ki te zahteve in pričakovanja izpolnjujejo.

[6] Istega leta je organizacija ISO vpeljala razvoj standardov družine ISO27k s številčenjem od 27000 dalje.
[7] Podrobnejši opis zgodovine razvoja standarda presega vsebinski okvir tega magistrskega dela.
[8] Po podatkih o objavi standardov z dne 11.7.2012.

Slika 3:Povezava med koraki PDCA-modela



Vir: International Organization for Standardization, ISO/IEC 27001 Information technology – Security technique s– Information security management systems – Requirements, 2005a, str. vi.

V praksi se ta standard pogosto uporablja v kombinaciji s standardom ISO/IEC 27002, saj, kot je navedeno, opredeli elemente in zahteve za vzpostavitev SUIV, medtem ko ISO/IEC 27002 navaja in predlaga varnostne kontrole, ki jih podjetje lahko uporabi glede na lastne značilnosti in posebne zahteve po varovanju informacij.

- **ISO/IEC 27002 – Pravila obnašanja pri kontrolah informacijske varnosti**
  Kodeks ravnanja združuje najboljše prakse za varovanje informacij (ne glede na obliko, v kateri se nahajajo), pri čemer informacijsko varnost opredeljuje s konceptom CIA-trikotnika. Standard opredeljuje varnostne kontrole za vsako področje upravljanja informacijske varnosti, pri čemer podaja navodila za njihovo implementacijo na način, ki zagotavlja izpolnjevanje opredeljenih ciljev. Osnovni namen standarda, na katerem temeljijo vse njegove verzije, je minimiziranje tveganj in vplivov na poslovanje podjetja ob hkratnem maksimiziranju izkoristka poslovnih priložnosti in zagotavljanju nemotenega poslovanja.

- **ISO/IEC 27003 – Smernice za izvedbo sistema upravljanja informacijske varnosti**
  Zagotavlja pomoč in podaja napotke za vzpostavitev SUIV glede na specifikacije, ki jih podaja ISO/IEC 27001. Poleg tega podaja še dodatne informacije glede uporabe PDCA-modela in deluje kot vodilo za izpolnjevanje zahtev na njegovih posameznih stopnjah.

- **ISO/IEC 27004 – Upravljanje informacijske varnosti - merjenje**
  Uporabnikom podaja specifikacije za uporabo postopkov in tehnik merjenja učinkovitosti SUIV, pri čemer vsebinsko obsega procese upravljanja informacijske varnosti (opredeljene v ISO/IEC 27001) in področje varnostnih kontrol (opredeljenih v ISO/IEC 27002).

- **ISO/IEC 27005 – Upravljanje tveganj informacijske varnosti**
  Vsebuje navodila za upravljanje s tveganji v okviru SUIV za vse vrste podjetij in organizacij. Vsebinsko dopolnjuje temeljne koncepte iz ISO/IEC 27001 ter pomaga pri implementaciji in zagotavljanju informacijske varnosti na osnovi ocenjevanja tveganj.

- **ISO/IEC 27006 – Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti**
  Za akreditirane revizorje podaja zahteve in navodila za izvedbo procesov pri podeljevanju certifikatov za SUIV, pri čemer dopolnjuje zahteve iz standarda ISO/IEC 17021.

- **ISO/IEC 27007 – Smernice za revizijo sistemov upravljanja informacijske varnosti**
  Akreditiranim podjetjem in posameznikom daje navodila za izvedbo revizije SUIV pri naročnikih, pri čemer se osredinja na revizijo skladnosti zahtev, podanih v ISO/IEC27001.

Poleg predstavljenih družino standardov ISO27k sestavljajo še številni drugi standardi, pri čemer so še v različnih fazah razvoja, kar ISO redno in ažurno objavlja na svojih spletnih straneh.

1.3.2 Serija standardov NIST SP800

Ameriška organizacija NIST od leta 1990 izdaja publikacije iz serije SP800 (Special Publications 800) s področja računalniške varnosti. NIST je bil ustanovljen leta 1901, deluje pa kot vladna agencija, razdeljena na različne oddelke, od katerih je oddelek za računalniško varnost odgovoren za izdajo standardov in smernic serije SP800. To serijo standardov sestavlja več sto publikacij in dokumentov, ki obsegajo praktično vsa področja in vidike informacijske varnosti. Temeljni dokument serije iz leta 1995 »An Introduction to Computer Security: The NIST Handbook« obsega vse pomembne principe informacijske varnosti, njegov namen pa je dajati pomoč in smernice pri vzpostavitvi sistema varovanja informacijskih virov (strojne in programske opreme, informacij). Ta priročnik sicer podrobno ne specificira uporabe točno določenih varnostnih kontrol, vendar pa skupaj s sočasno uporabo preostalih vsebinsko specializiranih publikacij iz serije SP800 opredeljuje specifične strategije, postopke in varnostne kontrole za točno določene primere in področja informacijske varnosti. Ker se področje informacijske varnosti nenehno razvija, tudi NIST izvaja stalne revizije in posodobitve publikacij, oddelek za računalniško varnost pa v povprečju šestkrat na leto izdaja publikacijo »ITIL Security Bulletin«, ki v vsaki številki poglobljeno predstavlja določeno aktualno tematiko s področja informacijske varnosti.

1.3.3 ITIL

Information Technology Infrastructure Library (v nadaljevanju ITIL) je zbirka najboljših praks upravljanja storitev IT (angl. *IT Service Management* – v nadaljevanju ITSM). V svoji trenutno zadnji izdaji,[9] poznani kot »ITIL V3« in »ITIL 2011 Edition«, zajema serijo petih publikacij, od katerih vsaka posebej obsega določeno stopnjo cikla uvedbe ITSM. Zbirka opisuje procese, funkcije in strukture, ki podpirajo večino področij ITSM z vidika ponudnika storitev, pri čemer promovira uporabo načina za doseganje poslovne uspešnosti in učinkovitosti storitev IT. ITIL-zbirka dobrih praks je skupek znanja in izkušenj strokovnjakov z vsega sveta, pri čemer se z rednimi revizijami in posodobitvami zagotavlja aktualnost vsebin in primere praks, ki so v danem trenutku sprejete in preverjene kot najboljše oziroma najučinkovitejše. Clinch (2009, str. 7) meni, da je prav dejstvo, da posameznik pri tolikšnem znanju in raznovrstnih izkušnjah v vsakem trenutku ne zmore posedovati poglavitnih prednosti uporabe dobrih praks, kar seveda velja na splošno za vse zbirke in standarde. Osnovni namen ITIL ni, da od podjetij izrecno zahteva kakšne poslovne procese morajo vpeljati, pač pa podaja okvir dobrih praks, na osnovi katerih podjetja sama razvijajo svoje procese v skladu z značilnostmi in posebnostmi, ki jih imajo. Na področju ITSM je uveljavljen mednarodni standard ISO/IEC 20000, ki se sicer v nekaterih točkah razlikuje od ITIL, vendar pa prav slednji ponudnikom storitev predstavlja način in pot do pridobitve certifikata ISO/IEC 20000.

1.3.4 COBIT

The Control Objectives for Information and related Technology (v nadaljevanju COBIT) je podobno kot ITIL drug primer nabora najboljših praks za upravljanje varnosti IT, ki je prvič izšel leta 1996, skupaj pa ga izdajata mednarodno združenje Information Systems Audit and Control Association in IT Governance Institute. Osnovno poslanstvo COBIT-a so raziskave in razvoj, objavljanje in promoviranje uporabe sodobnih mednarodnih in splošno sprejetih informacijsko-tehnoloških kontrolnih ciljev, ki so namenjeni upravljavcem in revizorjem za vsakodnevno uporabo (Tryfonas, 2010, str. 229). COBIT-ove najboljše prakse so tako strokovnjakom in drugim uporabnikom v pomoč pri razumevanju njihovih IS ter s tem v pomoč pri optimizaciji koristi in uporabi ustreznih varnostnih kontrol z naslova razvoja in uporabe primernega modela upravljanja IT (angl. *IT governance*). Ladan, Yari in Khodabandeh (2006, str. 150) ob tem še dodajo, da je COBIT uporabno orodje, s katerim upravljavci uspešno premostijo vrzel med vpeljavo potrebnih kontrol, tehnološkimi zahtevami in poslovnimi tveganji na način, ki ga je mogoče uporabiti v podjetjih različnih velikosti in vrst. Sedanja zadnja izdaja[10] COBIT 5.0 iz junija 2012 tako kot prejšnje izdaje izhaja in gradi na spoznanjih in principih predhodne izdaje COBIT 4.1, ki jo še dodatno razširi, s čimer omogoča celovito upravljanje IT na ravni celotnega podjetja z upoštevanjem interesov notranjih in zunanjih deležnikov podjetja.

[9] Po podatkih o objavi z dne 18.7.2012.
[10] Po podatkih o objavi z dne 18.7.2012.

1.3.5 ISF-standardi najboljše prakse

Mednarodna, neodvisna in neprofitna organizacija Information Security Forum (v nadaljevanju ISF) za svoje člane oziroma naročnike redno izdaja publikacije za najboljše prakse in vodila s področja informacijske varnosti in upravljanja tveganja. ISF je bila ustanovljena leta 1989, združuje pa mednarodno članstvo večjih in manjših organizacij iz številnih sektorjev gospodarstva (transport, finančne storitve, telekomunikacije, ...). Njena temeljna publikacija za področje informacijske varnosti »The Standard of Good Practice« je bila prvič objavljena leta 1996, vsebinsko pa pomeni praktično osnovo in temelj za vzpostavitev, vodenje in vzdrževanje ustrezne ravni informacijske varnosti v podjetju. Publikacija je za zagotavljanje aktualnosti vsebine redno revidirana in izhaja dvakrat na leto, najboljše prakse pa črpa iz številnih mednarodnih standardov (ISO, NIST, COBIT, ITIL, ...), v svoji zadnji izdaji[11] pa s štirimi temeljnimi področji (upravljanje varnosti, varnostne zahteve, varnostne kontrole, spremljanje in izboljšave) podrobno zajema vse vidike informacijske varnosti ter s podrobnimi opisi primerov in ilustracijami nazorno podaja vodila za uporabo standarda v praksi.

Z uporabo standardov in najboljših praks lahko podjetja vzpostavijo učinkovite sisteme za varovanje informacij in implementirajo varnostne kontrole, s katerimi zadostijo zahtevam in potrebam po informacijski varnosti. Ker pa je ponudba standardov in najboljših praks velika, se uporabniki pogosto znajdejo pred vprašanjem, katerega od standardov izbrati, še posebej zaradi visokih stroškov implementacije (IT Governance Institute, 2008, str. 6). Pregled standardov in najboljših praks v tem poglavju je pokazal, da se slednji v nekaterih točkah medsebojno povezujejo in dopolnjujejo[12], istočasno pa se v nekaterih vidikih razlikujejo, in kot navajajo Ladan et al. (2006, str. 151), informacijsko varnost obravnavajo iz različnih zornih kotov. Zato je za zagotavljanje višje ravni informacijske varnosti priporočljivo smiselno kombiniranje različnih standardov in nacionalne zakonodaje (Ladan et al., 2006, str. 151; Sahibudin, Sharifi & Ayat, 2008, str. 753). Konkretno v Republiki Sloveniji po podatkih Slovenskega centra za obravnavo omrežnih incidentov SI-CERT zakonodajo, ki obravnava omrežno in informacijsko varnost, sestavljajo: Kazenski zakonik (Ur. l. RS, št. 95/2004-UPB1), Zakon o elektronskih komunikacijah (Ur. l. RS, št. 13/2007-UPB1), Zakon o elektronskem poslovanju (Ur. l. RS, št. 96/2009-UPB2) in Zakon o elektronskem poslovanju in elektronskem podpisu (Ur. l. RS, št. 98/2004-UPB1). Da se podjetja vedno bolj zavedajo pomena kombiniranja različnih standardov in dobrih praks, potrjujejo tudi rezultati ankete Security Management Survey (2008), kjer je po podatkih iz leta 2008 med 207 severnoameriških podjetij z več kot 1000 zaposlenimi največji delež vprašanih uporabljal kombinacijo standardov ITIL, ISO in COBIT.

Vpogled v stanje informacijske varnosti v posameznih državah in o smereh razvoja v svetu podajajo številne raziskave. Nekatere med njimi so naročene in financirane od vladnih služb, druge so rezultat raziskovalnega dela akademskih ustanov, še najpogostejše pa so letne raziskave proizvajalcev in ponudnikov zaščitne programske opreme in varnostnih storitev. Rezultati

[11] Po podatkih o objavi z dne 12.6.2012.
[12] Na primer COBIT in ISO/IEC 27002 opredelita *kaj* je potrebno narediti, ITIL pa *kako* oziroma *na kakšen način* zagotoviti ustrezno raven informacijske varnosti (IT Governance Institute, 2008, str. 6).

raziskav o številu varnostnih dogodkov in o višini stroškov, ki zaradi njih nastanejo, pritrjujejo trditvam iz točke 1 in 1.2 o tem, da gre za zelo pomembno področje, ki mu morajo uprave podjetij namenjati vedno več pozornosti. V nadaljevanju so povzete temeljne ugotovitve raziskav z rezultati, ki kažejo na stanje informacijske varnosti ter smeri razvoja v prihodnosti.

1.4 Informacijska varnost in rezultati raziskav

Raziskave o informacijski varnosti lahko v grobem razdelimo v dve skupini. V prvo spadajo tiste, ki jih izvajajo neodvisne strokovne organizacije, največkrat financirane od vladnih služb. Tovrstne raziskave neodvisno poročajo o stanju informacijske varnosti, podatki in ugotovitve iz njih pa veljajo za temeljna spoznanja, predvsem zaradi zagotovljene neodvisnosti poročanja in konsistentnosti letnih poročil. Sem spada najpogosteje citirana letna raziskava »CSI Computer Crime and Security Survey«, ki jo v sodelovanju z ameriškim Zveznim preiskovalnim uradom (angl. *Federal Bureau of Investigation*) izdaja ameriški Inštitut za računalniško varnost (angl. *Computer Security Institute*, v nadaljevanju CSI). Raziskave o informacijski varnosti posebej za področje Evropske unije (v nadaljevanju EU) od leta 2011 dalje izvaja in objavlja Agencija za mrežno in informacijsko varnost (angl. *European Union Agency for Network and Information Security*, v nadaljevanju ENISA). Njeno poročilo v analizah zajema pomembne[13] varnostne dogodke, ki so v posameznem koledarskem letu onemogočili elektronske komunikacije in storitve ponudnikov stacionarnega in mobilnega internetnega dostopa. Podatke objavlja ločeno glede na storitve stacionarne in mobilne telefonije in glede na stacionarni in mobilni internetni dostop v agregatni obliki za EU kot celoto.

Predstavitev stanja informacijske varnosti v tem poglavju temelji zlasti na rezultatih CCSS-raziskave, pri čemer bodo slednji za primerjavo postavljeni ob bok rezultatom nekaterih drugih raziskav, ki spadajo v drugo skupino. Vanjo prištevamo raziskave, ki jih izvajajo specializirana podjetja (npr. revizorske hiše), ter raziskave, ki jih izvajajo komercialni ponudniki varnostnih produktov in storitev. Zanje velja prepričanje, da so nagnjeni k ustvarjanju splošnega mnenja o zaostrovanju razmer na področju informacijske varnosti za doseganje boljše prodaje svojih proizvodov in storitev. Nikakor pa to ne pomeni, da so tovrstne raziskave zavajajoče in njihovi rezultati neresnični. Ravno nasprotno so te (večinoma brezplačne) raziskave lahko vir velikega števila uporabnih informacij ter so rezultat dela strokovnjakov z dolgoletnimi izkušnjami in odličnim poznanjem področja in razmer informacijske varnosti.

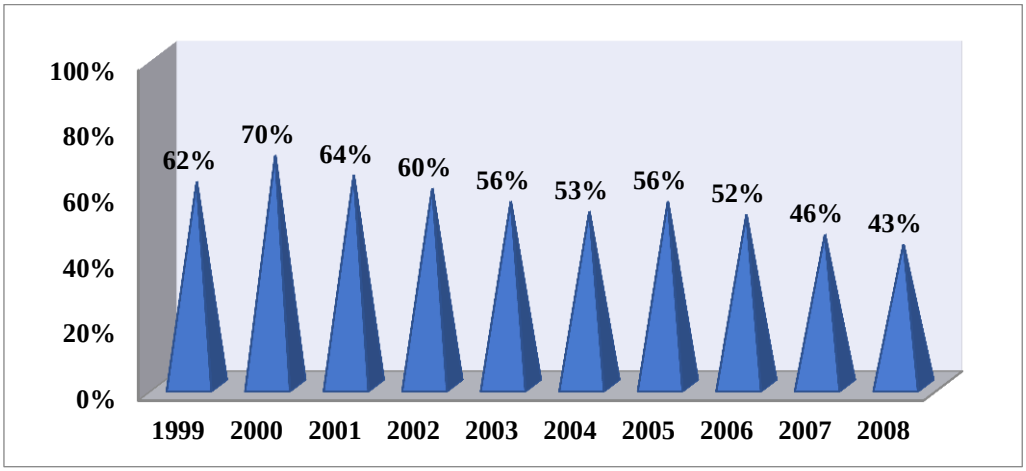
1.4.1 Rezultati raziskav

O stanju informacijske varnosti v določenem obdobju (navadno v enem letu) v prvi vrsti priča število varnostnih dogodkov, ki so jim bila podjetja izpostavljena oziroma so jih zaznala. Pri tem še pojasnilo, da gre za število vseh varnostnih dogodkov in ne zgolj za tiste, ki so jih anketiranci[14] imeli za nevarne. Po podatkih raziskave CCSS (Computer Security Institute, 2003,

[13] Tiste, ki glede na trajanje in delež prizadetih uporabnikov presegajo prag, določen za njihovo vključitev v analizo.
[14] Pri vseh raziskavah, ki jih magistrsko delo omenja, so bili rezultati pridobljeni na osnovi anket, poslanih odgovornim strokovnjakom s področja informacijske tehnologije oziroma informacijske varnosti v podjetjih.

str. 6) je večina vprašanih na letni ravni zaznala (nameren ali nenameren) napad na lasten sistem, saj se je njihovo število v obdobju 1999─2002 gibalo med 60 % in 70 %. Slika 4 razkriva, da se je leta 2005 usmeritev obrnila in kaže na upadanje števila zaznanih varnostnih dogodkov, tako da CSI (Computer Security Institute, 2010, str. 11) v svoji aktualni raziskavi CCSS poroča le še o 41 % tistih, ki so v obdobju raziskave[15] zaznali vsaj en varnostni dogodek.

Slika 4: Delež podjetij, ki so zaznala varnostni dogodek v preteklem letu



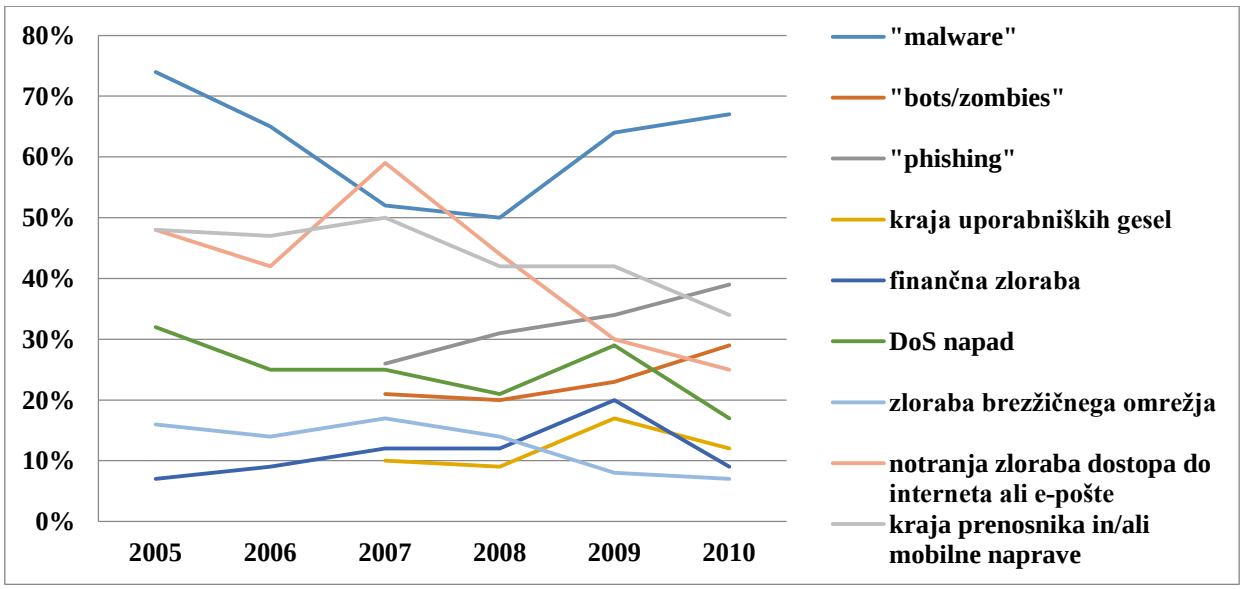
Vir: Computer Security Institute, 2005 CSI/FBI Computer Crime and Security Survey, 2005, str. 12; Computer Security Institute, 2006 CSI/FBI Computer Crime and Security Survey, 2006, str. 10; Computer Security Institute, 2007 CSI Computer Crime and Security Survey, 2007, str. 10; Computer Security Institute, 2008 CSI Computer Crime and Security Survey, 2008, str. 13.

O upadanu v zadnjih letih poroča tudi Symantec (2011, str. 12), ki v poročilu »State of Security Survey« za leto 2011 ugotavlja, da se je delež organizacij, ki so zaznale varnostne dogodke, znižal za štiri odstotke glede na podatke predhodnega leta. V poročilu leto pred tem pa omenja tudi upadanje zlonamernih aktivnosti, ki so jih v letih 2007─2009 zaznale največje države na svetu, kot so ZDA, Kitajska, Brazilija, Nemčija in Rusija (Symantec, 2010, str. 19). Poročilo ENISA (Karsberg, Skouloudi & Dekker, 2013, str. iii) za področje EU in za obdobje poročanja 2011─2013 nasprotno izkazuje povečevanje števila sporočenih varnostnih dogodkov od 51 v letu 2011 do 90 v letu 2013. Vendar podrobnejši pregled vzrokov za nastanek dogodkov pokaže, da so računalniški napadi na elektronske komunikacije le majhen delež, ki od leta 2012 tudi izkazuje upadanje (Karsberg, Skouloudi & Dekker, 2013, str. 18). Odgovor na vprašanje, katere vrste napadov[16] so bile v okviru ugotovljenih varnostnih dogodkov najpogostejše, prikazuje slika 5. Že zgodovinsko gledano je med vodilnimi vrstami napadov, ki so od leta 2008 močno v porastu, napad z uporabo zlonamerne programske opreme[17] (angl. *malware*), s katero je bilo po podatkih CCSS (Computer Security Institute, 2010, str. 17) v zadnjih dveh letih poročanja napadenih med 60 % in 70 % vprašanih. Tudi podjetje Kaspersky Lab (2012b, str. 13) za obdobje 2010─2011 ugotavlja, da je bil najpogostejši napad z zlonamerno programsko opremo,

[15] Od leta 2009 obdobje raziskave ni več preteklo koledarsko leto, temveč obdobje od julija preteklega do junija tekočega leta.
[16] Nekatere izmed vrst napadov, prikazanih v sliki 5, so podrobneje opisane v prilogi 1.
[17] Obe raziskavi (CCSS in Kaspersky) sem vključujeta še okužbo z računalniškim virusom, črvom in »spyware.«

kar so v njegovi raziskavi »Global IT Security Risks« v podobnem deležu (65─61 %) izkusila v raziskavo zajeta podjetja. V porastu je še v letu 2007 dodana kategorija napada z uporabo tehnike ribarjenja (angl. *phishing*) in uporaba programske opreme, s katero ima napadalec popolno oblast nad zlorabljenim računalnikom v mreži napadenega podjetja, v žargonu imenovanega »zombi« (angl. *bot* ali *zombie*). Tudi v Republiki Sloveniji je bila leta 2012 od SI-CERT (Slovenski center za obravnavo omrežnih incidentov, 2012, str. 10) najpogosteje obravnavana oblika varnostnega dogodka preiskava zlonamerne kode, ribarjenje in vdor v sistem. Za področje EU v prikazanih raziskavah o tem ni podatka, saj poročilo ENISA vrst in oblik napadov na elektronske komunikacije podrobneje ne prikazuje. Visoko na lestvici s slike 5 je še vedno kraja prenosnega računalnika in/ali druge mobilne naprave, ki pa je z drugimi oblikami napadov v upadanju.

Slika 5: Vrste napadov, ki jih je podjetje utrpelo v preteklem letu



Vir: Computer Security Institute, 2010/2011 Computer Crime and Security Survey, 2010, str. 15

Čeprav podjetja v zadnjih letih zaznavajo manjše število varnostnih dogodkov, so stroški oziroma izgube, ki nastanejo kot njihova posledica izredno visoki. Po podatkih inštituta Ponemon[18] (2010, str. 14) so celotni stroški varnostnega dogodka od leta 2005 naraščali in so v letu 2009 ameriško podjetje v povprečju obremenili že za 6,75 mio. USD. Da stroške, nastale zaradi varnostnih dogodkov v podjetjih, ne gre jemati zlahka, dokazuje tudi podatek, da je v istem letu najdražji varnostni dogodek ameriško podjetje stal skoraj 31 mio. USD, najcenejši pa tudi ne ravno skromnih 750 000 USD. Poleg ameriških so se v istem obdobju tudi podjetja iz Velike Britanije srečevala z visokimi in eksponentno naraščajočimi stroški te vrste. Po podatkih Infosecurity Europe in PricewaterhouseCoopers (2010, str. 18) je v letu 2009 najdražji varnostni dogodek veliko podjetje stal med 280 000 in 690 000 GBP, majhno pa med 27 500 in 55 000

[18] Nasprotno od CSI pa Ponemon v raziskavah zajema samo podjetja, ki so v preteklem letu ugotovila vsaj en varnostni dogodek.

GBP. V obeh primerih pa so podjetja ugotovila tudi več kot sto odstotno povečanje stroškov v primerjavi z letom 2007.

Iz zapisanega lahko ugotovimo, da so prav visoki in naraščajoči stroški varnostnih dogodkov med ključnimi razlogi, da podjetja kljub kriznim razmeram vse večji delež sredstev namenjajo za zagotavljanje in vzdrževanje ustrezne ravni informacijske varnosti. To trditev potrjuje podatek, da se je v obdobju od leta 2005 do 2010 delež podjetij, ki za informacijsko varnost namenijo več kot 10 % celotnega proračuna za IT, več kot podvojil (Computer Security Institute, 2010, str. 27; Computer Security Institute, 2005, str. 5). Istočasno je v tem obdobju opazno tudi upadanje deleža tistih anketirancev letnih CCSS-raziskav, ki za informacijsko varnost porabijo manj kot dva odstotka sredstev iz lastnega IT-proračuna (zmanjšanje deleža podjetij za slabih deset odstotkov).

To, da se podjetja v vse večji meri zavedajo pomena informacijske varnosti potrjujejo tudi rezultati anket, pri katerih Kaspersky Lab (2012b, str. 3─4) ugotavlja, da ima polovica vprašanih možnosti napada na IS podjetja za drugo najpomembnejšo grožnjo za poslovanje, takoj za ekonomsko negotovimi razmerami v gospodarstvu. Ob tem pa hkrati največji delež (42%) vprašanih meni, da bodo v naslednjih dveh letih prav grožnje napada na IS postale prva nevarnost na seznamu groženj, predvsem zaradi pojava novih oblik napadov in vse večjega zavedanja nevarnosti tako imenovanih napredno trajnih groženj (angl. *advanced persistent threat*, v nadaljevanju APT), ki so posledica uspešnih ciljanih napadov (angl. *targeted attacks*).

