Model ekonomski održivoga sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima

Aksentijević, Saša

IZJAVA

kojom izjavljujem da sam doktorsku disertaciju s naslovom **„MODEL EKONOMSKI ODRŽIVOGA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA“** izradio samostalno pod voditeljstvom prof.dr.sc. Zvonka Čapka. U radu sam primjenio metodologiju znanstvenoistraživačkog rada i koristio literaturu koja je navedena na kraju doktorske disertacije. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo u diplomskom radu na uobičajen, standardan način citirao sam harvardskim načinom citiranja i povezao fusnotama s korištenim bibliografskim jedinicama. Rad je pisan u duhu hrvatskog jezika.

Suglasan sam sa objavom doktorske disertacije na službenim stranicama Fakulteta.

Doktorand

Saša Aksentijević

SVEUČILIŠTE U RIJECI
EKONOMSKI FAKULTET

SAŠA AKSENTIJEVIĆ

MODEL EKONOMSKI ODRŽIVOGA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA

DOKTORSKA DISERTACIJA

Rijeka, 2013.

SVEUČILIŠTE U RIJECI
EKONOMSKI FAKULTET

MODEL EKONOMSKI ODRŽIVOGA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA

DOKTORSKA DISERTACIJA

Mentor: prof.dr.sc. Zvonko Čapko
Doktorand: Saša Aksentijević
Studijski smjer: Ekonomija i poslovna ekonomija
JMBAG: 37/09 (matični broj)

Rijeka, 03.12.2013.

PREDGOVOR

Doktorska disertacija je nastala kao plod mog osobnog interesa u području poslovne informatike, ali i činjenice da sam zadnjih deset godina proveo u poslovnom kontekstu baveći se upravljanjem poslovnom funkcijom informatike, informacijske i integralne sigurnosti u velikom poduzeću. Prihvativši sugestiju prof.dr.sc. Ratka Zelenike koji je doktorandima predavao na prvoj godini i dao mnoge korisne savjete vezane uz izradu doktorske disertacije, od samog početka sam počeo trasirati put ka konačnom cilju kroz pristupne radove koje sam izrađivao tijekom prve i druge godine doktorskog studija, objavu članaka, sudjelovanje referatima na desetak međunarodnih znanstvenih konferencija s objavom u zbornicima radova,a jednim dijelom i naslanjajući se na vlastiti završni rad specijalističkog poslijediplomskog studija koji sam dovršio sredinom 2008. godine. Tijekom istraživanja i proučavanja bibliografske građe sam se uvjerio kako je čitavo tematsko područje vrlo slabo obrađeno i u Republici Hrvatskoj i šire, a neki moji radovi koji su nastali kao osnova razvoja doktorske disertacije su ubrzo po objavi bili citirani – u jednom dijelu sukladno akademskim pravilima, u drugom nažalost bez korektnog navođenja izvora. U slučajevima u kojima je to bilo moguće a ja sam za njih saznao na vrijeme, kontaktirao sam Internet servise putem kojim su takvi radovi bili objavljeni i zatražio njihovo uklanjanje. Ta me činjenica dodatno učvrstila u nastavku provođenja istraživanja jer je ukazivala na oskudnost znanstvenog bavljenja problematikom poveznice informacijske sigurnosti i ekonomskih pokazatelja u hrvatskom okruženju.

Ovom prigodom zahvaljujem se mentoru pri izradi doktorske disertacije, prof.dr.sc. Zvonku Čapku na strpljenju pri zajedničkom radu na izradi doktorske disertacije, ali i završnog rada na poslijediplomskom specijalističkom studiju. Nadalje, zahvaljujem na suradnji predsjednici i članu Povjerenstva za obranu prijave teme, prezentaciju rezultata istraživanja i doktorske disertacije, prof.dr.sc. Marini Čičin Šain i prof. dr. sc. Velimiru Srići, svim profesorima Katedre za informacijske znanosti Ekonomskog fakulteta u Rijeci, Povjerenstvu za doktorske studije i fakultetskom Vijeću, te osoblju Referade za poslijediplomske studije, a osobito Tamari Rašetina, univ.bacc.oec. i Đenet Molnar, univ.spec.oec., mag.oec.

Naposljetku, želim zahvaliti prof.dr.sc. Saši Žikoviću, doc.dr.sc. Edvardu Tijanu i kolegi Goranu Laziću, mag.oec.na podršci i sugestijama tijekom trajanja doktorskog studija, te prof.dr.sc. Ratku Zeleniki na prenesenom znanju iz metodologije istraživanja i izrade znanstvenog djela.

SAŽETAK

MODEL EKONOMSKI ODRŽIVOGA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA

Poslovna funkcija informacijske sigurnosti u malim i srednjim poduzećima je zanemarena od strane rukovoditelja i vlasnika, ali i zakonodavca, strukovnih organizacija koje određuju mjere najbolje prakse te dobavljača softverskih i hardverskih rješenja kojima se otklanjaju rizici informacijske sigurnosti. Ovaj problem je prisutan usprkos činjenici kako većinu obujma hrvatske, europske i svjetske privrede predstavlja upravo poslovna aktivnost malih i srednjih poduzeća. Razlozi za ovu činjenicu su raznoliki, a moguće ih je uglavnom locirati u nedostatku znanja rukovoditelja i vlasnika, nedovoljnoj raspoloživosti financijskih sredstava za implementaciju mjera informacijske sigurnosti te nepostojanju zakonske legislative i najbolje prakse koja bi bila osobito prilagođena specifičnostima malih i srednjih poduzeća. Osim toga, čak niti postojeći alati poput sustava upravljanja kvalitetom ne koriste se adekvatno kao potpora postizanju ciljeva informacijske sigurnosti poduzeća, a to je osiguravanje informacijskog kapitala. U disertaciji se analiziraju mogućnosti korištenja metoda financijskog odlučivanja u kontekstu primjene na informacijsku sigurnost u malim i srednjim poduzećima u Republici Hrvatskoj te metode analitičkih hijerarhijskih procesa pri odlučivanju o investiranju u rješenja informacijske sigurnosti.

Po provedenom istraživanju korištenjem statistički relevantnog uzorka promatrane populacije poduzeća postavljen je model za ocjenu dostignute razine funkcionalnosti poslovne funkcije informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj, procijenjena je dostignuta razina zrelosti (funkcionalnosti) informacijske sigurnosti, te su identificirane varijable koje su ključne u postizanju te zrelosti, kao i u podizanju navedene funkcije na stratešku razinu.

U perspektivnom dijelu disertacije, u fokus interesa je stavljen prijedlog koraka uvođenja modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima korištenjem ARIS BPM metodologije modeliranja poslovnih procesa. Identificirane su i pojašnjene glavna i podržavajuća vertikala tog procesa, te u okviru obje vertikale, glavni i podržavajući makro-procesi poslovne funkcije informacijske sigurnosti u malim i srednjim poduzećima, kao i potencijalni efekti uvođenja opisanog modela.

Ključne riječi: informacijska sigurnost, model upravljanja informacijskom sigurnošću, ekonomika informacijske sigurnosti, modeliranje poslovnih procesa, mala i srednja poduzeća

SUMMARY

SUSTAINABLE ECONOMIC MODEL OF INFORMATION SECURITY MANAGEMENT IN SMALL AND MEDIUM ENTERPRISES

Information security in SMEs is a neglected business function, both by management, the owners, but also the lawmaker and best practice organizations and vendors of software and hardware solutions used to mitigate information security risks. This problem is omnipresent despite the fact that majority of Croatian, European and world economy consists of SMEs' activities. There are many contributing factors to this issue, and most important of them are lack of funds, knowledge and related best practice. Even existing tools, like quality assurance used by SMEs are not adequately utilized in order to enhance information security. In this dissertation, possibilities of usage of financial analysis and AHP method during decision-making related to information security in SMEs is being evaluated.

A research using statistically significant sample of the total population of SMEs in the Republic of Croatia has been undertaken and a model to evaluate current state of achieved functionality of information security across Croatian SMEs has been established. Main contributing variables to the level of functionality are identified, and so are those variables that are contributing to information security being a strategic business function.

In the final part of the dissertation, steps to introduce a new model of information security in SMEs have been proposed using ARIS BPM business process modelling methodology. Primary and supporting process hierarchy have been identified and explained, including expected potential effects of its introduction.

Key words: information security, information security management model, information security economics, business process modelling, small and medium enterprises

KAZALO

1. UVOD

Obrazloženje teme i radnih teza doktorske disertacije obuhvaća sljedeće elemente: **1) Obrazloženje teme (naslova) doktorske disertacije, 2) Problem, predmet i objekt istraživanja, 3) Znanstvenu hipotezu i pomoćne hipoteze, 4) Svrhu i ciljeve istraživanja, 5) Ocjenu dosadašnjih istraživanja, 6) Znanstvene metode, 7) Obrazloženje strukture doktorske disertacije, 8) Očekivane rezultate istraživanja, 9) Očekivani doprinos znanosti i 10) Primjenu rezultata istraživanja.**

1.1. Obrazloženje teme (naslova) doktorske disertacije

Informacijski sustavi su u današnje doba integralni dijelovi poslovnih sustava svih poduzeća, neovisno o njihovoj veličini ili vrsti poslovne aktivnosti. Oni se koriste kao temeljna podrška operativnom dijelu poslovanja, ali i kao izvor podataka i informacija nužnih za donošenje adekvatnih poslovnih odluka od strane vrhovnog menadžmenta ili vlasnika. Ukoliko informacije sadržane u informacijskim sustavima zbog izostanka adekvatne zaštite postanu netočne, javno dostupne, uništene ili korumpirane na način da je ugrožen njihov integritet, povjerljivost ili raspoloživost, često se postavlja pitanje nastavka poslovne aktivnosti u opsegu i na način na koji je to bilo moguće do nastupa takvog neželjenog događaja, odnosno opredmećenja sigurnosnog rizika. Osim kvalitativne štete u obliku rušenja imidža poduzeća u njegovoj poslovnoj okolini, u takvim slučajevima nužno dolazi i do nastupa kvantitativno mjerljivog negativnog učinka uslijed zastoja, gubitka poslovnih odnosa i konkurentske prednosti u odnosu na druga poduzeća. Budući da su danas informacijski sustavi poduzeća nužno umreženi, dolazi do pojave multiplikacije rizika sigurnosnih incidenata, kako onih namjernih, tako i slučajnih, uslijed neznanja, nemara uključenih korisnika informacijskih sustava ili negativnih utjecaja okruženja poduzeća. Prema tome, navedeno se odnosi na sigurnosne propuste čiji je izvor unutar poduzeća, ali i na one koji dolaze iz njegove okoline.

Do naglog uvođenja moderne informacijske tehnike i tehnologije u poslovanje poduzeća došlo je završetkom Drugog svjetskog rata tijekom kojega su uočeni i znanstveno objašnjeni temeljni postulati informacijsko-sigurnosne znanosti. Sve do početka devedesetih godina prošlog stoljeća poduzeća su informacijsku sigurnost uglavnom promatrala kao integralni i prateći dio upravljanja poslovnom funkcijom informatike unutar odgovarajućih odjela ili sektora. Budući da je upravljanje informacijskom sigurnošću bilo povjereno menadžerima informatike koji su uglavnom dolazili iz tehničkog okruženja, većina primijenjenih mjera bile su prvo tehničke, a tek onda i logičke prirode, odnosno bile su usmjerene fizičkom osiguravanju pristupa računalnoj opremi i mrežama, a zatim i logičkom ograničavanju pristupa odgovarajućim klasama podataka i informacijama. Ovakav pristup bio je zadovoljavajući i iz tog razloga što je razvoj računalnih

mreža omogućio njihovu praktičnu i raširenu uporabu u poslovanju poduzeća tek u posljednja dva desetljeća.

Iz navedenih razloga došlo je do jačanja zasebne funkcije upravljanja poslovnim sustavom informacijske sigurnosti koja se odvojila od informatičke poslovne funkcije, a koja u modernim poduzećima nosi sobom uglavnom tehničke konotacije te organizacijski kontekst. Razlozi za taj proces su mnogobrojni, i kreću se u rasponu od zakonske regulative, preko rastuće kompleksnosti sustava upravljanja informacijskom sigurnošću koji zahtijeva vlastitu poslovnu funkciju koja ima ne samo hijerarhijsku nego i linijsku, koordinativnu ulogu, pa sve do modernih smjernica „najbolje prakse" informacijske sigurnosti koje zahtijevaju odvajanje poslovne funkcije informatike od upravljanja sustavom informacijske sigurnosti s ciljem izbjegavanja situacije u kojoj jedna poslovna funkcija revidira samu sebe. Kao što je izloženo, ovaj se proces dogodio vrlo brzo, u svega dva desetljeća, te je ostavio nespremnim ne samo velika poduzeća koja imaju na raspolaganju značajne resurse, nego i srednja i mala poduzeća čije se poslovanje nalazi pred istim izazovima i rizicima kao i poslovanje velikih poduzeća. Iako je zbog samog opsega poslovanja malih i srednjih poduzeća vjerojatnost nastupa sigurnosnih incidenata manja, kao i njihove posljedice, slaba raspoloživost financijskih, ljudskih i organizacijskih resursa i interno raspoloživog znanja baca sjenu na mogućnost oporavka takvih poduzeća u slučaju značajnih sigurnosnih incidenata.

Štoviše, čak i zakonodavac, uvriježeni standardi i sustavi „*najbolje prakse*" mala i srednja poduzeća zaboravljaju ili im propisuju iste obrasce ponašanja i kontrole sustava upravljanja informacijskom sigurnošću kao i velikim poduzećima. Takvi su obrasci doista u teoretskom smislu univerzalni i primjenjivi na sva poduzeća, no u praksi su za mala i srednja poduzeća neprovedivi jer su previše kompleksni, zahtijevaju velika financijska sredstva koja su im često nedostupna ili je financijski utjecaj ulaganja vlasnicima i menadžerima neprihvatljivo visok u odnosu na subjektivno percipirani i kvantitativno neodređeni rizik. Nepostojanje jasne povezanosti između ulaganja u sustav upravljanja informacijskom sigurnošću i mogućnosti kvantificiranja troškova te nemogućnost menadžera informacijske sigurnosti da kvantitativno predoče vrhovnom menadžmentu i vlasnicima ekonomske pokazatelje ulaganja u informacijsku sigurnost čestu su razlozi svjesnog prihvaćanja objektivno neprihvatljivih rizika unutar velikih poduzeća. Istovremeno je nepostojanje zasebnog, opće prihvaćenog modela za mala i srednja poduzeća koji bi bio prilagođeniji njihovoj veličini i potrebama uzrok nesvjesnog pristajanja na nerazumno visoke razine rizika u takvim sredinama.