1.4.2 Smer razvoja dogodkov v prihodnje

Glede na razvoj dogodkov, kot ga kažejo raziskave, je v prihodnosti pričakovati nadaljevanje upadanja števila varnostnih dogodkov. Razlog je večja ozaveščenost uporabnikov IT, večanje deleža sredstev, namenjenih varnosti in vse več naprednih varnostnih rešitev, ki jih proizvajalci vgrajujejo v samo jedro operacijskega sistema[19]. Vendar pa omenjena pričakovanja ne smejo postati vir pretiranega optimizma, še posebej zato, ker se je že v preteklosti pokazalo, da se napadalci izredno hitro prilagajajo na vgrajene rešitve, najdejo vedno nove načine izkoriščanja ranljivosti in so že pregovorno rečeno vedno korak pred proizvajalci varnostnih rešitev. Zato se v prihodnjih letih pričakuje porast sofisticiranih ciljanih napadov, ki so, statistično gledano, sicer še vedno redki, vendar pa se njihovo število od leta 2005 eksponentno povečuje (Symantec Intelligence, 2011, str. 2). Širi se tudi nabor potencialnih tarč ciljanih napadov, saj slednji niso več omejeni zgolj na velika multinacionalna podjetja in državne organizacije, niti več na točno določene sektorje gospodarstva. Če je še pred nekaj leti veljalo, da so ciljani napadi in APT problem zlasti velikih podjetij iz obrambne industrije, finančnih storitev, energetike ali farmacije, je že v preteklem letu jasno vidna njihova širitev v vse sektorje gospodarstva. Ker se takšna smer razvoja dogodkov pričakuje tudi v prihodnje, je posledično vse močnejša tudi veja industrije, ki ponuja produkte za odkrivanje in zaščito pred ciljanimi napadi, s čimer se stopnja zaščitenosti sistemov potencialnih tarč (podjetij) izboljšuje. To dalje sili napadalce v iskanje

[19] Varnostne rešitve, vgrajene v operacijskem sistemu Windows 8 so natančneje predstavljene v članku Rashida (2012).

novih metod in tehnik za napade, imenovane tudi »zero-day attacks[20]«, s katerimi izkoriščajo določeno ranljivost aplikacije, ki jo proizvajalci in javnost med napadom še ne poznajo, zaradi česar zaščita in obramba pred njimi ne obstaja.

Druga usmeritev, ki prav tako izvira iz vse strožjih varnostnih ukrepov, je preusmeritev napadalcev neposredno na izkoriščanje napak in ranljivosti na strani uporabnika. Kaspersky Lab (2012a, str. 3) v poročilu »Cyberthreat forecast for 2012« ugotavlja, da število napadov na spletne bančne sisteme po svetu kljub uporabi visokotehnoloških varnostnih rešitev hitro narašča, kar se bo v še večjem obsegu nadaljevalo tudi v prihodnosti. Pri tem prednjačijo »phishing«-napadi, s katerimi napadalci uporabnika preusmerijo na lažno stran spletne banke, preko katere pridobijo uporabniška imena in gesla za dostop do bančnih računov. Tudi v Sloveniji so znani pogosti primeri teh vrst napadov na uporabnike NLB Klik, nazadnje v decembru 2012 (Slovenski center za obravnavo omrežnih incidentov, 2012) in v zadnjih dveh letih napad na komitente spletne banke Abanet (Phishing napad na uporabnike spletne banke Abanet, 2010) in SKB banke (Phishing napad na komitente SKB banke, 2012).

Glede na podatke o rasti in številu uporabnikov najpopularnejših socialnih omrežij, med katerimi je imel Facebook oktobra 2012 že več kot milijardo aktivnih uporabnikov (Facebook Newsroom, 2012), je v prihodnosti pričakovati, da se bo usmeritev uporabe socialnih omrežij kot trženjsko-komunikacijski kanal pri podjetjih še naprej krepila. Tako velika[21] in konstantno naraščajoča baza uporabnikov bo vsekakor še naprej zelo privlačna tarča za napade z uporabo prijemov socialnega inženiringa. Zato bodo podjetja še toliko bolj primorana skrbno tehtati med koristmi in nevarnostmi glede uporabe socialnih omrežij. Tista podjetja, ki razvijajo in uporabljajo strategije izkoriščanja prednosti uporabe socialnih omrežij, morajo skrbeti, da s tem ne ogrožajo lastnih poslovnih mrež (podatkov o poslovnih partnerjih, dobaviteljih, kupcih, ...). Na drugi strani pa se glede na podatke aktualne raziskave podjetja Kaspersky Lab (2011, str. 15) vedno bolj zavedajo nevarnosti uhajanja poslovno občutljivih informacij preko socialnih omrežij. Podatki namreč pokažejo, da okoli 70 % anketiranih podjetij zaposlenim onemogoča ali vsaj v določeni meri omejuje dostop do najpopularnejših socialnih omrežij.

Pri napovedih razvoja dogodkov s področja informacijske varnosti v zadnjem času ne gre zanemariti pomena groženj z napadi na mobilne naprave (pametne telefone, tablične računalnike). Čeprav so prenosni telefoni v razvitih državah v množični uporabi že več kot dvajset let, zgodovinsko gledano še ni bilo zaznati grožnje, ki bi množično odmevala po vsem svetu (Trend Micro Inc., 2009, str. 11). To se utegne kaj hitro spremeniti, saj so sodobni telefoni in druge mobilne naprave postali medij za hrambo in prenos velikih količin podatkov, zaradi česar so vse pogostejša tarča napadalcev. Z množično uporabo elektronskega bančništva na

[20] Verjetno najbolj znan računalniški črv Stuxnet, odkrit leta 2010, je izkoriščal kar štiri »zero-day«-ranljivosti operacijskega sistema Windows.

[21] Poleg že omenjenega podatka o številu uporabnikov Facebooka, Larson (2012) navaja, da je bilo maja 2012 več kot pol milijarde uporabnikov Twitterja, sledila pa sta mu še Google+ z več kot 170 mio. in LinkedIn z več kot 150 mio. uporabnikov.

mobilnih napravah je pričakovati vse pogostejše, predvsem pa bolj sofisticirane napade[22] neposredno na ranljivosti mobilnih aplikacij, ki tečejo na najbolj razširjenih operacijskih sistemih.

Vse pogostejša uporaba storitev računalništva v oblaku (angl. *cloud computing*), ki jo po raziskavi CCSS (Computer Security Institute, 2010, str. 29) vsaj v določeni meri uporablja že slaba polovica anketirancev, odpira tudi vprašanja glede varnosti teh storitev. Rast števila uporabnikov je pričakovati tudi v prihodnje, predvsem zaradi prednosti v obliki zniževanja stroškov za informacijsko infrastrukturo in večje fleksibilnosti poslovanja. Podobno kot v primeru socialnih omrežij in uporabe mobilnih naprav bodo ponudniki storitev računalništva v oblaku zaradi vse večjega števila uporabnikov in posledično večje količine (tudi zaupnih) podatkov bolj zanimiva tarča napadalcev. Ker se v osnovi grožnje za okolja in infrastrukturo računalništva v oblaku ne razlikujejo od groženj za »klasične« informacijske sisteme oziroma so lahko celo večje in zahtevnejše za obravnavo, PricewaterhouseCoopers (2012, str. 1) opozarja, da prinašajo še dodatna varnostna tveganja za izgubo in razkritje podatkov, nedelovanje storitve in krajo intelektualne lastnine. Zato morajo uporabniki teh storitev pri izbiri ponudnika skrbno preveriti tehnologije in procedure, s katerimi slednji zagotavlja zasebnost in varnost podatkov.

1.4.3 Kritika in uporabnost raziskav

Uporabniki raziskav ob branju in analiziranju njihovih rezultatov kaj hitro in povsem upravičeno podvomijo v njihovo resničnost, reprezentativnost in posledično verodostojnost. Dvom v resničnost in s tem v uporabnost rezultatov izhaja že iz dejstva, da v raziskavah zaradi anonimnosti anketirancev ni zagotovljena reprezentativnost, s čimer bi rezultate na podlagi vzorca lahko s statistično gotovostjo posploševali za celotno populacijo. Problem reprezentativnosti za CCSS-raziskave še posebej poudarja Walsh (2006), ki dvomi, da je relativno majhen delež tistih, ki se na ankete odzovejo[23], res reprezentativno mnenje celotne populacije strokovnjakov za informacijsko varnost v Združenih državah Amerike. Anonimnost anketirancev sicer spodbuja iskrenost pri odgovorih, vendar pa še vedno ohranja dvom o njihovi pristranskosti in ustrezni strokovnosti. Še dodatna težava anonimnosti je, da onemogoča izdelavo statistično pravilne longitudinalne primerjave rezultatov več let, saj je zelo verjetno, da so odgovore na vprašanja po letih podajali povsem različni ljudje. Guillot in Kennedy (2007, str. 66) posebej poudarjata še pomanjkljivost pogostih vprašanj v raziskavah, ki merijo učinkovitost in uspešnost uporabe določenih tehnoloških rešitev brez zagotovila, da so uporabljene tehnologije pravilno implementirane. Garreston in Messmer (2006) še ostreje kritizirata raziskave, ki jih označita za učinkovito marketinško orodje proizvajalcev in prodajalcev varnostnih rešitev, saj z njimi uspešno širijo negativne in nejasne informacije o stanju informacijske varnosti. Tako med uporabnike oziroma kupce širijo strah, negotovost in dvom (angl. *fear, uncertainty and doubt*), kar je nedvomno uspešna strategija za zagotavljanje prodaje

[22] Virus »ZeuS-in-the-Mobile« je primer zlonamernega programa, s katerim napadalci obidejo sistem dvofaktorske avtentikacije pri uporabi storitev spletne banke, tako da prestrežejo varnostno SMS-sporočilo, ki ga banka ob transakciji pošlje uporabniku.

[23] Za CCSS 2010 je bil dosežen odziv le 6,5 odstoten, kar je 351 vrnjenih anket, od skupno 5412 poslanih (Computer Security Institute, 2010, str. 3).

varnostnih rešitev ali kot meni Berinato (2002), ki prav, da dokler bodo ljudje prestrašeni, bodo za varnost tudi trošili.

Kljub kritikam pa se mora bralec tovrstnih raziskav zavedati, da gre v večini primerov za neformalne raziskave, ki primarno niso namenjene statističnim obdelavam. Glede na delitev raziskav v skupine iz poglavja 1.4 lahko ugotovimo, da je primarni cilj prve skupine spremljanje stanja in poročanje o usmeritvah na področju informacijske varnosti. Rezultati CCSS-raziskav kljub pomanjkljivostim pri vzorčenju in pridobivanju podatkov kažejo na konsistentnost odgovorov v več letih[24]. To kaže, da je kljub anonimnosti anketirancev vzorec raziskave glede na demografske značilnosti v obdobjih poročanja konsistenten. Vseeno pa ne gre spregledati dejstva, da je sklepanje o usmeritvah lahko le subjektivne narave, saj temelji zgolj na podobnosti in konsistentnosti podatkov in ne na podlagi statističnih dokazov. Za drugo skupino raziskav podjetje Deloitte (Melek & MacKinnon, 2006, str. 4) navaja, da je cilj gospodarskim subjektom dajati pomoč in osnovo za oceno in primerjavo stanja njihove lastne informacijske varnosti. Zato pri uporabnosti raziskav nikakor ne smemo zanemariti konteksta, v okviru katerega je rezultate potrebno razumeti, interpretirati in navsezadnje uporabiti. Po mnenju Guillota in Kennedyja (2007, str. 68) je raziskave mogoče uporabiti predvsem kot orodje za odločanje in upravičenje naložb v informacijsko varnost. Tako se uporabljajo zlasti za izdelavo primerjalnih analiz in za upravičenje porabe proračuna za informacijsko varnost, saj vodstvo podjetij v vedno večji meri zahteva ekonomsko upravičenost naložb, tudi za projekte informacijske varnosti.

V končni fazi pa se uporabnost raziskav v največji meri izkaže, kadar jih strokovnjaki za informacijsko varnost ustrezno interpretirajo in v okviru pravega konteksta uporabijo za povečanje stopnje varnosti lastnega podjetja. Raziskave so tako dodatno orodje, ki ob že prej vpeljanih procedurah in orodjih zagotavljanje informacijske varnosti v podjetjih dopolnijo in dodatno okrepijo. Takšno uporabo raziskav Guillot in Kennedy (2007, str. 70) označujeta kot primer dobre prakse upravljanja informacijske varnosti v podjetjih v sistemu upravljanja s tveganji. Informacijska varnost je področje, ki je umeščeno v okvir celovitega sistema upravljanja s tveganji, pri čemer je tak sistem, če je pravilno implementiran in kontroliran **pogoj** in **podpora** procesom za zagotavljanje ustrezne ravni informacijske varnosti.

2 SISTEM UPRAVLJANJA INFORMACIJSKE VARNOSTI

Sodobno poslovno okolje z nenehnim, hitrim in pogosto nepredvidljivim spreminjanjem od vodilnih v podjetjih zahteva hitro odzivnost za izkoriščanje trenutnih poslovnih priložnosti. Hkrati pa se mora vodstvo zavedati, da so jasna dolgoročna vizija, strateško odločanje in uresničevanje dolgoročnih ciljev nujni za ohranitev in učvrstitev pozicije, ki jo ima podjetje na globalnem trgu, saj si le tako lahko zagotovi nenehno rast in dolgoročen obstoj. Za sprejemanje pravilnih (kratkoročnih in dolgoročnih) odločitev so temeljnega pomena zadostne, pravočasno pridobljene in točne informacije, ki jih mora podjetje prepoznati kot lastna sredstva, ki jih mora varovati, saj imajo strateško vrednost za uresničevanje vizije in poslanstva.

[24] Avtorji CCSS-raziskave ugotavljajo, da bi mnoge rezultate lahko pravilno predvideli in napovedali z analizo podatkov iz preteklih letnih raziskav (Computer Security Institute, 2010, str. 1).

Za uspešno varovanje informacij morajo podjetja najprej prepoznati in upoštevati vsa tveganja, ki so jim izpostavljena. Le tako lahko z njimi učinkovito upravljajo in zagotovijo varnostne ukrepe, s katerimi jih minimizirajo oziroma ohranjajo na sprejemljivem nivoju. S tovrstnimi spoznanji se pogled na naložbe v informacijsko varnost v zadnjih letih korenito spreminja. Če so še do nedavnega vodilni v podjetjih izdatke za informacijsko varnost imeli za nujnost, ki ne prinaša ekonomskih koristi, jih imajo sedaj vse pogosteje za naložbo, ki ustvarja dodano vrednost (Cavusoglu, 2004, str. 73). Ker pa se vodstvo podjetja pri naložbah srečuje s problemom omejenosti sredstev, se mora tudi v primeru takšnih naložb racionalno odločati. Ker popolne varnosti ne glede na količino sredstev in vrsto uporabljenih ukrepov nikoli ni mogoče zagotoviti (Jenkins, 1998, str. 1), je načrtno in sistematično strateško upravljanje s tveganji toliko pomembnejše. Caballero (2010, str. 1) v tem kontekstu poudarja, da je informacijska varnost poslovni in ne zgolj tehnološki problem, saj se morajo vsi deležniki v podjetju pri reševanju varnostnih vprašanj do določene mere angažirati in jih reševati v skladu z uresničevanjem strateških ciljev.

Ker je poslovanje vedno povezano s tveganjem, je tudi vsakršen sistem upravljanja v določeni meri sistem upravljanja s poslovnimi tveganji. Sistem upravljanja v splošnem pomenu Pattinson (2007, str. 2) opredeli kot celovit sistem, ki v podjetju zajema ljudi, procese in uporabljene tehnologije, pri čemer vsi skupaj delujejo s skupnim namenom doseganja in uresničevanja zastavljenih ciljev. Del celovitega sistema upravljanja v podjetju, ki se osredinja na zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij, razumemo kot SUIV, ki je po opredelitvi BSI-standarda[25] (Bundesamt für Sicherheit in der Informationstechnik, 2008, str. 14) skupen nabor ukrepov in metod z uporabo katerih vodstvo podjetja zagotavlja ustrezno raven varnosti informacij. Čeprav vsako podjetje ali organizacija razvije in v skladu s svojimi potrebami, cilji, varnostnimi zahtevami in organizacijsko strukturo in uporablja lasten SUIV, ki mora v skladu z določilih ISO/IEC 27001 (International Organization for Standardization, 2005a, str. v) biti strateška odločitev, pa imajo vsi sistemi upravljanja skupne elemente, ki temeljijo na enem izmed modelov cikličnega izboljševanja. Na področju informacijske varnosti se je najbolje uveljavil že omenjeni PDCA-model (slika 3), ki se uporablja kot vodilo pri načrtovanju vseh procesov SUIV, s katerimi se zahteve in pričakovanja interesnih skupin glede informacijske varnosti izpolnjujejo.

2.1 Proces upravljanja s tveganji

Upoštevajoč opredelitev iz podpoglavja 1.2.3, tveganje v osnovi lahko razumemo kot verjetnost nastanka neljubega dogodka, zaradi katerega podjetje utrpi škodo. Ker so posledice varnostnih dogodkov lahko zelo hude, jih podjetja v okviru lastnega SUIV skušajo ohranjati na sprejemljivem nivoju z izvajanjem procesa upravljanja s tveganji. Pri tem lahko uporabljajo dva načina upravljanja s tveganji: reaktivni (kurativni) in proaktivni (preventivni) način (Stroie & Rusu, 2011, str. 229−230). Pri prvem se aktivno odzovejo na vsak varnostni dogodek, ga analizirajo, ugotovijo vzroke za nastanek in na podlagi spoznanj implementirajo varnostne

[25] Je del kataloga standardov, ki jih izdaja nemška vladna agencija – Zvezna agencija za informacijsko varnost (Bundesamt für Sicherheit in der Informationstechnik – BSI).

rešitve, s katerimi preprečijo nastanek teh dogodkov v prihodnosti. Pri tem načinu je ključnega pomena to, da ima podjetje že vnaprej določene in dokumentirane postopke za zavarovanje podatkov v trenutku nastanka in reševanja posledic varnostnega dogodka (obveščanje uporabnikov, zaustavitev sistema, varnostne kopije, ...). Proaktivni način pa pomeni, da ima podjetje že vnaprej pripravljen načrt in implementirane varnostne rešitve, s katerimi zavaruje strateško najpomembnejša sredstva in tako zmanjša tveganje za nastanek varnostnih dogodkov in njihovih posledic. Prednost tega načina je, da je v večini primerov cenejše zmanjšati možnost nastanka varnostnih dogodkov, kot pa odpravljati posledice. Slabost pa je, da ne zagotavlja popolne varnosti, saj določeno tveganje za nastanek dogodkov vedno obstaja (Stroie & Rusu, 2011, str. 230). Prav zato morajo podjetja z uporabo proaktivnega načina vzporedno imeti izdelane načrte in postopke ravnanja v primeru nastanka varnostnih dogodkov.

Korake v procesu upravljanja s tveganji različni standardi[26] sicer različno razčlenjujejo, so si pa te členitve vsebinsko zelo podobne. Strnjen in vsebinsko zaokrožen proces upravljanja s tveganji po opredelitvi standarda NIST 800−30 (National Institute of Standards and Technology, 2002) sestavljajo trije zaključeni procesi, ki si zaporedno sledijo in skupaj tvorijo ponavljajočo se zanko (slika 6).

Slika 6: Upravljanje s tveganji – zaporedni procesi

Vir: povzeto po National Institute of Standards and Technology, Risk Management Guide for Information Technology Systems, 2002, str. 8−41.

Upravljanje s tveganji je ponavljajoč proaktiven proces za vzpostavitev in vzdrževanje sprejemljive ravni tveganja v dnevnih aktivnostih (Jenkins, 1998, str. 2). Ker okolje, v katerem podjetje deluje ni statično mora vodstvo podjetja zagotoviti, da koraki, ki tvorijo zanko s slike 6, tečejo konstantno, nemoteno in nadzorovano.

2.1.1 Ocena tveganja

Ocena tveganja (angl. *risk assessment*) je prvi proces v okviru metodologije upravljanja s tveganji, kot jo opredeljuje standard NIST 800−30 (National Institute of Standards and Technology, 2002, str. 8). Namen je določitev obsega potencialnih groženj, izvedba analize ranljivosti ter ocena tveganj za IS. Cilj oziroma rezultat procesa je določitev varnostnih ukrepov za zmanjšanje tveganj, ki so implementirana v okviru drugega zaporednega procesa upravljanja s tveganji. Poleg tega pa je temelj za ekonomsko upravičenje naložb v informacijsko varnost (Al-Humaigani & Dunn, 2003, str. 483), ki sledi v nadaljevanju. Ocena tveganja je torej celovit in sklenjen proces, ki poteka z izvedbo naslednjih korakov (National Institute of Standards and Technology, 2002, str. 8−41; Chen, 2009, str. 4; Stroie & Rusu, 2011, str. 231−236):

[26] ISO/IEC 27005, NIST 800-30, BSI-Standard 100-1.

- **Opredelitev sistema**

Z opredelitvijo sistema se jasno določi področje in obseg ocene tveganja, se ugotovi omejitve IS ter opredeli informacije in njihove vire, ki ga tvorijo. Informacije, potrebne za identifikacijo tveganj IS, standard NIST 800−30 (National Institute of Standards and Technology, 2002, str. 10) deli v dve skupini. Prvo tvorijo informacije o uporabljeni IT (strojna oprema, programska oprema, računalniška mreža, podatki, …), drugo pa informacije o operativnem okolju, v katerem IS deluje (funkcionalne zahteve sistema, uporabniki, varnostna arhitektura, varnostna politika, tehnične, upravljavske in operativne kontrole,…). Informacije obeh skupin za opredelitev sistema odgovorne osebe pridobijo na različne načine, na primer z vprašalniki, preko intervjujev z uporabniki, s pregledom dokumentacije in z uporabo avtomatiziranih orodij za pregled sistema (npr. NetScanTools, Nmap, CyberKit). Rezultat prvega koraka je torej natančna opredelitev sistema in okolja, v katerem deluje skupaj z opisom in upoštevanjem njegovih omejitev.

- **Identifikacija groženj**

Za učinkovito načrtovanje in vpeljavo obrambne strategije je treba predhodno poznati in opredeliti grožnje (njihove vzroke in vire), ki pomenijo možnost za izkoriščanje določene ranljivosti sistema, ter s tem možnost nastanka škode. Zato je cilj tega koraka identificirati potencialne vire groženj in jih zapisati v dokument, v katerem se lahko opredeli vpliv groženj in njihovih posledic na informacije skozi prizmo koncepta CIA-trikotnika (primer v prilogi 2). Pri ocenjevanju potencialnih virov groženj je pomembno, da se upošteva vse vrste potencialnih virov groženj, ki jih v grobem lahko delimo na človeške (namerne ali nenamerne) in nečloveške (zunaj ali znotraj operativnega okolja) vire (Stroie & Rusu, 2011, str. 232). Grožnje od človeških virov so tipično najpogostejše in najnevarnejše, zlasti ko gre za namerne napade notranjih uporabnikov, ki lahko imajo dostop do zaupnih podatkov ali uporabniških računov z administratorskimi pravicami. Grožnje od nečloveških virov pa največkrat zajemajo naravne grožnje zunaj operativnega okolja (potres, poplave, ekstremne vremenske razmere, …) in grožnje v okolju delovanja (izpad električne energije, poplava zaradi okvare vodovoda, …).

- **Identifikacija ranljivosti**

Namen koraka je ugotoviti ranljivosti sistema, ki jih potencialni viri groženj lahko (namerno ali nenamerno) izkoristijo, zaradi česar pride do kršenja varnosti informacij. Za odkrivanje in identifikacijo tehnoloških ranljivosti so uporabni različni viri informacij, kot so objave proizvajalcev računalniške opreme, javno dostopne podatkovne baze znanih ranljivosti (BUGtrack, US-CERT, NIST National Vulnerability Database), varnostni svetovalci in podobno. Za odkrivanje sistemskih ranljivosti so na voljo različne metode, kot je uporaba avtomatiziranih orodij (Nmap, Nexpose, Nessus) in preizkušanje varnosti s simuliranjem dejanskih napadov na sistem (National Institute of Standards and Technology, 2008, str. 5−2). Chen (2009, str. 6) poleg tehnoloških ranljivosti opozarja še na ranljivosti, ki izhajajo iz upravljanja varnosti (kadrovsko pomanjkanje za obseganje vseh področij, pomanjkljiva izobrazba in usposobljenost zaposlenih) in na ranljivosti, ki izhajajo iz sistemskih napak posameznih postopkov (npr. odslužena dokumentacija in podatkovni mediji se trajno ne uničijo). Cilj oziroma končni rezultat tega koraka je tako izdelava seznama vseh ranljivosti sistema (priloga 3).

- **Določitev verjetnosti tveganja**

Za določitev verjetnosti oziroma lestvice verjetnosti, da bi določena potencialna grožnja dejansko bila udejanjena (prišlo bi do zlorabe ranljivosti sistema), je po navodilih standarda NIST 800−30 (National Institute of Standards and Technology 2002, str. 21) potrebno upoštevati motivacijo in zmožnosti posameznega vira grožnje, naravo obstoječih ranljivosti in obstoj ter učinkovitost obstoječih varnostnih kontrol. Pogosto uporabljena kvalitativna lestvica za ocenjevanje verjetnosti tveganja, ki jo poleg NIST-standarda predlaga tudi ISO/IEC 27005 (International Organization for Standardization, 2008, str. 14), verjetnost ocenjuje na visoko tvegano (vir grožnje je visoko motiviran in zadostno sposoben grožnje udejanjiti, obstoječe kontrole pa so neučinkovite), srednje tvegano (vir grožnje je visoko motiviran in zadostno sposoben grožnje udejanjiti, obstoječe kontrole pa so lahko učinkovite), nizko tvegano (vir grožnje ni motiviran in/ali ni zadostno sposoben grožnje udejanjiti, obstoječe kontrole pa so v večini primerov učinkovite).

- **Analiza vpliva**

Z izvedbo analize vpliva se opredelijo potencialne neugodne posledice grožnje, ki uspešno izkoristijo določeno ranljivost sistema. Po standardu NIST 800−30 (National Institute of Standards and Technology 2002, str. 22) je te negativne posledice mogoče opredeliti in opisati v kontekstu izgube ali ogrozitve principov varnosti informacij iz CIA-trikotnika. Nekatere posledice je možno kvantitativno izmeriti (zmanjšanje prihodka, stroški odpravljanja posledic, …), posledic, kot je na primer izguba javnega zaupanja, pa ni mogoče izraziti v denarnih enotah, zato jih lahko opredelimo kot posledice z visokim, srednjim in nizkim negativnim vplivom (priloga 4). Iz tega izhaja, da je analiza vpliva lahko povsem opisna (kvalitativna), striktno matematična (kvantitativna) ali pa kombinacija obeh metodologij. Standard ISO/IEC 27005 (International Organization for Standardization, 2008, str. 14) predpostavlja, da se v praksi najprej uporabi kvalitativni način za oceno splošne ravni tveganja. V nadaljevanju se nato za glavna tveganja izdela kompleksnejša kvantitativna analiza, ki zahteva veliko časa za pridobitev in obdelavo vhodnih podatkov, sodelovanje številnih ljudi v podjetju, posledično pa tudi višje stroške za izdelavo ocene v primerjavi s kvalitativno metodo, ki je sicer primernejša za manjša podjetja z omejenimi človeškimi viri (Bojanc, 2010, str. 41). Ker kvalitativnih kategorij ni mogoče uporabiti za izdelavo kvantitativnih ocen tveganja (Schechter, 2004, str. 30), se za tovrstno merjenje uporabljajo različne specializirane mere tveganja. Med njimi je temeljna in najpogosteje uporabljena mera tveganja informacijske varnosti, imenovana »pričakovana letna izguba« (angl. *Annual Loss Expectancy*, v nadaljevanju *ALE*), ki jo je leta 1979 National Bureau of Standards objavil in definiral v standardu FIPS 65 (1979). Ta kazalec povezuje dva ključna elementa, povezana s tveganjem: pogostost dogodkov in velikost izgube, pri čemer prvi pove, kolikokrat na leto lahko podjetje pričakuje določen dogodek, drugi pa skupno vsoto izgubljenega prihodka, zaradi ene ponovitve tveganja (Bojanc, 2010, str. 66). Kazalec *ALE* se za točno določen varnostni dogodek izračuna kot produkt pričakovane izgube (angl. *Single Loss Expectancy*, v nadaljevanju *SLE*) in pričakovane letne stopnje pogostosti nastanka (angl. *Annual Rate of Occurence*, v nadaljevanju *ARO*) tega dogodka (Böhme & Nowey, 2008, str. 177):

$$ALE = SLE \times ARO \tag{1}$$

Iz enačbe (1) izhaja, da je *ALE* določene investicije v informacijsko varnost (I) za večje število različnih varnostnih dogodkov v enem letu (n), enak vsoti produktov letne izgube v denarni enoti $SLE_i(I)$, ki jo podjetje utrpi ob dogodku (i) in investiciji (I) ter pogostosti $ARO_i(I)$, da se dogodek (i) zgodi v danem letu ob investiciji (I) (Bojanc, 2010, str. 67; Böhme & Nowey, 2008, str. 178):

$$ALE(I) = \sum_{i=1}^{n} SLE_i(I) \times ARO_i(I) \qquad (2)$$

V poenostavljenem primeru izračuna za manjše trgovsko podjetje (podrobneje v prilogi 5) ob vrednosti prenosnega računalnika 1 500 € in verjetnosti kraje 33 % ter verjetnosti fizičnega poškodovanja 25 %, je vrednost *ALE* omenjenih dogodkov enaka 724,50 €. Če je relativna enostavnost samega izračuna *ALE* prednost, pa je slabost v določanju točnih vrednosti za vhodne podatke modela, ki je težavno, še posebej za človeške grožnje v primerjavi s podatki za naravne nesreče (Schechter, 2004, str. 29). Pri naravnih nesrečah se lahko predvideva na podlagi zgodovinskih podatkov, ki jih po potrebi prilagodimo aktualnim usmeritvam. Pri dogodkih, ki jih povzroči človeški faktor in ko napadalci (zlonamerni uporabniki) ravnajo taktično, pa je določanje vrednosti zelo nezanesljivo. Zlasti zato, ker napadejo najšibkejšo točko sistema, izboljšujejo svoje znanje in onemogočajo merjenje in modeliranje njihovega vedenja (Schechter, 2004, str. 30). Druga slabost, ki izhaja iz dejstva, da *ALE* združuje koristi vseh uporabljenih varnostnih rešitev v en sam kazalec, je predpostavka o enakih neugodnih finančnih posledicah za vse varnostne dogodke[27] (Lockstep Consulting, 2004, str. 10).