Opisana situacija nije posebnost poduzeća koja posluju u Republici Hrvatskoj, već je prisutna na globalnoj razini. Prvi međunarodno priznati standard koji regulira ovu problematiku organizacije sustava upravljanja informacijskom sigurnošću donesen je tek 1995. godine – radi

se o britanskom standardu BS 7799. Nasljednik ovog standarda je ISO/IEC 27000 obitelj standarda sukladno kojemu je certificirano u cijelom svijetu prema zadnjim raspoloživim obrađenim podacima koji obuhvaćaju period do kolovoza 2012. oko 8.000 poduzeća i organizacija, pri čemu 57 % otpada na dalekoistočne zemlje, koje s 28 % udjela slijede Europa i s 12 % udjela Afrika i Zapadna Azija, dok iznenađujućih 3 % otpada na ostatak svijeta koji uključuje čitav američki kontinent i Australiju. Navedeni apsolutni i relativni pokazatelji su vrlo nezadovoljavajući, tim više uzme li se u obzir kako je opseg certifikacije sustava upravljanja informacijskom sigurnošću značajno uži od cjelokupnog poslovanja poduzeća, odnosno da se na formalnu certifikaciju koja je inicijalno, te u procesu održavanja vrlo zahtjevna po sve resurse poduzeća, uglavnom odlučuju velika poduzeća i razne državne (neprofitne) organizacije. Ovom prigodom potrebno je navesti i činjenicu kako prema podacima iz kolovoza 2012. u Republici Hrvatskoj ima dvadeset i sedam certificiranih poduzeća.

Iz navedenih spoznaja proizlazi i potreba sustavnog i znanstveno utemeljenog istraživanja primjene novog modela ekonomski održivog sustava upravljanja informacijskom sigurnošću koji bi bio posebno prilagođen malim i srednjim poduzećima u Republici Hrvatskoj, s ciljem da se temeljem znanstvenih činjenica stvore najvažnije pretpostavke za uspješnost poslovanja i racionalnije upravljanje njihovom poslovnom funkcijom informacijske sigurnosti.

Sukladno tome tema (naslov) doktorske disertacije je:

MODEL EKONOMSKI ODRŽIVOGA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA

te je ona podobna za daljnja znanstvena istraživanja uslijed činjenice da danas takva problematika nailazi na veliko zanimanje istraživača, aktualna je i za područje upravljanja financijama, menadžment, ekonomiku informatičke poslovne funkcije i općenito ekonomiku poduzeća. Ova je tema također teorijski i neposredno praktično primjenjiva i odražava problematiku, strukturu i sadržaj doktorske disertacije iz područja društvenih znanosti, polja ekonomskih znanosti te grane poslovna informatika.

1.2 Problem, predmet i objekt istraživanja

Sva poduzeća, neovisno o njihovoj veličini, obliku, organizaciji i grani privrede u kojoj djeluju, nužno u svom poslovanju koriste poslovne informacijske sustave koje omogućuju povezanost zaposlenika i jedinica unutar poduzeća, ali i poduzeća s okolinom, dobavljačima, klijentima,

širom poslovnom zajednicom i tijelima državne uprave koja nadziru poslovanje poduzeća, odnosno, sa svim uključenim nositeljima interesa u poslovanju poduzeća. Pritom se stvara velika količina podataka koji se agregiraju u obliku strukturiranih ili nestrukturiranih podataka i informacija koje su značajne za poslovanje poduzeća, a čije kompromitiranje, otkrivanje ili promjena mogu imati negativne posljedice po poduzeće. Teorija i praksa prepoznali su značaj ovog procesa te je stoga unutar poduzeća došlo do diferencijacije zasebne poslovne funkcije zaštite sigurnosti informacijskih sustava koja je potekla iz poslovne funkcije upravljanja. Zbog tehničkog konteksta koji je snažno povezan uz ovu poslovnu funkciju, poduzeća su tradicionalno orijentirana ka osiguranju mjera tehničke zašite informacijskih sustava. Pritom se često zanemaruju organizacijske mjere i procjena utjecaja primjene tih mjera na poslovni rezultat poduzeća.

Paralelno s opisanim procesom, zakonodavac u Republici Hrvatskoj donosi nove zakonske propise koji se odnose na područje upravljanja informacijskom sigurnošću, i to u financijskim djelatnostima u kojima postoji inherentna potreba mjerenja i upravljanja raznorodnim vrstama rizika. Zajednički izazov pred kojim se nalaze sva poduzeća neovisno o njihovoj veličini je nepostojanje univerzalno primjenjivog modela kojim bi se moglo procijeniti utjecaj ulaganja u sustav upravljanja informacijskom sigurnošću na rezultat poslovanja poduzeća. Istovremeno, mala i srednja poduzeća koja nemaju raspoloživa financijska sredstva i internu ekspertizu za provođenje složenih tehničkih i organizacijskih obrazaca zaštite svojih informacijskih sustava prepuštena su sama sebi i slučajnoj procjeni prioriteta u osiguranju sustava upravljanja informacijskom sigurnošću.

U kontekstu navedene problematike istraživanja definira se **znanstveni problem istraživanja**:

U malim i srednjim poduzećima u Republici Hrvatskoj još uvijek se nedovoljno teorijski istražuju i praktički primjenjuju metode kojima se procjenjuju potrebe, ali i utjecaj ulaganja u sustav upravljanja informacijskom sigurnošću na poslovanje poduzeća, što za posljedicu ima nedovoljnu razinu sigurnosti poslovnih informacija od značaja za poduzeće i povećanu incidenciju pojave sigurnosnih incidenata, smanjenu mogućnost kontrole troškova takvog sustava i sukladnosti sa zakonskim propisima, što posljedično umanjuje sposobnost postizanja željenog poslovnog rezultata. Taj je problem nužno znanstveno istražiti te predložiti konzistentan i sveobuhvatan model procjene utjecaja ulaganja u sustav upravljanja informacijskom sigurnošću na poslovanje malih i srednjih poduzeća.

Navedenu problematiku i problem opravdavaju sljedeća **obilježja** koja su karakteristična za okruženje u kojemu mala i srednja hrvatska poduzeća obavljaju svoju poslovnu aktivnost i organiziraju svoje sustave upravljanja informacijskom sigurnošću;

1. Zakon o informacijskoj sigurnosti kao temeljni zakon koji regulira predmetnu problematiku ne rješava složene izazove pred kojim se po tom pitanju nalaze mala i srednja poduzeća. Taj zakon ima vrlo općenit zahvat i odnosi se isključivo na tijela državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.

2. Ostali vezani pravni akti reguliraju zasebna područja poput financijskog sektora ili funkcioniranja tajnih službi, odnosno određene tehničke aspekte upravljanja sustavima informacijske sigurnosti, te stoga nisu primjenjivi na mala i srednja poduzeća zbog različitog poslovnog konteksta i financijskog potencijala raspoloživog za razvoj sustava upravljanja informacijskom sigurnošću.

3. Ulaganja u sustav upravljanja informacijskom sigurnošću malih i srednjih poduzeća temelje se na profesionalnoj procjeni kumulativnog rizika te subjektivnoj procjeni vlasnika ili menadžera o opravdanosti ulaganja u odnosu na percipiranu razinu rizika. Raspoloživi sustavi najbolje prakse i certifikacije ne referiraju se niti u jednom koraku postupka na utjecaj ulaganja u sustav informacijske sigurnosti na poslovni rezultat poduzeća.

4. Mala i srednja poduzeća ne posjeduju interne ljudske resurse a često niti financijsku snagu koja bi mogla adekvatno pratiti rastuće zahtjeve za provođenjem mjera informacijske sigurnosti. Nedostatna vlastita sredstva za financiranje ulaganja u sustav upravljanja informacijskom sigurnošću rezultira povećanom razinom sigurnosnih incidenata i troškovima njihovog saniranja, propuštanjem dobiti i smanjenjem konkurentnosti poduzeća. Ova je činjenica pogoršana nepostojanjem specifičnih znanja i vještina unutar poduzeća koja su potrebna za uspostavljanje sustava upravljanja informacijskom sigurnošću i kompleksnošću te vremenom potrebnim za provođenje mjera pri uspostavljanju sustava.

5. U Republici Hrvatskoj ne postoje poduzeća ili organizacije koje se isključivo fokusiraju na pružanje usluga sigurnosnog konzaltinga za mala ili srednja poduzeća, što dodatno pogoršava stanje upravljanja sustavom informacijske sigurnosti. Poduzeća koja pružaju usluge uspostavljanja sustava upravljanja informacijskom sigurnošću uglavnom su orijentirana na velika poduzeća i postizanje sukladnosti sustava sukladno međunarodnim standardima najbolje prakse i certifikacije, dok se poduzeća koja pružaju usluge savjetovanja u odnosu na sigurnosne sustave orijentiraju na uspostavljanje organizacijskih obrazaca, odnosno isporuku tehničkih rješenja.

6. Upravljanje sustavom informacijske sigurnosti promatra se u poslovnom kontekstu isključivo kao problem minimalne sukladnosti sa zakonskim propisima, ili kao tehnička disciplina, uz nejasan odnos prema poslovnom rezultatu. Nepostojanje općenito prihvaćenog modela koji dovodi u vezu ulaganje u sustav upravljanja informacijskom sigurnošću s poslovnim rezultatom poduzeća dodatno pogoršava ovu pojavnost.

7. Temeljna strategija koju instinktivno koriste mala i srednja poduzeća u upravljanju vlastitom informacijskom sigurnošću je implicitno i eksplicitno preuzimanje nerazumno visoke razine rizika i izbjegavanje ulaganja u istu, uz primjenu minimalnih mjera tehničke zaštite vlastitih informacijskih sustava. Na određeni način na ovakvo ponašanje potiče ih i zakonodavac koji ne regulira ovu problematiku na način koji bi bio primjeren malim i srednjim poduzećima. Ulaganja u sustave upravljanja informacijskom sigurnošću percipiraju se isključivo kao nepovratni trošak.

8. Poslovni bankarski sektor ne prepoznaje važnost sigurnosti informacijskih sustava malih i srednjih poduzeća. Kod osiguravanja eksternih izvora financiranja od strane poslovnih banaka ne traže se posebne analize ekonomskog utjecaja osiguravanja informacijskih sustava poduzeća iako u današnjim uvjetima ta poslovna funkcija ima odlučujući utjecaj na poslovni rezultat poduzeća. Na taj način su i poduzeća i banke podložni nerazvrstanim, implicitno preuzetim rizicima.

Iz navedene problematike i problema istraživanja determiniran je i **predmet znanstvenog istraživanja:**

Istražiti, analizirati, elaborirati i konzistentno utvrditi sve relevantne **teorijske i praktične značajke sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima**. Dokazati kako je **primjena ekonomskih kriterija** u odlučivanju o ulaganjima u sustav upravljanja informacijskom sigurnošću **ravnopravni čimbenik** koji je potrebno razmatrati pri donošenju odluka o takvom ulaganju. Preispitujući raspoloživa teoretska razmatranja te inozemnu i hrvatsku praksu, **predložiti i znanstveno utemeljeno elaborirati primjereniji pristup zadanoj tematici** – novi model ekonomski održivoga sustava upravljanja informacijskom sigurnošću koji će omogućiti adekvatno organizacijsko i ekonomski izvedivo uspostavljanje te poslovne funkcije, primjereno potrebama malih i srednjih poduzeća, a sukladno zakonskim propisima Republike Hrvatske i direktivama Europske unije.

Znanstveni problem i predmet znanstvenoga istraživanja se odnosi na dva primarna **objekta** znanstvenoga istraživanja, a to su: **sustav upravljanja informacijskom sigurnošću** te **mala i srednja poduzeća** u Republici Hrvatskoj.

1.3 Znanstvena hipoteza i pomoćne hipoteze

Sukladno determiniranom znanstvenom problemu istraživanja, predmetu znanstvenog istraživanja i objektu znanstvenoga istraživanja postavljena je i **temeljna znanstvena hipoteza:**

Upotrebom utemeljenih spoznaja ekonomske znanosti, te uz uvažavanje zakonom određenih zahtjeva, i međunarodno prihvaćenih normi najbolje prakse, moguće je predložiti ekonomski utemeljen model upravljanja sustavom informacijske sigurnosti koji je posebno prilagođen potrebama malih i srednjih poduzeća u Republici Hrvatskoj, a koji će osigurati poboljšanje poslovnog rezultata, te povećati razinu sukladnosti sa zakonskim propisima i predmetnim međunarodnim standardima.

Tako postavljena temeljna znanstvena hipoteza, implicira više **pomoćnih hipoteza (P.H.):**

P.H. 1. Upravljanje sustavom informacijske sigurnosti poduzeća ključna je poslovna funkcija koja se temelji na primjeni tehničkih, organizacijskih i zakonskih obrazaca zaštite informacijskog kapitala poduzeća. Ispravnom implementacijom i korištenjem te poslovne funkcije moguće je poboljšati poslovni rezultat poduzeća, smanjiti izvanredne troškove sigurnosnih incidenata te poboljšati imidž poduzeća.

P.H. 2. Za uspješno sagledavanje institucionalnog okvira informacijske sigurnosti unutar kojega posluju mala i srednja poduzeća u potpunosti znanstveno analizirati referentne normirane sustave unutar kojih ona posluju. Ti sustavi se sastoje od zakonskih propisa Republike Hrvatske koji reguliraju problematiku informacijske sigurnosti u poduzećima, formalnih strukovnih standarda i certifikacijskih sustava koji definiraju najbolju praksu uspostavljanja i upravljanja tim sustavima.

P.H. 3. Razvoj tehničkih, tehnoloških i organizacijskih zahtjeva koje je potrebno zadovoljiti kako bi se uspješno uspostavio sustav upravljanja informacijskom sigurnošću doveo je do iznimne kompleksnosti sustava pri čemu donosioci poslovnih odluka nisu upoznati sa strukturom i potrebnim iznosom kapitalnih i investicijskih ulaganja u poslovnu funkciju informacijske sigurnosti te opravdanosti navedenih troškova. Za vrednovanje i dobivanje kvalitetnog pregleda ukupnih troškova i koristi od sustava upravljanja informacijskom sigurnošću od velike je važnosti provesti detaljnu analizu svih vidljivih i skrivenih troškova sustava upravljanja informacijskom sigurnošću.

P.H. 4. Uvriježeni autonomno - tehnički pristup upravljanju poslovnim sustavima informacijske sigurnosti je rezultat stihijskog odgovora na rizike, a lišen je ekonomskog konteksta i procjene ukupnog troškovnog efekta na poslovanje poduzeća. Ciljeve poslovne funkcije upravljanja informacijskom sigurnošću u malim i srednjim poduzećima moguće je postići sustavnom korekcijom navedenog obrasca upravljanja putem primjene novog, transparentnog modela, utemeljenog na ekonomskim principima procjene investicija u sustav upravljanja informacijskom sigurnošću.

P.H. 5. Za kreiranje adekvatnog modela sustava upravljanja informacijskom sigurnošću potrebno je u proces modeliranja uključiti relativno statičke ulaze poput zakonskih zahtjeva i dinamičke ulaze predstavljene ekonomskim pokazateljima aktivnostima uvođenja i održavanja takvog sustava, uz uvažavanje odgovarajućih posebnosti koje proistječu iz tehničkih i organizacijskih osobitosti. Poslovna funkcija sustava upravljanja informacijskom sigurnošću može se analizirati kvantitativnim instrumentarijem financijske analize.

P.H. 6. Temeljem analize stanja funkcije upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj te ostalih znanstvenih spoznaja o upravljanju informacijskom sigurnosti moguće je predložiti odgovarajući novi model upravljanja informacijskom sigurnošću, taj model testirati, predložiti mjere i aktivnosti potrebne za njegovu uspješnu implementaciju te vrednovati njegove osnovne ekonomske učinke u svrhu poboljšanja poslovnog rezultata malih i srednjih poduzeća i usklađenosti sa zakonskim propisima.