- **Določitev tveganja**

Pri določitvi stopnje tveganja je cilj ocenitev IS z uporabo kvalitativne metode ─ matrika stopenj tveganja (National Institute of Standards and Technology, 2002, str. 24). V stolpcih matrike so vrednosti za verjetnost grožnje, v vrsticah pa vrednosti za velikost oziroma obseg negativnega vpliva ali posledic grožnje (Primer matrike 3 × 3 dimenzije prikazuje priloga 6.). Končna ocena stopnje tveganja je produkt med stolpci in vrsticami za posamezen negativni vpliv, ki se uporabi za opredelitev tolerance za tveganje (Stroie & Rusu, 2011, str. 235): zanemarljivo tveganje (periodično se spremlja, ne zahteva ukrepov), sprejemljivo tveganje (ne zahteva takojšnjih ukrepov, se konstantno spremlja, v primeru naraščanja je predmet dodatnih aktivnosti za znižanje nivoja) in nesprejemljivo tveganje (zahteva takojšnje ukrepanje z uporabo varnostnih ukrepov za njegovo zmanjšanje).

- **Predlogi varnostnih ukrepov in sklepna dokumentacija**

Določitvi stopnje tveganja sledijo predlogi uporabe različnih varnostnih ukrepov, katerih končni namen je znižanje te stopnje na sprejemljivo raven. Predlogi ukrepov so rezultat procesa ocene tveganja in so hkrati vhodni elementi za naslednji proces metodologije upravljanja s tveganji −

[27] Če so npr. skupni letni stroški varnostnih dogodkov 1 000 € in je naš varnostni sistem 90 odstotno učinkovit, ni nujno res, da nam prihrani 900 € stroškov. Če se določen, finančno drag varnostni dogodek uvrsti med 10 % tistih, ki jih varnostni sistem ne prepreči, bo predvidevanje na podlagi izračunanega *ALE* preveč optimistično in posledično nezanesljivo.

proces zmanjšanja tveganja (National Institute of Standards and Technology, 2002, str. 26). Ko je ocena tveganja v celoti končana, morajo biti rezultati zapisani in predstavljeni v okviru uradnega poročila, ki je namenjeno vodstvu podjetja za odločanje o alokaciji omejenih sredstev za zmanjšanje tveganj in posledično za zmanjšanje potencialnih ali že nastalih izgub.

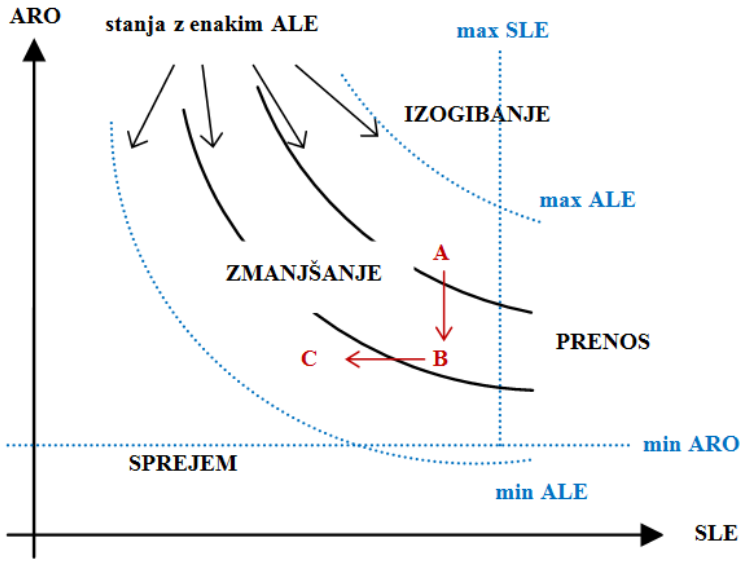
2.1.2 Zmanjšanje tveganja

Po izdelavi končne ocene tveganja se celovito upravljanje s tveganji nadaljuje s procesom zmanjšanja tveganja (angl. *risk mitigation*), ki sledi neposredno iz njenih rezultatov in ugotovitev. Zmanjšanje tveganja je proces, v okviru katerega podjetja implementirajo varnostne rešitve s ciljem znižanja obstoječega tveganja na sprejemljivo raven (Chen ,2009, str. 8). Ker tveganja v celoti nikoli ni mogoče odpraviti, standard NIST 800−30 (National Institute of Standards and Technology, 2002, str. 27) priporoča zmanjševanje tveganja z uporabo najučinkovitejših in stroškovno ugodnih varnostnih rešitev, ki imajo minimalni negativni vpliv na uresničevanje zastavljenih ciljev in poslanstvo podjetja. Proces zmanjševanja tveganja je tako sistematičen način, ki se izvaja z različnimi metodami (National Institute of Standards and Technology, 2002, str. 27; International Organization for Standardization, 2008, str. 17−21):

- **Izogibanje** tveganju, kar pomeni odstranitev vzroka za tveganje. Na primer preselitev podatkovnih strežnikov na lokacijo, kjer je tveganje za nevarnost potresa minimalna (če je to stroškovno najugodnejša mogoča rešitev).
- **Omejevanje** tveganja z uporabo rešitev in orodij, ki zmanjšajo škodo zaradi varnostnega dogodka (varnostne kopije) in/ali znižajo pričakovano verjetnost napada (požarni zid, sistem za zaznavanje vdorov).
- **Prenos** tveganja na drugo stranko. Največkrat je to zavarovalnica, na katero podjetje v zameno za plačilo zavarovalne premije prenese tveganje nastanka visokih izgub ob morebitnem varnostnem dogodku.
- **Sprejem** tveganja je smiselna strategija v primerih, ko so potencialne koristi, ki spremljajo določen tvegan način poslovanja visoke. Smiselna je tudi, kadar se tveganju ni mogoče izogniti, ali pa so stroški zaščitnih ukrepov občutno višji od potencialnih izgub.

Odločitev o tem, katero metodo za zmanjšanje tveganja izbrati, je lahko precej težavna, saj podjetje z izbiro posamezne metode ne sme ogroziti lastnih strateških ciljev in poslanstva (National Institute of Standards and Technology, 2002, str. 27). Poleg tega se lahko zgodi, da mora zaradi narave in posebnosti svojih poslovnih procesov kombinirati uporabo dveh ali več metod hkrati. Izbira ustrezne metode tveganja je prikazana na sliki 7 z grafom verjetnosti za varnostni dogodek in izgube zaradi njega. Krivulje na diagramu prikazujejo točke z enakim tveganjem, pri čemer velja, da metoda, ki zniža *ALE*, pomeni premik na nižje ležečo krivuljo v dveh mogočih smereh. Če izbrana metoda zmanjša verjetnost nastanka varnostnega dogodka, to povzroči navpični premik iz točke A v nižje ležečo točko tveganja B, če pa je rezultat izbrane metode znižanje pričakovane izgube, pride do vodoravnega premika iz točke B v točko C na nižje ležeči krivulji enakega tveganja.

Slika 7: Grafični prikaz izbire metode zmanjšanja tveganja, glede na verjetnost za nastanek varnostnega dogodka in izgubo zaradi varnostnega dogodka



Vir: R. Bojanc & B. Jerman−Blažič, An economic modelling approach to information security risk management, 2008, str. 417.; R. Bojanc & B. Jerman−Blažič, Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System, 2012, str. 280.

Področje odločitve med štirimi omenjenimi metodami je tako razdeljeno na območja, ki jih medseboj ločujejo štiri mejne črte (Bojanc & Jerman-Blažič, 2008, str. 417; Bojanc & Jerman-Blažič, 2012, str. 280). Prva meja določa najnižjo verjetnost za varnostni dogodek (minimalni *ARO*), kar pomeni, da se za *ARO* pod to vrednostjo tveganja sprejmejo. Enako se tveganja sprejmejo, kadar so le-ta pod drugo mejo, ki označuje zanemarljivo nizko tveganje (minimalni *ALE*), saj implementacija varnostne rešitve pod to mejo ni finančno upravičena. Tretjo mejo določa največja mogoča izguba posameznega varnostnega dogodka (maksimalni *SLE*), kar pomeni, da ima učinek dogodka nad to mejo za podjetje lahko pogubne posledice. Za grožnje te vrste (tega območja) ima podjetje na voljo dve možnosti. Tveganja lahko prenese na zavarovalnico ali pa implementira rešitve, s katerimi zniža verjetnost dogodka pod mejno vrednost *ARO*. Četrto mejo določa največja mogoča vrednost tveganja (maksimalni *ALE*), pri kateri se z grožnjami nad to mejo podjetje tveganju izogne. Tveganja v preostalem območju pa podjetje zmanjša z naložbami v varnostne ukrepe, ki jih v okviru procesa zmanjšanja tveganja izbere in implementira.

Schechter (2004, str. 13) **varnostni ukrep** opredeli kot politiko, proces, algoritem ali kak drug ukrep za preprečevanje ali omejevanje škode. Ker se to implementira na različnih nivojih v podjetju, obstajajo v različnih oblikah in kombinacijah (tabela 1). Vse od povsem enostavnih fizičnih ovir, uporabe varnostnih gesel pa do zapletenih programskih algoritmov in izčrpnih varnostnih politik. Uporaba vseh vrst in oblik varnostnih ukrepov pa ima skupen cilj, ki je zagotavljanje varnega IS za nemoteno delovanje in potek poslovnih procesov. Varnostni ukrepi so glede na delovanje preventivni, torej usmerjeni v preprečevanje nastanka varnostnega dogodka (vertikalni premik A → B na sliki 7), korektivni, ker zmanjšujejo posledice nastalega

dogodka (horizontalni premik B → C na sliki 7), ali pa detekcijski, ki zaznajo varnostni dogodek in sprožijo delovanje korektivnih ukrepov (Slay & Koronios, 2006, str. 20). Pri implementaciji izbranih varnostnih ukrepov mora podjetje zagotoviti največji mogoč učinek njihove uporabe, kar doseže z vpeljavo in medsebojnim kombiniranjem tehničnih, vodstvenih in operativnih ukrepov (National Institute of Standards and Technology, 2002, str. 32). Tehnični ukrepi so nameščeni na ravni izvedbe posameznih poslovnih procesov in aktivnosti, ki temeljijo na smernicah operativne ravni. Zanje Slay in Koronios (2006, str. 21) posebej poudarita, da morajo preventivno delovati tako na zunanje kot tudi na notranje napade, saj slednji za podjetje v mnogih primerih pomenijo večjo grožnjo. Vodstveni ukrepi obsegajo celotno podjetje (vse procese) in so večinoma implementirani v obliki varnostnih politik. S tem zajamejo socialne, ekonomske, okoljske in kulturne vidike delovanja, pri čemer mora biti zagotavljeno, da se striktno izvajajo v praksi (Slay & Koronios, 2006, str. 59). Operativni ukrepi pa vključujejo tiste za fizično varovnje sredstev (kraja, požar, vlaga, ...) in tako zagotavljajo nemoteno delovanje tehničnih in vodstvenih ukrepov (Slay & Koronios, 2006, str. 61).

Tabela 1: Primeri vrst varnostnih ukrepov, po nivojih upravljanja

	PREVENTIVNI	**KOREKTIVNI**	**DETEKCIJSKI**
TEHNIČNI	požarni zid navidezno zasebno omrežje protivirusna zaščita šifriranje podatkov sistem avtentikacije	samodejno varnostno kopiranje dodatna strojna oprema	dnevnik dogodkov (angl. *event log*) spremljanje prometa na mreži sistem za zaznavanje vdorov v omrežju
VODSTVENI	ustrezna varnostna infrastruktura varnostna politika izobraževanje uporabnikov	zagotavljanje finančnih sredstev zagotavljanje infrastrukture	neprekinjeno ocenjevanje tveganj preverjanje novih zaposlenih
OPERATIVNI	varnostniki protokoli za zunanje obiskovalce protivlomna in protipožarna vrata ključavnice na prstne odtise	pomožni generatorji gasilni aparati in škropilci	video nadzor dimni in požarni detektorji alarmi

Poleg učinkovitosti na izbiro vplivajo tudi stroški in koristi uporabe in implementacije posameznega ukrepa oziroma kombinacije več različnih ukrepov. Za ekonomsko učinkovito izbiro primernih ukrepov v podjetjih uporabljajo različna orodja, med katerimi prednjači uporaba analize stroškov in koristi (angl. *cost–benefit analysis*). Tovrstna analiza daje oceno in primerjavo relativnih koristi in stroškov, povezanih s posameznim predlaganim ukrepom (Stroie & Rusu, 2011, str. 239) z namenom identificiranja tistih ukrepov, katerih uporaba zniža tveganja v tolikšni meri, da upraviči stroške, povezane z njihovo nabavo, implementacijo in vzdrževanjem. Še pred izvedbo analize pa mora podjetje imeti jasno opredeljeno mejo za sprejem tveganja, ki ob upoštevanju naslednjih pravil določa, ali bo posamezen ukrep implementiran (National Institute of Standards and Technology, 2002, str. 39):

- če ukrep zniža tveganje za več, kot je treba, izberemo cenejšo alternativo;
- če stroški ukrepa presegajo učinek znižanja tveganja, poiščemo drugo alternativo;
- če ukrep ne zniža tveganja v zadostni meri, izberemo dodaten ali povsem drug ukrep;
- če ukrep zniža tveganje na sprejemljivo raven in je hkrati stroškovno učinkovit, ga implementiramo.

Kljub uporabi učinkovitih in stroškovno upravičenih varnostnih ukrepov, s katerimi se zniža ocenjeno tveganje na sprejemljivo raven, pa noben IS ni popolnoma varen. Če preostalo tveganje (angl. *residual risk*) po implementaciji izbranih varnostnih ukrepov ostaja na ravni pod mejo sprejemljivega tveganja, dodatni ukrepi niso potrebni.

2.1.3 Ocenjevanje učinkovitosti

Z izbiro in implementacijo varnostnih ukrepov proces upravljanja s tveganji ni končan. Nadaljuje se z ocenjevanjem učinkovitosti, ki je po svoji vsebini proces kontrole doseženih rezultatov zmanjšanja tveganja. Nasprotno od ocene in zmanjšanja tveganja, ki potekata v nekem določenem trenutku, mora biti ocenjevanje učinkovitosti konstantno trajajoč proces (National Institute of Standards and Technology, 2002, str. 41). Prvi razlog je nenehno spreminjanje okolja, v katerem podjetje deluje, zaradi česar se pojavljajo vedno nova tveganja, ki jih je treba v procesu upravljanja s tveganji ustrezno obravnavati. Drugi razlog so spremembe v samem podjetju in njegovem informacijskem sistemu (širitev mreže, uporaba novih aplikacij, fluktuacija zaposlenih), zaradi katerih se obstoječa že obravnavana tveganja ponovno pojavijo, spremenijo in tako ponovno postanejo predmet obravnave. Poleg omenjenih sprememb v notranjem in zunanjem okolju pa Chen (2009, str. 13) opozarja še, da oba predhodna procesa spremljajo negotovosti, povezane s subjektivnimi ocenami (npr. določitev verjetnosti tveganja, ocena stroškov in koristi varnostnega ukrepa), zaradi katerih prihaja do napačnih odločitev in posledično do uporabe neustreznih ukrepov. Zato je konstantno ocenjevanje učinkovitosti nujno in hkrati uporabno orodje za pridobivanje povratnih informacij glede pravilnosti sprejetih odločitev.

Informacijska varnost je torej konstanten poslovni proces upravljanja s tveganji, preko katerega vodstvo podjetja obvladuje poslovne prakse in izboljšuje poslovne procese. Podjetja se v globalnem poslovnem okolju nenehno srečujejo z različnimi potrebami, med katerimi je tista po informacijski varnosti vse bolj v ospredju. Ker pa zadovoljevanje potrebe po ustrezni ravni informacijske varnosti zahteva porabo omejenih sredstev, prav učinkovit sistem upravljanja s tveganji lahko odigra ključno vlogo pri zagotavljanju orodij za racionalno odločanje.

3 EKONOMIKA INFORMACIJSKE VARNOSTI

Potreba po ekonomskem načinu upravljanja informacijske varnosti je v zadnjih dvajsetih letih vse bolj v ospredju. Razlog je veliko število varnostnih dogodkov, s katerimi se gospodarski subjekti srečujejo, med katerimi je vedno več takšnih, ki so povezani z visokimi in zanje lahko celo pogubnimi stroški. Tako se je tradicionalno dojemanje informacijske varnosti posledično precej spremenilo. Vodilni v podjetjih informacijsko varnost v vse večji meri dojemajo kot enega osnovnih pogojev za zagotavljanje varnega poslovnega okolja, v katerem podjetje deluje in ustvarja dodano vrednost. Izdatke za zagotavljanje varnosti informacij, informacijskih sredstev in sistemov ne dojemajo več le kot nujne stroške poslovanja, temveč vedno bolj kot naložbene izdatke. Tako kot velja za vsakršno investicijsko trošenje, morajo biti tudi naložbe v informacijsko varnost ekonomsko upravičene. Zato sta Gordon in Loeb (2006, str. 121) mnenja,

da morajo gospodarski subjekti izdatke za informacijsko varnost presojati z ustreznimi analizami stroškov in koristi, ter tako ekonomsko učinkovito upravljati s tveganji.

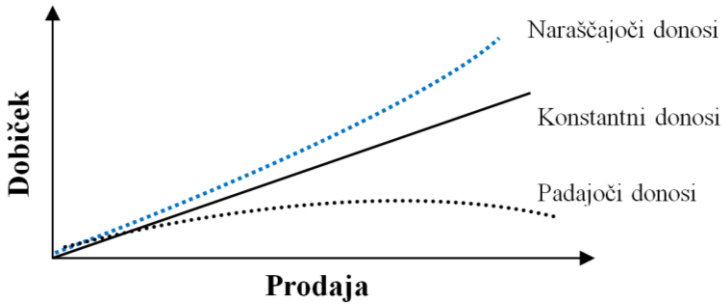
Zato se v praksi vse pogosteje uporabljajo metode, ki temeljijo na tehnikah, poznanih iz mikroekonomije, saj so gospodarski subjekti prisiljeni konstantno tehtati med stroški in koristmi, ki jih izdatki za zagotavljanje informacijske varnosti prinašajo. To trditev dokazujejo tudi rezultati različnih empiričnih raziskav, kjer npr. Gordon in Loeb (2006, str. 125) ugotavljata, da vodstva v večini ameriških podjetij zahtevajo ekonomsko upravičenje naložb v informacijsko varnost, kar je glede na odgovore na odprta vprašanja iz njune raziskave v vedno večji meri pričakovati tudi v prihodnje. Podobno kažejo tudi rezultati raziskav CCSS (Computer Security Institute, 2010, str. 36; Computer Security Institute, 2009, str. 34), ki od leta 2004 dalje anketirance sprašuje po najpogosteje uporabljeni metodi upravičenja tovrstnih naložb. Med njimi je v vseh letih na prvem mestu uporaba kazalnika donosnosti naložbe (angl. *Return on Investment*, v nadaljevanju *ROI*), sledi uporaba kazalnika neto sedanja vrednost (angl. *Net Present Value*, v nadaljevanju *NPV*) in notranja stopnja donosa (angl. *Internal Rate of Return*, v nadaljevanju *IRR*).

Ekonomika informacijske varnosti je kot znanstvena disciplina relativno novo področje, kjer je zanimanje raziskovalcev za ekonomske dimenzije reševanja vprašanj, povezanih z informacijsko varnostjo, vedno večje. Delo, ki je povzročilo številne znanstvene razprave in je postavilo temelje raziskovanja ekonomskih dimenzij informacijske varnosti (Camp, 2004, str.190) z naslovom »*Why information security in hard: An economic perspective*«, velja za prelomno, saj gre za prvi primer znanstvenega sestavka, v katerem je Anderson (2001) določena vprašanja nedvoumno pojasnil z uporabo mikroekonomskih konceptov. Tako od leta 2002 dalje vsako leto poteka konferenca »Workshop on the Economics of Information Security (WEIS)«, kjer so predstavljene najnovejše znanstvene ugotovitve s področja ekonomike informacijske varnosti. Ne glede na to, da so se v številnih prispevkih pogledi na ekonomiko informacijske varnosti spreminjali, pa ostaja dejstvo, da izhajajo iz temeljnih ekonomskih zakonitosti sodobnega gospodarstva.

3.1 Ekonomske zakonitosti trga informacijske tehnologije

Trg informacij spada v novejše obdobje razvoja tržne ekonomije in se po določenih zakonitostih razlikuje od tradicionalne ekonomske misli, kot jo je v šestih knjigah, zbranih pod naslovom »Principles of Economics«, ob koncu devetnajstega stoletja zapisal Alfred Marshall (1920). Gospodarstvo tistega časa je poganjala predvsem proizvodnja fizičnih dobrin (železo, kava, živilska industrija), ki za proizvodnjo zahtevajo velik vložek sredstev in relativno majhen vložek znanja. Tako se tudi največji proizvajalci soočajo s **padajočimi donosi** (Marshall, 1920, str. 92), saj kljub izkoriščanju ekonomije obsega v določenem trenutku dosežejo točko, ko stroški dodatno proizvedenih enot proizvoda naraščajo hitreje kot dohodek od njihove prodaje (slika 8).

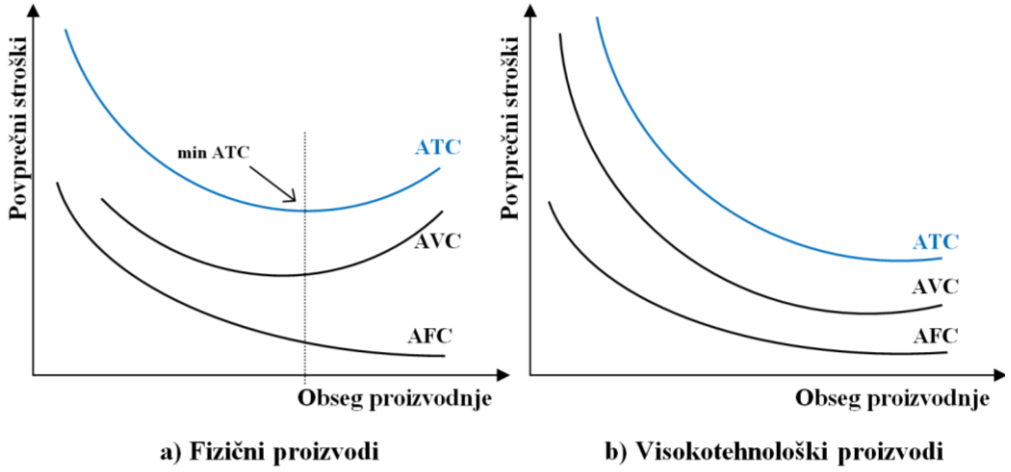
Slika 8: Padajoči in naraščajoči donosi



Vir: E. Turban, J. K. Lee, D. King, J. McKay & P. Marshall, Electronic Commerce. A Managerial Perspective, 2008, str. 638.

Situacija v sodobnem gospodarstvu, katerega glavno gonilo so informacije in znanje, je po mnenju ekonomista Briana W. Arthurja povsem drugačna (1996, str. 100). Zaradi preobrata mehanizmov, ki določajo vedenje gospodarskih subjektov, se ti soočajo z **naraščajočimi donosi**. Slednji ustvarjajo težnjo in pogoje, da subjekti, ki že imajo določeno prednost pred konkurenti v panogi, to izkoristijo in svojo prednost še dodatno povečajo, s čimer se na trgu ustvarja neravnovesje (ravno nasprotno padajočim donosom, ki trg vodijo v ravnovesje cen in tržnih deležev). Konkretno to pomeni, da podjetje z vodilnim položajem v panogi na račun naraščajočih donosov oziroma hitrejšega naraščanja dobičkonosnosti v primerjavi s proizvodnjo (slika 8) še dodatno povečuje svoj tržni delež, dodaten dobiček pa investira (izboljšanje produktov, trženje, ...) v utrditev svoje vodilne pozicije (Turban et al., 2008, str. 638). To, da dobiček narašča hitreje od rasti prodaje, je posledica odnosa med povprečnimi (angl. *average total costs*, v nadaljevanju *ATC*) in povprečnimi spremenljivimi stroški (angl. *average variable costs*, v nadaljevanju *AVC*), kar prikazuje slika 9. Krivulja *ATC* prikazuje gibanje povprečnih stroškov (v kratkoročnem obdobju) v odvisnosti od sprememb obsega proizvodnje. Krivulja ima značilno obliko črke U, ker *ATC* sprva z večanjem proizvedene količine pada kot posledica padajočih povprečnih stalnih stroškov (angl. *average fiksed costs*, v nadaljevanju *AFC*). Z nadaljnjim večanjem obsega proizvodnje je vpliv padajočih *AFC* čedalje manjši, zato prevlada vpliv naraščajočih *AVC*, ki krivuljo *ATC* potiskajo navzgor (Prašnikar, 1999, str. 137). V primeru večine visokotehnoloških proizvodov pa so *AVC* nizki oziroma skorajda fiksni ne glede na proizvedeno količino (učinek visokih začetnih stroškov, ki je pojasnjen v nadaljevanju), potem ko je začetna investicija že povrnjena (graf b na sliki 9). Tako v ilustriranem primeru celotni stroški na enoto (*ATC*) z večanjem proizvodnje padajo (so razpršeni na večje število enot), kar posledično zagotavlja naraščajočo dobičkonosnost prodaje.

Slika 9: Krivulje povprečnih stroškov za fizične in visokotehnološke proizvode



Vir: E. Turban et al.,Electronic Commerce. A Managerial Perspective, 2008, str. 638.; J. Prašnikar, Uvod v mikroekonomijo, 1999, str. 139.

Poleg višje dobičkonosnosti Arthur (1996, str. 102) omenja še tri učinke, s katerimi vodilno podjetje v panogi še dodatno krepi svoj položaj:

- Učinek visokih začetnih stroškov (angl. *up-front costs*): Visokotehnološki izdelki, ki zahtevajo velik vložek znanja in majhne vložke materiala imajo visok začetni strošek raziskav in razvoja, še posebej v primerjavi z njihovimi proizvodnimi stroški na enoto. S povečevanjem proizvodnje strošek na enoto izdelka skokovito upade[28], zaradi česar vodilno podjetje v panogi zasiči trg in s tem močno oteži vstop novim konkurentom v panogo. Anderson (2001, str. 359) tu doda še, da cenovna konkurenca v teh panogah potiska prihodke od prodaje na raven mejnih stroškov proizvodnje (ki so v panogi IT lahko tudi enaki nič), zaradi česar morajo proizvajalci v očeh kupcev prodajati vrednost izdelka in ne stroške njegove izdelave.

- Učinek mreže (angl. *network effects*): Vodilni izdelek v panogi pritegne veliko število uporabnikov, kar vodi v razvoj in prodajo novih komplementarnih proizvodov, s čimer se položaj izdelka in s tem njegovega proizvajalca še dodatno krepi. Primer je podjetje mimovrste, d. o. o., ki je leta 2002 začelo kot spletna prodajalna, specializirana za računalniško opremo. Ker je že v prvem letu pritegnila veliko število kupcev, je z izkoriščanjem tržnega deleža že dve leti kasneje ponudbo razširila na program zabavne elektronike, leta 2011 pa je njihova ponudba presegala 100 000 artiklov iz različnih prodajnih oddelkov (O mimovrste, d. o. o., 2012).

- Učinek zaklenjenega trga (angl. *lock-in effect*): Do učinka pride, kadar izdelek od uporabnika zahteva določeno znanje, s čimer pa postavi ovire in dodatne stroške za prehajanje

[28] Proizvodni stroški prve enote operacijskega sistema Windows so znašali 50 mio USD, vseh naslednjih enot pa zgolj 3 USD (Arthur, 1996, str. 102).

uporabnikov h konkurenčnim proizvodom. Predvsem visokotehnološki izdelki (na primer navigacijska naprava) od uporabnika zahtevajo vnos začetnih nastavitev in učenje uporabe, za kar mora investirati svoj prosti čas. Posledično ni motiviran za uporabo konkurenčnega izdelka, če med konkurenčnimi izdelki ni visoke diferenciacije glede funkcionalnosti in nabavne cene.