1.4 Svrha i ciljevi istraživanja

U izravnoj vezi sa znanstvenim problemom, predmetom i objektom znanstvenog istraživanja postavljene znanstvene hipoteze determinirani su **svrha i ciljevi istraživanja:**

Istražiti i analizirati u okviru ekonomskih znanosti spoznaje o sustavima upravljanja informacijskom sigurnošću i njihovim ekonomskim značajkama te znanstveno utemeljeno formulirati rezultate istraživanja i predstaviti interpretirane rezultate istraživanja kako bi se realizirao njegov **glavni cilj**: predložiti novi model sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima Republike Hrvatske koji uključuje ekonomske pokazatelje funkcioniranja, a **u svrhu** racionalizacije poslovanja, povećanja sukladnosti sa zakonskim propisima i formalnim sustavima certifikacije, povećanje raspoloživosti vanjskih izvora financiranja, poboljšanja imidža te pozicije poduzeća na tržištu.

Kako bi se primjereno riješio postavljeni problem istraživanja, ostvario predmet istraživanja, dokazala postavljena hipoteza te postigli svrha i ciljevi istraživanja, u ovom su radu primjenom znanstvenih metoda dani odgovori na brojna pitanja od kojih su najvažnija sljedeća:

1. Koja su teorijska i ekonomsko – politička polazišta na kojima je utemeljena poslovna funkcija upravljanja sustavima informacijske sigurnosti?
2. Koji je utjecaj percipirane razine rizika na potrebnu razinu ulaganja u sustave upravljanja informacijskom sigurnošću?
3. Kako se identificira informacijski kapital poduzeća u odnosu na cjelokupnost poslovnih podataka i informacija poduzeća?

4. Koje su mogućnosti mjerenja i praćenja troškova ulaganja u sustave upravljanja informacijskom sigurnošću i kvantitativnog izražavanja povrata na investiciju?
5. Kakav je utjecaj formalnih sustava normizacije i zakonskih propisa okruženja na zahtjeve za investicijama u informacijsku sigurnost poduzeća?
6. Kakvo je iskustvo država u svijetu u primjeni sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima?
7. Kakav je utjecaj zakonskih propisa u Republici Hrvatskoj po pitanju zahtjeva za investicijama u informacijsku sigurnost poduzeća?
8. Koje su specifičnosti sustava upravljanja informacijskom sigurnošću malih i srednjih poduzeća u Republici Hrvatskoj?
9. Kakva je struktura investicijskih ulaganja i troškova održavanja sustava upravljanja informacijskom sigurnošću malih i srednjih poduzeća u Republici Hrvatskoj?
10. Koji su relevantni kriteriji za ocjenjivanje elemenata modela ekonomski održivog sustava upravljanja informacijskom sigurnošću malih i srednjih poduzeća u Republici Hrvatskoj?
11. Kakve su mogućnosti implementacije ekonomski održivog modela sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj?
12. Koji su očekivani pozitivni učinci primjene ekonomski održivog modela sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj?

1.5. Ocjena dosadašnjih istraživanja

Tijekom izučavanja izložene problematike proučeno je oko dvije stotine i pedeset bibliografskih jedinica od kojih su u ovom uvodu navedene samo najvažnije. Informatičko poslovanje poduzeća spominje se gotovo u svim citiranim bibliografskim jedinicama. Principi informacijske sigurnosti, sustavi upravljanja informacijskom sigurnošću i certifikacija informacijsko sigurnosnih sustava spominju se u pedesetak citiranih bibliografskih jedinica. Sustavi upravljanja informacijskom sigurnošću u malim i srednjim poduzećima zasebno su obrađeni u manjem opsegu u manje od pet citiranih bibliografskih jedinica dok prema raspoloživim informacijama ekonomski utjecaj ulaganja u sustave upravljanja informacijskom sigurnošću u malim i srednjim poduzećima uopće nije istraživan, iz čega slijedi kako je u Republici Hrvatskoj ova problematika vrlo slabo obrađena. Većina bibliografskih jedinica obrađuje problematiku na način da je zauzeta pozicija orijentacije ka velikim poslovnim sustavima te samim time zaključci nisu neposredno primjenjivi na mala i srednja poduzeća zahvaljujući nizu inherentnih specifičnosti i ograničenja. Iznenađujuće je kako se pretraživanjem dostupnih informacijskih resursa ne nalaze naznake autora radova iz Republike

Hrvatske koji bi ovu tematiku istražili i u cjelini prezentirali javnosti. Velimir Srića i Mario Spremić raspoznaju kako su znanje, utemeljeno na ključnim poslovnim informacijama, temeljne odrednice poslovnog uspjeha, što jasno iznose u svom djelu „Informacijskom tehnologijom do poslovnog uspjeha“. Informatička tehnologija, inovacije i strategija po njima su ključni čimbenici konkurentske prednosti dok se za uspješnost modernih poduzeća ključnim određuje utjecaj informacijske tehnologije na upotrebu intelektualnog kapitala. Autor Davor Delišimunović u svojoj knjizi „*Management zaštite i sigurnosti*" smatra kako su promišljanja o integralnoj zaštiti i pravila štićenja zbog svoje univerzalnosti primjenjiva na većinu financijskih institucija i drugih objekata koji se štite u Republici Hrvatskoj. Alen Ostojić, Darija Ivandić Vidović i Lidija Karlović u knjizi „*Korporativna sigurnost*“ obrađuju sve sastavnice integralne sigurnosti poduzeća (informacijska sigurnost, privatna zaštita, zaštita intelektualnog vlasništva, zaštita podataka, privatna istražna djelatnost, *business intelligence*, sprječavanje pranja novca i financiranja terorizma, zaštita na radu, zaštita od požara, zaštita okoliša, zaštita i spašavanje, obrambene pripreme) te mapiraju sve navedene procese stavljajući ih u okvire zakonskih propisa i sustava najbolje prakse. Autor Haris Hamidović u svojoj knjizi "*Standardi informacijske sigurnosti*“ dovodi u vezu nastupe sigurnosnih incidenata s financijskim gubicima. Zajedničko je svim domaćim autorima promatranje sustava upravljanja informacijskom sigurnošću isključivo kao tehničkih i organizacijskih sustava lišenih ekonomskog konteksta i utjecaja na poslovni rezultat poduzeća, koncentrirajući se na organizacijske obrasce i tehnička rješenja kojima valja težiti u idealnim uvjetima apsolutne raspoloživosti resursa.

Strani autori dublje su ušli u problematiku upravljanja informacijskom sigurnosti i dovođenjem u vezu uspješnosti tog upravljanja s uspješnošću poduzeća ili organizacija. Autor knjige "*Managing Information Risk and the Economics of Security*", Eric M. Johnson prepoznaje kako je ekonomika upravljanja informacijskom sigurnošću jedan od čimbenika odlučivanja o investiranju rukovoditelja poduzeća, ali i dionika koji odlučuju o investicijama u javnom sektoru te građana kao pojedinaca. Upravljanje informacijskom sigurnošću promatra iz perspektive rukovoditelja informacijskom sigurnošću te državnih agencija koje su uključene u obradu informacijsko sigurnosnih incidenata. Christopher Alberts i Adrey Dorofee u svojoj knjizi „*Managing Information Security Risks: The OCTAVE (SM) Approach*“ predlažu procesni pristup procjeni rizika informacijske sigurnosti utemeljen na jedinstvenoj OCTAVE metodi koji je u praksi doživio primjenu u medicinskom i financijskom sektoru. Sama metoda utemeljena je na procjeni rizika informacijske sigurnosti koji pomaže poduzećima i organizacijama odlučivati ovisno o potencijalnom utjecaju nastupa neželjenih događaja. Osobito su značajne spoznaje iznesene u djelu „*Information Security Cost Management*“ autora Ioana V. Bazavan i Iana Lim. Autori ispravno primjećuju kako informacijska sigurnost predstavlja izazov za sve tipove

organizacija (pri čemu očito shvaćaju kako se ova problematika ne odnosi samo na poduzeća, već i na neprofitne oblike organizacija) te smatraju kako bi pragmatičan pristup primjeni mjera informacijske sigurnosti trebao obuhvaćati i uvažavati proračunska i realna ograničenja te je jedno od rijetkih djela u kojima se predlaže radni okvir za primjenu mjera informacijske sigurnosti koji omogućuje kreiranje najbolje strategije poslovne informacijske sigurnosti uzimajući u obzir raspoložive tehničke, ljudske i financijske resurse.

Dva su djela stranih autora od ključnog značaja u smislu konkretizacije i kvantificiranja vrijednosti informacija sadržanih u informacijskim sustavima poduzeća te ispravne procjene gubitaka koji mogu nastati uslijed nastupa sigurnosnih incidenata. Prvo je knjiga autora Ursa Birchlera i Monike Butler – „*Information Economics*". Autori kvantificiraju vrijednost informacija u kontekstu čovjeka i prirode, a zatim u taj odnos uvode i moderne konstrukte poput tržišta, važnost raspolaganja informacijama koje nisu raspoložive drugim igračima na tržištu te na taj način podižu razinu apstrakcije od odnosa pojedinca i informacije u smjeru makroekonomskog konteksta. Drugo djelo je knjiga Jacka Hirshleifera i Johna G. Rileya „*The Analytics of Uncertainty and Information*". Ona predstavlja kapitalno djelo u području ekonomike informacija te je zapravo nastavak klasične ekonomske analize poslovnih informacija korištenjem termina ekonomike nesigurnosti. Autori ukazuju na socijalni značaj distribucije koja nastaje preuzimanjem različitih razina rizika te je po prvi put dovode u odnos s modelima kao što je klasični model kapitalnog budžetiranja (*CAPM model*). Prvi dio knjige posvećen je situacijama u kojima se odlučivanje odvija u uvjetima nepotpunih informacija dok se u drugom dijelu knjige obrađuju situacije u kojima je pojedinac aktivni subjekt odlučivanja te tako može utjecati na ishod.

Temeljem raspoloživih informacija do kojih se došlo tijekom priprema za izradu prijedloga teme doktorske disertacije, a koje obuhvaćaju brojne i raznorodne bibliografske jedinice domaćih i stranih autora, može se uočiti kako su samo opći principi informacijske sigurnosti, organizacije poslovne funkcije informacijske sigurnosti te organizacije poslovne funkcije informatike i telekomunikacija istraživani i prezentirani javnosti. Osobito je nedostatno obrađen utjecaj ulaganja u informacijsku sigurnost na poslovni rezultat poduzeća, nejasno su definirani oni elementi sustava upravljanja informacijskom sigurnošću koji su obvezujući s obzirom na zakonske zahtjeve i gotovo da nije istraživan utjecaj poslovne funkcije informacijske sigurnosti na poslovni rezultat malih i srednjih poduzeća. Domaće zakonodavstvo ne prepoznaje potrebu za postavljanjem izdvojenih minimalnih zahtjeve za primjenama mjera informacijske sigurnosti u odnosu na mala i srednja poduzeća. Štoviše, niti domaći niti strani autori nisu se bavili ovom specifičnom problematikom a jedini međunarodni standard informacijske sigurnosti za mala i

srednja poduzeća, britanski standard *ISSA 5173*, predložen je u obliku nacrta u ožujku 2011. godine i još nije službeno izdan.

Budući da opći okvir teme doktorske disertacije nije u dovoljnoj i znanstvenoj razmjeri istražen, a konkretna tema na opisani način i s predloženim naslovom nije uopće istražena, niti su rezultati takvoga istraživanja prezentirani javnosti, postoje teorijski interes te praktično opravdanje provođenja opisanog istraživanja.

1.6. Znanstvene metode

Tijekom znanstvenog istraživanja, te u procesu formuliranja i prezentiranju rezultata istraživanja doktorske disertacije korištene su kombinacije brojnih i raznovrsnih znanstvenih metoda. One se mogu grupirati u tri različite grupe znanstvenih metoda:

1. Klasične znanstvene metode u parovima,
2. Samostalne klasične znanstvene metode,
3. Kvantitativne znanstvene metode.

Klasične znanstvene metode u parovima koje su korištene su metoda analize i sinteze, metoda dokazivanja i opovrgavanja, metoda apstrakcije i konkretizacije, induktivna i deduktivna metoda, metoda generalizacije i specijalizacije. Metode analize i sinteze korištene su u odnosu na opisani predmet istraživanja. Naime, budući kako je predmetom istraživanja definirano da je potrebno istražiti sve relevantne teorijske i praktične značajke sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima, sukladno rezultatima dobivenim analizom svih identificiranih značajki određene su one koje su odlučujuće pri odlučivanju o investiranju u sustave upravljanja informacijskom sigurnošću te se temeljem njih pristupilo postupku znanstvene sinteze. Njome je uz preispitivanje raspoloživih i analiziranih teoretskih razmatranja i praktičnih iskustava kreiran novi model ekonomski održivoga sustava upravljanja informacijskom sigurnošću, primjeren malim i srednjim poduzećima.

Metoda dokazivanja i opovrgavanja korištena je na način da je temeljem znanstvenih činjenica izvođena istinitost pojedinih stavova, u odnosu na metodu dokazivanja. Naime, u odnosu na postavljenu hipotezu koja se tiče predmeta istraživanja traženi su argumenti za njeno opravdavanje. Metodom opovrgavanja se teze odbacuju i pobijaju. U slučaju korištenja metode opovrgavanja, radilo se uglavnom o izravnom opovrgavanju čime su se pobijale odgovarajuće teze ili argumentacije, a u manjoj mjeri o dokazivanju ispravnosti antiteze korištenjem neizravnog opovrgavanja. Metoda dokazivanja korištena je afirmativno u odnosu na naprijed opisane pomoćne hipoteze dok je metoda opovrgavanja korištena u odnosu na trenutačno uvriježene sustave upravljanja informacijskom sigurnošću koji ne uključuju financijski utjecaj

na poslovanje poduzeća i istim tehničko-organizacijskim mjerama pokušavaju tretirati sve organizacije neovisno o njihovoj veličini i poslovnom sektoru.

Induktivna i deduktivna metoda predstavljaju temeljnu korištenu metodu u parovima. Proces izrade doktorske disertacije je obavljen na način da se po uočavanju problema istraživanja polazi od pojedinačnih, izučenih činjenica ka onima neizučenima što znači da su se uopćavanja činila od većeg broja pojedinačnih pojava. (zaključivanje od pojedinačnog prema općem). Induktivna se metoda obilato koristila u cijelom postupku izrade doktorske disertacije, počevši od preliminarnog istraživanja navedenih bibliografskih jedinica u kojemu je istražen veći broj reprezentativnih jedinica što povećava vrijednost induktivnog zaključivanja. Induktivnom su metodom otkriveni uzročno-posljedični odnosi između pojava koje prethode i pojava koje slijede. Deduktivna metoda korištena je u formuliranju novog modela upravljanja poslovnom funkcijom informacijske sigurnosti na način da je definiran posve novi, do formuliranja rezultata istraživanja nepostojeći model, koji je nastao zaključivanjem od općih sudova ka drugim općim sudovima. Primjenom metode indukcije i dedukcije u parovima verificirana je postavljena hipoteza na način da je indukcija bila metoda korištena u početnom stadiju istraživanja a dedukcija u završnom stadiju istraživanja i definiranju novog modela.

Metoda apstrakcije i konkretizacije korištena je u dijelu metode apstrakcije u odnosu na predmet istraživanja na način da je iz promatranog predmeta eliminirano ono što je opće a koncentriralo se na ono što je posebno. Korištenjem metode apstrakcije odvojene su one specifičnosti sustava upravljanja informacijskom sigurnošću koje su relevantne za proces dokazivanja. U suprotnom smjeru, u procesu korištenja metode konkretizacije ukazano je na jedinstvo općeg i posebnog, jer je predloženi model rezultat procesa kretanja mišljenja i saznanja od općeg ka posebnom i pojedinačnom.

Metoda generalizacije i specijalizacije u paru osobito je korištena u izradi doktorske disertacije. Primarno je korištena metoda specijalizacije primjenom koja je indicirana već naslovom doktorske disertacije koji se odnosi na mala i srednja poduzeća kao podskup svih poduzeća i organizacija u kojima se mogu primjenjivati mjere informacijske sigurnosti. Generalizacija, u smislu poopćavanja, odnosno prijelaza s razmatranja danog skupa objekata na odgovarajuće razmatranje njegovog nadskupa korištena je u onom dijelu doktorske disertacije u kojemu će je predložen novi model upravljanja informacijskom sigurnošću koji u sebi sadrži i ekonomske pokazatelje.

Nadalje, korištene su **samostalne znanstvene metode** tijekom čitavog procesa istraživanja i pismenog formuliranja rezultata istraživanja, i to komparativna metoda te metoda klasifikacije. Metoda klasifikacije korištena je pri razvrstavanju podataka od interesa za istraživanje na

osnovu nekih njihovih osobina, a osobito pri opisu osobina odgovarajućih pojmova iz područja upravljanja informacijskom sigurnošću, procjene i tretmana rizika, opisa zahtjeva zakonodavca i različitih metoda procjene financijskog utjecaja sustava upravljanja informacijskom sigurnošću malih i srednjih poduzeća na poslovni rezultat. Komparativna metoda korištena je u svrhu uočavanja sličnosti i zajedničkih obilježja, a samim time i različitosti dvaju ili više pojava. U kontekstu izrade doktorske disertacije njome je uspoređivan sustav upravljanja informacijskom sigurnošću u velikim (korporativnim) sustavima i malim i srednjim poduzećima koja raspolažu ograničenim resursima. Metoda je korištena oprezno kako bi vodila valjanim zaključcima.

Važno je napomenuti kako su korištene i metoda deskripcije, odnosno opisivanja pojava iz domene poslovne funkcije informacijske sigurnosti točno određenim i precizno definiranim pojmovima te metoda eksplanacije, odnosno naučnog opisivanja. Temeljni zadatak ove metode je objasniti prirodu povezanosti ulaganja u sustave upravljanja informacijskom sigurnošću s poslovnim rezultatom malih i srednjih poduzeća na način da će se utvrditi postojanje povezanosti između ta dva fenomena, vremenski tok smještaja oba fenomena te logički odbaciti druge mogućnosti povezanosti i uzročnosti. U izradi cijele doktorske disertacije i tijekom postupka dokazivanja preuzimane su tuđe znanstvene spoznaje uz odgovarajuće i pravilno navođenje izvora.

Sukladno modernim zahtjevima izrade doktorskih disertacija korištene su i **kvantitativne znanstvene metode**, i to statistička metoda te neke podvrste matematičkih metoda. Integralni dio doktorskog rada je istraživanje provedeno korištenjem anketne metode na odabranom uzorku koji se sastoji od malih i srednjih poduzeća u Republici Hrvatskoj. Cilj takve ankete je ispitivanje i statistička obrada njihovog poznavanja zakonskih obveza po pitanju informacijske sigurnosti, saznavanje dostignutog stupnja zrelosti uvođenja poslovne funkcije upravljanja informacijskom sigurnošću u svakodnevno poslovanje te percipirana razina utjecaja aktivnosti vezanih uz sustav upravljanja informacijskom sigurnošću na poslovni rezultat. U operacionalizaciji ankete dostavljeni su anketni upitnici odgovornim osobama u poduzećima korištenjem elektroničke pošte, poštanske službe te putem Internet sustava za anketiranje kreiranom posebno u tu svrhu.

U doktorskoj disertaciji je za donošenje odluka vezanih uz ulaganje u sustave upravljanja informacijskom sigurnošću i vrednovanje ekonomski održivog modela za mala i srednja poduzeća, istražena mogućnost korištenja matematičkih metoda poput metode analitičkih hijerarhijskih procesa koja je strukturna tehnika za organizaciju i analizu kompleksnih odluka a u ovoj doktorskoj disertaciji korištena je za određivanje prioriteta pri odlučivanju o investiranju u sustave upravljanja informacijskom sigurnošću u uvjetima ograničenosti raspoloživih resursa dominantnih kod malih i srednjih poduzeća

1.7. Obrazloženje strukture doktorske disertacije

Uzevši u obzir osnovni problem, zadane ciljeve, i ocjenu dosadašnjih istraživanja, rezultati istraživanja bit će prezentirani primjenom znanstvenih metoda u doktorskoj disertaciji u osam međusobno povezanih dijelova.

U prvom dijelu doktorske disertacije ***Uvodu,*** definirani su problem, predmet i objekt istraživanja, postavljena je znanstvena hipoteza i pomoćne hipoteze koje potkrepljuju znanstvenu hipotezu, određeni su svrha i ciljevi istraživanja, dana je ocjena dosadašnjih istraživanja drugih znanstvenika, navedene su najvažnije znanstvene metode korištene u znanstvenom istraživanju i prezentiranju rezultata istraživanja te je obrazložena struktura doktorske disertacije.

U drugom dijelu s naslovom ***Teorijske odrednice poslovne funkcije upravljanja sustavom informacijske sigurnosti poduzeća*** pojašnjeni su značaj informacijske sigurnosti u upravljanju poduzećima, teoretska podloga identifikacije informacijskog kapitala u poduzećima te je praktično razjašnjen proces funkcioniranja ciklusa upravljanja informacijskom sigurnošću u poduzećima. Poseban naglasak stavljen je na značaj koncepta rizika koji je temeljni koncept koji utječe na odabir i funkcioniranje sustava upravljanja informacijskom sigurnošću te ima direktan utjecaj na poslovni rezultat poduzeća. Također, ukazano je na ključne čimbenike uspješnosti uvođenja sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima.

Normiranje sustava upravljanja informacijskom sigurnošću poduzeća naslov je trećega dijela doktorske disertacije. Istraživanje i oblikovanje modela ekonomski održivog upravljanja sustavom informacijske sigurnosti malih i srednjih poduzeća u Republici Hrvatskoj nije moguće bez proučavanja makro, mezo i mikro institucionalnih zahtjeva vezanih uz njihovo poslovanje i informacijsku sigurnost u okviru Republike Hrvatske i Europske unije. Nadalje, ukazano je na zahtjeve nekih zakonskih sustava relevantnih svjetskih država (Sjedinjene Američke Države, Europska unija, države regije) te su izložena promišljanja funkcioniranja sustava upravljanja informacijskom sigurnošću u okviru opće prihvaćenih standarda upravljanja informacijskom sigurnošću i poslovne funkcije informatičkog poslovanja. Posebna pažnja posvećena je primjenjivosti svakog od ovih formalnih modela na mala i srednja poduzeća u Republici Hrvatskoj.

Naslov je četvrtog dijela rada ***Analiza i ocjena mogućnosti primjene ekonomskih kriterija na funkciju upravljanja informacijskom sigurnošću malih i srednjih poduzeća.*** U ovom dijelu analizirane su investicijske i troškovne komponente uvođenja i održavanja sustava upravljanja informacijskom sigurnošću u mala i srednja poduzeća te potencijal utjecaja na poslovni rezultat.

Posebna pozornost usmjerena je na mogućnost mjerenja povrata investicije u funkciju upravljanja informacijskom sigurnošću kao i na svjetsku praksu reguliranja te problematike.

Prikaz i analiza rezultata anketnog istraživanja naslov je petog dijela. U ovom dijelu na znanstveni način su analizirani rezultati preliminarnog istraživanja dostignute razine uporabe sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj. Posebna pažnja posvećena je poznavanju zakonskih propisa i korištenju sustava certifikacije. U ovom dijelu predstavljeni su rezultati istraživanja u odnosu na ekonomske učinke uporabe sustava upravljanja informacijskom sigurnošću.

Posebna pozornost posvećena je šestom dijelu s naslovom ***Kvantificiranje modela upravljanja sustavom informacijske sigurnosti u malim i srednjim poduzećima***. U prvom dijelu poglavlja analizira se metodologija, točnije, mogućnosti korištenja analitičkog hijerarhijskog procesa te korištenje metoda financijske analize primijenjene na investicije i troškove informacijske sigurnosti. Ovo je poglavlje priprema za prijedlog modela sustava upravljanja informacijskom sigurnošću te odabir kriterija vrednovanja odgovarajućeg modela koji će uslijediti.

Prijedlog ekonomski održivog modela upravljanja sustavom informacijske sigurnosti u malim i srednjim poduzećima naslov je sedmog dijela rada. U ovom dijelu istražene su mogućnosti implementacije postavljenog modela. Također, ukazano je na aktivnosti potrebne za implementaciju novoga modela sustava upravljanja informacijskom sigurnošću kao i na osnovne ekonomske učinke primjene modela u malim i srednjim poduzećima u Republici Hrvatskoj.

U posljednjem dijelu, ***Zaključku***, sustavno i koncizno su formulirani i prezentirani najvažniji rezultati znanstvenih istraživanja, koji su detaljno elaborirani u doktorskoj disertaciji, a kojima se dokazuju postavljena hipoteza i pomoćne hipoteze.

1.8. Očekivani rezultati istraživanja

Doktorska disertacija je polučila po završetku istraživanja sljedeće **rezultate:**

1) Znanstveno su utemeljene i određene najvažnije značajke sustava upravljanja informacijskom sigurnošću malih i srednjih poduzeća u Republici Hrvatskoj,
2) Analiziran je utjecaj zakonskih propisa i sustava najbolje prakse, odnosno certifikacije sustava upravljanja informacijskom sigurnošću malih poduzeća,
3) Istraženi su institucionalni okvir i zahtjevi Europske unije te ostalih referentnih država kao i mogući trendovi po pitanju zahtjeva sukladnosti,

4) Istražene su specifičnosti malih i srednjih poduzeća po pitanju zahtjeva postavljenih pred sustav upravljanja informacijskom sigurnošću te jasno određeni posebni zahtjevi i izazovi uvođenja takvog sustava u relevantna poduzeća u Republici Hrvatskoj,
5) Uporabom znanstvene metode anketiranja i statističke znanstvene metode je analizirano situacijsko stanje u Republici Hrvatskoj po pitanju internih sustava upravljanja informacijskom sigurnošću, utjecaja na poslovni rezultat i iskustava malih i srednjih poduzeća,
6) Istražene su mogućnosti primjene ekonomskih pokazatelja u ocjenjivanju investicija u informacijsku sigurnost te utjecaj troškova sustava upravljanja informacijskom sigurnošću na poslovni rezultat,
7) Korištenjem odgovarajućih kriterija vrednovanja i višekriterijske analize analiziran je odgovarajući model ekonomski održivoga sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima,
8) Predložene su potrebne mjere i aktivnosti za implementaciju novoga modela u malim i srednjim poduzećima u Republici Hrvatskoj,
9) Upotpunjene su uočene praznine u domaćoj i stranoj literaturi na navedenom području,
10) U nastavku procesa, a u slučaju uspješne obrane doktorske disertacije, navedene spoznaje bit će sintetizirane na način i u obliku koji je primjeren izdavanju znanstvene knjige pod istoimenim naslovom.

1.9. Očekivani doprinos znanosti

Rezultati znanstvenih istraživanja, prezentirani u doktorskoj disertaciji s naslovom **MODEL EKONOMSKI ODRŽIVOGA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA,** daju znanstveni doprinos ekonomskim znanostima u teorijskom i aplikativnom smislu.

Očekivani doprinos ekonomskim znanostima u **teorijskom smislu** može se izraziti u sljedećem:

- U razvoju znanstvene misli o ekonomiji općenito, a posebice o poslovnoj funkciji upravljanja sustavima informacijske sigurnosti,
- U poticanju daljih istraživanja specifičnosti malih i srednjih poduzeća u Republici Hrvatskoj a posebice njihove funkcije poslovne informatike i podsustava upravljanja informacijskom sigurnošću,
- U utvrđivanju razvojnih trendova koji proizlaze iz zakonskih zahtjeva i razvoja najbolje prakse u Republici Hrvatskoj, Europskoj Uniji i ostalim svjetskim državama,

- U determiniranju važnosti uspostavljanja sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima i ekonomskom promišljanju načina njihovog funkcioniranja,
- U razvoju znanstvenih spoznaja o stupnju dostignutog razvoja korištenja sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj,
- U primjeni znanstvenih metoda na selekciju adekvatnih mjera i kontrola potrebnih za postizanje ciljeva sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj,
- U primjeni znanstvenih teorijskih postavki i znanstvenih metoda na konkretne situacije primjene sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima,
- U ideji svjesnog i racionalnog modeliranja ekonomski održivog i kvantitativno mjerljivog sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj koji jednako uključuje ekonomske kriterije i pokazatelje kao i institucionalne zahtjeve i najbolju praksu,
- U razvoju znanstvenih spoznaja pri oblikovanju, dizajniranju i implementaciji modela upravljanja sustavom informacijske sigurnosti koji bi mogao pozitivno utjecati na unaprjeđenje cjelokupne organizacije malih i srednjih poduzeća u Republici Hrvatskoj.

Očekivani doprinos ekonomskim znanostima u **aplikativnom smislu,** može se odrediti implementacijom novoga, ekonomski utemeljenog modela sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj koji će znatno i izravno utjecati na njihovu uspješnost i ubrzati njihov razvoj.

1.10. Primjena rezultata istraživanja

Rezultati znanstvenoga istraživanja, prezentirani u doktorskoj disertaciji, potvrdili su temeljnu hipotezu i dokazali da je znanstveno utemeljenim spoznajama o organizaciji i funkcioniranju sustava upravljanja informacijskom sigurnošću u ekonomskom okviru funkcioniranja takvog sustava moguće ne samo ostvariti racionalno i efikasno upravljanje, već i poboljšati poslovni rezultat, konkurentnost i imidž poduzeća.

Rezultate istraživanja moći će koristiti institucije koje se izravno ili neizravno bave organizacijom poslovanja i informacijskom sigurnošću, nadležna tijela ministarstava koja sudjeluju u izradi zakonskih propisa, državne agencije, fakulteti i poslovne obrazovne institucije

i certifikacijska tijela koja se bave područjem informacijske sigurnosti. Osim njih, rezultati istraživanja bit će interesantni gotovo svim malim i srednjim poduzećima, svima uključenima u poslovne odnose s njima te bankarskim institucijama koje donose odluke o financiranju takvih poduzeća. Time će se postići cilj podizanja svijesti među vlasnicima i menadžerima malih i srednjih o potrebi promišljanja poslovne funkcije upravljanja informacijskom sigurnošću u okviru ekonomske održivosti.