Iz zapisanega ter prikazanega v slikah 8 in 9 lahko sklenemo, da je sodobno gospodarstvo glede na donose obsega proizvodnje sestavljeno iz dveh medsebojno povezanih delov. Podjetja se v delovno in kapitalsko intenzivnih panogah soočajo s padajočimi donosi, podjetja iz panog visokotehnoloških proizvodov in storitev, kamor spada tudi področje IT v najširšem smislu pa z naraščajočimi donosi. Ker v obeh delih gospodarstva veljajo drugačne ekonomske zakonitosti, kultura in vedenje gospodarskih subjektov, Arthur (1996, str. 100) opozarja, da takšno gospodarstvo zahteva različne in prilagojene načine upravljanja, različne strategije poslovanja in ustrezno poslovno okolje, ki ga z zakonodajo ureja država. Na tem mestu se zastavlja vprašanje, v katerega od obeh delov gospodarstva spada ekonomika informacijske varnosti, če se presoja skozi prizmo investicijske teorije. V iskanju odgovora na to vprašanje, kjer gre za določanje optimalnega obsega vlaganj v informacijsko varnost, je treba poznati značilnosti stroškov, koristi in njihovih medsebojnih odnosov, ki jih pojasnjujejo spoznanja iz ekonomije.

3.2 Ekonomika naložb v informacijsko varnost

Uporaba tehnik in modelov klasične investicijske teorije je tudi v primeru naložb v informacijsko varnost postala vse pomembnejši del načrtovanja investicijskih izdatkov podjetja. Namen je ugotavljanje in merjenje vpliva teh naložb na uspešnost poslovanja podjetja (Böhme & Nowey, 2008, str. 2). Poleg tega se način uporablja še za presojanje upravičenosti naložb, za primerjanje alternativnih naložbenih možnosti ter za ugotavljanje stroškov in koristi uporabe različnih varnostnih rešitev. Vendar pa uporaba teh modelov v primeru naložb v informacijsko varnost zahteva nekatere prilagoditve zaradi pomembnih vsebinskih razlik med obema vrstama naložb. Aoufi (2009, str. 33) meni, da je temeljni vzrok, ki onemogoča neposredno uporabo klasičnih finančnih metod, težavnost opredlitve in finančnega merjenja koristi naložb v informacijsko varnost. Slednje v večini primerov ne ustvarjajo neposrednih dodatnih prihodkov oziroma pozitivnega denarnega toka, saj so večinoma v obliki prihrankov iz naslova manjše verjetnosti nastanka varnostnih dogodkov. Pri tem izdelava realne ocene zmanjšanja iz naslova uporabe točno določenega varnostnega ukrepa še dodatno otežuje oceno koristi tovrstnih naložb. Böhme in Nowey (2008, str. 2) ob tem opozarjata še na težavnost ocenjevanja celotnih stroškov informacijske varnosti, saj v večini primerov prihaja do podcenjevanja višine posrednih (neotipljivih) stroškov, s čimer so tudi celotni stroški kot vhodna spremenljivka v modelih za presojanje upravičenosti naložb podcenjeni. Rezultati modelov pa posledično lahko vodijo do nepravilnih poslovnih odločitev.

Namen uporabe tovrstnih modelov je, da se z njimi formalno zapiše in obravnava odnos oziroma razmerje med stroški in koristmi uporabe varnostnih rešitev (Böhme, 2010, str. 11), s čimer so ti modeli v pomoč pri odločanju in optimiziranju izdatkov za informacijsko varnost. Če so stroški

in koristi teh naložb izraženi v denarnih enotah, je izračun njihove ekonomske upravičenosti dokaj enostavna naloga. Veliko večja težava je že omenjena realna ocena stroškov in koristi, kjer je treba izhajati iz pravilne opredelitve in ustreznega poznanja strukture obeh kategorij.

3.2.1 Stroški vlaganj v informacijsko varnost

Stroške v primeru naložb v informacijsko varnost v prvi vrsti razdelimo na stroške ukrepa (stroški za zagotavljanje varnosti) in stroške dogodka (finančne posledice nastalega varnostnega dogodka). **Stroške ukrepa**, ki pomenijo denarne izdatke za nakup in uvedbo varnostnega ukrepa, lahko v splošnem delimo na naložbene in operativne (Neubauer, Klemen & Biffl, 2005, str. 3). Za prve je značilno, da so permanentne narave in imajo dolgoročni vpliv na prihodnje denarne tokove, kot je na primer oprema za identifikacijo pooblaščenih oseb, ki lahko vstopajo v strežniško sobo s preverjanjem prstnih odtisov. Pri drugih pa gre za načrtovane in znane izdatke za vzdrževanje želene ravni varnosti, kot je npr. letna pogodbena licenca, ki zagotavlja vzdrževanje sistema s posodobitvami in varnostnimi popravki. Enačbo, ki pomeni naložbo v varnostni ukrep oziroma celotne stroške ukrepa (C), Mizzi (2005, str. 2) definira kot vsoto začetnih (enkratnih) stroškov, letnih stroškov nadgradenj in posodobitev ter stroškov vzdrževanja. Bojanc (2010, str. 115) stroške ukrepa razčleni nekoliko podrobneje, vendar prav tako na enkratne stroške in tiste, ki se periodično ponavljajo:

$$C = C_b + C_i + C_f + C_m + C_o \tag{3}$$

Pri tem sta strošek nabave opreme (C_b) in strošek uvedbe, preizkušanja in izobraževanja (C_i) enkratna in sta znesek začetne naložbe ($I_0 = C_b + C_i$). Stroški nadgradenj in popravkov (C_f), vzdrževanja (C_m) in drugi stroški, povezani z uvedbo ukrepa (C_o), pa se periodično ponavljajo.

Na podoben način tudi Cavusoglu (2004, str. 7) ločuje stroške dogodka na kratkoročne in dolgoročne, kjer med prvimi omenja izpad prihodkov zaradi nedelovanja, beg kupcev k bolj varnim in zanesljivim dobaviteljem in dodatne materialne stroške in stroške dela IT-službe zaradi vzpostavitve prvotnega stanja pred dogodkom. Med dolgoročne stroške prišteva izgubo strank in zaupanja poslovnih partnerjev, stroške morebitnih tožb, višje zavarovalne premije in višje obrestne mere, ker podjetje na trgu kapitala po varnostnem dogodku velja za bolj tvegano. Kratkoročne oziroma takojšnje izgube Bojanc (2010, str. 107) kvantitativno zapiše kot vsoto posameznih vsebinskih stroškov oz. izgub:

$$L = L_s + L_r(t) + L_i(t) + L_p(t) + L_{SLA} + L_{posredne} \tag{4}$$

kjer L_s pomeni strošek zamenjave oziroma nakupa nove opreme, $L_r(t)$ strošek popravila oz. vzpostavitve delujočega stanja, $L_i(t)$ izgubo prihodkov, $L_p(t)$ pa izgubo produktivnosti zaradi nedelovanja sistema. Izgubo zaradi neizpolnjevanja pogodbenih obveznosti ali nespoštovanja zakonskih predpisov L_{SLA} podjetje utrpi na primer, če zaradi motenj v delovanju sistema, ki je posledica varnostnega dogodka, kupcem, s katerimi ima sklenjeno tovrstno pogodbo, ne zagotovi storitve pravočasno in/ali v celotnem obsegu. V zapis enačbe (4) za izgubo v primeru

varnostnega dogodka (L), Bojanc (2010, str. 108) prišteje še posredne izgube ($L_{posredne}$), ki imajo dolgoročne negativne posledice (stroške).

Ker so določene vrste izgub odvisne od časa nedelovanja IS (t_{NA}), slednji pa je odvisen od časa detekcije (t_d), torej časa, v katerem se odkrije nastanek varnostnega dogodka in časa popravila (t_r), ki je potreben za ponovno vzpostavitev delovanja sistema, Bojanc (2010, str. 109) enačbo (4) poenostavljeno zapiše:

$$L = (L_1 \times t_r) + (L_2 \times t_d) + L_3 \tag{5}$$

kjer je $L_1 = L_r + L_i + L_p$ izguba odvisna od dolžine časa popravila, $L_2 = L_i + L_p$ izguba, odvisna od časa detekcije, in $L_3 = L_s + L_{SLA} + L_{posredne}$ izguba, ki nastane neodvisno od časa nedelovanja sistema.

Podjetje izgubo L utrpi v primeru, da nastane varnostni dogodek, kar pa je v prvi vrsti odvisno od same verjetnosti za njegov nastanek. Verjetnost za varnostni dogodek p, torej, da bo izvedena grožnja uspešna, je odvisna od verjetnosti grožnje T in ranljivosti sredstva v, na katerega je grožnja napadalca usmerjena. Bojanc (2010, str. 104,105) verjetnost grožnje T opredeli kot verjetnost $0 \leq T \leq 1$, da povzročitelj grožnje izvede dogodek, ki ima neželene učinke na napadeno informacijsko sredstvo, ranljivost sredstva v pa kot verjetnost $0 < v < 1$, da bo izvedena grožnja uspešna. Verjetnost za varnostni dogodek $0 \leq p \leq 1$ je glede na zapisane opredelitve produkt verjetnosti grožnje T in ranljivosti sredstva v:

$$p = T \times v \tag{6}$$

V skrajnih primerih tako velja, da je verjetnost za varnostni dogodek enaka nič ($p = 0$), če ni napadov na sredstvo ($T = 0$) in/ali če sredstvo ni ranljivo ($v = 0$). Na podlagi ocenjene verjetnosti za varnostni dogodek p in izgube L se lahko izračuna varnostno tveganje R:

$$R = p \times L \tag{7}$$

kjer je R merjen v enakih denarnih enotah kot L, Bojanc (2010, str. 110) pa ga v skladu z enačbama (5) in (6) zapiše :

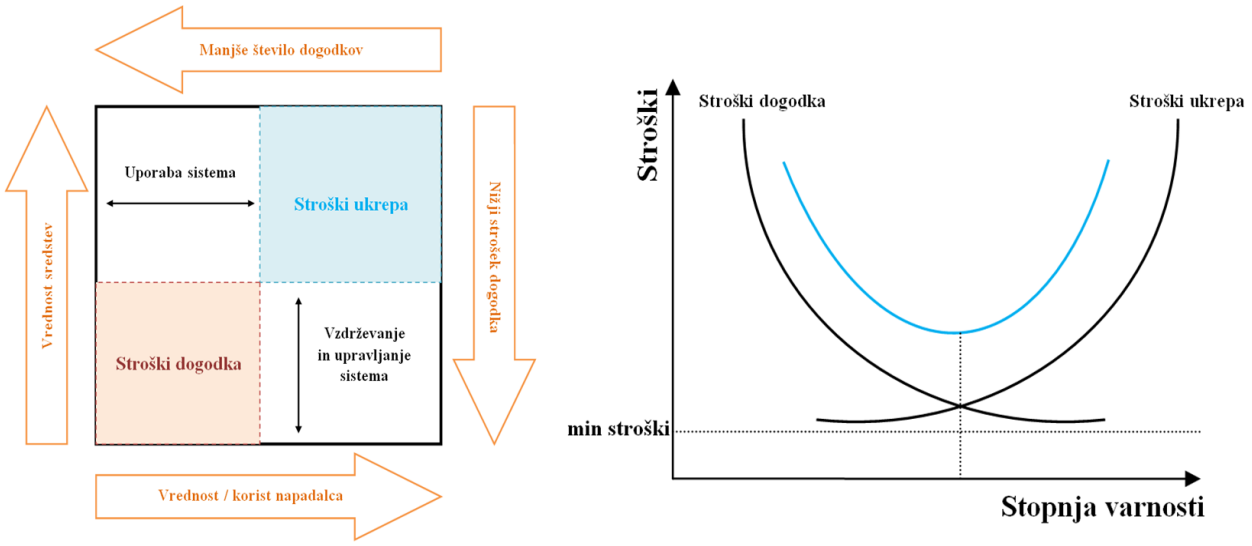
$$R = T \times v \times [\,(L_1 \times t_r) + (L_2 \times t_d) + L_3] \tag{8}$$

Varnostno tveganje je enako kot grožnja usmerjeno na temeljne principe informacijske varnosti (CIA-triada), pomeni pa pričakovano finančno izgubo zaradi varnostnega dogodka.

Poleg opisanih načinov pa stroške lahko delimo tudi drugače: neposredni – posredni, fiksni – variabilni ali enkratni – ponavljajoči, pri čemer izberemo način delitve, ki vsebinsko najbolje ustreza značilnostim obravnavanega primera oziroma je najprimernejši za uporabo izbrane metode presojanja upravičenosti naložbe. Slika 10 na levi shemi prikazuje kvalitativno razmerje

med obema vrstama stroškov, kjer je razvidno, da večanje izdatkov za varnost sicer znižuje stroške varnostnih dogodkov, vendar na račun večje kompleksnosti vzdrževanja in restriktivnosti uporabe sistema.

Slika 10: Optimalno razmerje med stroški in varnostjo



Vir: V. Aceituno, Return On Security Investment , 2006, str. 1; T. Neubauer, M. Klemen & S. Biffl, Business Process−based Valuation of IT−Security , 2005, str. 3.

Ob upoštevanju ekonomskega pogleda na določitev optimalnega obsega izdatkov za informacijsko varnost podjetja ugotavljajo optimalno razmerje med obema vejama stroškov, kot je prikazano na desni shemi slike 10.

V presečišču obeh krivulj, kjer so izdatki za varnostne ukrepe enaki stroškom nastalih varnostnih dogodkov, je doseženo optimalno razmerje (krivulja skupnih stroškov doseže minimum), saj podjetje v varnost investira točno toliko, kolikor bi sicer utrpelo škode, če ne bi uporabljalo nikakršne zaščite (ob predpostavki, da uporabljeni varnostni ukrepi izničijo tveganja za nastanek dogodkov). Levo od presečišča vzdolž horizontalne osi so točke stanja, ko podjetje (pre)malo vlaga v varnostne ukrepe in ima zato visoke stroške sanacije pogostih varnostnih dogodkov, desno pa točke, ko podjetje varnosti namenja veliko sredstev, s čimer praviloma močno zmanjša stroške sanacije dogodkov, vendar obstaja možnost, da takšna vlaganja glede na tveganje niso ekonomsko upravičena. Torej tudi v tem primeru obstaja optimalno razmerje med stroški in varnostjo, določitev katerega je vse prej kot enostavno, pri čemer se kot orodje pogosto uporablja že omenjena analiza stroškov in koristi.

3.2.2 Koristi vlaganj v informacijsko varnost

Koristi varnega IS so v večini primerov predstavljene kot vsota prihrankov iz naslova preprečitve nastanka varnostnih dogodkov in z njimi povezanih stroškov. Vendar pa je izgube (stroške) zaradi neustrezne varnosti izredno težavno oceniti, pri čemer dejstvo, da varnostna naložba pomeni trenutni finančni izdatek za ustvarjanje pričakovanih (ocenjenih) prihodnjih prihrankov

in še dodatno otežuje njihovo finančno upravičenje. Zato je pomembno dobro poznanje značilnosti in vsebine mogočih koristi, s katerimi vodstvo podjetja pri lastnikih upraviči izdatke za informacijsko varnost. Slika 11 podaja pregled mogočih potencialnih koristi, pri čemer so lete vsebinsko razporejene v tri skupine. Prvo skupino tvorijo koristi iz naslova znižanja ali odprave verjetnosti nastanka izgub, pri katerih se najpogosteje uporabljajo metode za primerjanje pričakovanih stroškov prihodnjih varnostnih dogodkov s stroški varnostnih ukrepov, ki jih preprečujejo. Tipično so to modeli z uporabo *ALE*-metodologije (Stewart, 2012, str. 316), ki so pogostna izbira zlasti zaradi preventivne narave delovanja najpogosteje uporabljenih varnostnih ukrepov (požarni zid, protivirusna zaščita, ...). Za kvantitativno vrednotenje koristi *E* te skupine Bojanc (2010, str. 121) v skladu s podano opredelitvijo uporabi enačbo:

$$E = R_0 - R(C) - \delta + \mu \tag{9}$$

Pri čemer so R_0 varnostno tveganje pred uvedbo ukrepa, R(C) varnostno tveganje po uvedbi ukrepa, δ negativni vpliv ukrepa na poslovanje, saj večja varnost po pričakovanjih omejuje funkcionalnost sistema, s tem pa negativno vpliva na produktivnost, in μ, ki pomeni posredni pozitivni učinek uvedbe ukrepa (večji ugled, nižja zavarovalna premija, …).

Slika 11: Potencialne koristi vlaganj v informacijsko varnost

Vir: A. Stewart, Can spending on information security be justified?, 2012, str. 315.

V drugo skupino spadajo koristi, ki jih podjetje brez določene stopnje varnosti v prihodnosti na kak drug način ne bi uspelo pridobiti. Tipičen primer je storitev spletnega bančništva, ki jo banka svojim komitentom brez ustreznega (certificiranega) varnostnega sistema niti ne sme ponuditi, pa tudi druge storitve (npr. elektronsko arhiviranje, brezpapirno poslovanje), za katere je treba izpolnjevati določene standarde. Po drugi strani pa lahko podjetja prav na račun visoke stopnje varnosti in na primer lastnega (unikatnega) varnostnega sistema ustvarja konkurenčne prednosti in tako pridobiva nove stranke. Tretjo skupino pa sestavljajo koristi, ki jih podjetje doseže z

ukrepi, s katerimi poveča učinkovitost svojega delovanja predvsem na račun zgodnjega odkrivanja in odprave lastnih ranljivosti. Takšen primer so ukrepi, s katerimi razvijalci programske opreme ranljivosti zaznajo že v zgodnji fazi razvoja, ko so stroški varnostnih popravkov neprimerno nižji, kot bi bili v kasnejših fazah ali celo po postavitvi izdelka na trg.

3.2.3 Optimalen obseg vlaganj v informacijsko varnost

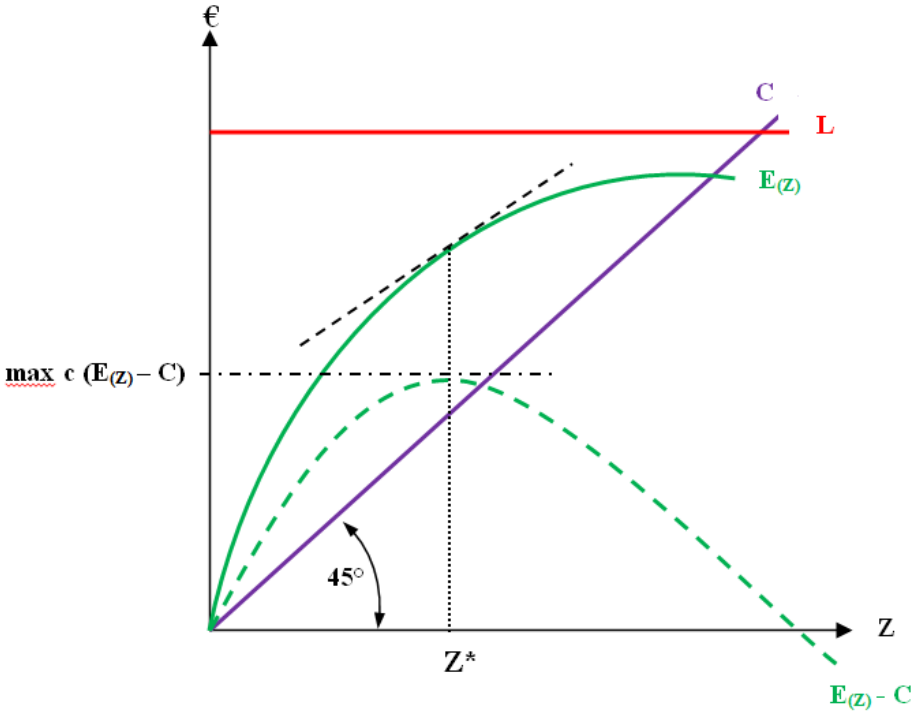
Če je odločanje o naložbah v informacijsko varnost v preteklosti temeljilo na tehnoloških rešitvah in FUD-strategiji, pa ti načini ne dajejo odgovora na vprašanje, kako zagotoviti želeno stopnjo varnosti na stroškovno učinkovit način. Zaradi sprememb in pritiskov poslovnega okolja se tako omenjene strategije vse bolj umikajo v preteklost, v ospredje pa prihajajo ekonomske metode presojanja upravičenosti naložb v informacijsko varnost ali, kot trdi Schneier (v Su, 2006, str. 14): »*Ekonomija – ne tehnologija – določa katera varnostna tehnologija bo uporabljena.*« Ekonomske modele za ugotavljanje optimalnega obsega vlaganj v informacijsko varnost glede na način ki ga uporabljajo, vsebinsko razvrstimo v skupine.

Prvo skupino sestavljajo modeli, ki temeljijo na tradicionalnih načinih odločanja v razmerah negotovosti, s katerimi se skuša identificirati tveganje, ki je posledica varnostnih dogodkov. Bojanc (2010, str. 84) jih imenuje **analitični modeli**, med katerimi so najbolj znani ekonomski modeli, ki so jih razvili Longstaff, Chittister, Pethia in Haimes (2000), Soo Hoo (2000) in Gordon in Loeb (2002). Longstaff et al. (2000, str. 46) predlagajo hierarhični holografski model (angl. *Hierarhical Holographic Model*) za odkrivanje in ocenjevanje varnostnih tveganj oziroma njihovih virov. Takšen model analitikom in vodstvu s sistematičnim procesom omogoča identifikacijo tveganj z upoštevanjem različnih vidikov (vidik vodstva, okolja, tehnologije, …), kar je ključnega pomena za uspešno upravljanje s tveganji, saj strategija varovanja informacijskih sredstev, ki ne upošteva vseh virov tveganj ne more biti uspešna. Kevin J. Soo Hoo (2000, str. 19) je predstavil analitično-odločitveni okvir za ocenjevanje različnih varnostnih politik, v okviru katerega za izbiro ustreznih zaščitnih ukrepov uporablja tehniko diagramov, s katerimi oriše medsebojne vplive vseh ključnih spremenljivk modela. Namesto medsebojne primerjave posameznih ukrepov in politik jih Soo Hoo (2000, str. 18) združuje v skupine in z analizo stroškov in koristi ugotavlja, kakšen je primeren kompromis med ukrepi za vsako skupino posebej. Model, ki sta ga razvila Gordon in Loeb (2002), posebej upošteva vpliv ranljivosti in posledično potencialne izgube na optimalni obseg sredstev, potrebnih za varovanje določene informacije. Z drugimi besedami: model omogoča oceno optimalnega obsega naložbe v informacijsko varnost z upoštevanjem temeljnega ekonomskega načela izenačitve mejnih finančnih koristi in mejnih stroškov naložbe. Gre za statičen[29] model, ki kot parametre upošteva izgubo zaradi varnostnega dogodka, verjetnost nastanka grožnje in ranljivost, ki je definirana kot verjetnost, da je realizirana grožnja brez dodatnih varnostnih ukrepov uspešna (Gordon & Loeb, 2002, str. 440). Tako sta s funkcijo verjetnosti za varnostni dogodek povezala mogočo izgubo, verjetnost, da do nje pride, in produktivnost naložbe v varnost, pri čemer sta upoštevala in tudi matematično dokazala zakon padajočih mejnih koristi naložbe. To pomeni, da se verjetnost za

[29] V takšnem modelu se vse odločitve in posledice zgodijo sočasno, v istem trenutku. Tako ni prednosti zaradi zgodnje reakcije, pa tudi časovna vrednost denarja se ne upošteva.

nastanek varnostnega dogodka s povečevanjem izdatkov za informacijsko varnost znižuje, vendar s padajočo stopnjo, saj vsaka dodatna enota naložbe v manjši meri zniža verjetnost za varnostni dogodek. Ob tem pa ne gre zanemariti dejstva, da je investiranje v informacijsko varnost neskončno trajajoč proces, saj noben IS ni popolnoma varen, ne glede na višino izdatkov za varnost. Za določitev optimalnega obsega naložbe *Z**, ki ga prikazuje slika 12, podjetje primerja pričakovane koristi *E* s stroški naložbe *C*. Če podjetje ne investira v varnost in pride do varnostnega dogodka, utrpi izgubo *L*, medtem ko z naložbami v varnost pričakuje koristi v obliki zmanjšanja pričakovane izgube (konkavna funkcija $E_{(Z)}$), pri tem stroške naložbe, izražene v denarnih enotah, prikazuje črta pod kotom petinštirideset stopinj.

Slika 12: Optimalen obseg vlaganj v informacijsko varnost



Vir: L. A. Gordon & M. P. Loeb,The Economics of Information Security Investment, 2002, str. 445.

Podjetje torej povečuje obseg naložb vse do točke, kjer se mejne koristi naložbe izenačijo z menjimi stroški, to je do točke optimalnega obsega naložb *Z**, kjer je razlika med krivuljama koristi in stroškov največja. Dodaten dokaz sta matematično izpeljala Böhme in Moore (2012, str. 18), v sliki 12 pa je prikazano, da prav v točki *Z** funkcija koristi, od katere odštejemo stroške $E_{(Z)} - C$ doseže svoj maksimum. Tako je že s slike 12 neposredno razvidno, da je optimalni obseg naložbe precej nižji od pričakovane izgube v primeru brez vsakršnega investiranja v varnost. Prav to je ena od dveh glavnih ugotovitev modela, ki pravi, da podjetja za dosego maksimalne donosnosti naložbe v informacijsko varnost namenijo veliko manjši del sredstev, kot bi jih sicer v primeru varnostnega dogodka utrpeli. Avtorja sta ugotovila, da optimalen obseg naložb nikoli ne preseže 37% pričakovanih izgub, ki so posledica varnostnih dogodkov oziroma, da se ta obseg v veliki večini primerov niti ne približa tretjini pričakovanih izgub (Gordon & Loeb, 2002, str. 451). Druga pomembna ugotovitev modela je, da v primerih,

ko grožnja povzroči dve ali več mogočih izgub, ni vedno najprimerneje, da podjetje večino sredstev nameni za varovanje največje ranljivosti (Gordon & Loeb, 2002, str. 450). Saj je v določenih primerih zaščita največje ranljivosti povezana s stroški, ki močno presegajo koristi oziroma mogoče prihranke, tako da je smotrneje sredstva usmeriti v naložbe za znižanje ranljivosti srednjega nivoja, pri katerih podjetje lahko ustvari bistveno višjo donosnost. Predstavljeni model je eden izmed temeljev ekonomike informacijske varnosti in eden najpogostejše citiranih modelov v literaturi, ki je bil pogosto predmet kritik (Willemson, 2010; Willemson, 2006; Cavusoglu, 2004), kot tudi nadgradenj in vsebinskih razširitev (Matsuura, 2008; Baryshnikov, 2007, Hausken, 2006), pri čemer pri vseh modelih ostaja skupno dejstvo, da pri naložbah v informacijsko varnost velja zakon padajočih mejnih koristi.

Druga skupina združuje načine, ki za določitev optimalne naložbe uporabljajo modele **teorije iger**, pri katerih so koristi udeležencev igre odvisne od njihovih strategij. Cavusoglu (2004, str. 79) trdi, da so analitični modeli pomanjkljivi, ker ne upoštevajo dejstva, da se pri informacijski varnosti podjetja srečujejo oziroma spopadajo s strateškimi napadalci, ki iščejo priložnosti in načine izkoriščanja ranljivosti v sistemih. Tako je informacijsko varnost mogoče razumeti kot igro med podjetji in napadalci, kjer podjetja z naložbami v varnost skušajo prikriti ranljivosti lastnih sistemov, medtem ko jih napadalci skušajo prehiteti in napasti tam, kjer so najslabše zavarovana. Kot primer Cavusoglu, Mishra in Raghunathan (2004, str. 90) opišejo razmerja med podjetjem in zlonamernim napadalcem (hekerjem), ki želi vdreti v sistem in se dokopati do zaupnih podatkov. Z uporabo dreves teorije iger orišejo strategije obeh deležnikov, kjer je korist naložbe podjetja odvisna od obsega (frekvence) napadov, korist napadalca pa od verjetnosti, da bo med poskusom napada razkrinkan. Tako predstavijo možnost razširitve modela za ugotavljanje optimalnega obsega naložb v informacijsko varnost, ki sta ga razvila Gordon in Loeb (2002), kjer vodstvo podjetja pri investicijskih odločitvah poleg lastnih strategij upošteva tudi motive (koristi) in mogoče strategije napadalcev. V tem kontekstu Cremonini in Martini (2005) predlagata način z razširitvijo kazalnika *ROI* z vpeljavo novega kazalnika, imenovanega donosnost napada (angl. *Return On Attack*). Ta kazalnik meri korist (donos), ki jo napadalec lahko pričakuje v od uspešnega napada, pri čemer velja, da se korist znižuje z dodatnimi naložbami podjetja (tarče napadalca) v informacijsko varnost. Tudi v tem primeru gre za igro koristi in strategij med deležniki, kjer podjetje išče tisti optimalni obseg naložb, ki ustvarja pozitiven donos in hkrati povzroči, da je podjetje napadalcem zaradi visokih stroškov napada kot tarča nezanimivo.

Tretjo večjo skupino sestavljajo načini, ki temeljijo na teoriji **realnih možnosti** (angl. *Real Options*), ki je bila prvotno razvita za uporabo na področju kapitalskih naložb (Khan, 2011, str. 109). Gre za tehniko oziroma orodje, ki vodstvu olajša odločanje in spreminjanje naložbenih strategij pri nastanku nepredvidenih dogodkov in pri pridobitvi novih informacij. V zadnjih letih se vse pogosteje uporablja tudi na področju informacijske varnosti (Gordon, Loeb & Lucyshyn, 2003; Franqueira, Houmb & Daneva, 2010; Khan, 2011), saj odpravlja nekatere pomanjkljivosti ekonomskih kazalnikov, ki se najpogosteje uporabljajo za presojanje upravičenosti naložb v varnost. Glavna prednost analize realnih možnosti je, da omogoča upoštevanje različnih realnih situacij, ki jih v podjetju predvidijo, in hkrati omogoča sprotno upoštevanje nepredvidenih

dogodkov med trajanjem naložbe. V nasprotju s kazalcem *NPV*, kjer se presoja upravičenost naložbe v danem trenutku, omogoča reagiranje (npr. spremembo obsega naložbe, časovni odlog naložbe) ob nastanku nepredvidenega dogodka tako, da vodstvo v podjetju še vedno ohrani obseg naložb na predvideni optimalni ravni. Konkretno Gordon, Loeb in Lucyshyn (2003, str. 4) empirično dokažejo, da je v določenih primerih strategija čakanja na nastanek nepredvidenega dogodka (angl. *wait-and-see*) in ustrezne reakcije nanj lahko ekonomsko bolj upravičena od strategije, kjer so vsa predvidena sredstva za varnost porabljena kot preventivna naložba.

Poleg predstavljenih modelov, so se v skladu s potrebami razvili tudi številni drugačni modeli in načini za presojanje upravičenosti naložb v informacijsko varnost. Slednji iz različnih zornih kotov in z uporabo različnih metod skušajo določiti optimalen obseg vlaganj v informacijsko varnost, pri čemer pa jim je skupno to, da na različne načine kombinirajo tehnološke zahteve in spoznanja iz ekonomije za upravičenje tovrstnih naložb.

4 UPRAVIČENOST NALOŽBE V INFORMACIJSKO VARNOST – PRIMER JAVNEGA RAZISKOVALNEGA ZAVODA

Načrtovanje naložb v podjetju je za njegov obstoj in dolgoročno delovanje med najpomembnješimi procesi, ki jih je treba izvajati neprekinjeno in z visoko mero strokovnosti in odgovornosti. Gre za proces ocenjevanja in analize posameznih, mogočih naložb in odločitev o njihovi izvedbi (Berk, Lončarski & Zajc, 2004, str. 96), kar velja tudi za naložbe v informacijsko varnost. Pri teh še posebej velja, da se učinki poznajo v daljšem časovnem obdobju, s čimer podjetje, ko zanje angažira finančna sredstva, izgubi določeno fleksibilnost. Primarni cilj investitorja je ustvariti kar se da velik donos na vložena sredstva (Berk, Lončarski & Zajc, 2004, str. 54), ki se v primeru naložb v informacijsko varnost praviloma kaže v koristih, ki jih podjetje s tovrstnimi naložbami lahko doseže.

S pojmom naložba označujemo projekte, za katere je značilen začetni denarni vložek, denarni tokovi v določenem časovnem obdobju in končna vrednost ob koncu naložbe v obliki dodane vrednosti oziroma koristi, ki jo investitor ustvari (Reisman et al., 2012, str. 4/2 – 3). Naložbe lahko v grobem delimo na tiste, ki povečujejo prihodke in/ali znižujejo stroške, mogoča pa so tudi drugačne delitve, denimo glede na časovno premico, po kateri ločimo med prednaložbami, medsebojno dopolnjujočimi, neodvisnimi in izključujočimi naložbami. Ker so naložbe sredstvo, s katerim podjetje dosega zastavljene cilje in tako uresničuje vizijo, je izrednega pomena, da se naložbe ustrezno načrtujejo in presojajo z uporabo različnih metod.

4.1 Presojanje načrtovanih naložb

V okviru presoje upravičenosti naložbe je najprej potrebno utemeljiti, zakaj je določena naložba potrebna, kakšne so potrebne tehnične rešitve, katere so potencialne ovire, kakšne so alternative in kakšne so mogoče posledice, če se naložba ne izvede (Reisman et al., 2012, str. 4/2 – 4(2)). V

naslednji fazi analiziranja se z izračunom kazalcev in kazalnikov[30] ter upoštevanjem različnih mogočih scenarijev preveri, kakšen je finančni učinek naložbe. Tako je v primeru, ko koristi naložbe presegajo stroške za njeno izvedbo, odločitev upravičena, saj takšna naložba povečuje vrednost podjetja, ki je po definiciji Reismana et al. (2012, str. str. 4/2–4) vsota vrednosti denarnih tokov preteklih naložb in diskontiranih denarnih tokov načrtovanih naložb. Naložbe v informacijsko varnost so orodje v okviru strategij za zmanjšanje tveganj, pri procesu upravljanja s tveganji (podrobneje v podpoglavjih 2.1 in 2.1.2), kjer je njihov glavni namen zmanjšanje verjetnosti in posledic nastanka varnostnih dogodkov. Zanje enako velja, da so smiselne, dokler koristi (prihranki) presegajo stroške, investitor pa povečuje njihov obseg, vse dokler neto koristi ne dosežejo maksimuma, ko je realiziran optimalen obseg investiranja.

Za presojanje naložb z vidika finančne upravičenosti obstajajo različne metode in kazalniki, pri čemer ima vsak svoje prednosti in slabosti. Univerzalna metoda ali kazalnik, ki bi vedno in v vseh primerih dajal najboljše rezultate, ne obstaja, zato se pogosto uporabljajo njihove različne kombinacije in/ali ustrezne prilagoditve. Kot je bilo omenjeno v tretjem poglavju naloge, se na področju presojanja naložb v informacijsko varnost še vedno najpogosteje uporabljajo tradicionalni kazalniki, ki morajo biti glede na značilnosti področja ustrezno prilagojeni, pogosto pa se kombinirajo tudi s kazalniki, posebej razvitimi za to področje. Vsem predstavljenim kazalnikom je skupno dejstvo, da izhajajo iz splošne investicijske teorije, zaradi česar so primarno uporabljeni kot komunikacijsko orodje v rokah strokovnakov za informacijsko varnost, kadar z naložbami v varnost opravičujejo porabo proračunskih sredstev podjetja.

V nadaljevanju sledi vsebinski in praktični prikaz uporabe kazalnikov, pri večjem javnem raziskovalnem zavodu v Republiki Sloveniji (v nadaljevanju zavod). Kazalniki so uporabljeni za odločanje o nakupu protivirusnega programskega paketa za raziskovalno enoto, ki samostojno deluje v okviru zavoda. Slednja se odloča med dvema ponudbama, ki sta s tehničnega vidika medsebojno primerljivi[31].

4.2 Analiza finančne upravičenosti nakupa protivirusne zaščite – klasična metoda presojanja upravičenosti naložb

Vodstvo raziskovalne enote (v nadaljevanju enota) se odloča za naložbo oziroma nakup protivirusne zaščite za delovne postaje za obdobje petih let, pri čemer se v skladu s priporočili službe za informatiko in izkušenj drugih raziskovalnih enot odloča med dvema ponudnikoma oziroma produktoma. Ker vodstvo enote nobenega od produktov iz katerega koli upravičenega razloga ne postavlja v ospredje, svojo odločitev v nadaljevanju sprejme izključno na podlagi rezultatov analize finančne upravičenosti naložbe. Z analizo se najprej ugotovi, ali je nakup katerega od obeh produktov v danem primeru ekonomsko upravičen, v nadaljevanju pa rezultati analize pokažejo še, katera od obeh možnosti je za enoto finančno ugodnješa.

[30] Med orodji analize razlikujemo med kazalci in kazalniki. S prvimi merimo velikosti, spremembe in razlike, kazalniki pa so relativna števila, ki pomenijo primerjavo določenih (različnih) kategorij med seboj (Bergant, 2010, str. 45, 48).

[31] Velja predpostavka, da se za nakup odločajo zgolj na podlagi cene in plačilnih pogojev, ter da niso nobenemu ponudniku posebej naklonjeni npr. zaradi varnostne tehnologije, uporabniških vmesnikov ali priporočil.

Enota se za protivirusno zaščito delovnih postaj (osebnih in prenosnih računalnikov) odloča med ponudnikoma AhnLAB in ESET oziroma njunima produktoma V3 Internet Security (v nadaljevanju V3) in ESET Smart Security (v nadaljevanju ESET), kjer je za izdelavo analize uporabljen cenik oziroma ponudba, objavljena na spletni strani proizvajalca. Sicer so podatki za izdelavo analize pridobljeni tudi iz zaupnih internih virov zavoda, zaradi česar so v nekaterih primerih drugače poimenovani ali prilagojeni. Vhodni podatki za oceno donosnosti naložbe oziroma njene ekonomske upravičenosti (izračun kazalnikov) so:

- V enoti je zaposlenih 30 ljudi (je enako številu delovnih postaj), za naslednjih pet let pa ne načrtujejo dodatnega zaposlovanja.
- Povprečna bruto plača v enoti je 2 162,14 € na mesec, kar pri upoštevanju 2 088 delovnih ur (261 delovnih dni, 8-urni delavnik) pomeni povprečni strošek dela v višini 12,43 € na uro.
- Povprečni prihodki enote na zaposlenega so v zadnjih petih letih bili 4 316,98 € na mesec, kar je 24,81 € na delovno uro, pri čemer bistvene rasti prihodkov v naslednjem pet letnem obdobju ne pričakujejo.
- Delo sistemskega administratorja opravlja zunanji pogodbeni izvajalec po ceni 40 € za servisno uro.
- Diskontna stopnja (k) je enaka povprečni letni obrestni meri zadnjih petih let in je 2,13 % (Zakladnica enotnega zakladniškega računa države, 2014). Gre za obrestno mero zakladniškega računa države, po kateri se zavod kot posredni proračunski porabnik lahko zadolžuje ob predhodni odobritvi ministrstva za finance (87. člen Zakona o javnih financah).
- Obrestna mera za reinvestiranje prostih denarnih sredstev (q) je enaka povprečni letni obrestni meri zakladniškega računa države (Zakladnica enotnega zakladniškega računa države, 2014) zadnjih petih let in je 1,94 %, pri čemer se predpostavlja, da se v prihodnjem pet-letnem obdobju ne bo bistveno spremenila.

Za preučitev ekonomske upravičenosti obeh ukrepov se najprej predpostavi stanje, ko ni uvedena nikakršna zaščita pred tveganjem okužbe z virusom (varnostno tveganje pred uvedbo ukrepa R_0, tabela 2) in glede na izračunano produktivnost posameznega ukrepa primerja njegove koristi (varnostno tveganje po uvedbi ukrepa $R(C)$, tabela 3), s celotnimi stroški (C), tabela 4.

Tabela 2: Izračun varnostnega tveganja pred uvedbo ukrepa R_0

Spremenljivka	Vrednost	Opis
L_s	0,00	V primeru virusa ni potrebno zamenjati opreme, zato je strošek enak nič.
$L_r(t)$	100,00	Čas popravila = 2,5 servisne ure (čiščenje okužbe, povrnitev dokumentov).
$L_i(t)$	0,25	Zanemarljiv vpliv na prihodek (EF_I = 0,01); $L_i(t) = 0{,}01 \times 24{,}81$ €
$L_p(t)$	24,60	V primeru dogodka bi se okužilo 20 % računalnikov, vpliv na produktivnost pri okuženih uporabnikih je tretjino časa nedelovanja; $L_p(t) = 6 \times 0{,}33 \times 12{,}43$ €
L_{SLA}, $L_{posredne}$	0,00	Izgub zaradi nespoštovanja pogodb ni, posredne izgube so zanemarljive.
t_{NA}	4,5	Čas nedelovanja = 4,5 h (od tega 2 h za ugotovitev in sporočanje dogodka).
t_r	2,5	Čas za odpravo posledic okužbe = 2,5 h.
t_d	2	Čas za ugotovitev in sporočanje dogodka (v urah).
L_1	124,85	$L_1 = L_r + L_i + L_p$ (v EUR)
L_2	24,85	$L_2 = L_i + L_p$ (v EUR)
L_3	0,00	$L_3 = L_s + L_{SLA} + L_{posredne}$ (v EUR)
L	361,83	Izguba (v EUR) zaradi okužbe z računalniškim virusom (izračun po enačbi (5)).
T	0,143	Pogostost prejema okuženih datotek je ocenjena na enkrat na teden.
v_0	0,25	Glede na ozaveščenost bi v okolju brez zaščite virus aktivirala četrtina zaposlenih.
p_0	0,036	Verjetnost za okužbo z računalniškim virusom v enačbi (6) na dan.
R	12,92	Varnostno tveganje (v EUR) v enačbi (7) na dan.
R_0	3 372,80	Varnostno tveganje pred uvedbo ukrepa, ob upoštevanju 261 delovnih dni na leto.

Za izračun koristi uvedbe varnostnega ukrepa po enačbi (9) je v naslednjem koraku potreben izračun varnostnega tveganja po uvedbi ukrepa $R(C)$. Omenjeni parameter se izračuna z upoštevanjem produktivnosti ukrepa V po enačbi (Bojanc, 2010, str. 159):

$$V = (1 - u) \times V_0 \tag{10}$$

kjer je parameter V_0 ranljivost pred uvedbo zaščite, parameter u pa učinkovitost protivirusne zaščite, pridobljen iz podatkov o stopnji detekcije groženj iz zadnjega[32] poročila organizacije AV Comparatives »File Detection Test of Malicious Software«. Po podatkih poročila (AV Comparatives, 2014, str. 7) je učinkovitost produkta ESET (u_{ESET}) 98,8 odstotna, učinkovitost produkta V3 (u_{V3}) pa 89,0 odstotna. Z upoštevanjem navedenih podatkov za oba preučevana produkta in enačbe (10) tabela 3 prikazuje izračun varnostnega tveganja po uvedbi ukrepa $R(C)$.

[32] Med pisanjem magistrskega dela, je bilo aktualno poročilo iz marca 2014, sicer pa poročilo izhaja dvakrat na leto.

Tabela 3: Izračun varnostnega tveganja po uvedbi ukrepa R(C)

Spremenljivka	Vrednost	Opis
V_{ESET}	0,0030	Produktivnost ukrepa ESET po enačbi (10)
V_{V3}	0,0275	Produktivnost ukrepa V3 po enačbi (10)
p_{ESET}	0,000429	Verjetnost za okužbo z računalniškim virusom ob ukrepu ESET na dan
p_{v3}	0,003929	Verjetnost za okužbo z računalniškim virusom ob ukrepu V3 na dan
R_{ESET}	0,16	Varnostno tveganje (v EUR) ob ukrepu ESET v enačbi (7) na dan
$R(C)_{ESET}$	40,47	Varnostno tveganje (v EUR) po uvedbi ESET za 261 delovnih dni na leto
R_{v3}	1,42	Varnostno tveganje (v EUR) ob ukrepu V3 v enačbi (7) na dan
$R(C)_{v3}$	371,01	Varnostno tveganje (V EUR) po uvedbi V3 za 261 delovnih dni na leto

Glede na izračunano varnostno tveganje po uvedbi obeh ukrepov, lahko ugotovimo, da so letne koristi uvedbe ukrepa ESET v višini E_{ESET} = 3 332,33 €, ukrepa V3 pa v višini E_{V3} = 3 001,79 €. Pri tem se predpostavlja, da nakup in uvedba protivirusne zaščite negativnega vpliva na poslovanje ne povzroči ($\delta = 0$), enako posrednega pozitivniega učinka ni pričakovati ($\mu = 0$).

Celotni stroški naložbe v varnostni ukrep (C) so izračunani po enačbi (3) in za oba ukrepa ločeno prikazani v tabeli 4. Nakup protivirusnega programa glede na sedanjo informacijsko infrastrukturo enote ne zahteva nabave dodatne opreme ($C_b = 0$), enkraten strošek uvedbe, preizkušanje in izobraževanja (C_i) je za oba produkta enako ocenjen na 2 322,78 €. Začetna naložba je tako sestavljena iz stroška namestitve in preizkušanja ter stroška izvedbe kratkega tečaja za varno delo s podatki. Za namestitev in preizkušanje zunanji izvajalec zaračuna 15 servisnih ur (30min na računalnik), izobraževalnemu tečaju za zaposlene po ceni 45,00 € na osebo pa je treba prišteti še povprečni strošek dela ene ure, kolikor traja tečaj v prostorih enote za 30 zaposlenih. Strošek naročnine za protivirusne definicije (C_f) produkta ESET za prvi dve leti in 30 delovnih postaj je 2 104,50 €, letna obnovitvena licenca v naslednjih letih pa 981,00 € (ESET Smart Security cenik, 2014). Za produkt V3 je po ceniku ponudnika licence (Ahnlab V3 Internet Security cenik, 2014) mogoče plačevati le za eno leto, kar je za 30 delovnih postaj 860,00 €. Strošek rednega vzdrževanja (C_m) je za oba produkta ocenjen na eno uro mesečno, kar na leto po ceniku zunanjega izvajalca pomeni letni strošek v višini 480,00 €.

Tabela 4: Celotni stroški naložbe v varnostna ukrepa ESET in V3

Strošek (v EUR) / Produkt	C_b	C_i	C_f	C_m	C_o
ESET	0,00	2 322,78	2 104,50 leto 1 0,00 leto 2 981,00 leto 3-5	480,00	0,00
V3	0,00	2 322,78	860,00	480,00	0,00

Na podlagi ocene koristi in stroškov naložbe lahko preverimo njeno ekonomsko upravičenost z izračunom in primerjanjem kazalnikov, ki so del osnovne oziroma klasične metode presojanja upravičenosti naložb (Götze, Northcott & Schuster, 2008) in ki se v praksi najpogosteje uporabljajo. Po rezultatih raziskav CCSS (Computer Security Institute, 2010, str. 36; Computer Security Institute, 2009, str. 34; Computer Security Institute, 2008, str.10) so to *ROI*, *NPV* in

IRR, katerim so v okviru analize za dodatno podporo odločitvi dodani še kazalniki doba vračanja naložbe (angl. *payback period*), popravljena notranja stopnja donosa (angl. *modified internal rate of return*, v nadaljevanju *MIRR*) in indeks donosnosti (angl. *profitability index*, v nadaljevanju *PI*). Vrednotenje obeh ukrepov za izračun omenjenih kazalnikov je prikazano v tabeli 5.

Tabela 5: Ekonomsko vrednotenje varnostnih ukrepov ESET in V3

Leto	**0**	**1**	**2**	**3**	**4**	**5**	**vsota**	**ukrep**
Koristi (*E*)	0,00	3 332,33	3 332,33	3 332,33	3 332,33	3 332,33	16 661,64	ESET
Stroški (*C*)	2 322,78	2 584,50	480,00	1 461,00	1 461,00	1 461,00	9 770,28	
Denarni tok (*CF*)	–2 322,78	747,83	2 852,33	1 871,33	1 871,33	1 871,33	6 891,35	
Kumulativni (*CF*)	–2 322,78	–1 574,96	1 277,37	3 148,70	5 020,03	6 891,35	-	
Koristi (*E*)	0,00	3 001,79	3 001,79	3 001,79	3 001,79	3 001,79	15 008,97	V3
Stroški (*C*)	2.322,78	1 340,00	1 340,00	1 340,00	1 340,00	1 340,00	9 022,78	
Denarni tok (*CF*)	–2 322,78	1 661,79	1 661,79	1 661,79	1 661,79	1 661,79	5 986,18	
Kumulativni *CF*	–2 322,78	–660,99	1 000,80	2 662,60	4 324,39	5 986,18	-	

4.2.1 Doba vračanja naložbe

Kazalnik pove, kakšno je pričakovano časovno obdobje (število let), v katerem se z donosi povrne začetni znesek naložbe brez upoštevanja časovne vrednosti denarja (Berk, Lončarski & Zajc, 2004, str. 97). Enačba (11) za izračun dobe vračanja za posamezno naložbo primerja začetni denarni vložek in pričakovane denarne prilive ali prihranke ter tako pove, kdaj se naložba sama poplača:

$$PP = nNCF_{t-1} + \left(\frac{\left| NCF_{t-1} \right|}{NCF_t} \right) \tag{11}$$

Doba vračanja (*PP*) je torej vsota števila let pred poplačilom naložbe ($nNCF_{t-1}$) in razmerja med absolutnim zneskom neto denarnega toka v letu pred poplačilom (NCF_{t-1}) in neto denarnim tokom v letu poplačila (NCF_t), kjer je leto poplačila naložbe (t) tisto, v katerem pričakovani denarni tok (prihranek) naložbe v celoti poplača preostanek začetnega vložka. Glede na podatke iz tabele 5 in enačbe (11) je doba vračanja naložbe v ESET eno leto in dobrih sedem mesecev ($PP_{\mathrm{ESET}} = 1{,}55$), naložbe v V3 pa slabo leto in pol ($PP_{\mathrm{V3}} = 1{,}39$).

Prednost uporabe te metode je poleg enostavnosti izračuna še, da do določene mere lahko sklepamo o tveganosti in likvidnosti naložbe (Berk, Lončarski & Zajc, 2004, str. 97), iz česar izhaja, da je zaželena čim krajša doba in s tem večja likvidnost sredstev. Po tem kazalniku bi med obema možnostma izbrali produkt V3, vendar pa je pred sprejetjem dokončne odločitve

potrebno upoštevati pomanjkljivosti metode in kazalnik primerjati z rezultati drugih kazalnikov, ki analizo dopolnjujejo. Pomanjkljivost metode, da ne upošteva časovne vrednosti denarja, je sicer mogoče odpraviti z izračunom diskontirane dobe vračanja, torej z upoštevanjem ustrezne diskontne stopnje. Vendar pa glavna pomanjkljivost metode, da ne upošteva denarnih tokov po dobi vračanja, vseeno ostaja, kar pomeni, da ni primerna za izbiro med vsebinsko različnimi naložbenimi možnostmi. Razlog je, da bi lahko zavrnili projekte, ki zahtevajo več časa, da se poplačajo, a hkrati zagotavljajo pozitivne denarne tokove po pokritju začetnega vložka (imajo pozitivno *NPV*).

4.2.2 Donosnost naložbe

Kazalnik *ROI* (enačba (12)) je razmerje med neto koristmi (prihodki in/ali prihranki zmanjšani za celotne stroške) in celotnimi stroški naložbe, izražen v odstotkih (Jeffery, 2004, str. 216):

$$ROI = \frac{koristi(E) - stroški(C)}{stroški(C)} \tag{12}$$

Kazalnik torej pove, kolikšen je delež vrnjene naložbe v določenem časovnem obdobju, pri čemer se lahko računa za vsako posamezno leto ali za celotno časovno obdobje skupaj. Pri primerjavi več mogočih varnostnih rešitev se v primeru, da so drugi dejavniki med rešitvami enaki, sprejme tisto, ki daje največjo dodano vrednost glede na vložena denarna sredstva (rešitev z najvišjim *ROI*). Po tem merilu bi v enoti izbrali naložbo v produkt ESET, katerega kumulativna donosnost obdobja je višja (ROI_{ESET} = 70,5 % > ROI_{V3} = 66,3 %). Še dodaten argument je višji kumulativni neto denarni tok iz tabele 5 (CF_{ESET} = 6 891,35 € > CF_{V3} = 5 986,18 €), kar pomeni, da naložba v produkt ESET v primerjavi z V3 enoti prinaša večji prihranek in je glede na *ROI* bolj donosna.

Prednost uporabe kazalnika v prvi vrsti izhaja iz njegove enostavnosti razumevanja, izračuna in pridobivanja podatkov iz uradnih računovodskih izkazov. Pogostost in popularnost uporabe Botchkarev in Andru (2011, str. 248) pripisujeta dejstvu, da gre za kazalnik, ki se osredinja na eno glavnih poslovnih meril – dobičkonosnost. Pri naložbah v informacijsko varnost se pogosto uporablja tudi zato, da vodje služb za informatiko upravam dokažejo, da je njihova služba tudi center, ki ustvarja donose in ne zgolj stroškovni center v podjetju. Slabost uporabe kazalnika je, da pokaže, ali je določena naložba donosna, ne pove pa ničesar o njeni velikosti (Bojanc, 2010, str. 94) oziroma o tem ali povečuje vrednost podjetja za lastnike. Poleg tega je vrednost kazalnika odvisna od dolžine časovnega obdobja, ki mora biti za izračun vnapej točno poznano, in od dinamike stroškov in prihodkov v njem. Pogosto se namreč zgodi, da naložba generira prihodke in povzroča stroške v obdobju, ki je daljše od začetno predvidenega, kar pomeni, da je vrednost *ROI* v tem daljšem obdobju lahko precej drugačna, lahko celo takšna, da je vodstvo niti ne bi odobrilo. Jeffery (2004, str. 216) zato meni, da *ROI* ni primeren kot samostojen kazalnik za presojanje ekonomske upravičenosti naložb, zlasti kadar prihodki in stroški naložbe v času močno nihajo, kot tudi ne pri odločanju med naložbami, ki učinke povzročajo v različno dolgih časovnih obdobjih. Zato se v primeru dolgoročnih naložb za njihovo presojanje namesto ali v

kombinaciji z *ROI* uporabljajo tudi drugi kazalniki, kot sta *NPV* in *IRR*, v primeru naložb v informacijsko varnost pa tudi posebej prilagojeni kazalniki, izpeljani iz *ROI*.

4.2.3 Neto sedanja vrednost

To je metoda ocenjevanja naložb z uporabo tehnike diskontiranih denarnih tokov (Berk, Lončarski & Zajc, 2004, str. 97), pri kateri gre za primerjavo prihodnjih koristi in stroškov z začetnimi stroški naložbe ob upoštevanju ustrezne diskontne stopnje (strošek kapitala). *NPV* je nasprotno od *ROI* finančni kazalec (stroški in koristi so izraženi v denarni enoti), s katerim lahko primerjamo stroške in koristi v različnih časovnih obdobjih. Z diskontranjem nasprotno od kazalnika *PP* se vključuje časovna komponenta oziroma upošteva vrednost denarja v času. Poleg tega pa se upoštevajo vsi pričakovani denarni tokovi naložbe, tudi tisti po trenutku poplačila naložbe. V postopku izračuna (enačba (13)) se najprej opredelijo vsi pričakovani denarni tokovi (ocenjene koristi E_t zmanjšane za ocenjene stroške C_t) in se z upoštevanjem diskontne stopnje (k) izračuna vsota njihove sedanje vrednosti. Od te vsote odštejemo še začetni izdatek naložbe (I_0) in glede na odločitvena merila sprejmemo odločitev (Berk, Lončarski & Zajc, 2004, str. 97).

$$NPV = \sum_{t=0}^{n} \frac{E_t - C_t}{(1+k)^t} = \sum_{t=1}^{n} \frac{E_t - C_t}{(1+k)^t} - I_0 \qquad (13)$$

Odločitveno merilo pove, da se naložba sprejme vedno, kadar je *NPV* večji od nič (povečuje vrednost podjetja), razen pri medsebojno izključujočih naložbah, kjer se sprejme tista z višjim *NPV*. Če je *NPV* enak nič, so neto denarni tokovi enaki investiranemu kapitalu, zaradi česar pri odločitvi pomembno vlogo odigrajo druga merila. Vsakokrat, ko je *NPV* manjši od nič, se naložba zavrne, saj v tem primeru sedanja vrednost pričakovanih stroškov presega sedanjo vrednost pričakovanih koristi, naložba pa ustvarja izgubo. Glede na opisana merila, bi se v enoti odločili za produkt ESET, saj izkazuje višji *NPV* kot produkt V3 (NPV_{ESET} = 6 305,95 € > NPV_{V3} = 5 481,45 €) in v večji meri prispeva k povečanju vrednosti zavoda.

Kot druge metode ima tudi uporaba *NPV* določene omejitve. Z njegovo uporabo lahko ugotovimo, ali in katera naložba povečuje vrednost podjetja, ne pove pa kdaj[33] oziroma v katerem trenutku se donos ustvari. Ker gre za absolutno mero, ki prikazuje rezultat v denarni vrednosti, se ne upošteva velikost naložbe (Reisman et al., 2012, str. 4/2–10) oziroma se ne upošteva omejenost sredstev (kapitala). Tako bi lahko med izključujočima naložbama izbrali tisto z višjim pozitivnim *NPV*, ki pa hkrati zahteva veliko večji začetni vložek, za katerega se postavlja vprašanje, ali si ga podjetje sploh lahko privošči. Ravno to pomanjkljivost pa je mogoče odpraviti z vključitvijo kazalnika *IRR* v analizo ekonomske upravičenosti naložbe.