2. TEORIJSKE ODREDNICE POSLOVNE FUNKCIJE UPRAVLJANJA SUSTAVOM INFORMACIJSKE SIGURNOSTI PODUZEĆA

Upravljanje sustavom informacijske sigurnosti poduzeća postalo je ravnopravnom poslovnom funkcijom koja je povjerena samom vrhu rukovodstva uslijed razvoja uslužnog sektora nacionalnih ekonomija, povećanja količine informacije koje u svom radu koriste poduzeća te razvoja kompleksnosti i prisutnosti informacijsko-komunikacijskih tehnologija. Dio informacija pohranjenih u informacijskim sustavima poduzeća čije korištenje može rezultirati poboljšanjem poslovnih procesa ili konkurentskim prednostima predstavljaju nematerijalni, informacijski kapital poduzeća. U svrhu objašnjenja ovih pojava, u ovoj glavi doktorske disertacije istražit će se sljedeće cjeline: **1) Pojam, razvoj i važnost informacijske sigurnosti 2) Čimbenici informacijskog kapitala malih i srednjih poduzeća i 3) Ciklus upravljanja informacijskom sigurnošću malih i srednjih poduzeća.**

2.1. POJAM, RAZVOJ I VAŽNOST INFORMACIJSKE SIGURNOSTI

Pri razmatranju ove tematike posebnu pozornost treba posvetiti sljedećim tematskim jedinicama: **1) pojam i razvoj informacijske sigurnosti**, **2) strateški značaj informacijske sigurnosti u upravljanju poduzećem** i **3) utjecaj koncepta rizika na informacijsku sigurnost poduzeća.**

2.1.1. Pojam i razvoj informacijske sigurnosti

Informacijska sigurnost je zaštita informacija i informacijskih sistema od neautoriziranog pristupa, uporabe, otkrivanja, prekida, promjena ili uništenja. (Institute, Cornell Information, 2013), a osigurava se kroz principe zaštite **povjerljivosti, integriteta i raspoloživosti** informacija.[1] Od najranijih dana pisane povijesti, vladari i vojni vođe shvaćali su važnost mehanizma kojim bi se štitila povjerljivost pisane korespondencije i postojanje mehanizma kojim bi se detektiralo da je povjerljivost narušena. U početku su se u tu svrhu koristili pečati od voska i slične tehnike koje su davale dokumentima značajku autentičnosti i osiguravali povjerljivost korespondencije. Prva osoba koju pisana povijest spominje kao nekoga tko je formalizirao ovakav postupak je bio Julije Cezar koji je 50 godina prije Nove ere osmislio

[1] U informacijskoj sigurnosti ovaj koncept poznat je prema svojoj engleskoj kratici „*C-I-A trijada*“ (eng. „*CIA triad*“), pri čemu pojedina slova znače redom – eng. *Confidentiality* (povjerljivost) – eng. *Integrity* (integritet) – eng. *Availability*(raspoloživost))

sustav „*Cezarovog šifriranja*“ (SecretCodeBreaker.com, 2013) kako bi spriječio da njegove tajne poruke dođu do neželjenih ruku.

Drugi svjetski rat doveo je do značajnog napretka po pitanju teorije i praktičnih mjera informacijske sigurnosti i tada dolazi do profesionalizacije te aktivnosti. Najveći naglasak stavljan je na pitanja fizičke zaštite informacija kojima je priječen pristup informacijskim centrima. Također, dolazi do potrebe formalizacije i klasifikacije podataka ovisno o njihovoj osjetljivosti. Uvode se osobne provjere prije davanja pristupa podacima. Poznat je primjer njemačke naprave za kodiranje poruka "*Enigma*" koju su prvi dekodirali poljski inženjeri još prije početka II. svjetskog rata. Englezima i Amerikancima je to pošlo za rukom tek tijekom II svj. rata kada je i sama *"Enigma"* doživjela novu inačicu. Informacije koje su dobivene iz dekodiranih poruka korištene su kako bi se predvidjele vojne akcije njemačkih oružanih snaga.

Promjena fokusa informacijske sigurnosti ka sferi informatičke tehnologije osobito je došla do izražaja tijekom Hladnog rata kada su se masovno počela koristiti *mainframe* računala.[2] Primarna prijetnja u to doba je bila usmjerena ka fizičkom pristupu informacijama koje su još uvijek bile uglavnom pohranjene na papirnatom mediju, pa su tako i akcije špijunaže i sabotaže bile usmjerene ka neovlaštenom pristupu arhiviranim dokumentima. Jedan od prvih problema informacijske sigurnosti koji nije bio fizičke naravi pojavio se u prvoj polovici 1960. godine kada je uslijed greške računala došlo do ispisivanja lozinke pristupa na svakoj stranici štampane datoteke.[3]

Krajem dvadesetog i početkom dvadeset i prvog stoljeća dolazi do naglog napretka u tehničkim mogućnostima telekomunikacija, informatičkoj opremi, elektroničkim mrežama za razmjenu podataka i metodama šifriranja podataka. Raspoloživost manjih, snažnijih i jeftinijih računala omogućila je obradu podataka i u manjim poduzećima te domovima zaposlenika. Nagli rast i široka primjena elektronske obrade podataka te pojava tzv. *e-businessa*[4] paralelno s prijetnjom međunarodnog terorizma (Canzer, 2005, p. 24) iznjedrila je potrebu za boljim načinima zaštite računala i informacija koje ona pohranjuju, obrađuju i razmjenjuju. Stoga u današnje doba sigurnost računalnih sustava postaje akademska disciplina unutra raznih profesionalnih organizacija, radeći na zajedničkom cilju osiguranja zaštite i sigurnosti informacijskih sustava.

---

[2] *„Mainframe računala“* je izraz koji je često korišten u prošlosti za velike računalne sustave koji su obavljali transakcijske obrade, npr. kod popisa stanovništva ili planiranja resursa poduzeća. Danas se taj izraz nešto manje koristi no ta vrsta serverskih računala i dalje postoje, koriste se i razvijaju.

[3] Ovaj je problem prvi prijavio i objasnio William D. Matthews s *Massachussets Institute of Technology*. Radilo se o sustavu dijeljenog vremena Multics CTSS koji je pokrenut na IBM 7094 računalu.

[4] „Intenzivno umrežavanje poslovnih organizacija i razvoj Interneta stvorili su pretpostavke za razvoj elektroničkog poslovanja koje uključuje poslovanje unutar poslovnih organizacija, među poslovnim organizacijama (eng. *business to business*), između poslovnih organizacija i pojedinačnih kupaca (eng. *business to costumer*). Za više detalja, cf. Čapko, Z: „**Elektroničko poslovanje**“,skripta,Ekonomski fakultet u Rijeci, Rijeka, 2007.

2.1.2. Strateški značaj informacijske sigurnosti u upravljanju poduzećem

Strateška važnost informacijske sigurnosti u upravljanju poduzećem razvidna je već i iz činjenice da identificirane strateške, taktičke i operativne jedinice unutar poduzeća koje su uključene u provođenje funkcije informacijske sigurnosti nemaju izoliranu odgovornost po pitanju provođenja plana informacijske sigurnosti budući da su njihove odgovornosti obično međusobno isprepletene, ali je isto tako i s rizicima koji su dijeljeni kroz cijelu organizacijsku strukturu poduzeća. (Tijan, 2011, p. 45) Tako jedan odjel može biti vlasnik osobnih podataka koji se odnose na npr. zdravlje zaposlenika, stoga njihov značaj nadilazi operativnu razinu i prelazi na stratešku. Odjel kontrole projekata koji posjeduje povijesni pogled na izvedene projekte u biti radi s podacima koji imaju ne samo strateški, već i operativni značaj. Iz tog razloga, kada se procjenjuje kritičnost primjene zaštite informacija, a zbog kompleksnosti poslovnih organizacija, potrebno je ne oslanjati se isključivo na klasifikacije koje se izvode na početku izrade plana već je potrebno svako razmatranje staviti u odgovarajuću perspektivu koja izvire iz stvarnih operativnih potreba.

U okviru ovih aktivnosti unutar poduzeća potrebno je jasno identificirati organizacijske cjeline, odjele i ključne korisnike koji ravnopravno dijele odgovornost za sigurnost informacijskog sustava u cjelini. Sve razine u provođenju plana informacijske sigurnosti moraju u suradnji sa stručnjakom za informacijsku sigurnost periodički testirati i prilagođavati plan informacijske sigurnosti novonastalim zahtjevima. Iz tog razloga potrebno je izrađivati minimalno godišnje izvještaje o stanju informacijske sigurnosti koji propituje adekvatnost postojećih kontrola informacijske sigurnosti u skladu s procedurama i preporukama za implementaciju istih. Godišnji izvještaj o stanju informacijske sigurnosti **strateški je izvještaj** koji mora biti odobren od strane odgovarajuće instance unutar poduzeća a treba sadržavati sljedeće elemente: (Aksentijević, 2012, p. 17)

1. Dodatke planu informacijske sigurnosti koji proističu iz tehnološkog i operativnog razvoja informacijske tehnologije i poslovnih zahtjeva u prošlom periodu,
2. Procjenu stanja primjene postojećeg plana informacijske sigurnosti,
3. Status primjene postojećeg plana informacijske sigurnosti,
4. Prijedlog mjera za poboljšanje informacijske sigurnosti poduzeća,
5. Vrijeme potrebno za primjenu mjera poboljšanja,
6. Vezane troškove i proračun potreban za primjenu predloženih mjera.

Odgovornost je i pravo svakog ključnog korisnika razvijati i primjenjivati vlastiti strateški plan čuvanja povjerljivih informacija i dokumenata. Iako ne postoji propisani format takvog plana,

minimalni zahtjev je da je takav dokument potpisan od strane ključnog korisnika, da sadrži datum donošenja te definira sljedeće **zahtjeve (Aksentijević, 2012, p. 13)**:

1. Naziv ureda, odjela, projekta ili organizacijske jedinice koja manipulira povjerljivim podacima,
2. Imena osoba koje imaju pristup takvim podacima,
3. Administrativne kontrole koje su poduzete kako bi se minimizirao broj ljudi koji imaju pristup povjerljivim informacijama,
4. Opis metoda fizičke zaštite informacija,
5. Opis roka trajanja zadržavanja povjerljivih informacija,
6. Opis načina uništavanja povjerljivih dokumenata,
7. Opis sadržaja treninga o informacijskoj sigurnosti, učestalosti te način dostave povjerljivih informacija.

Zbog specijaliziranih znanja koja su potrebna za dizajniranje, primjenu te servisiranje nove tehnologije, te zbog kratkog roka na raspolaganju za njihovu primjenu, poduzeća vrlo često ne posjeduju obrazovani kadar koji može samostalno operacionalizirati strategiju informacijske sigurnosti poduzeća. Iz tog razloga ona ponekad moraju angažirati vanjske specijaliste u određenim područjima, odnosno konzultante. Isto tako, vanjske službe ponekad se angažiraju kako bi pomogle u uništavanju dokumentacije koja se nalazi u papirnatom obliku, te na magnetnim ili optičkim medijima a koja nastaje tijekom odvijanja poslovne aktivnosti poduzeća. Iz tog razloga potrebno je da pružatelji takvih usluga predoče certifikate iz kojih je razvidno da su osposobljeni za manipulaciju povjerljivim dokumentima na odgovarajući način. Ovisno o tim certifikatima, poduzeća često traže provjeru poštivanja ugovorenih procedura. Svi ugovori s pružateljima usluga moraju sadržavati klauzulu o privatnosti koja zahtijeva od njih primjenu adekvatnih mjera kako bi se očuvala povjerljivost informacija i kako bi se spriječilo slučajno ili namjerno otkrivanje takvih informacija. Vrlo često od dobavljača i partnera se traži dodatno osiguranje u slučaju otkrivanja povjerljivih informacija ili ukoliko dođe do pravno utemeljenih odštetnih zahtjeva od strane osoba ili poduzeća čija je privatnost povrijeđena.

Strategija informacijske sigurnosti poduzeća ostvaruje se kroz primjenu kontrola pristupa informacijama koje su sadržane unutar informacijskog sustava poduzeća. To je vrlo kompleksna aktivnost koja može biti zaseban predmet vrlo opširnog razmatranja. Ona obuhvaća sve radnje koje se poduzimaju unutar programskog i hardverskog podsustava kako bi se ograničio pristup povjerljivim informacijama unutar sustava i kako bi se pristup odgovarajućim kategorijama podataka dozvolio samo određenim osobama. U ovu skupinu **kontrola** između ostalog pripadaju sljedeće instance (Canzer, 2005, pp. 103,104):

1. Kreiranje kriterija pristupa računalnoj mreži,
2. Kreiranje korisničkih grupa,
3. Kontrola pristupa elektroničkoj pošti,
4. Kontrola pristupa Internet servisima,
5. Kontrola pristupa telefonskom sustavu,
6. Kontrola daljinskog pristupa,
7. Kontrola pristupa preko virtualnih privatnih mreža.

2.1.3. Utjecaj koncepta rizika na informacijsku sigurnost poduzeća

Rizik je stohastički koncept koji opisuje potencijalno negativan utjecaj na poslovanje poduzeća ili neku karakteristiku promjene vrijednosti koja može proizaći iz nekog postojećeg procesa ili budućeg događaja. U svakodnevnoj uporabi, termin rizik se često koristi simultano s mogućnošću poznatog gubitka. Prema tome, rizik je u direktnoj povezanosti s ljudskim očekivanjima. Kod profesionalne procjene rizika, on kombinira vjerojatnost nastanka događaja s time koliki je utjecaj tog događaja na poslovanje poduzeća. Vrlo često u poslovnom kontekstu rizik se može izraziti novčano, dakle bilo kao direktan dodani trošak ili propuštena dobit.

Glavni **cilj** procjene rizika nije samo identificirati sve potencijalne rizike i prijetnje podacima i sigurnosti informacijskog kapitala nego i stvoriti osnovu za konstantno poboljšavanje plana i strategije informacijske sigurnosti s obzirom na najnovije rizike i prijetnje koji proizlaze iz operativnih potreba i činjenice da su informacijski sustavi dinamični te se stalno razvijaju. Po definiciji takav plan nikada nije posve primijenjen budući da se mora stalno dopunjavati. Identificiranje rizika podrazumijeva predviđanje razumnih i predvidivih vanjskih i unutrašnjih opasnosti po informacijski sustav i integritet povjerljivih podataka koji bi mogli rezultirati slučajnim i neautoriziranim otkrivanjem, zlouporabom, promjenom, uništenjem ili nekim drugim načinu kompromitiranja takvih informacija.

Sve moguće rizike informacijske sigurnosti je izrazito teško identificirati. Razvoj tehnologije je dinamična a ne statična kategorija, te se stalno pojavljuju novi rizici koje u trenutku klasifikacije vjerojatno nije niti moguće predvidjeti. Zbog pojave novih rizika i tehnologija za njihovo umanjenje, metodologiju identifikacije i obrade rizika treba stalno iznova provjeravati u periodičkim intervalima (Rogalski, 2013) kako bi se na vrijeme prepoznali i uklonili novi rizici ili makar smanjio njihov utjecaj.