[33] Ali je to na začetku, na sredini ali morda pri koncu ocenjenega obdobja, ko naložba ustvarja denarne tokove?

4.2.4 Notranja stopnja donosa

Enako kot *NPV*, tudi *IRR* temelji na diskontiranju prihodnjih denarnih tokov, vendar pa ta kazalnik upošteva tudi velikost naložbe. Definirana je kot diskontna stopnja, pri kateri je sedanja vrednost pričakovanih prihodnjih neto koristi enaka sedanji vrednosti stroškov naložbe oziroma tista, pri kateri je *NPV* naložbe enak nič (Berk, Lončarski & Zajc, 2004, str. 97):

$$\sum_{t=0}^{n} \frac{E_t - C_t}{(1+IRR)^t} = 0 \qquad (14)$$

Postopek izračuna *IRR* je v osnovi enak izračunu *NPV*, le da se v enačbi (14) predpostavi, da je *NPV* naložbe enak nič. Tudi odločitveno merilo je podobno kot pri *NPV* in pravi, da se naložba sprejme vedno, kadar je *IRR* večji od diskontne stopnje *k*, razen pri medsebojno izključujočih naložbah se sprejme tista z višjim *IRR*. Prednost metode poleg tega, da gre za relativno mero, je, da upošteva vse pričakovane denarne tokove naložb. Njena slabost pa, da ni povsem zanesljivo merilo, kadar se odloča med medsebojno izključujočimi naložbami, kjer se lahko zgodi, da sta si kazalnika *NPV* in *IRR* v nasprotju. Ravno to se zgodi v obravnavanem primeru, kjer produkt V3 izkazuje višji *IRR* (IRR_{ESET} = 65,0 % < IRR_{V3} = 65,8 %) in hkrati nižji *NPV* kot ESET. Do takšne situacije pride zaradi različnega obsega naložb ali zaradi različnega časovnega razporeda denarnih tokov. V obravnavanem primeru gre predvsem za slednje, kar je posledica plačila prve dvoletne naročnine za protivirusne definicije za ESET v enem obroku, medtem ko se za V3 od prvega leta dalje plačuje letna naročnina v enakih zneskih glede na objavljene cenike. Berk, Lončarski in Zajc (2004, str. 99) svetujejo, da se v takšnih primerih izbere naložbo z višjim *NPV*, saj se tako izbere naložba, ki v večji meri prispeva k povečanju premoženja lastnikov. Poleg tega se analiza lahko dopolni še z preverjanjem kazalnikov, ki so nastali kot odgovor na slabosti *IRR*, kot sta to kazalnika *MIRR* in *PI*.

4.2.5 Popravljena notranja stopnja donosa

Ker je vrednost denarnih tokov naložbe odvisna od stopnje, po kateri je presežek mogoče ponovno investirati in kazalnik *IRR* pomeni reinvestiranje denarnih prejemkov iz naslova naložbe po izračunanem *IRR*, slednji kot odločitveno merilo v primeru medsebojno izključujočih naložb ni zanesljiv. Pogosto namreč velja, da podjetje v primeru visokega izračunanega *IRR* pričakovanega presežka na trgu ne zmore reinvestirati po tako visoki stopnji. Zato je primernejše upoštevati diskontno stopnjo, ki jo bo po pričakovanjih ob reinvestiranju sredstev mogoče doseči, oziroma stopnjo, po kateri je bilo mogoče sredstva za naložbo pridobiti (*k*).

MIRR je tako opredeljen kot diskontna stopnja, ki izenači sedanjo vrednost izdatkov s sedanjo vrednostjo pričakovanih denarnih prihodkov ob koncu trajnostne dobe naložbe (Berk, Lončarski & Zajc, 2004, str. 101). V postopku izračuna po enačbi (15) se glede na sedanjo vrednost (*PV*) izdatkov, izračunano po diskontni stopnji (*k*), ki izraža tveganost naložbe, in glede na prihodnjo

vrednost (*FV*) pričakovanih denarnih prilivov, izračunano po izbrani diskontni stopnji *q*, poišče *MIRR*, pri čemer je *n* število obdobij v trajnostni dobi naložbe[34]:

$$MIRR = \sqrt[n]{\frac{FVprilivi}{PVizdatki}} - 1 = \sqrt[n]{\frac{\sum_{t=0}^{n} E_t - C_t * (1+q)^{n-t}}{\sum_{t=0}^{n} \frac{I_t}{(1+k)^t}}} - 1 \qquad (15)$$

Ob upoštevanju možnosti, da bi zavod prihranke iz naslova naložbe v protivirusno zaščito po najbolj konzervativnem scenariju investiral v obliki depozita pri zakladniškem računu države, torej po pričakovani letni obrestni meri q = 1,94 %, se produkt ESET izkaže za boljšo od obeh možnosti ($MIRR_{ESET}$ = 32,7 % > $MIRR_{V3}$ = 30,0 %).

Prednost uporabe kazalnika *MIRR* se pokaže prav v primerih, kot je obravnavani, saj pri medsebojno neodvisnih naložbah z enakim začetnim vložkom in enako trajnostno dobo potrdi enako odločitev, kot bi jo sprejeli po kazalniku *NPV*. Poleg tega gre za kazalnik, ki kot *NPV* upošteva vse pričakovane denarne tokove naložbe, upošteva vrednost denarja v času in donosnost reinvestiranja. Ravno slednje je lahko tudi slabost, saj ocenjevanje donosnosti v prihodnje v analizo vnaša dodatno negotovost. Poleg tega pa se lahko ponovno pokaže konflikt, ko kazalnika *NPV* in *MIRR* pri medsebojno izključujočih naložbah kažeta vsak drugačno izbiro. Do tega lahko pride v primerih, ko se naložbi v obsegu oziroma potrebnem začetnem vložku močno razlikujeta. Te težave v obravnavanem primeru ni, saj je potrebna začetna naložba za oba produkta enaka.

4.2.6 Indeks donosnosti

Indeks donosnosti je kot kriterij presojanja upravičenosti naložb podobno kot *MIRR* nastal kot odgovor na slabosti kazalnika *IRR*. Kaže relativno donosnost oziroma je razmerje med sedanjo vrednostjo pričakovanih koristi in sedanjo vrednostjo ene denarne enote pričakovanih stroškov (Berk, Lončarski & Zajc, 2004, str. 103).

$$PI = \frac{\sum_{t=1}^{n} \frac{E_t - C_t}{(1+k)^t}}{I_0} = 1 + \frac{NPV}{I_0} \qquad (16)$$

Odločitveno pravilo pravi, da se sprejmejo naložbe, katerih izračunani *PI* je večji od 1 oziroma se med izključujočimi naložbami izbere tista z višjim *PI* (PI_{ESET} = 3,71 > PI_{V3} = 3,36). Ker kazalnik *NPV* prikazuje sedanjo vrednost neto pričakovanih koristi, zmanjšanih za začetno naložbo, razmerje (NPV / I_0) iz enačbe (16) pokaže, da naložba v ESET prinese neto sedanjo

[34] Če se primerja naložbi z različnima trajnostnima dobama, se upošteva *n* od naložbe, ki ima daljšo trajnostno dobo (Reisman et al., 2006, str. 4/2 – 48).

vrednost v višini 2,71 €, naložba v V3 pa 2,36 € za vsak investiran evro. Prednost kazalnika je, da gre za relativno mero, ki dopolnjuje izbiro naložbe po merilu NPV in omogoča rangiranje naložb, kadar omejena sredstva ne zadostujejo za izvedbo vseh projektov, ki povečujejo vrednost podjetja. Slabost kazalnika je, da podobno kot *NPV* ne pokaže, kdaj se donos naložbe dejansko ustvari, ter da je lahko na enak način kot *MIRR* nezanesljivo merilo v primeru medsebojno izključujočih naložb.

4.2.7 Primerjava rezultatov analize in izbira naložbe

V okviru analize ekonomske upravičenosti naložb je treba pri primerjavi več alernativnih možnosti upoštevati različne kazalnike, saj lahko posamezni med njimi dajejo prednost različnim rešitvam. V splošnem tovrstne analize, kjer so vse druge spremenljivke med naložbenimi možnostmi enake, temeljijo na naslednjih predpostavkah (Tkatch, 2010, str. 7):

- Prednost imajo naložbe z višjim neto denarnim tokom.
- Prednost imajo naložbe, ki ustvarijo donos v krajšem času.
- Prednost imajo manj tvegane naložbe.
- Primarni cilj vodstva je maksimiranje vrednosti za lastnike.

Ekonomsko optimalen varnostni ukrep (Bojanc, Mörec, Tekavčič & Jerman-Blažič, 2012, str. 59) je tisti, ki ima med primerjanimi naložbami največje vrednosti za kazalnike *ROI*, *NPV*, *IRR*, *MIRR* in *PI*, izjema je edino kazalnik dobe vračanja naložbe, kjer so naložbe, ki se časovno prej povrnejo bolj zaželene. Glede na rezultate analize obravnavanega primera, ki jih zbirno prikazuje tabela 6, je razvidno, da kazalniki niso vedno med seboj usklajeni.

*Tabela 6: Izračuni kazalnikov za naložbo v protivirusno zaščito**

Ukrep	*PP* (v letih)	*ROI* (%)	*NPV* (€)	*IRR* (%)	*MIRR* (%)	*PI*
ESET	1,55	70,5	6 305,95	65,0	32,7	3,71
V3	1,39	66,3	5 481,45	65,8	30,0	3,36

Legenda: *Zeleno so obarvane celice, kjer kazalnik nakazuje izbiro ukrepa.

Konkretno kazalnika *PP* in *IRR* kažeta izbiro produkta V3, drugi pa favorizirajo produkt ESET. Berk, Lončarski in Zajc (2004, str. 105) menijo, da kazalnik *PP* ni primeren kot samostojno odločitveno merilo med naložbenimi možnostmi, čeprav vsebuje določene informacije. Poleg tega je v obravnavanem primeru razlika med produktoma glede na kazalnik *PP* zelo majhna in tako praktično zanemarljiva. Kazalnik *IRR* je v primeru medsebojno izključujočih naložb prav tako lahko problematičen, zaradi česar je treba biti pozoren na njegove pomanjkljivosti in jih ustrezno odpravljati z uporabo kazalnikov, kot sta *MIRR* in *PI*. Zato je v obravnavanem primeru kot odločitveno merilo za nakup protivirusne zaščite najprimernejši kazalnik *NPV*, po katerem se v enoti odločijo za nakup produkta ESET. Slednji zadosti večini odločitvenih predpostavk, saj zagotavlja večjo dodano vrednost (*ROI*), višji neto denarni tok (višji prihranek) ter v večji meri prispeva k povečanju vrednosti podjetja (*NPV*, *MIRR*, *PI*).

Ker presojanje ekonomske upravičenosti naložb v informacijsko varnost zahteva kompleksno obravnavo vseh medsebojno povezanih dejavnikov (v podjetju in iz njegovega okolja) v dolgoročnem obdobju, se klasična metoda izkaže kot pomanjkljiva (vom Brocke, Strauch & Buddendick, 2007, str. 24). Zlasti zaradi številnih poenostavitvenih predpostavk (npr. kazalnika *NPV* in *IRR* predpostavljata enotno diskontno stopnjo za zadolževanje in reinvestiranje) in neustreznega upoštevanja posrednih davčnih učinkov in učinkov obresti je klasično analizo smiselno ustrezno dopolniti ali celo povsem nadomestiti z ustreznejšo metodo. Götze, Northcott in Schuster (2008, str. 101) predlagajo metodo vizualizacije finančnih posledic (angl. *visualisation of financial implications method*, v nadaljevanju VoFI), ki v dolgoročnem obdobju ustrezno upošteva vse neposredne in posredne učinke naložbe ter jih eksplicitno prikaže v obliki denarnih tokov.

4.3 Analiza finančne upravičenosti nakupa protivirusne zaščite – metoda vizualizacije finančnih posledic VoFI

VoFI je dinamična metoda, ki se v podjetjih uporablja na ravni določanja obsega in porabe proračunskih sredstev za različne naložbe. Gre za vizualno metodo, ki vse denarne tokove iz operativnega nivoja združuje v standardizirano tabelo, s katero eksplicitno in strukturirano prikaže finančni načrt naložbe v njeni celotni (dolgoročni) trajnostni dobi (vom Brocke, Recker & Mendling, 2010, str. 344). Prav tabelarični prikaz denarnih tokov, ki nastanejo kot posledica vseh notranjih in zunanjih učinkov v dobi trajanja naložbe, je poglavitna prednosti metode VoFI v primerjavi s kazalniki klasične metode, kjer je transparentnost dogodkov veliko slabša. Druga ključna prednost metode VoFI pa je njena prilagodljivost (vom Brocke & Lindner, 2004, str. 207), saj omogoča upoštevanje različnih diskontnih stopenj, različnih virov financiranja, možnosti reinvestiranja presežnih sredstev in pregled nad finančnim stanjem za vsako obdobje trajanja naložbe posebej, kot tudi končno stanje ob koncu naložbe.

Standardna tabela metode VoFI v prvem delu vsebuje prikaz pričakovanih denarnih tokov in učinkov, ki so posledica financiranja naložbe z lastnimi sredstvi, z različnimi oblikami posojil in morebitnega reinvestiranja presežnih denarnih sredstev na finančnem trgu. Temeljno pravilo pri sestavi in prikazu denarnih tokov je, da so v vsakem obdobju (letu) izdatki in prejemki usklajeni in je v računovodskem terminu bilanca plačil usklajena, tako da je finančno stanje vsakega obdobja enako nič (Götze, Northcott & Schuster, 2008, str. 102). Drugi del tabele pa je prikaz stanja financiranja naložbe, kjer je za vsako obdobje prikazano stanje zadolženosti in finančnih naložb presežnih denarnih sredstev. Metoda VoFI tako omogoča spremljanje stanja naložbe ločeno za posamezna obdobja njenega trajanja, neto stanje zadnjega obdobja ($t = n$) pa je končna vrednost naložbe (angl. *terminal* ali *compound value of investment*), ki pokaže, v kolikšni meri slednja povečuje premoženje lastnikov. Končna vrednost je tako odločitveno merilo v primeru medsebojno izključujočih oziroma alternativnih naložb.

4.3.1 Postopek izračuna končne vrednosti naložbe

Izračun končne vrednosti naložbe s finančnim načrtom VoFI poteka v treh korakih (Götze, Northcott & Schuster, 2008, str. 103). Za potrebni začetni izdatek naložbe (I_0) se opredeli in zabeleži, kako bo financiran. Če proračun to omogoča, podjetje začetni izdatek pokrije iz lastnih sredstev, lahko se odloči za delno financiranje z dolgom oziroma se v primeru, da lastnih sredstev nima dovolj v celoti, zadolži. Ker metoda VoFI omogoča upoštevanje različnih možnosti financiranja hkrati, se lahko izdela različne finančne načrte, s čimer se ugotovi, katere kombinacije lastnih sredstev in dolga ter katere vrste zadolževanja so finančno najugodnejše. V drugem koraku se za vsa naslednja obdobja v trajnostni dobi naložbe beležijo pričakovani neto denarni tokovi, pri čemer se z upoštevanjem obresti, razdolževanja, morebitnega dodatnega zadolževanja in reinvestiranja presežkov za vsako obdobje posebej računa vrednost oziroma neto stanje naložbe (angl. *net balance*). V zadnjem koraku se za potrditev in izbiro naložbe v primeru angažiranja lastnih sredstev preveri njena absolutna in za medsebojno izključujoče naložbe še relativna dobičkonosnost.

Naložba je absolutno dobičkonosna, če je njena končna VoFI-vrednost višja od dohodka, ki bi ga podjetje ustvarilo z naložbo lastnih sredstev za pokritje začetnega izdatka naložbe na finančnem trgu (na primer z vezano vlogo pri banki za obdobje trajanja naložbe). Relativna dobičkonosnost pa se ugotavlja med dvema ali več naložbami, kjer izmed alternativ v primerjavi izberemo tisto, ki ima glede na kazalnik iz enačbe (17) najvišjo stopnjo donosa (Götze, Northcott & Schuster, 2008, str. 103):

$$q_{IF} = \sqrt[n]{\frac{NB_{t=n}}{IF}} - 1 \tag{17}$$

kjer je q_{IF} stopnja donosa naložbe lastnih sredstev *IF*, *NB* pa končna vrednost naložbe ob koncu njene trajnostne dobe ($t = n$). Za ugotavljanje relativne dobičkonosnosti je treba alternativne naložbe prilagoditi tako, da so medsebojno primerljive. To pomeni, da če nimajo enake trajnostne dobe, tiste s krajšo dobo preračunamo[35] na obdobje trajanja naložbe z najdaljšo dobo. Izenačiti[36] pa je treba tudi začetne naložbene izdatke za tiste alternativne naložbe, pri katerih je začetni izdatek nižji od angažiranih lastnih sredstev naložbe, kjer so ta sredstva predvideno najvišja.

Vodstvo enote svojo odločitev za nakup produkta ESET na podlagi rezultatov klasične analize iz podpoglavja 4.2 še dodatno preveri z izračunom končne vrednosti naložbe po metodi VoFI. Tako izbiro ponudnika in predvideno porabo sredstev proračuna za varnost pri vodstvu zavoda upraviči tudi z vidika njenega učinka na denarni tok. V nadaljevanju je za potrebe prikaza uporabe in možnosti, ki jih omogoča metoda VoFI, izbira produkta preverjena za dva različna načina financiranja naložbe.

[35] Njihovo končno vrednost po metodi VoFI metode obrestujemo z obrestno mero za vezane vloge.
[36] Predpostavimo dodatno naložbo v višini razlike do potrebne vrednosti, z obrestno mero enako vsaj tisti za vezano vlogo.

4.3.2 Izračun končne vrednosti naložbe – financiranje z dolgom

Pri prvem načinu se za potrebni začetni izdatek (I_0 = 2 322,78 €) zavod v celoti zadolži pri zakladniškem računu Republike Slovenije. Torej gre za enako financiranje naložbe, kot je bilo upoštevano za izračun kazalnikov klasične metode, kjer enota najame posojilo za obdobje petih let z enakomernim odplačilom glavnice, z zapadlostjo obrokov in pripisom obresti na koncu posameznega obdobja (leta). Vhodni podatek v VoFI-tabelo je pričakovani neto denarni tok (*CF*) po posameznih letih iz tabele 5, izračunan na operativnem nivoju v skladu s podatki in predpostavkami, opredeljenimi v podpoglavju 4.2.

Iz tabele 7, ki prikazuje izračun končne vrednosti naložbe za produkt ESET, je razvidno, da pričakovani neto denarni tok že v prevem letu zadošča ($CF_{t=1}$ = 747,83 €) za plačilo obroka glavnice ($G_{t=1}$ = 464,56 €) in pripadajočih obresti ($k_{t=1}$ = 49,38 €). Tako enota s pričakovanimi prihranki (presežek koristi nad stroški) v tem letu hkrati ustvari presežna denarna sredstva v višini 233,89 €, ki jih reinvestira v vezano vlogo pri zakladniškem računu in iz tega naslova po pripadajoči obrestni meri (q) v naslednjem letu (t = 2) ustvari prihodek od obresti v višini 4,53 €. Pri tem se upoštevata določbi 9. člena Zakona o davku od dohodkov pravnih oseb (ZDDPO-2) in 4. člena Pravilnika o opredelitvi pridobitne in nepridobitne dejavnosti o oprostitvi plačila davka od obresti do višine 1 000,00 € na leto. V nadaljevanju se na enak način izračunajo postavke za najeto posojilo in reinvestiranje še za druga obdobja z upoštevanjem temeljnega pravila o izenačenosti bilance plačil (finančno stanje vsakega leta je enako nič). Končna vrednost naložbe v produkt ESET iz drugega dela tabele 7, je 6 981,59 €, kar pomeni, da naložba glede na pričakovani denarni tok in način financiranja povečuje vrednost premoženja lastnikov. To je tudi v skladu s pričakovanji glede na kazalnike klasične analize iz podpoglavja 4.2.7.

Poleg tega lahko glede na neto stanje naložbe po letih ugotovimo, da se naložba v produkt ESET poplača v drugem letu, točneje v letu in sedmih mesecih, kolikor je potrebno, da pričakovani neto denarni tok v višini 2 852,33 € pokrije[37] negativno neto stanje iz konca prvega leta naložbe.

[37] Predpostavimo enakomerni prihodek (prihranek) po mesecih v višini 237,69 €.

Tabela 7: Končna vrednost naložbe (v EUR) v produkt ESET – financiranje z dolgom

Leto	**0**	**1**	**2**	**3**	**4**	**5**
Denarni tok (*CF*)	–2 322,78	747,83	2 852,33	1 871,33	1 871,33	1 871,33
Najeto posojilo (*k* = 2,13 %)						
(+) zadolževanje	2 322,78	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	–464,56	–464,56	–464,56	–464,56	–464,56
(–) obresti na dolg	0,00	–49,38	–39,51	–29,63	–19,75	–9,88
Finančno reinvestiranje (*q* = 1,94 %)						
(–) naložba	0,00	–233,89	–2 352,79	–1 427,22	–1 464,73	–1 502,96
(+) obresti na reinvesticije	0,00	0,00	4,53	50,08	77,71	106,07
Finančno stanje	0,00	0,00	0,00	0,00	0,00	0,00
Stanje posojila / naložbe						
Najeto posojilo	–2 322,78	–1 858,23	–1 393,67	–929,11	–464,56	0,00
Finančna naložba	0,00	233,89	2 586,68	4 013,90	5 478,63	6 981,59
NETO STANJE (*NB*)	**–2 322,78**	**–1 624,34**	**1 193,01**	**3 084,79**	**5 014,07**	**6 981,59**

Na enak način se izračuna tudi končna vrednost naložbe v produkt V3 (tabela 8), ki je 6 066,53 €, kar pomeni, da se v enoti glede na odločitveno merilo metode VoFI odločijo za nakup produkta ESET (NB_{ESET} = 6 981,59 € > NB_{V3} = 6 066,53 €).

Tabela 8: Končna vrednost naložbe (v EUR) v produkt V3 – financiranje z dolgom

Leto	**0**	**1**	**2**	**3**	**4**	**5**
Denarni tok (*CF*)	–2 322,78	1 661,79	1 661,79	1 661,79	1 661,79	1 661,79
Najeto posojilo (*k* = 2,13 %)						
(+) zadolževanje	2 322,78	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	–464,56	–464,56	–464,56	–464,56	–464,56
(–) obresti na dolg	0,00	–49,38	–39,51	–29,63	–19,75	–9,88
Finančno reinvestiranje (*q* = 1,94 %)						
(–) naložba	0,00	–1 147,85	–1 179,95	–1 212,67	–1 246,03	–1 280,03
(+) obresti na reinvesticije	0,00	0,00	22,22	45,07	68,54	92,67
Finančno stanje	0,00	0,00	0,00	0,00	0,00	0,00
Stanje posojila / naložbe						
Najeto posojilo	–2 322,78	–1 858,23	–1 393,67	–929,11	–464,56	0,00
Finančna naložba	0,00	1 147,85	2 327,81	3 540,48	4 786,51	6 066,53
NETO STANJE (*NB*)	**–2 322,78**	**–710,37**	**934,14**	**2 611,37**	**4 321,95**	**6 066,53**

V nadaljevanju je izdelan še izračun končne vrednosti naložbe za oba produkta z drugačnim načinom financiranja. Prav to je dodatna prednost metode VoFI, saj se z njeno uporabo lahko preverijo različne možnosti financiranja naložb (Schuster, 2007, str. 25) in ugotovi, katera je glede na lastna sredstva in pričakovane denarne tokove s finančnega vidika najugodnejša.

4.3.3 Izračun končne vrednosti naložbe – delno financiranje z lastnimi sredstvi in različnimi oblikami zadolževanja

Nasprotno od prve možnosti tokrat enota začetni izdatek naložbe delno financira iz lastnih sredstev v višini 1 000,00 €, razliko pa s tremi različnimi oblikami posojil v višini tretjine potrebnega zneska (440,93 € za posamezno posojilo). Prva oblika posojila je enaka kot v prvem primeru, kjer gre za enakomerno obročno odplačilo glavnice in obresti na koncu leta, druga oblika je posojilo z enkratnim odplačilom glavnice na koncu zadnjega leta in letnim plačilom obresti, tretja oblika pa je zadolžitev na lastnem računu oziroma uporaba limita. Vhodni podatki za izračun končne vrednosti naložbe so za oba produkta enaki kot v podpoglavju 4.3.3, pri čemer upoštevamo enako obrestno mero za prvi dve obliki posojila (k) in letno obrestno mero za uporabo limita, ki je višja za 1,5 % (kl = 3,63 %).

Tudi pri takšnem načinu financiranja neto denarni tok pri obeh produktih že v prvem letu zadošča za pokritje obroka glavnice, uporabljenega limita in obresti za vse tri oblike zadolžitve. V primeru nakupa produkta ESET enota preostali del pričakovanega priliva v višini 183,98 € (tabela 9) reinvestira v vezano vlogo, s čimer v drugem letu ustvari prihodek od obresti v znesku 3,56 €. Pri produktu V3 je v prvem letu znesek reinvesticije zaradi višjega pričakovanega neto denarnega toka bistveno višji in je 1 097,94 € (tabela 10), čemur sledi tudi višji prihodek od obresti v znesku 21,26 €. Ker tudi pri takšnem financiranju letne obresti na vezano vlogo za oba produkta ne presežejo 1 000,00 €, obdavčenje v izračunu VoFI ni upoštevano.

Tabela 9: Končna vrednost naložbe (v EUR) v produkt ESET – delno financiranje z lastnimi sredstvi

Leto	**0**	**1**	**2**	**3**	**4**	**5**
Denarni tok (*CF*)	–2 322,78	747,83	2 852,33	1 871,33	1 871,33	1 871,33
Lastna sredstva	1 000,00	0,00	0,00	0,00	0,00	0,00
Najeto posojilo (obročno odplačilo glavnice) (*k* = 2,13 %)						
(+) zadolževanje	440,93	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	–88,19	–88,19	–88,19	–88,19	–88,19
(–) obresti na dolg	0,00	–9,37	–7,50	–5,62	–3,75	–1,87
Najeto posojilo (odplačilo glavnice na koncu) (*k* = 2,13 %)						
(+) zadolževanje	440,93	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	0,00	0,00	0,00	0,00	–440,93
(–) obresti na dolg	0,00	–9,37	–9,37	–9,37	–9,37	–9,37
Koriščenje limita (*k*l = 3,63 %)						
(+) zadolževanje	440,93	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	–440,93	0,00	0,00	0,00	0,00
(–) obresti na dolg	0,00	–15,99	0,00	0,00	0,00	0,00
Finančno reinvestiranje (*q* = 1,94 %)						
(–) naložba	0,00	–183,98	–2 750,83	–1 824,96	–1 862,17	–1 459,17
(+) obresti na reinvesticije	0,00	0,00	3,56	56,82	92,15	128,20
Finančno stanje	0,00	0,00	0,00	0,00	0,00	0,00
Stanje posojila / naložbe						
Najeto posojilo (obročno)	–440,93	–352,74	–264,56	–176,37	–88,19	0,00
Najeto posojilo (končno)	–440,93	–440,93	–440,93	–440,93	–440,93	0,00
Limit	–440,93	0,00	0,00	0,00	0,00	0,00
Finančna naložba	0,00	183,98	2 934,81	4 759,77	6 621,94	8 081,10
NETO STANJE (*NB*)	**–1 322,78**	**–609,69**	**2 229,32**	**4 142,47**	**6 092,82**	**8 081,10**

Po izračunu postavk še za preostala leta ugotovimo, da je končna vrednost naložbe ESET višja (NB_{ESET} = 8 081,10 € > NB_{V3} = 7 166,05 €), oba produkta pa absolutno dobičkonosna, ker končna vrednost naložbe v obeh primerih presega končno vrednost naložbe lastnih sredstev ob vezavi[38]. Glede na to se upošteva odločitveno merilo relativne dobičkonosnosti po enačbi (17), kar pomeni, da odločitev o nakupu produkta ESET ostaja nespremenjena (q_{IF_ESET} = 51,88 % > q_{IF_V3} = 48,27 %).

Ob primejavi končne vrednosti naložbe za izbrani produkt se delno financiranje z lastnimi sredstvi in opisanimi oblikami zadolžitve izkaže za finančno ugodnejše. Zato se v enoti zanj odločijo, če je to v skladu s politiko poslovanja zavoda.

[38] Prihodnja vrednost naložbe lastnih sredstev ob neprekinjeni vezavi pri zakladniškem računu za 5 let: 1 000 × $1{,}019^5$ = 1 100 €.

Tabela 10: Končna vrednost naložbe v produkt V3 – delno financiranje z lastnimi sredstvi

Leto	**0**	**1**	**2**	**3**	**4**	**5**
Denarni tok (*CF*)	–2 322,78	1 661,79	1 661,79	1 661,79	1 661,79	1 661,79
Lastna sredstva	1 000,00	0,00	0,00	0,00	0,00	0,00
Najeto posojilo (obročno odplačilo glavnice) (*k* = 2,13 %)						
(+) zadolževanje	440,93	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	–88,19	–88,19	–88,19	–88,19	–88,19
(–) obresti na dolg	0,00	–9,37	–7,50	–5,62	–3,75	–1,87
Najeto posojilo (odplačilo glavnice na koncu) (*k* = 2,13 %)						
(+) zadolževanje	440,93	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	0,00	0,00	0,00	0,00	–440,93
(–) obresti na dolg	0,00	–9,37	–9,37	–9,37	–9,37	–9,37
Koriščenje limita (*k*l = 3,63 %)						
(+) zadolževanje	440,93	0,00	0,00	0,00	0,00	0,00
(–) razdolževanje	0,00	–440,93	0,00	0,00	0,00	0,00
(–) obresti na dolg	0,00	–15,99	0,00	0,00	0,00	0,00
Finančno reinvestiranje (*q* = 1,94 %)						
(–) naložba	0,00	–1 097,94	–1 577,99	–1 610,42	–1 643,47	–1 236,23
(+) obresti na reinvesticije	0,00	0,00	21,26	51,81	82,98	114,80
Finančno stanje	0,00	0,00	0,00	0,00	0,00	0,00
Stanje posojila / naložbe						
Najeto posojilo (obročno)	–440,93	–352,74	–264,56	–176,37	–88,19	0,00
Najeto posojilo (končno)	–440,93	–440,93	–440,93	–440,93	–440,93	0,00
Limit	–440,93	0,00	0,00	0,00	0,00	0,00
Finančna naložba	0,00	1 097,94	2 675,93	4 286,35	5 929,82	7 166,05
NETO STANJE (*NB*)	**–1 322,78**	**304,27**	**1 970,45**	**3 669,05**	**5 400,70**	**7 166,05**

Na enak način se z metodo VoFI lahko preveri še druge možnosti financiranja, kjer se v analizo po potrebi vključijo tudi davčni učinki in se tako s finančnega vidika ustrezno upraviči naložba v informacijsko varnost.

4.3.4 Odločitev o izbiri naložbe

Načrtovana naložba enote v protivirusno zaščito se glede na kazalnike klasične metode, kot tudi rezultate metode VoFI, izkaže za ekonomsko upravičeno. Po obeh kazalnikih se z naložbo ustvari pričakovane prihranke v višini, ki zadošča in celo občutno presega sredstva, potrebna za pokritje pričakovanih stroškov, s čimer se rezultati analize po obeh metodah vsebinsko dopolnjujejo. Tudi sicer metoda VoFI po mnenju Götzeja, Northcotta in Schusterja (2008, str. 106) smiselno dopolnjuje odločanje glede na rezultate *NPV*, saj nasprotno od slednjega ne pomeni enotne diskontne stopnje zadolževanja in reinvestiranja presežkov. Poleg tega VoFI ne pomeni obstoja popolne informiranosti deležnikov na kapitalskih trgih ter hkrati omogoča vizualno predstavitev in optimalno izbiro med različnimi možnostmi financiranja.

Rezultati analize po obeh metodah ob upoštevanju odločitvenih meril za medsebojno izključujoče naložbe kažejo na izbiro produkta ESET, kjer se hkrati izkaže, da je financiranje z

lastnimi sredstvi in predlaganimi oblikami zadolževanja finančno ugodnejše. S tem enota pri vodstvu zavoda upraviči izbiro naložbe, s čimer pa aktivnosti niso končane. Naložbo je treba v času njenega trajanja spremljati in nadzorovati s ciljem čimprejšnje prepoznave težav in odmikov ter posledično pravočasnega ukrepanja. Še zlasti je pomembno, da se v procesu oblikovanja metod vrednotenja postavke kvalitativno in kvantitativno zapišejo. S tem je omogočeno sprotno ocenjevanje uresničevanja načrta dejanske porabe naložbenih sredstev in spremljanje uresničevanja časovnega načrta izvedbe. Ob zaključku naložbe pa ne sme manjkati tudi vrednotenje učinkov projekta (Reisman et al., 2012, str. 4/2 – 56), saj se tako v podjetju gradi baza znanja in izkušenj za prihodnje naložbe, ki so osnova za izboljšanje delovanja v prihodnosti.

Ne glede na uporabljeno metodo in kazalnike se je treba zavedati, da so preverjanje smiselnosti in upravičenosti naložb z uporabo kvantitativnih metod zgolj pomoč in dodatne informacije pri odločitvah. Noben kazalnik ali metoda ne preverja smiselnosti vhodnih podatkov, uporabljenih predpostavk in vseh mogočih parametrov, zaradi česar rezultati analize ne smejo biti nadomestilo subjektivne presoje (Reisman et al., 2012, str. 4/2–21). Kvantitativne metode so orodje za pridobitev informacij v procesu odločanja, dobljeni rezultati pa ne smejo biti edino vodilo pri sprejetih odločitvah.

SKLEP

Informacijski sistem je ena temeljnih komponent vsake organizacije, ki je poslovodstvu in zaposlenim osnova in podpora pri uresničevanju zastavljenih ciljev. Ker je od kvalitete informacij odvisna uspešnost poslovanja in dolgoročni obstoj vseh gospodarskih subjektov, je njihovo zavedanje o nujnosti zagotovitve varnega informacijskega sistema, ki zmanjša tveganja izgube informacij ali njihovo razkritje, vse večje. Nedvomno je to tudi posledica potencialno izredno visokih stroškov varnostnih dogodkov, čemur pritrjujejo tudi rezultati različnih raziskav s področja informacijske varnosti. Iz slednjih je razvidno, da podjetja kljub kriznim razmeram in upadanju števila zaznanih varnostnih dogodkov vedno večji delež proračuna za naložbe namenjajo zaščiti in varovanju svojih informacijskih sredstev. Ker popolne varnosti s kakršnim koli obsegom in kombinacijo vlaganj ni mogoče zagotoviti, je toliko pomembnejše, da so naložbena sredstva uporabljena ekonomično. To pomeni, da vsaka organizacija s sistemom upravljanja informacijske varnosti kvantitativno ovrednoti potrebe in opredeli zahtevani nivo varnosti, ki ga zagotavlja z ekonomsko upravičenimi vlaganji v varnostne ukrepe.

Informacijsko varnost po različnih opredelitvah razumemo kot proces varovanja informacij in informacijskega sistema, s katerim se zagotavljajo temeljni principi CIA-trikotnika z vsemi razširitvami. Orodje za zagotavljanje principov informacijske varnosti je nenehno izvajanje korakov procesa upravljanja s tveganji, s katerim podjetja v okviru lastnega sistema upravljanja informacijske varnosti načrtujejo potrebne naložbe. Za naložbe na splošno velja, da tisti, ki so zanje odgovorni, z uporabo različnih metod presojajo ekonomsko in finančno upravičenost porabe sredstev, pri čemer to v vedno večji meri velja tudi za naložbe v informacijsko varnost. Z razvojem dogodkov in usmeritev v informacijski tehnologiji je ekonomika naložb v

informacijsko varnost vse pogostejše predmet zanimanja akademske javnosti. To se kaže v razvoju različnih modelov določanja optimalnega obsega vlaganj, med katerimi je največ pozornosti deležen analitičen Gordon-Loebov model. Z njim avtorja ugotavljata, da optimalni obseg naložb za ukrepe informacijske varnosti v večini primerov ne preseže niti tretjine izgub, ki bi jih podjetja utrpela v primeru varnostnih dogodkov. Ne glede na kritike, kasnejše vsebinske razširitve in razvoj metodološko povsem drugačnih modelov Gordon-Loebov model dokazuje, da so naložbe v informacijsko varnost v večini primerov ekonomsko upravičene. Model je tako vsebinska osnova za različne načine ekonomskega upravičenja porabe sredstev, med katerimi se v praksi še vedno najpogosteje uporabljajo kazalniki klasične analize presojanja upravičenosti načrtovanih naložb. Predstavitev v analizi uporabljenega modela, teoretični in grafični prikaz optimalnega obsega vlaganj v informacijsko varnost iz tretjega poglavja vsebinsko zaključujejo teoretični del naloge. Hkrati so tudi uvod in osnova za empirični del, v katerem je z uporabo teoretičnih spoznanj izdelana kvantitativna analiza naložbe v protivirusno zaščito z uporabo dveh različnih metod.

Naložbe v informacijsko varnost so z ekonomskega vidika v primerjavi z drugimi naložbami nekoliko posebne. Posebne zato, ker podjetje z njimi praviloma ne ustvarja dodane vrednosti, dobička ali denarnega toka v obliki denarnih prilivov. Dejansko gre za naložbe, katerih cilj je preprečevanje nastanka mogočih varnostnih dogodkov, končni rezultat pa ustvarjanje prihrankov, ki so v finančnih modelih za ekonomsko upravičenje upoštevani kot koristi oziroma prosta finančna sredstva za reinvestiranje. V skladu z namenom in cilji magistrskega dela je ob upoštevanju značilnosti stroškov in koristi vlaganj v informacijsko varnost v četrtem delu naloge izdelana analiza koristi in stroškov za nakup protivirusne zaščite na primeru večjega slovenskega javnega raziskovalnega zavoda. Izbira za nakup protivirusne zaščite med dvema ponudbama je najprej upravičena na podlagi klasične metode presojanja upravičenosti naložb, konkretno z izračunom kazalnikov, poznanih iz investicijske teorije. Slednji v tem konkretnem primeru kažejo, da zavod oziroma raziskovalna enota z nakupom in implementacijo protivirusne zaščite po pričakovanjih ustvari prihranke oziroma koristi, ki presegajo ocenjene stroške, s čimer je naložba ekonomsko upravičena. V nadaljevanju izračunani kazalniki glede na upoštevane značilnosti in odločitvena merila kažejo na izbiro produkta ESET, ki izkazuje višjo pričakovano neto sedanjo vrednost. Odločitev potrjujeta tudi kazalnika popravljene notranje stopnje donosa in indeks donosnosti, ki se računata v okviru klasične analize, še posebej v primerih, ko kazalnik notranje stopnje donosa kaže drugačno izbiro kot neto sedanja vrednost med izključujočima se naložbama.

Analiza izbire protivirusnega produkta med obema ponudnikoma je v drugem delu četrtega poglavja dodatno dopolnjena še z metodo vizualizacije finančnih posledic. Gre za metodo, ki eksplicitno izkazuje denarne tokove v trajnostni dobi naložbe, s čimer se bistveno razlikuje od drugih analitičnih metod. Tako smiselno dopolnjuje klasično analizo ekonomske upravičenosti, saj omogoča upoštevanje različnih virov in možnosti financiranja naložbe ter njeno upravičenje tudi z vidika vpliva na pričakovane denarne tokove, ki si jih podjetje glede na lastne finančne zmožnosti lahko privošči. Zato sta v primeru zavoda z uporabo te metode preverjena dva mogoča načina financiranja naložbe: najprej financiranje z dolgom in nato še delno financiranje z

lastnimi sredstvi. Glede na merilo izbire je ESET, enako kot v primeru klasične analize, primernejši od obeh alternativ, in to pri obeh preverjenih načinih financiranja, saj po metodi VoFI izkazuje višjo končno vrednost od naložbe v produkt V3. Iz tabel metode VoFI ugotovimo tudi, da naložba v primeru obeh produktov in obeh načinov financiranja s pričakovanim neto denarnim tokom izdatke pokrije že v prvem letu po začeti naložbi. Tudi v naslednjih letih je pričakovano, da bo naložba ustvarjala pozitivne neto denarne tokove, ki se ob konservativni naložbeni politiki v obliki vezave sredstev pri zakladniškem računu države seštevajo v pozitivno končno vrednost naložbe v zadnjem letu trajanja. Torej analiza z metodo VoFI potrjuje ugotovitev kazalnika neto sedanje vrednosti iz klasične analize, pri čemer še dodatno kaže, da z naložbo v produkt ESET in delnem financiranju z lastnimi sredstvi zavod v največji meri od preverjenih možnosti povečuje svoje premoženje oziroma premoženje lastnikov. S tem je dosežen namen praktičnega dela naloge, torej izvedba kvantitativne analize in prikaz ekonomskega upravičenja naložbe v informacijsko varnost.

Predstavljena analiza in njene ugotovitve ob opisanih značilnostih in mogočih šibkih točkah oziroma pomanjkljivostih odpira dodatna vprašanja in možnosti za nadaljnje preučevanje področja in nadgradnje ekonomike informacijske varnosti. Uporabljen model bi bil v nadaljevanju lahko dopolnjen s kombiniranjem večjega števila različnih varnostnih ukrepov hkrati, konkretno tistih, ki so oziroma bi morali biti implementirani na podlagi določil varnostne politike posamezne organizacije. Tako bi s kombinacijo klasične analize in metode VoFI, predstavljene v magistrski nalogi, lahko preverili ekonomsko upravičenost varnostnega sistema kot celote. Model za izračun varnostnega tveganja za v nalogi preučevan raziskovalni zavod temelji na podlagi ocene o pogostosti prejema okuženih datotek. Gre za predpostavko, ki se lahko kaj hitro izkaže za napačno oziroma pomanjkljivo. Če denimo zavod postane tarča ciljanih napadov, se lahko število prejetih okuženih datotek na službene elektronske naslove zaposlenih bistveno poveča, kar sicer pomeni, da so dejanske koristi nakupa protivirusne zaščite večje od ocenjenih. Po drugi strani pa bi večje zmanjšanje števila prejetih okuženih datotek po prikazanih izračunih lahko pomenilo neupravičeno porabo sredstev z ekonomskega vidika. Predpostavko v modelu tako nadomesti npr. simulacija Monte Carlo z generiranjem naključnega števila prejetih okuženih datotek, dodatno kombinirana s simulacijo učinkovitosti protivirusne zaščite, če zaupanje v objavljene preizkuse učinkovitosti protivirusnih produktov ni zadostno. Na tej podlagi se lahko izračunajo vrednosti kazalnikov klasične analize in končne vrednosti naložbe po metodi VoFI ter s statistično analizo rezultatov ugotavlja verjetnost, da so koristi naložbe nižje od pričakovanih stroškov. V okviru preverjanja ekonomske upravičenosti varnostnega sistema kot celote predvsem metoda VoFI omogoča dodatne razširitve, denimo z upoštevanjem pozitivnega vpliva amortizacije na davčno osnovo, pri varnostnih ukrepih, ki se računovodsko vodijo kot neopredmetena osnovna sredstva in podobno. Ne glede na način in vrsto pa morajo biti razširitve modelov vedno v smeri njihovega približevanja realnosti in praksi. Pri tem je pomembno, da ne postanejo preveč kompleksni in posledično težko obvladljivi in nerazumljivi.

Glede na podatke o pogostosti nastanka varnostnih dogodkov iz raziskav, zlasti pri njihovih stroških in smereh razvoja dogodkov v prihodnosti, pričakujem, da se bodo zahteve vodilnih po ekonomskem upravičenju naložb v informacijsko varnost še okrepile. Zlasti v javnem sektorju,

kjer je pri neposrednih in posrednih proračunskih uporabnikih porabo sredstev potrebno vsebinsko, namensko in ekonomsko upravičiti. V nalogi opisana teoretična izhodišča in empirični izračuni za konkretni primer javnega zavoda prikazujejo način takšnega upravičenja. Slednje je za finančno večje varnostne projekte nujno, za manjše, kot je to primer nakupa protivirusne zaščite pa zaželeno. To še posebej zaradi dejstva, da ne gre za naložbe v osnovno oziroma temeljno dejavnost zavoda, temveč za režijske izdatke podpornih dejavnosti, ki so konstantno pod drobnogledom financerjev.

LITERATURA IN VIRI

1. Aceituno, V. (2006). Return On Security Investment. *ISSA Journal, 5*, 1─4.
2. *AhnLab V3 Internet security cenik*. Najdeno 22. junija 2014 na spletnem naslovu http://global.ahnlab.com/en/site/store/storeSubDetail.do?prod_class=N&prod_type=NF&prod_seq=58054
3. Al-Humaigani, M., & Dunn, D. B. (2004). A Model of Return on Investment for Information Systems Security. *46th IEEE International Midwest Symposium on Circuits and Systems* (str. 483─485). Cairo: IEEE.
4. Anderson, R. (2001). Why information security is hard: An economic perspective. *The 17th Annual Computer Security Applications Conference* (str. 358─365). Los Alamitos: IEEE Computer Society.
5. Aoufi, E. S. (2009). *Economic Evaluation of Information Security*. Amsterdam: VU University Amsterdam.
6. Arthur, B. W. (1996). Increasing Returns and the New World of Business. *Harvard Business Review*, *74*(4), 100─109.
7. AV Comparatives. (2014, marec). File Detection Test of Malicious Software. Najdeno 27. maja 2014 na spletnem naslovu http://www.av-comparatives.org/file-detection-test-march-2014/
8. Banday, M. T., Qadri, J.A., & Shah, N. A. (2009). Study of Botnets and Their Threats to Internet Security. *Sprouts: Working Papers on Information Systems, 9*(24), 1–13.
9. Baryshnikov, Y. (2012). IT Security Investment and Gordon-Loeb's 1/e Rule. *Workshop on the Economics of Information Security (WEIS 2012)*. Najdeno 22. julija 2013 na spletnem naslovu http://ect.bell-labs.com/who/ymb/ps/cyber.pdf
10. Bergant, Ž. (2010). *Osnove analize poslovanja*. Ljubljana: Inštitut za poslovodno računovodstvo.
11. Berinato, S. (2002, april). Finally, a Real Return on Security Spending. *CIO*. Najdeno 25. julija 2012 na spletnem naslovu http://www.cio.com.au/article/52650/finally_real_return_security_spending/
12. Berk, A., Lončarski, I., & Zajc, P. (2004). *Poslovne finance*. Ljubljana: Ekonomska fakulteta.
13. Bhasker, R., & Kapoor, B. (2010). Information Technology Security Management. V J.R. Vacca (ur.), *Managing Information Security* (str. 1–46). Burlington: Elsevier.
14. Böhme, R. (2010). Security Metrics and Security Investment Models. V I. Echizen, N. Kunihiro & R. Sasaki (ur.), *Advances in Information and Computer Security* (str. 10–24). Berlin: Springer─Verlag.
15. Böhme, R., & Nowey, T. (2008). Economic Security Metrics. V I. Eusgeld, F.C. Freiling & R. Eussner (ur.), *Dependability Metrics: Advanced Lectures* (str. 176–187). Berlin: Springer.
16. Böhme, R., & Moore, T. (2012). Security Metrics and Security Investment. *Working draft*. Najdeno 17. septembra 2013 na spletnem naslovu http://lyle.smu.edu/~tylerm/courses/econsec/f12/reading/lnse-secinv1.pdf
17. Boisot, M., & Canals, A. (2004). Data, information and knowledge: have we got it right? *IN3: UOC Working Paper Series: DP04-002*. Najdeno 5. maja 2012 na spletnem naslovu

http://in3wps.uoc.edu/ojs/index.php/in3-working-paper-series/article/viewFile/n4-boisot-canals/n2-boisot-canals
18. Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *Internaional Journal of Information Management, 28,* 413─422.
19. Bojanc, R., & Jerman-Blažič, B. (2012). Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Organizacija, 45*(6), 276─288.
20. Bojanc, R., Mörec, B., Tekavčič, M., & Jerman-Blažič, B. (2012). Model določitve optimalnega obsega vlaganj v informacijsko varnost. *IB Revija, 3-4,* 53─61.
21. Bojanc, R. (2010). *Modeli zagotavljanja varnosti v poslovnih informacijskih sistemih* (Doktorska disertacija). Ljubljana: Ekonomska fakulteta.
22. Botchkarev, A., & Andru, P. (2011). A Return on Investment as a Metric for Evaluating Information Systems: Taxonomy and Application. *Interdisciplinary Journal of Information, Knowledge and Management, 6,* 245─269.
23. Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI Standard 100-1. Information Security Management Systems (ISMS).* Bonn: Bundesamt für Sicherheit in der Informationstechnik.
24. Caballero, A. (2010). Information Security Essentials for IT Managers: Protecting Mission–Critical Systems. V J.R. Vacca (ur.), *Managing Information Security* (str. 55–71). Burlington: Elsevier.
25. Camp, J. L. (2004). The State of Economics of Information Security. *A Journal of Law and Policy for the Information Society, 2,* 189─205.
26. Canal, V. A. (2005). On Information Security Paradigms. *ISSA – The Global Voice of Information Security*. Najdeno 2. junija 2012 na spletnem naslovu http://www.issa.org/Library/Journals/2005/September/Aceituno%20Canal%20-%20On%20Information%20Security%20Paradigms.pdf
27. Cavusoglu, H. (2004). Economics of IT Security Management. V J. L. Camp & S. Lewis (ur.), *Economics of Information Security* (str. 71–83). Dordrecht: Klower Academic Publishers.
28. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM, 47*(7), 87─92.
29. Chen, T. M. (2009). Information Security and Risk Management. *Encyclopedia of Multimedia Technlogy and Networking*. Najdeno 20. maja 2012 na spletnem naslovu http://lyle.smu.edu/~tchen/papers/info-sec-risks.pdf
30. Clinch, J. (2009). ITIL V3 and Information Security. *Clinch Consulting White Paper*. Najdeno 7. junija 2012 na spletnem naslovu http://www.best-management-practice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf
31. Computer Security Institute. (2003). 2003 CSI/FBI Computer Crime and Security Survey. Najdeno 15. julija 2012 na spletnem naslovu http://www.yle.fi/mot/kj040524/fbiraportti.pdf
32. Computer Security Institute. (2005). 2005 CSI/FBI Computer Crime and Security Survey. Najdeno 15. julija 2012 na spletnem naslovu http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

33. Computer Security Institute. (2006). 2006 CSI/FBI Computer Crime and Security Survey. Najdeno 15. julija 2012 na spletnem naslovu http://gocsi.com/sites/default/files/uploads/FBI2006.pdf
34. Computer Security Institute. (2007). 2007 CSI Computer Crime and Security Survey. Najdeno 15. julija 2012 na spletnem naslovu http://gocsi.com/sites/default/files/uploads/2007_CSI_Survey_full-color_no%20marks.indd_.pdf
35. Computer Security Institute. (2008). 2008 CSI Computer Crime and Security Survey. Najdeno 15. julija 2012 na spletnem naslovu https://www.hlncc.com/docs/CSIsurvey2008.pdf
36. Computer Security Institute. (2009). 2009 CSI Computer Crime and Security Survey. Najdeno 15. julija 2012 na spletnem naslovu http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive%20Edition.pdf
37. Computer Security Institute. (2010). 2010 / 2011 CSI Computer Crime and Security Survey. Najdeno 15. julija 2012 na spletnem naslovu https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf
38. Cremonini, M., & Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). *Workshop on the Economics of Information Security (WEIS 2005)*. Najdeno 3. marca 2013 na spletnem naslovu http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.9925&rep=rep1&type=pdf
39. Crume, J. (2001). *Inside Internet Security: What Hackers Don't Want You To Know*. Boston: Addison Wesley.
40. Dimensional Research. (2011). The Risk of Social Engineering on Information Security: A Survey of IT Professionals. Najdeno 23. maja 2012 na spletnem naslovu http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf
41. Duff, A. S. (2005). Social Engineering in the Information Age. *The Information Society, 21*(1), 67–71.
42. *ESET Smart Security cenik*. Najdeno 22. junija 2014 na spletnem naslovu http://www.eset.com/si/spletni-nakup/cenik/
43. *Facebook Newsroom*. Najdeno 23. oktobra 2012 na spletnem naslovu http://newsroom.fb.com/news/
44. Feruza, Y. S., & Kim, T. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering, 2*(2), 17–32.
45. Franqueira, V. N. L., Houmb, S. H., & Daneva, M. (2010). Using Real Option Thinking to Improve Decision Making in Security Investment. V R. Meersman, T. Dillon & P. Herrero (ur.), *On the Move to Meaningful Internet Systems: OTM 2010* (str. 619–638). Berlin: Springer.
46. Gareston, C., & Messmer, E. (2006, marec). It's raining IT security surveys. *Network World*. Najdeno 25. julija 2012 na spletnem naslovu http://www.networkworld.com/news/2006/032006-security-surveys.html?page=1

47. Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.
48. Gordon, L. A., & Loeb, M. P. (2006). Budgeting Process for Information Security Expenditures. *Communications of the ACM, 49*(1), 121–125.
49. Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information Security Expenditures and Real Options: A Wait-and-See Approach. *Computer Security Journal, 19*(2), 1–7.
50. Götze, U., Northcott, D., & Schuster, P. (2008). *Investment Appraisal: Methods and Models*. Berlin: Springer.
51. Grobler, C. P. (2003). *A Model to assess the Information Security status of an organization with special referenceto the Policy Dimension*. Johannesburg: Faculty of Natural Science at Rand Afrikaans University.
52. Guillot, A., & Kennedy, S. (2007). Information Security Surveys: A Review of the Methodologies, the Critics and a Pragmatic Approach to their Purposes and Usage. *Proceedings of The 5th Australian Information Security Management Conference* (str. 62─72). Perth: Edith Cowan University.
53. Gunasekaran, A., Love, P. E. D., Rahimi, F., & Miele, R. (2001). A model for investment justification in information technology projects. *International Journal of Information Management, 21*(5), 349–364.
54. Harsh, B. S. (2008, 31. marec). Management Information Systems. ICT in Agriculture: Perspectives of Technological Innovation. Najdeno 15. maja 2012 na spletnem naslovu http://departments.agri.huji.ac.il/economics/gelb-manag-4.pdf
55. Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5), 338–349.
56. Henry, K. (2004). The Human Side of Information Security. V H. F. Tipton & M. Krause (ur.), *Information Security Management Handbook 2004 edition on CD-ROM (*str. 18–30) [zgoščenka]. Boca Raton: Auerbach Publications.
57. Humphreys, E. (2007). *Implementing the ISO/IEC 27001 Information Security Management System Standard*. Norwood: Artech House Inc.
58. Infosecurity Europe & PricewaterhouseCoopers. (2010). Information Security Breaches Survey 2010 | technical report. Najdeno 15. julija 2012 na spletnem naslovu http://www.ukmediacentre.pwc.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1723
59. International Organization for Standardization. (2005a). *International Standard ISO/IEC 27001*. Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization.
60. International Organization for Standardization. (2005b). *International Standard ISO/IEC 27002*. Information technology – Security techniques – Code of practice for information security management. Geneva: International Organization for Standardization.
61. International Organization for Standardization. (2008). *International Standard ISO/IEC 27005*. Information technology – Security techniques – Information security risk management. Geneva: International Organization for Standardization.

62. IT Governance Institute. (2008). Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. *A Management Briefing From ITGI and OGC*. Najdeno 12. junija 2012 na spletnem naslovu http://www.best-management-practice.com/gempdf/Aligning_COBITITILV3ISO27002_Bus_Benefit_9Nov08_Research.pdf
63. Jahankhani, H., Nkhoma, M. Z., & Mouratidis, H. (2010). Security Risk Management Strategy. V H. Jahankhani, D.L. Watson, G. Me & F. Leonhardt (ur.), *Handbook of Electronic Security and Digital Forensics* (str. 237–262). Toh Tuck: World Scientific Publishing Co.
64. Jeffery, M. (2004). Return on Investment Analysis for E-business Projects. V H. Bidgoli (ur.), *The Internet Encyclopedia. Volume 3* (str. 211–228). New Jersey: John Wiley & Sons.
65. Jenkins, B. D. (1998). Security Risk Analysis and Risk Management. *Countermeasures, Inc. white paper*. Najdeno 22. septembra 2012 na spletnem naslovu http://www.nr.no/~abie/RA_by_Jenkins.pdf
66. Karsberg, C., Skouloudi, C., & Dekker, M. (2013). *Annual Incident Reports 2013*. Heraklion: European Union Agency for Network and Information Security.
67. Kaspersky Lab. (2011). Global IT Security Risks: 2011. Najdeno 15. julija 2012 na spletnem naslovu https://www.kaspersky.com/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf
68. Kaspersky Lab. (2012a). Cyberthreat forecast for 2012. Najdeno 15. julija 2012 na spletnem naslovu http://www.kaspersky.com/images/Kaspersky%20report-10-134377.pdf
69. Kaspersky Lab. (2012b). Global IT Security Risks: 2012. Najdeno 15. julija 2012 na spletnem naslovu http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf
70. Kazenski zakonik. *Uradni list RS* št. 95/2004-UPB1, 37/2005 Odl.US: U-I-335/02-20, 17/2006 Odl.US: U-I-192/04-16, 55/2008 (66/2008 popr.), 89/2008 Odl.US: U-I-25/07-43, 5/2009 Odl.US: U-I-88/07-17.
71. Khan, R. H. (2011). The Use of Real Option Analysis (ROA) to assist in Security Solution Decisions. *IJCSNS International Journal of Computer Science and Network Security, 11*(10), 108–119.
72. Ladan, S., Yari, A., & Khodabandeh, H. (2006). Combination of Information Security Standards to Cover National Requirements. *World Academy of Science, Engineering and Technology, 13*, 148–152.
73. Larson, D. (2012, 15. maj). Infographic: Spring 2012 Social Media User Statistics. *TweetSmarter*. Najdeno 20. julija 2012 na spletnem naslovu http://blog.tweetsmarter.com/social-media/spring-2012-social-media-user-statistics/
74. Lockstep Consulting. (2004). A Guide for Government Agencies Calculating Return on Security Investment. Najdeno 13. junija 2012 na spletnem naslovu http://www.services.nsw.gov.au/sites/default/files/ROSI%20Guideline%20SGW%20%282.2%29%20Lockstep.pdf
75. Longstaff, T. A., Chittister, C., Pethia, R., & Haimes Y. Y. (2000). Are We Forgetting the Risks of Information Technology? *IEEE Computer, 33*(12), 43–51.