Neki najčešći **rizici** od kompromitiranja podataka i informacijskog kapitala poduzeća su opisani u nastavku.

1. **Pristup povjerljivim informacijama od strane neovlaštene osobe.** Povijesno gledano, kao što su uvijek postojali unutrašnji korisnici informacijskog sustava koji su pokušavali neovlašteno pristupiti informacijama, postojat će i osobe ili organizacije izvan organizacijskog sustava koji će htjeti dobiti neautorizirani pristup informacijama. Razlozi za takav pristup su višestruki, od puke zabave do krađe informacija zbog materijalne koristi ili jednostavno iz malicioznih poriva, kako bi se kompromitirala cjelovitost informacijskog sustava.

2. **Kompromitiranje sistemske sigurnosti kao rezultat pristupa od strane „*hakera*“.**[5] U početku termin „*haker*“ je izazivao poštovanje informatičke zajednice koji se koristio samo između programera, dizajnera sustava i inženjera. (Harvey, 1985) „*Hakeri*“ su kreirali originalne programe koji su rješavali određene probleme. Nažalost, danas se termin koristi za opis ljudi koji neovlašteno pristupaju informacijskim sustavima, uništavaju ili kradu podatke i zaštićene programe te čine ostale destruktivne ili ilegalne zahvate na računalima i mrežama.

3. **Presretanje podataka tijekom transakcije.** Internet je izgrađen kao mješavina distribuiranog i hijerarhijskog sustava: krajnji korisnici poput individualnih osoba ili poduzeća su spojeni na mrežu pružatelja usluga kabelskih veza ili bežično, dok su pružatelji usluga spojeni na veće pružatelje usluga koji se protežu preko više država a oni su pak spojeni između sebe. Posebna računala ili mrežna oprema - usmjernici[6] i *gatewayi*[7] - imaju zadaću pronaći ispravan put kojim će paketi podataka proći i biti proslijeđeni sve dok ne stignu do svog odredišta. Stoga se put podataka od izvora do odredišta naziva rutom podataka. Rute podataka odabiru se ovisno o raspoloživosti mrežnih resursa i opterećenju mreže. One se mogu dinamički mijenjati, ponekad više puta tijekom dana. Iz tog razloga paketi podataka putuju do odredišnog poslužitelja kroz mnoge različite mreže i preko više različitih usmjernika i *gatewaya*. Nakon što paket podataka napusti mrežu pružatelja usluge gotovo je nemoguće predvidjeti njegovu rutu, budući da ona primarno ovisi o odredištu. Ukoliko je odredište isto, ruta do njega se svejedno može promijeniti. Kako bi se mogla pratiti nečija aktivnost na Internetu potrebno je pratiti promet koji ide preko mreže pružatelja usluga. Na taj način funkcioniraju sustavi poput *Carnivorea* (SearchSecurity, 2013) ili *Echelona* (Federation of American Scientists, 2013) unutar Europske Unije.[8] Neke manje države te dosta arapskih država imaju svega nekoliko ili

[5] Po definiciji, hakiranje je neovlašteno korištenje ili pokušaj neovlaštenog korištenja kako bi se zaobišli sigurnosni mehanizmi zaštite informacijskog sustava ili računalne mreže.

[6] U praksi je češće korišten engleski izraz „r*outer"* umjesto hrvatskog, „*usmjernik*“.

[7] Eng. izraz „*gateway*“ u praksi se odnosi na uređaj ili, rječe, na softversku implementaciju uređaja koji predstavlja vezu između dvaju mreža te obavlja potrebne translacije kako bi se postigla interoperabilnost. Budući da za taj izraz ne postoji adekvatan hrvatski prijevod, ovom prigodom koristi se izvorni engleski izraz.

[8] Navedeni sustavi su pod sumnjom kako se nalaze u centru sustava analize cjelokupnog telekomunikacijskog prometa. Sustav *Carnivore* implementiran je 1997., preimenovan u DCS1000 a kasnije zamijenjen komercijalnim sustavom *NarusInsight*. Sustav *Echelon* za nadzor telekomunikacija i dalje se koristi, primarno za nadzor satelitskih i radio komunikacija.

čak jedan jedini glavni podatkovni izlaz iz države, što omogućuje nadzor čitave države ili geografskog područja te je tehnički vrlo jednostavno analizirati promet ili ga čak blokirati. Minimalni zahtjev zaštite od presretanja podataka tijekom transakcije je da su oni šifrirani na hardverskom ili bar softverskoj razini nakon što napuste mrežu štićene organizacije, poduzeća ili pojedinca. Ista se tehnologija mora primijeniti i kada se koristi tehnologija virtualnih privatnih mreža ili daljinskog spajanja korisnika na domicilni informacijski sustav. (Mason, 2002)

4. **Gubitak podataka ili povjerljivosti informacija zbog greške korisnika.** U praksi najčešći razlog zbog kojega dolazi do otkrivanja povjerljivih podataka i informacija je greška korisnika. Priroda i veličina štete ovise o osjetljivosti podataka. Načini na koje može doći do greške korisnika, nenamjerne ili namjerne, su doista mnogobrojni (Aksentijević, 2012, p. 8):

- Korisnik može ostaviti u štampaču papire s povjerljivim informacijama ili se podaci greškom šalju na krivi printer,
- Optički ili drugi memorijski mediji mogu biti poslani na krivu adresu bez da su prije toga obrisani osjetljivi podaci s njih,
- Zbog neadekvatne administracije korisničkih prava korisnik može promijeniti ili obrisati podatke bez da je svjestan kakav je utjecaj takve akcije,
- Nova aplikacija koja vrši dohvat nad postojećim podacima uvodi se u poduzeće, posljedica je da neautorizirane osobe mogu doći u posjed povjerljivih informacija,
- Dokumentacija u papirnatom obliku se baca u smeće bez da je prije toga izrezana u posebnim rezačima papira,
- Pokvarena računala šalju se na servisiranje s podacima koji se još nalaze na njima,
- Informacije se šalju na krivu adresu zbog pogrešnog odabira mail adrese,
- Papirnati dokumenti (npr. ugovori) se šalju na krive adrese,
- *„Cut and paste“*[9] funkcija je korištena kada to nije trebalo.

5. **Fizički gubitak podataka uslijed katastrofe.** Fizički gubitak podataka uslijed prirodne ili čovjekom izazvane katastrofe (npr. požar, poplava, potres, terorističke akcije) može djelomično ili u potpunosti paralizirati poduzeće. Ograničeni događaj, npr. požar u serverskoj sobi ili podatkovnom centru može imati katastrofalne posljedice po informacijsku infrastrukturu poduzeća. Međutim, čak i nenadani događaj izvan poduzeća može rezultirati posljedicama po samo poduzeće, ukoliko poduzeće koristi u potpunosti ili djelomično udaljene poslužitelje za spremanje svojih podataka i servisa, u slučaju katastrofe moguće je da bude pogođena infrastruktura poduzeća iako nije njegova vlastita. Isto se može dogoditi u slučaju posljedica po strujnu mrežu, sustav fiksne telefonije, međunarodne i satelitske veze i mrežu mobilne

[9] „*Izreži i zalijepi*“ (eng. „*cut and paste“)* je funkcionalnost koja omogućuje premještanje objekata korištenjem opcija operativnog sustava računala ili raznih instaliranih aplikacija.

telefonije. Iz tog razloga poduzeća bi trebala poduzeti sve moguće razumne mjere za svođenje ovih rizika na minimum. Mjere koje se poduzimaju obično se definiraju posebnim dokumentom.[10]

6. **Nekompletnost i nedokumentiranost transakcije.** Svaka transakcija koja se odvija unutar informacijskog sustava, osobito ukoliko su uključeni povjerljivi podaci i informacije trebala bi biti dokumentirana, no trebala bi imati i vlasnika koji mora osigurati njenu potpunost i adekvatnu dokumentiranost. Ako transakcija nije dokumentirana, odgovornost je ključnog korisnika osigurati njezinu potpunost i pratiti je do kraja izvršenja. Dokumentacija koja prati transakciju trebala bi biti dovoljno detaljna i morala bi biti procesirana kroz odgovarajuće informacijske i hijerarhijske kanale u poduzeću. Sve možebitno zainteresirane strane morale bi biti upoznate s njenim postojanjem, no posebna pažnja mora se pridati tome da količina informacija bude održana na razumnim razinama kako bi se izbjeglo preopterećivanje zaposlenika irelevantnim informacijama ili informacijama koje im nisu potrebne. Iz tog razloga svi izvještaji i dokumentacija trebali bi biti prezentirani na koncizan i precizan način.

7. **Neautorizirani pristup zaposlenika povjerljivim informacijama.**[11] Pristup podacima i informacijama iz informacijskog sustava ali i papirnatim dokumentima treba biti ograničen na one zaposlenike koji ih moraju znati iz poslovnih razloga. U svakom informacijskom sustavu potrebna je segmentacija elemenata prema vlasniku i svrsi, gdje god je moguće podsustavi moraju biti zaštićeni lozinkama a promjena lozinke mora se vršiti ciklički. Baze podataka koje sadrže osjetljive ili povjerljive informacije moraju biti raspoložive samo rukovodiocima ili ključnim korisnicima na odgovarajućim pozicijama koje moraju biti dokumentirane u Matrici autorizacija i odgovarajućim punomoćima koje mogu biti ili formalne, nakon imenovanja na poziciju ili neformalne. Odjeli zaduženi za informacijske sustave moraju poduzeti razumne i adekvatne akcije kako bi se držali u korak s trenutačnim tehnološkim stupnjem razvijenosti i kako bi osigurali sigurnost informacija u tranzitu, te dostupnost pohranjenih informacija samo onim instancama koje su autorizirane za pristup. To se odnosi na održavanje operativnog sustava, aplikacija, ali i pravovremenu primjenu adekvatnih sigurnosnih zakrpa[12]. Fizički pristup serverskoj sobi te kritičnim dijelovima mrežnog sustava smije biti dozvoljen samo autoriziranim zaposlenicima. O pristupu se mora voditi pisana evidencija.

---

[10] U profesionalnoj terminologiji upravljanja oporavkom nakon katastrofe i kontinuitetom poslovanja ovakav dokument se naziva "*Plan sanacije nakon nastupa katastrofalnog događaja"*.

[11] Dodjela pristupa korisnicima sukladno razinama pristupa, čime se omogućuje pristup podacima i informacijama samo onim korisnicima koji ga trebaju imati predstavlja okosnicu tzv. logičke kontrole pristupa informacijama. Za detalje cf. Nilsen, Odd: „**Protection of Information Assets**", SANS Institute InfoSec Reading Room, SANS Institute, 2002.

[12] Sigurnosna zakrpa je prijevod od eng „*security patch*". Radi se o nadogradnjama programa ili sustava koje omogućuju zaštitu od onih ugroza sustava informacijskog sustava koje su se pojavile od prethodnog izdavanja sigurnosne zakrpe, ili izvorne instalacije nekog programa ili sustava.

8. **Neautorizirani zahtjev osobno, putem telefona ili elektroničke pošte za povjerljivim informacijama.** [13] To je oblik kriminalne aktivnosti kojim je moguće doći do povjerljivih informacija koristeći tehnike socijalnog inženjeringa. (Microsoft, 2013) Obično se radi o pokušajima dolaska do osjetljivih informacija prevarom, predstavljanjem da se radi o povjerenja vrijednim osobama ili poduzećima. Često se lažno traže korisničko ime, lozinka i ostali osobni podaci pod izlikom provjere. Isto tako je moguće da se korisnicima daju lažne Internet poveznice preko kojih je moguće doći do korisničkih podataka.

9. **Neautorizirani pristup preko dokumenata u papirnatom obliku i izvještaja.** Papirnati dokumenti moraju se držati u ormarima ili sefovima koji se zaključavaju. Samo ovlašteni zaposlenici trebaju znati kombinacije šifri i lokaciju ključeva. Papirnati dokumenti ne smiju se bacati u obične kante za smeće, osobito ako nisu izrezani. [14] Tijekom radnog vremena radni dokumenti trebaju biti stavljeni licem prema dolje i trebaju biti pohranjeni u registratorima koji su neprozirni kako bi se izbjeglo slučajno otkrivanje informacija. Radni stolovi i ekrani trebaju biti čisti od sadržaja. [15]

10. **Neautorizirani transfer povjerljivih informacija preko treće strane.**[16] Kako bi se osiguralo od neautoriziranog transfera informacija preko treće strane, potrebno je organizirati barijere fizičkom pristupu. Pritom se primarno misli na naprave protiv provale, kamere, registraciju posjetitelja koji ulaze u poduzeće, praćenje do njihovog odredišta i općenito, fizičku zaštitu perimetra zgrade i prostorija u kojima se obrađuju podaci.

Niti jedan zaposlenik, organizacija ili vanjski entitet ne smije dobiti pristup centralnom informacijskom sustavu koji sadrži povjerljive informacije bez izričite dozvole odgovornih instanci poduzeća. Internim dokumentom potrebno je nominirati sigurnosne funkcije unutar poduzeća.[17] Dozvola pristupa određuje se prema procjeni ključnog korisnika kako određeni zaposlenik treba dobiti pristup informacijama, no pritom je potrebno i da su ispunjeni svi uvjeti iz plana zaštite podataka, ali i zaštita privatnosti osoba na koje se odnose ti podaci, odnosno povjerljivost podataka ukoliko su oni općenite prirode. Nužno je voditi adekvatne evidencije u pisanom i elektroničkom obliku prema važećim procedurama u kojima će biti evidentirano tko je, kada i zašto dobio pristup određenim povjerljivim informacijama. Kopija potpisanih

[13] Ovaj oblik neautoriziranog zahtjeva u praksi se vrlo često naziva svojim engleskim izvornim nazivom – eng. *„phishing“*.
[14] U ovu svrhu koriste se posebni rezači dokumenata (eng. *„shredders*“), koji imaju i mogućnost rezanja disketnih i optičkih medija te spajalica.
[15] Ova politika čest je sastavni dio operativnih uputa informacijske sigurnosti a naziva se politikom čistog ekrana i stola (*eng. „clean desk policy“* i *„clean screen policy“*).
[16] Treća strana su suradnici i dionici poduzeća, ali koji dolaze izvan njegovog okruženja, npr. klijenti, dobavljači, partneri. Ovaj izraz je prijevod eng. „*third party*“.
[17] U korporativnoj praksi, ovakav interni dokument uobičajeno je odluka Uprave ili imenovanje od strane nadležne i ovlaštene osobe, odnosno funkcije.

formulara ove vrste mora biti sadržana u osobnoj arhivi zaposlenika. Ovakve evidencije mogu održavati i ključni korisnici te osoba posebno zadužena za informacijsku sigurnost. [18]

Novi zaposlenici obično ne posjeduju specifična znanja potrebna za održanje i poboljšanje informacijske sigurnosti sustava poduzeća. Iz tog razloga osoba zadužena za informacijsku sigurnost poduzeća bi trebala napraviti plan internog obrazovanja kadrova, odnosno angažirati vanjsku tvrtku ukoliko se za to ukaže potreba. Informacije o obrazovanju zaposlenih vezano uz informacijsku sigurnost su osobito važne u slučaju identificiranih sigurnosnih propusta te kod provođenja unutrašnje ili vanjske revizije.