76. Losee, M. R. (1997). A Discipline Independent Definition of Information. *Journal of the American Society for Information Science, 48*(3), 254–269.
77. Marshall, A. (1920). *Principles of Economics (8th ed.)*. London: Macmillan and Co.
78. Matsuura, K. (2008). Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. *Workshop on the Economics of Information Security (WEIS 2008)*. Najdeno 22. julija 2013 na spletnem naslovu http://weis2008.econinfosec.org/papers/Matsuura.pdf
79. Melek, A. & MacKinnon, M. (2006). *2006 Global Security Survey*. London: Deloitte
80. Mizzi, A. (2005). Return on Information Security Investment. The viability of an anti-spam solution in a wireless enviroment. *International Journal of Network Security, 10*(1), 18–24.
81. Mouratidis, H. (2010). Secure by Design: Considering Security from the Early Stages of the Information Systems Development. V H. Jahankhani, D. L. Watson, G. Me, & F. Leonhardt (ur.), *Handbook of Electronic Security and Digital Forensics* (str. 115–132). Toh Tuck: World Scientific Publishing Co.
82. National Bureau of Standards. (1979). Guideline for Automatic Data Processing Risk Analysis. FIPS PUB 65. Najdeno 9. junija 2012 na spletnem naslovu http://www.femto-second.com/Documents/FIPS65.pdf
83. National Institute of Standards and Technology. (1995). An Introduction to Computer Security: The NIST Handbook. Special Publication 800–12. Najdeno 11. junija 2012 na spletnem naslovu http://www.inf.unideb.hu/~ahuszti/An_introduction_to_computer_security_NIST_handbook.pdf
84. National Institute of Standards and Technology. (2002). Risk Management Guide for Information Technology Systems. Special Publication 800−30. Najdeno 11. junija 2012 na spletnem naslovu http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
85. National Institute of Standards and Technology. (2008). Technical Guide to Information Security Testing and Assessment. Special Publication 800−115. Najdeno 11. junija 2012 na spletnem naslovu http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
86. National Institute of Standards and Technology. (2011). Glossary of Key Information Security Terms. IR 7298 Revision 1. Najdeno 11. junija 2012 na spletnem naslovu http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
87. Neubauer, T., Klemen, M., & Biffl, S. (2005). Business Process–based Valuation of IT–Security. *ACM SIGSOFT Software Engineering Notes, 30*(4), 1–5.
88. *O mimovrste, d. o. o.* Najdeno 12. novembra 2012 na spletnem naslovu http://www.mimovrste.com/info/106/o-mimovrste
89. Organisation for Economic Co-operation and Development. (2008). Malicious Software (Malware): A Security Threat to the Internet Economy. Ministerial Background Report. Najdeno 15. avgusta 2012 na spletnem naslovu http://www.oecd.org/internet/interneteconomy/40724457.pdf
90. Pattinson, F. (2007, julij). Certifying Information Security Management Systems. Atsec information security corporation. Najdeno 26. septembra 2012 na spletnem naslovu http://www.atsec.com/downloads/pdf/CertifyingISMS.pdf

91. Phishing napad na komitente SKB banke. Najdeno 30. oktobra 2012 na spletnem naslovu http://www.cert.si/obvestila/obvestilo/article/si-cert-2012-09-phishing-napad-na-komitente-skb-banke.html
92. Phishing napad na uporabnike spletne banke Abanet. Najdeno 30. oktobra 2012 na spletnem naslovu http://www.cert.si/obvestila/obvestilo/article/phishing-napad-na-uporabnike-spletne-banke-abanet.html
93. Plate, A. (2011). ISO/IEC 27000 Family of Standards. *Telecommunications Regulatory Authority presentation*. Najdeno 7. junija 2012 na spletnem naslovu http://www.tra.gov.lb/Library/Files/Uploaded%20files/ISO%20IEC%2027000%20-%20Workshop%20-%20Lebanon%202011.pdf
94. Ponemon Institute. (2010). 2009 Annual Study: U.S. Cost of a Data Breach. Najdeno 14. julija 2012 na spletnem naslovu http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf
95. Prašnikar, J. (1999). *Uvod v mikroekonomijo*. Ljubljana: Gospodarski vestnik.
96. Pravilnik o opredelitvi pridobitne in nepridobitne dejavnosti. *Uradni list RS* št. 109/2007.
97. PricewaterhouseCoopers. (2012). Navigating security in the cloud. Najdeno 14. julija 2012 na spletnem naslovu http://www.pwc.com/en_US/us/it-risk-security/assets/pwc-navigating-security-in-cloud.pdf
98. Puangsri, P. (2009). *Quantified Return On Information Security Investment – A Model for Cost–Benefit Analysis.* Delft: University of Technology.
99. Rashid, Y. F. (2012, 30. oktober). Windows 8 Security: What's New?. *PCmag*. Najdeno 2. novembra 2012 na spletnem naslovu http://www.pcmag.com/article2/0,2817,2411464,00.asp
100. Reisman, M., Vahčič, T., Vahčič, A., Dimic, B., Ademovič, A., Šlamberger, M., Razboršek, D., Ivanuša, B., Kovač, M., & Novak, E. (2012). *Uspešen finančni menedžer.* Maribor: Forum Media.
101. Rouse, M. (2010, november). Distributed Denial of Service Attack (DDoS). *SearchSecurity*. Najdeno 22. julija 2012 na spletnem naslovu http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
102. Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., & Schwartz, A. (2003). *Information Technology Security Handbook*. Washington: World Bank.
103. Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *Second Asia International Conference on Modeling & Simulation*. (str. 749–753). Kuala Lumpur: University Teknologi Malaysia.
104. Sandrini, M. (2003). We want security but we hate it. The Foundations of security technoeconomics in the social world. From Control to Surveillance. *2nd Annual Workshop on Economics and Information Security* (str. 1–12). College Park: University of Maryland.
105. Schechter, S. E. (2004). *Computer Security Strength & Risk: A Quantitative Approach*. Cambridge, Massachusetts: Harvard University.
106. Schuster, P. (2007). Investment Appraisal At Imperfect Capital Markets. *International Business & Economics Research Journal*, *6*(9), 21–28.

107. *Security Management Survey – Security best practice survey*. Najdeno 19. junija 2012 na spletnem naslovu http://www.bsmreview.com/security_best_practice_survey.shtml
108. Shaurette, K. M. (2004). The Building Blocks of Information Security. V H.F. Tipton & M. Krause (ur.), *Information Security Management Handbook 2004 edition on CD-ROM* (str. 31–50) [zgoščenka]. Boca Raton: Auerbach Publications.
109. Slay, J., & Koronios, A. (2006). *Information Technology Security & Risk Management*. Milton: John Wiley & Sons.
110. Slovenski center za obravnavo omrežnih incidentov SI-CERT. (2012). Poročilo o omrežni varnosti za leto 2012. Najdeno 15. maja 2013 na spletnem naslovu https://www.cert.si/fileadmin/slike/si-cert/fokus/2013/SI-CERT_porocilo_2012.pdf
111. Soo Hoo, K. J. (2000). *How Much Is Enough? A Risk-Management Approach to Computer Security* (doktorska disertacija). Palo Alto: Stanford University.
112. Steichen, P. (b.l.). Advanced security methodologies – (Global) players in NIS. M2SSIC–Metz. Najdeno 11. junija 2012 na spletnem naslovu http://pst.libre.lu/m2ssic-metz/archive/2008-2009/01_players.pdf
113. Stewart, A. (2012). Can spending on information security be justified? Evaluating the security spending decision from the perspective of a rational actor. *Information Management & Computer Security, 20*(4), 312–326.
114. Stroie, E. R., & Rusu, A. C. (2011). Security Risk Management – Approaches and Methodology. *Informatica Economica, 15*(1), 228–240.
115. Su, X. (2006, junij). An Overview of Economic Approaches to Information Security Management. *UT publications*. Najdeno 11. junija 2012 na spletnem naslovu http://doc.utwente.nl/66172/1/00000177.pdf
116. Symantec. (2010). Symantec Global Internet Security Threat Report. Najdeno 13. julija 2012 na spletnem naslovu http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf
117. Symantec. (2011). 2011 State of Security Survey. Najdeno 13. julija 2012 na spletnem naslovu http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf
118. Symantec Intelligence. (2011). Symantec Intelligence Report: November 2011. Najdeno 17. julija 2012 na spletnem naslovu http://www.symantec.com/connect/sites/default/files/SYMCINT_2011_11_November_FINAL-en.pdf
119. Tipton, H. F. (2004). Purposes of Information Security Management. V H. F. Tipton & M. Krause (ur.), *Information Security Management Handbook 2004 edition on CD-ROM (*str. 18–30) [zgoščenka]. Boca Raton: Auerbach Publications.
120. Tkatch, I. (2010). FI 3300 Corporate Finance. [predstavitev]. Najdeno 2. avgusta 2014 na spletnem naslovu http://www2.gsu.edu/~fncitt/files/Fi3300_Chapter10.pdf
121. Tofan, D. C. (2011). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems, 3*(3), 128–135.
122. Trček, D. (2006). *Managing Information Systems Security and Privacy*. Berlin: Springer-Verlag.

123. Trend Micro Inc. (2009). The Future of Threats and Threat Technologies. How the Landscape Is Changing. Najdeno 15. julija 2012 na spletnem naslovu http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trend_micro_2010_future_threat_report_final.pdf
124. Tryfonas, T. (2010). Information Security Management and Standards of Best Practice. V H. Jahankhani, D. L., Watson, G. Me, & F. Leonhardt (ur.), *Handbook of Electronic Security and Digital Forensics* (str. 207–236). Toh Tuck: World Scientific Publishing Co.
125. Tsiakis, T. (2010). Information Security Expenditures: a Techno–Economic Analysis. *International Journal of Computer Science and Network Security, 10*(4), 7–10.
126. Turban, E., Lee, J. K., King, D., McKay, J., & Marshall, P. (2008). *Electronic Commerce. A Managerial Perspective*. Upper Saddle River: Prentice Hall.
127. Vidalis, S. (2003). A Critical Discussion of Risk and Threat Analysis Methods and Methodologies. *University of Glamorgan Tehnical Report*. Najdeno 12. aprila 2012 na spletnem naslovu https://docs.google.com/viewer?a=v&q=cache:9_QQrjvDTD8J:www.comp.glam.ac.uk/staff/svidalis/Technical%2520Reports/Threat%2520%26%2520Risk%2520TR.doc+a+critical+discussion+of+risk+and+threat+analysis+methods+and+methodologies&hl=sl&gl=si&pid=bl&srcid=ADGEEShAqUc5PFGPfK7nawWbVE6obzVJ40LPhb-rjCw0TyJi0vzZCFfQ79Owslm6nsYmiQk6qvX3Bg6LrIm3V4RLEQ5Kleox--Z1W5RDkQz49sWd5lZrHLSLSiFn8tGmqeawm5kzrMXa&sig=AHIEtbR7Ic0JDn73bNDnKEZiOX7usCgC9Q
128. Vidalis, S., & Jones, A. (2005). Analyzing Threat Agents and Their Attributes. *4th European Conference on Information Warfare and Security* (str. 369–379). Pontypridd: University of Glamorgan.
129. vom Brocke, J., & Lindner, M. A. (2004). Service Portfolio Measurement – A Framework for Evaluating the Financial Consequences of Out–tasking Decisions. *2th International Conference on Service Oriented Computing Applications ICSOC2004* (str. 203–211). New York: ACM Press.
130. vom Brocke, J., Recker, J. C., & Mendling, J. (2010). Value–oriented Process Modeling: Integrating Financial Perspectives into Business Process Re-design. *Business Process Management Journal*, *16*(2), 333–356.
131. vom Brocke, J., Strauch, G., & Buddendick, C. (2007). Return on Security Investments–Design Principles of Measurement Systems Based on Capital Budgeting. *6th International Conference on Information Systems Technology and its Applications ISTA2007* (str. 21–32). Kharkiv: ISTA.
132. Walsh, C. (2006, julij). CSI/FBI Survey considered harmful. *Emergent Chaos*. Najdeno 25. julija 2012 na spletnem naslovu http://emergentchaos.com/archives/2006/07/csifbi-survey-considered-harmful.html
133. Whitman, E. M., & Mattord, H. J. (2007). *Principles of Information Security*. Boston, Massachusetts: Thomson Learning, Inc.
134. Willemson, J. (2006). On the Gordon&Loeb Model for Information Security Investment. *Workshop on the Economics of Information Security (WEIS 2006)*. Najdeno 25. julija 2013 na spletnem naslovu http://weis2006.econinfosec.org/docs/12.pdf

135. Willemson, J. (2010). Extending the Gordon&Loeb Model for Information Security Investment. *2010 International Conference on Availability, Reliability and Security*. Najdeno 25. julija 2013 na spletnem naslovu http://research.cyber.ee/~jan/publ/aresGL.pdf
136. Wu, X. (2009). *Security Arhitecture for Sensitive Information Systems*. Caulfield East: Faculty of Information Technology.
137. Zakladnica enotnega zakladniškega računa države. Najdeno 7. julija 2014 na spletnem naslovu http://www.mf.gov.si/si/o_ministrstvu/direktorati/direktorat_za_zakladnistvo/zakladnica_enotnega_zakladniskega_racuna_drzave/
138. Zakon o davku od dohodkov pravnih oseb. *Uradni list RS* št. 117/2006.
139. Zakon o elektronskih komunikacijah. *Uradni list RS* št. 13/2007-UPB1, 102/2007-ZDRad, 110/2009, 33/2011.
140. Zakon o elektronskem poslovanju. *Uradni list RS* št. 96/2009-UPB2.
141. Zakon o elektronskem poslovanju in elektronskem podpisu. *Uradni list RS* št. 98/2004-UPB1, 61/2006-ZEPT.
142. Zakon o javnih financah. *Uradni list RS* št. 11/2011-UPB4.

PRILOGE

KAZALO PRILOG

Priloga 1: Najpogostejše vrste napadov

Po podatkih raziskve CSI Computer Crime and Security Survey (2010, str. 15) so v zadnjih letih najpogostejše naslednje vrste napadov (slika 5):

- Zlonamerna programska oprema (angl. *malicious software* ali krajše *malware*) je program, ki se infiltrira in širi po informacijskem sistemu, brez uporabnikovega vedenja oziroma privolitve z namenom oškodovanja informacijskega sistema (OECD, 2008, str. 10). Cilj te programske opreme je v večini primerov ogroziti in zlorabiti zaupnost, celovitost in razpoložljivost uporabnikovih informacij (NIST IR 7298, 2011, str. 115). Različne oblike zlonamerne programske opreme se navadno ločujejo na posamezne kategorije, kot so (NIST IR 7298, 2011, str. 182; NIST, 1995, str 27):

    - virus (angl. *virus*): program, ki se samodejno kopira in širi po sistemu, tako da se pripenja na zagonske datoteke obstoječih programov (gostitelji) ter s tem škoduje delovanju sistema ali celo trajno poškoduje strojno opremo.
    - črv (angl. *worm*): samostojen program, ki se kopira in širi po računalniški mreži, za aktivacijo pa ne potrebuje gostiteljskega programa ali uporabnikovega dejanja.
    - trojanski konj (angl. *trojan horse*): program z želeno in uporabno funkcijo, ki pa hkrati izvaja tudi neželjene operacije, ki so uporabniku neznane in skrite (npr. ob vsakokratni namenski uprabi prikrito izbriše tudi druge naključno izbrane podatke v sistemu).
    - vohunska programska oprema (angl. *spyware*): program, ki je brez uporabnikovega vedenja nameščen na računalnik, z namenom zbiranja in posredovanja zaupnih podatkov.

- Omrežje robotskih računalnikov (angl. *botnet*) je omrežje povezanih računalnikov, ki izvaja vnaprej določene zlonamerne funkcije, ki jih na daljavo in brez vedenja uporabnikov sproža zlonamerni napadalec (angl. *botmaster*) ali skupina napadalcev (Banday, Qadri & Shah, 2009, str. 2). Posamezni računalniki v tovrstnem omrežju, imenovani zombiji (angl. *zombies*), skupaj lahko tvorijo ogromno vojsko, ki je resna grožnja varnosti in zasebnosti na internetu z izvajanjem različnih vrst zlonamernih napadov (DDoS, malware, spyware, kraja idetnitete, e-mail spam, ...).

- Ribarjenje podatkov (angl. *phishing*) je kraja zaupnih osebnih podatkov in informacij z uporabo različnih računalniških metod prevare (NIST IR 7298, 2011, str. 138), s katerimi storilci pretentajo uporabnike, da jim omenjene podatke nevede razkrijejo. V najbolj navadni obliki prevare skuša storilec uporabnike z elektronskim sporočilom zvabiti na lažno spletno stran banke ali kake druge spletne storitve in jih napeljuje, da tam vpišejo svoje uporabniško ime in geslo. Tako pridobi podatke za dostop do bančnih računov, ki jih sam uporabi za krajo denarja ali pa jih na črnem trgu proda drugim kriminalcem.

- Ohromitev storitve oziroma kraja virov z DoS-napadom (angl. *Denial of Service – DoS* ali *Distributed Denial of Service – DDoS*) je poskus napadalca, da onemogoči uporabo računalniških virov (npr. računalniške mreže) ali storitev (npr. spletna trgovina) uporabnikom, katerim je namenjena. V tipični obliki napada zlonamerni uporabnik oziroma napadalec lahko z enim samim ukazom sproži množični napad (lahko tudi več milijonov) za ta namen okuženih računalnikov, ki na primer s pošiljanjem ogromne količine paketov podatkov točno določeni tarči (tarči napada) povzročijo ohromitev sistema (Rouse, 2010). Zaradi takšne »poplave« podatkov je delovanje storitve lahko za določen čas onemogočeno, lahko pa tudi trajno onesposobljeno. Podobno, kot to velja za računalniške viruse in zlonamerne programe, se tudi metode izvajanja napadov DoS in DDoS hitro spreminjajo, pri čemer napadalci uporabljajo vedno bolj izpopolnjene načine, s katerimi zaobidejo varnostne sisteme.

Priloga 2: Poročilo o potencialnih grožnjah glede na principe informacijske varnosti – razširjen koncept CIA-trikotnika

Tabela 1: Potencialne grožnje glede na principe informacijske varnosti

Grožnja	Principi informacijske varnosti		
	Zaupnost	**Celovitost**	**Razpoložljivost**
Kot posledica človeških dejanj (namernih in nenamernih)			
Vohunjenje in prestrezanje podatkovnega prometa	X		
Nepooblaščeno dostopanje do podatkov	X	X	
Poškodovanje z namenom uničenja podatkov		X	X
Nameščanje škodljive programske opreme	X	X	X
Ponarejanje podatkov	X	X	
Nenamerne napake uporabnikov podatkov		X	X
Kot posledica dogodkov v zunanjem in notranjem okolju			
Požar		X	X
Potres		X	X
Poplava		X	X
Izpad električne energije.			X

Vir: E. R. Stroie & A. C. Rusu, Security Risk Management – Approaches and Methodology, 2011, str. 232.; lasten prikaz

Priloga 3: Poročilo o ranljivostih sistema, glede na vir grožnje

Tabela 2: Ranljivosti sistema glede na vir grožnje

Ranljivost	Vir grožnje	Dejanje
Popravek za ugotovljeno varnostno pomanjkljivost operacijskega sistema še ni implementiran.	Nepooblaščeni uporabniki (hekerji, bivši zaposleni, nezadovoljni zaposleni, teroristi …)	Nepooblaščen dostop do sistemskih podatkov in nastavitev
Neustrezna namestitev programske opreme na delovne postaje	Tehnična okvara zaradi nepravilnega delovanja	Nižja produktivnost dela, dodatni stroški odpravljanja težav
Varnostna kamera v strežniški sobi še ni nameščena.	Nepooblaščeni uporabniki	Nepooblaščen dostop do strežnikov, opreme in podatkov
Avtomatsko izdelovanje varnostnih kopij podatkov ni nameščeno.	Požar, potres, poplava, izpad električne energije, nepooblaščeni uporabniki, izsiljevalski virusi …	Izguba, uničenje in/ali kraja osebnih in poslovnih podatkov

Vir: National Institute of Standards and Technology, Risk Management Guide for Information Technology Systems, 2002, str. 15; lasten prikaz

Priloga 4: Obseg vpliva negativnih posledic grožnje

Tabela 3: Obseg vpliva negativnih posledic grožnje

Obseg vpliva	Vpliv zaradi izkoriščene ranljivosti sistema
Visok	- Visoki stroški zaradi izgube pomembnih opredmetenih sredstev - Močno oškodovan ugled podjetja, nezmožnost opravljanja poslanstva - Hude poškodbe ali celo smrt ljudi
Srednji	- Nezanemarljivi stroški zaradi izgube pomembnih opredmetenih sredstev - Oškodovan ugled podjetja, ovirano opravljanje poslanstva - Lahko pride do poškodbe ljudi.
Nizek	- Manjša izguba pomembnih opredmetenih sredstev - Manjše oškodovanje ugleda podjetja

Vir: National Institute of Standards and Technology, Risk Management Guide for Information Technology Systems, 2002, str. 23

Priloga 5: Primer manjšega trgovskega podjetja za prikaz izračuna ALE

Opis primera: Manjše trgovsko podjetje, v katerem ima skrbnik ključnih kupcev službeni prenosni računalnik (v nadaljevanju prenosnik) s podatki o strankah. Vsi podatki na prenosniku so šifrirani, s čimer so nedostopni nepooblaščenim uporabnikom tudi v primeru kraje ali izgube prenosnika. Podjetje ima za vzdrževanje in servisiranje računalniškega omrežja in opreme sklenjeno vzdrževalno pogodbo z zunanjim izvajalcem. Vhodni podatki za izračun ALE za primer kraje in fizičnega poškodovanja prenosnika so:

- vrednost sredstva (angl. *asset value*, v nadaljevanju *AV*), torej prenosnika, izražena v denarnih enotah je 1 500,00 €;
- povrnitev podatkov iz varnostne kopije na drug računalnik zahteva eno servisno uro, popravilo poškodovanega ohišja pa dve uri zunanjega pogodbenega vzdrževalca, po ceni 150 €/h;
- faktor izpostavljenosti sredstva (angl. *exposure factor*, v nadaljevanju *EF*), ki pomeni izgubo v višini deleža od vrednosti sredstva, ki bi jo podjetje utrpelo v primeru varnostnega dogodka (kraje, izgube in/ali popolnega uničenja prenosnika) je 100 %, v primeru poškodovanja prenosnika (npr. poškodovano ohišje zaradi padca) je 40 %;
- glede na izkušnje in podatke iz preteklosti podjetje ocenjuje verjetnost kraje prenosnika 0,33 (enkrat v treh letih), verjetnost poškodovanja prenosnika pa 0,25 (enkrat v štirih letih).

Izračun ALE je prikazan v tabeli 4:

Tabela 4: Izračun ALE

kraja prenosnika	
vrednost prenosnika v EUR (*AV*)	1 500,00
ena servisna ura v EUR (povečanje *AV*)	150,00
faktor izpostavljenosti v % (*EF*)	100,00
$SLE = AV \times EF$ (v EUR)	1 650,00
letna stopnja pogostosti dogodka v % (*ARO*)	33,00
$\boldsymbol{ALE_1 = SLE \times ARO}$ (v EUR)	**544,50**
poškodovanje prenosnika	
vrednost prenosnika v EUR (*AV*)	1 500,00
dve servisni uri v EUR (povečanje *AV*)	300,00
faktor izpostavljenosti v % (*EF*)	40,00
$SLE = AV \times EF$ (v EUR)	720,00
letna stopnja pogostosti dogodka v % (*ARO*)	25,00
$\boldsymbol{ALE_2 = SLE \times ARO}$ (v EUR)	**180,00**
$\boldsymbol{ALE = ALE_1 + ALE_2}$ (v EUR)	**724,50**

Priloga 6: Matrika stopenj tveganja

Tabela 5: Matrika stopenj tveganja

Verjetnost grožnje	**Negativni vpliv grožnje**		
	Nizek (10)	**Srednji** (50)	**Visok** (100)
Visoka (1,0)	Nizek (10 × 1,0 = 10)	Srednji (50 × 1,0 = 50)	Visok (100 × 1,0 = 100)
Srednja (0,5)	Nizek (10 × 0,5 = 5)	Srednji (50 × 0,5 = 25)	Visok (100 × 0,5 = 50)
Nizka (0,1)	Nizek (10 × 0,1 = 1)	Srednji (50 × 0,1 = 5)	Visok (100 × 0,1 = 10)

Vir: National Institute of Standards and Technology, Risk Management Guide for Information Technology Systems, 2002, str. 25

Priloga 7: Seznam in razlaga uporabljenih kratic

***AFC* (Average Fiksed Costs)**	Povprečni stalni stroški
***ALE* (Annual Loss Expectancy)**	Pričakovana letna izguba
***APT* (advance persistent threat)**	Napredno trajna grožnja
***ARO* (Annual Rate of Occurence)**	Letna stopnja pogostosti nastanka
***ATC* (Average Total Costs)**	Povprečni celotni stroški
***AVC* (Average Variable Costs)**	Povprečni spremenljivi stroški
CCSS (Computer Crime and Security Survey)	
***CF* (Cash Flow)**	Denarni tok
CIA-triad oziroma **CIA triangle**	Koncept informacijske varnosti, sestavljen iz treh temeljnih atributov: zaupnost (confidentiality), celovitost (integrity) in razpoložljivost (availability).
COBIT (Control Objectives for Information and related Technology)	Skupek procesov za upravljanje informacijskih tehnologij
CSI (Computer Security Institute)	Inštitut za računalniško varnost
FBI (Federal Bureau of Investigation)	Ameriški zvezni preiskovalni urad
FUD (Fear uncertainty and doubt)	Strategija prodaje varnostnih storitev in produktov
***FV* (Future Value)**	Prihodnja vrednost
GBP (Great Britain Pound)	Valuta Velike Britanije
IEC (International Electrotechnical Commission)	Mednarodna komisija za elektrotehniko
IS (Information System)	Informacijski sistem
ISF (Information Security Forum)	
ISO (International Organization for Standardization)	Mednarodna organizacija za standardizacijo
ISO27k	Družina ISO standardov
***IRR* (Internal Rate of Return)**	Notranja stopnja donosa
IT (Information Technology)	Informacijska tehnologija
ITIL (Information Technology Infrastructure Library)	Knjižnica izbranih primerov praks upravljanja storitev informacijskih tehnologij
ITSM (Information Technology Service Management)	Upravljanje storitev informacijskih tehnologij
***MIRR* (Modified Internal Rate of Return)**	Popravljena notranja stopnja donosa
NIST (National Institute of Standards and Technology)	Državni inštitut za standarde in tehnologijo
***NB* (Net Balance)**	Neto stanje
NLB	Nova Ljubljanska Banka
***NPV* (Net Present Value)**	Neto sedanja vrednost

se nadaljuje

nadaljevanje

PDCA (plan-do-check-act) model	Ciklični model štirih faz za vzpostavitev ustrezne ravni informacijske varnosti
***PI* (Profitability Index)**	Indeks donosnosti
***PP* (Payback Period)**	Doba vračanja naložbe
***PV* (Present Value)**	Sedanja vrednost
***ROA* (Return on Attack)**	Donosnost napada
***ROI* (Return on Investment)**	Donosnost naložbe
SI–CERT (Slovenian Computer Emergency Response Team)	Slovenski center za obravnavo omrežnih incidentov
***SLE* (Single Loss Expectancy)**	Pričakovana izguba določenega dogodka
SP800	Serija publikacij organizacije NIST
SUIV	Sistem upravljanja informacijske varnosti
USD (United States dollar)	Valuta Združenih držav Amerike
VoFI (Visualisation of Financial Implications)	Metoda vizualizacije finančnih posledic
ZDA	Združene države Amerike