Svi tiskani materijali koji sadrže povjerljive informacije moraju biti štićeni od uništenja ili gubitka te mogućih katastrofa poput požara, izljeva vode, na način koji je određen od strane odjela za zaštitu na radu i važećih zakonskih propisa. Posebnu pozornost treba posvetiti ograničavanju fizičkog pristupa takvim informacijama korištenjem sustava prepoznavanja korisnika[19], ali i zaključavanjem osjetljivih materijalnih dokumenata te definiranjem liste onih koji imaju ključeve i korištenjem principa selektivne distribucije informacija. Čuvanje dokumenata i osjetljivih podataka dulje od potrebnog roka koji definiraju zakonski propisi[20] ili operativne potrebe poduzeća predstavlja značajan sigurnosni rizik. Zbog prostornog ograničenja, povijesne dokumente moguće je čuvati na udaljenim lokacijama ili za to angažirati poduzeća koja pružaju takve usluge, uz periodičke provjere da li je doista osigura na sigurnost podataka. Ukoliko ne postoje posebni zahtjevi, dokumenti koji sadrže povjerljive informacije trebaju se uništiti najkasnije tri mjeseca nakon što je istekao traženi rok zadržavanja dokumenata. Uništavanje dokumenata je odgovornost ključnih korisnika uključenih u odgovarajuće procese u poduzeću, odnosno vlasnika tih procesa. Sav tiskani materijal koji sadrži povjerljive informacije treba biti uništen kada je istekao rok zadržavanja. Uništavanje se mora izvesti na način da se spriječi neautorizirani pristup povjerljivim informacijama, dakle rezanjem ili paljenjem. Prije predavanja računalne opreme u proces recikliranja ili doniranja rashodovane računalne opreme, odnosno prije redistribucije računalne opreme od jednog

[18] U Republici Hrvatskoj su prema Zakonu o zaštiti osobnih podataka (Narodne novine 106/12) za osobne podatke odgovorni tzv. „*voditelji zbirke podataka*“. Njihov rad nadzire posebno osnovana *Agencija za zaštitu osobnih podataka* (azop). Za detalje cf. **http://www.azop.hr** (03.08.2013.)

[19] Ovi sustavi su u praksi autentikacija korisnika putem korisničkom imena i lozinke, dvije lozinke, dvofaktorska autentikacija ili autentikacija (provjera identiteta) korištenjem biometrijskih značajki, ili kombinacija više navedenih metoda u odgovarajućim točkama pristupa informacijskom sustavu.

[20] Za poduzeća je važno kako su rokovi čuvanja propisani sukladno Zakonu o računovodstvu. Trajno se moraju čuvati godišnji financijski izvještaji, isplatne liste, te analitičke evidencije o plaćama. 11 godina od zadnjeg dana poslovne godine na koju se odnose valja čuvati dnevnik i glavnu knjigu te isprave temeljem kojih su podaci u njih uneseni. 7 godina čuvaju se pomoćne knjige i isprave temeljem kojih su podaci uneseni u njih. 10 godina čuvaju se, u odnosu na početak tijeka zastare, evidencije i isprave o dnevnom gotovinskom prometu te druge poslovne knjige, isprave i evidencije. Za detalje cf. **Zakon o računovodstvu** (Narodne novine 109/07, 54/13) i **Opći porezni zakon** (Narodne novine 147/08, 18/11, 78/12, 136/12, 73/13).

korisnika drugom korisniku, izvorni korisnik treba biti odgovoran za brisanje i snimanje vlastitih sadržaja s tvrdog diska računala.

Povjerljive informacije se ne prikupljaju ukoliko to nije nužno potrebno i relevantno za svrhu za koju se prikupljaju. Ukoliko je moguće, one se moraju prikupljati direktno od izvora informacija a ne iz drugih izvora. U slučaju da to nije moguće, mora se voditi evidencija o tome iz kojih izvora je dobivena povjerljiva informacija. Bitno je istaknuti kako se takve informacije ne smiju prikupljati bez izričite dozvole relevantnih funkcija unutar poduzeća. U svakom slučaju, minimalan zahtjev po ovom pitanju je da kriterij prikupljanja informacija poštuje operativne potrebe i zakonske propise okoline u kojoj poduzeće posluje.

Upravljanje rizikom je, prema tome, **strateški i strukturirani** pristup rukovođenja nesigurnošću kroz procjenu rizika te razvoj strategija za upravljanje nesigurnostima. Te strategije uključuju **transfer** rizika na treće strane, **izbjegavanje** rizika, **smanjenje** negativnog utjecaja rizika te **prihvat** nekih ili svih posljedica određenog rizika. Tradicionalno upravljanje rizikom je fokusirano na rizike koji potječu od fizičkih ili pravnih izvora, dok se upravljanje financijskim rizicima fokusira na rizike koje je moguće umanjiti korištenjem financijskih instrumenata kojima se može trgovati. (Deloitte, 2013) Cilj upravljanja rizicima je smanjivanje ukupne razine rizika do one koju organizacija može prihvatiti.

2.2. ČIMBENICI INFORMACIJSKOG KAPITALA MALIH I SREDNJIH PODUZEĆA

Važnost i složenost ove problematike nameće potrebu da se detaljnije obrade ove tematske jedinice: **1) nastanak i pojam informacijskog kapitala, 2) podaci, informacije i znanje kao sastavnice informacijskog kapitala** i **3) upravljanje informacijskim kapitalom poduzeća**.

2.2.1. Nastanak i pojam informacijskog kapitala

Pojmovi informacijske sigurnosti i informacijskog kapitala čine se naizgled razumljivima na prvi pogled, no njihova međusobna interakcija u postizanju poslovnih ciljeva modernih poduzeća često je zamagljena uslijed utjecaja vrlo kompleksnih poslovnih obrazaca, oblika i alata koji se koriste za osiguravanje informacija i znanja koji postoje u poduzećima. Gotovo svaki zaposlenik koristi jedinstveni skup alata kojima pokušava postići svoje radne zadatke, dok u isto vrijeme način na koji to čini mora biti unutar organizacijskog okvira koji poduzeće postavlja poradi očuvanja informacijskog kapitala putem mjera informacijske sigurnosti. Povrh toga, dodatni problem predstavlja činjenica da je informacijski kapital poduzeća nematerijalnog oblika.

Informacijski kapital *je nematerijalni oblik kapitala čije korištenje u poslovnoj aktivnosti poduzeća djeluje katalitički u proizvodnji dobara i usluga, a reprezentiran je razvrstanim (klasificiranim) informacijama i znanjem pohranjenim u informacijskim i dokumentacijskim sustavima poduzeća*. (Aksentijević, 2010, p. 23) [21]

Prvi korak u uvođenju funkcije informacijske sigurnosti kojom se štiti informacijski kapital je priznavanje ili osvješćivanje činjenice da je poduzeće podložno gubicima (ASIS International, 2013). Poduzeća koja posluju na međunarodnom tržištu kao glavni i najveći ponuđači usluga redovito su pod povećanim rizikom od kompromitiranja informacija te čak i industrijske špijunaže.[22] Metodološki gledano, spoznaju o postojanju problema treba pratiti analiza rizika koja bi trebala identificirati razne opasnosti koje mogu utjecati na informacijski sustav. Osnovni problem na koji se pritom nailazi je problem proračuna, odnosno financiranja aktivnosti vezanih uz informacijsku sigurnost. Pravo pitanje pritom je – Koliko je poduzeće spremno platiti za gubitke koji su prouzrokovani nedostatkom takvog sustava?

Današnje poslovno okruženje postaje sve više neprijateljsko, kompleksno i međuzavisno, kako na domaćem planu tako i globalno. Efikasno upravljanje tim okruženjem postaje **fundamentalni** poslovni zahtjev. Uprava bi trebala očekivati da se u okviru operativnih procesa identificiraju i anticipiraju područja pod pojačanih rizikom i postave koherentne strategije i procedure unutar svih poslovnih funkcija kako bi se smanjili ili uklonili identificirani rizici. (National Research Council of the National Academies, 2003, p. 10) Također, od uprave se očekuje posjedovanje efikasnog odgovora na takve događaje i incidente koji prijete imovini organizacije. Proaktivna strategija uklanjanja rizika na samom kraju procesa daje pozitivan utjecaj na profitabilnost i trebala bi biti dio upravljačke odgovornosti vrhovnog rukovodstva tvrtke.

Vještine i kompetencije nužne za izvođenje aktivne zaštite i mjerljivo efikasnog odgovora na moderne prijetnje iz okoline trebale bi biti strateška orijentacija tvrtke jer su kritičnije nego ikada, a efikasno vođenje s visokih razina upravljanja i povezane sigurnosne funkcije su imperativ poslovanja. Organizacijska reputacija, neprekinuta pouzdanost tehničke infrastrukture i normalno izvođenje poslovnih procesa, zaštita fizičke i financijske imovine, sigurnost zaposlenika i povjerenje zainteresiranih strana se svi u određenoj mjeri naslanjaju na efikasnost rukovoditelja zaduženog za sigurnost.

[21] Izvorna doktorandova definicija

[22] Industrijska špijunaža definira se kao krađa tajnih podataka koji predstavljaju konkurentsku prednost uzimanjem, kopiranjem ili snimanjem povjerljivih ili vrijednih informacija u poduzeću, i to od strane konkurencije. Za detalje cf. Investopedia**, http://www.investopedia.com/terms/i/industrial-espionage.asp** (19.08.2013.)

Tradicionalno, ono što nedostaje je jedna pozicija unutar na vrhu rukovodstva koja bi imala odgovornost za izradu, utjecaj i upravljanje strategijom integralne funkcije zaštite unutar organizacije. U većini poduzeća odgovornost za ovu poslovnu funkciju je raspršena između više rukovoditelja unutar raznih odjela koji često imaju potencijalno konfliktne ciljeve. Široka lepeza rizika danas dolazi u obliku kompleksne matrice međusobno povezanih opasnosti, ranjivosti i utjecaja. Sposobnost utjecaja na poslovnu strategiju i adekvatnog adresiranja svih unutrašnjih i vanjskih rizika stvara potrebu za glavnim rukovoditeljem zaštite[23] na odgovarajućoj razini i fokusiranje napora kroz tu rukovodeću funkciju, uz eliminiranje redundantnih i uskih interesa koji mogu biti prisutni u vertikalnoj strukturi odjela tvrtke.

Ključni **čimbenici uspješnosti** uvođenja mjera informacijske sigurnosti koje je moguće identificirati unutar poduzeća su sljedeći:

1. Sposobnost izgradnje održivih prednosti kroz pragmatična i inovativna sigurnosna rješenja,
2. Demonstracija integriteta funkcije i sposobnost održavanja principa unatoč unutrašnjim i vanjskim pritiscima,
3. Visokokvalitetne analitičke sposobnosti, iskustvo u rukovođenju i izrazite sposobnosti održavanja odnosa sa drugim osobama unutar poduzeća (Norman , 2011, p. 19),
4. Kvalitativno iskustvo u strateškom planiranju i razvoju politika na višoj razini,
5. Sposobnost anticipiranja, utjecanja i pomaganja organizaciji pri procjeni i brzoj prilagodbi promjeni uvjeta poslovanja te internim i eksternim trendovima koji su od odlučujućeg značaja za smjer razvoja poslovanja poduzeća,
6. Efikasnost u komuniciranju preporučenih smjerova akcije za kreiranje inovativnih odgovora na prijetnje,
7. Strast za postizanjem ciljeva izvrsnosti i demonstriranje orijentacije ka uspješnom razvoju osoblja kojim rukovodi.

Ključna **odgovornost** funkcije informacijske sigurnosti je razvoj i primjena strategije koja pokazuje razumijevanje prirode i vjerojatnosti nastupanja katastrofalnih događaja te značajnih događaja koji bi mogli imati negativan utjecaj po informacijsku sigurnost. Strategija mora detaljno opisivati planove prevencije i pripreme nastupa takvih događaja, uključujući edukaciju i metodologiju moderne sigurnosne funkcije. Ta strategija bi također trebala pokriti kontinuitet poslovnih operacija, CISO mora biti sposoban jasno komunicirati strategiju sigurnosti, troškove

[23] U profesionalnom žargonu zaštite poslovnih informacija, najčešće se za ovu funkciju koristi kratica „CISO“ - eng. *Chief Information Security Officer*, glavni rukovoditelj informacijske zaštite. Pandan ovoj funkciji, no više razine, funkcija je „CSO“ – eng. *Chief Security Officer*, zadužena za cjelokupnu, integralnu zaštitnu funkciju poduzeća.

i povezane utjecaje najvišim razinama organizacije, upravi i operativnim grupama zaduženim za provođenje mjera informacijske sigurnosti.

2.2.2. Podaci, informacije i znanje kao sastavnice informacijskog kapitala

Pojmovi podataka, informacija, znanja i informacijskog kapitala u praksi često nisu dovoljno razgraničeni. Kako bi se oni jasno odvojili potrebno je definirati sve navedene pojmove i postaviti njihove međusobne odnose. **Podaci** su simboli koji sami po sebi nemaju značaj niti se mogu koristiti u poslovanju poduzeća.[24] Ono što nedostaje podacima kako bi ih poduzeće moglo koristiti je **poslovni kontekst** kao njihova vrijednosna značajka.

Informacija, za razliku od podatka, pokazuje se korisnom u kontekstu poslovanja poduzeća. Ona je predstavljena organiziranim odnosno strukturiranim podacima koji su obrađeni na način koji je relevantan za određenu svrhu ili kontekst, te stoga ima značenje, vrijednost, korisnost i relevantnost.

Znanje je koncept koji je najteže definirati i obično se definicija znanja naslanja na koncept informacije. Radi se o kombinaciji iskustva, vrijednosti, konteksta i stručnog uvida te utemeljene intuicije koji pružaju okvir i okolinu za procjenu i uključivanje novih iskustava i informacija u poslovnu okolinu poduzeća. U poduzećima, akumulirano se znanje ogleda ne samo u dokumentaciji, obrađenim informacijama pohranjenim u računalnom sustavu, nego i u organizacijskoj rutini, procesima, praksi i normama.[25] Povrh toga, iskustveno je poznato da upravo poduzeća koja imaju najvišu razinu stvorenog znanja i primjene novih tehnika i tehnologija baziranih na znanju postižu iznadprosječne stope rasta. Posebno važan oblik znanja je znanje liderstva koje se često naziva „*poslovnom mudrošću*".

Nakon navedenih definicija, potrebno je objasniti i kakav je odnos informacijskog kapitala prema podacima, informacijama i znanju, a taj odnos prikazan je na shemi 1 na sljedećoj stranici.[26]

[24] Podaci ostaju u svom izvornom stanju sve dok ne poprime korisni oblik. Oni ne moraju biti nužno simboli, to mogu biti i signali ili stimulusi, koji se često definiraju kao *subjektivni* podaci, za razliku od *objektivnih* podataka koji su proizvod opažanja.

[25] Jednim dijelom, znanje akumulirano u poduzeću može se poistovjetiti i s pojmom korporativne kulture poduzeća.

[26] Prikaz navedenih odnosa u obliku piramide poznat je u informacijskoj teoriji kao „*DIKW piramida*", pri čemu je *DIKW* kratica od eng. „*data-information-knowledge-wisdom*" ili „*podaci-informacije-znanje-mudrost*".

Shema 1. Piramida odnosa podataka, informacija, znanja i poslovne strategije

Izvor: prilagodio autor, prema Rowley, Jennifer: **„The wisdom hierarchy: representation of the DIKW hierarchy“**, Journal of Information Science 33, 2007.. p. 166.

Dok su informacije temelj odlučivanja rukovodstva poduzeća, jer odgovaraju na pitanje **kako** se nešto radi, lideri se bave time **zašto** je u poslovnom ozračju nešto tako kako je, što je najbolje učiniti i koji su najbolji mogući potezi u danoj situaciji. Liderstvo u poduzećima posjeduje suptilnu notu „*razumijevanja*“. Iz tog razloga, korištenje podataka, informacija i znanja okrenuto je prema prošlosti dok je korištenje „*poslovne mudrosti*“ okrenuti ka budućnosti.

Samo definiranje informacijskog kapitala poduzeća znači da odgovorni u poduzeću posjeduju svijest kako informacije imaju **intrinzičnu vrijednost** koja se može razmjenjivati između poduzeća i unutar poduzeća. Onaj informacijski kapital koji posve uklanja neizvjesnost o ishodu odlučivanja sačinjavaju **perfektne** (savršene) informacije. (Kirkwood, 1997., p. 27) Neki pak autori smatraju kako je informacijski kapital onaj dio informacija koji čini tzv. **kapital znanja** a koji se može razmjenjivati. (Yokakul, et al., 2011, p. 3) Međutim, identifikacija informacijskog kapitala poduzeća ovisi o poslovnoj strategiji promatranog poduzeća i razlikuje se od poduzeća do poduzeća i od grane do grane. Tako će npr. informacijski kapital koji je od velike važnosti unutar farmaceutske industrije biti posve bezvrijedan nekom poduzeću unutar drvne industrije, ali i nešto što predstavlja informacijski kapital, odnosno akumulirano i obrađeno znanje od važnosti za jedan odjel visokotehnološkog poduzeća bit će neupotrebljivo u poduzeću koje se bavi visokogradnjom. Stoga je potrebno naglasiti i važnost konteksta kao temeljne odrednice vrijednosti informacijskog kapitala.

2.3. CIKLUS UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU MALIH I SREDNJIH PODUZEĆA

Razmatranje ciklusa upravljanja informacijskom sigurnošću nameće potrebu da se detaljnije obradi više povezanih tematskih cjelina, i to: **1) identificiranje informacijskog kapitala i rizika, 2) klasifikacija podataka i informacija, 3) upravljanje životnim ciklusom podataka i informacija** i **4) izrada plana informacijske sigurnosti.**

2.3.1. Identificiranje informacijskog kapitala

Ključni problem koji se postavlja pred lidere poduzeća je – *kako identificirati informacijski kapital?* Računalni sustavi u pravilu pohranjuju podatke, ti podaci, ukoliko se promatraju u odgovarajućem kontekstu predstavljaju informacije a one mogu postati znanje, odnosno informacijski kapital, i to ukoliko pomažu svim rukovodećim razinama da poboljša poslovni rezultat. Međutim, vrlo je teško razgraničiti i identificirati informacijski kapital, a do tada ga je potrebno neovisno o njegovoj trenutačnoj klasifikaciji, štititi ga informacijsko-tehničkim i organizacijskim mjerama. Identificiranje informacijskog kapitala obavlja se u okviru mjera klasifikacije podataka i informacija, a korištenjem metodologije upravljanja životnim ciklusom podataka. Ova se aktivnost obavlja zbog sljedećih razloga: (Tijan, 2009, pp. 557-568)

1. **Postizanje ciljeva izvrsnosti.** Korištenjem informacijskog kapitala, poduzeća poboljšavaju efikasnost kako bi se postigla veća razina produktivnosti i posljedično, profitabilnosti.
2. **Kreiranje novih proizvoda, usluga i poslovnih modela.** Informacijski kapital je izvor kreiranja novih proizvoda i usluga te posve novih poslovnih modela. Poslovni modeli opisuju sustav koji poduzeće koristi za proizvodnju, isporuku i prodaju proizvoda i usluga kako bi zadovoljila potrebe klijenata.
3. **Povezanost s klijentima i dobavljačima.** Stvaranje povoljne klime prema klijentima i dobavljačima produžava i proširuje mogućnost suradnje što općenito rezultira povećanim prihodom i dobiti te smanjuje operativne troškove.
4. **Poboljšano donošenje odluka.** Rukovoditelji prepoznaju značaj prave informacije u pravom trenutku jer često moraju donositi odluke utemeljene na neadekvatnim i nepotpunim informacijama što rezultira lošim odlukama i gubitkom klijenata. Informacijski kapital, klasificiran i uskladišten na strukturiran način, omogućava korištenje stvarnih podataka u realnom vremenu pri donošenju kritičnih odluka.
5. **Komparativna prednost.** Kada se poduzeća orijentiraju na postizanje jednog od poslovnih ciljeva, poput postizanja ciljeva izvrsnosti, novih proizvoda, usluga i poslovnih

modela), moguće je da se već nalaze na određenom stupnju komparativne prednosti u odnosu na konkurenciju. Dodatno korištenje intelektualnog kapitala kako bi proizvod bio kvalitetniji od konkurencije, bio proizveden po nižoj cijeni uz direktno odgovaranje na stvarne potrebe klijenata put je do poslovne uspješnosti.

6. **Dnevne operacije.** Poduzeća investiraju u informacijske sustave i tehnologiju zato što su oni nužni za obavljanje posla, a te investicije diktiraju i granske promjene te se stoga ponekad uvode automatski, bez dubljeg promišljanje, jer konkurencija također uvodi određenu inovaciju baziranu na informacijskom kapitalu pa je minimalno radi održavanja postojeće pozicije potrebno da tu inovaciju uvede svako poduzeće u određenoj poslovnoj grani.

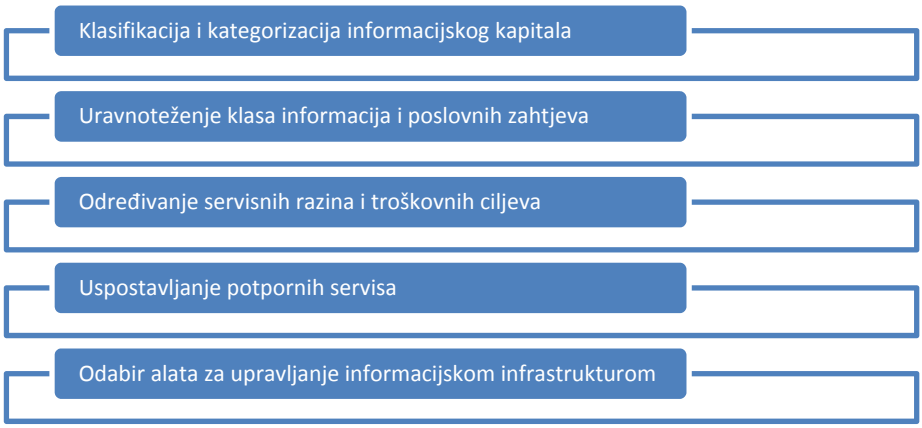
Prema izloženom, može se zaključiti da je informacijski kapital samo onaj **skup podataka, informacija i strukturiranog znanja** koji se koristi unutar poduzeća kao temelj novih oblika organizacije, upravljanja, proizvoda i usluga, a koji poduzećima omogućuje stratešku i komparativnu prednost. Informacijski kapital poduzeća štiti se tehničkim i organizacijskim mjerama organizacijske (integralne) i informacijske sigurnosti te kroz zakonske propise koji reguliraju, u širem opsegu, problematiku informacijske sigurnosti.

2.3.2. Klasificiranje podataka i informacija

Klasifikacija podataka i **upravljanje životnim ciklusom** podataka su dvije međusobno nužno povezane aktivnosti. (Short, 2007, p. 5) Jednom kada su podaci i informacije adekvatno klasificirani, pravila upravljanja podacima mogu biti selektivno primijenjena na različite kategorije podataka i informacija. Pravila klasifikacije podataka ne razlikuju se značajno od pravila klasifikacije objekata u domenskom sustavu gdje se objekti ili korisnici grupiraju i onda se na njih primjenjuje skup specifičnih pravila za tu grupu. Glavni **cilj** klasifikacije je **grupiranje** podataka u klase ili grupe podataka koje imaju slična svojstva te stoga zahtijevaju sličan pristup njihovom upravljanju. (Oracle, 2008) Klasifikacija podataka je zahtjevan i kompleksan zadatak zbog nekoliko temeljnih razloga. Uvođenje sustava klasifikacije podataka odnosi se ne samo na postojeće nego i nove informacije koje mogu postati sastavni dio poslovnog sustava nakon što je on inicijalno uveden. Uslijed zakonskih zahtjeva podaci se često moraju pohranjivati u **nestrukturiranom** obliku, te je stoga izazov ispravno ih klasificirati. Klasifikacija podataka može se odnositi na informacijski kapital poduzeća neovisno o tome koji oblik oni zauzimaju: može se raditi o dokumentima pohranjenim u papirnatom obliku, u digitalnom obliku na centralnim serverima, transakcijskim sustavima, drugim bazama podataka ili distribuirano pohranjenim informacijama. Klasifikacija informacija može se primjenjivati na poruke elektroničke pošte, ili podatke sadržane na prijenosnim ili telefonskim uređajima. Aktivnost klasifikacije informacijskog kapitala poduzeća mora biti sponzorirana od strane samog vrha rukovodstva unutar poduzeća te funkcije upravljanja informatikom. U samom

početku tog procesa potrebno je u njega uključiti sve koji su u mogućnosti doprinijeti razvoju modela. Koraci uvođenja upravljanja životnim ciklusom podataka prikazani su na shemi 2.

Shema 2: Koraci uvođenja upravljanja životnim ciklusom podataka



Izvor: prilagodio autor, prema Tijan, E**.:"Data Classification and Information Lifecycle Management in Port Community Systems",** Pomorstvo, Pomorski fakultet, Rijeka god. 23, br. 2, p.562.

Značajno je lakše dodati nove podatke u postojeći sustav klasifikacije nego primijeniti sustav klasifikacije na već postojeće podatke. Razlog za ovu pojavnost je vrlo jednostavan: nove se informacije mogu jednostavnije klasificirati i pohraniti sukladno postavljenom okviru dok postojeće informacije mogu biti pohranjene na taj način da manipulacija njima nije jednostavna. Razlozi za to mogu biti raznolike strukture baza podataka, raznolikost korištenih poslovnih aplikacija, hardverski ili aplikacijski slojevi ili vlasnici podataka.

Od velike je važnosti postaviti sustav klasifikacije podataka na način da on prati poslovne procese. On mora biti prilagođen formi poslovne organizacije, njenim stvarnim potrebama, ciljevima i osobito sustavu upravljanja kvalitetom. Ishod klasifikacije podataka je uspostavljen sustav koji poduzeću omogućuje ne samo zaštitu informacijskog kapitala, već i konkurentsku prednost koja proizlazi iz sistematskog upravljanja vlastitim znanjem.

Pet ključnih **koraka** u uspostavljanju sustava upravljanja životnim ciklusom podataka su sljedeći: (Tijan, 2009, p. 562)

1. Klasifikacija i/ili kategorizacija informacijskog kapitala,
2. Kreiranje odnosa između poslovnih zahtjeva i funkcija i klasa informacija,
3. Određivanje servisnih razina uključujući kriterije zadržavanja i brisanja informacija, pristupa, te troškovnih ciljeva,

4. Uspostavljanje potpornih servisa razvijanjem horizontalnog presjeka svih postojećih ugovora o razinama usluga[27] kako bi se kreirao katalog standardnih usluga. One npr. mogu uključivati usluge koje omogućavaju 100-postotnu raspoloživost podataka, raspoloživost podataka u vremenu ispod jedne sekunde, pristup informacijama unutar jednog dana po fiksnoj cijeni itd.,
5. Odabir odgovarajućih proizvoda uključujući alate za upravljanje infrastrukturom koji odgovaraju poslovnim zahtjevima poduzeća. Ova faza izvodi se kao logičan nastavak uspostavljanja standardnih razina usluga, procesa upravljanja i potporne infrastrukture.

Zatečeno stanje klasifikacije podataka u poduzećima u kojima se ta aktivnost sustavno ne provodi obično je posljedica hijerarhijskog čuvanja informacija pri čemu su najčešće korišteni kriteriji starost podataka te ostali zakonski postavljeni kriteriji. Podaci se općenito klasificiraju ovisno o zahtjevima koje postavljaju vrijeme raspoloživosti i pristupa te vezani troškovi. Moderna politika upravljanja životnim ciklusom podataka mora uključivati značajno širu perspektivu koju određuju poslovni zahtjevi među kojima se osobito ističu politika životnog ciklusa, upravljanje sadržajem informacija, upravljanje *Intranetom*[28], upravljanje *Ekstranetom*[29], povezanost informacijskog sustava poduzeća s informacijskim sustavima drugih poduzeća, zakonski zahtjevi, rudarenje podataka, te zahtjevi sustava za potporu odlučivanju vrha uprave poduzeća. Krajnji cilj klasifikacije podataka i ulazni signal procesa upravljanja životnog ciklusa podataka je dodjela poslovne vrijednosti različitim kategorijama podataka. To se najbolje može postići u tehnološki visoko razvijenim informacijskim okruženjima u kojima su razine servisnih usluga dobro određene i prevedene u standardnu ponudu informacijskih usluga.

Protivno uvriježenom mišljenju, informacije su **dinamične** prirode i atributi prema kojima se klasificiraju se mijenjaju. To znači da se kretanjem informacija između različitih korisničkih grupa njihovi atributi također mogu mijenjati što rezultira u promjeni klasifikacije. Stoga se potreba za upravljanjem promjenama obično materijalizira u obliku konzistentnog sustava najbolje prakse te implementacije upravljanja informacijskim uslugama, kao što je *ITIL*[30].

[27] Ugovori o razinama usluga je prijevod uvriježenog engleskog izraza u upravljanju poslovnom informatikom – eng. *SLA - „Service Level Agreements"*
[28] *Intranet* poduzeća predstavljen je računalnom mrežom koja koristi standardne Internet tehnologija za dijeljenej informacija, aplikacija, servisa i usluga unutar granica poduzeća.
[29] *Ekstranet* poduzeća (eng. *Extranet*) je računalna mreža koja omogućava kontrolirani i autorizirani pristup iz okoline poduzeća interno raspoloživim resursima, sukladno strogo definiranim poslovnim potrebama. Prema tome, Ekstranet poduzeća su usluge koje su dane znanim dionicima (dobavljači, klijenti). U slučaju da se usluge pružaju nepoznatim dionicima, tada se ne bi radilo o ekstranetu već o b2c informacijskom sustavu, „od poduzeća ka klijentu" (eng. *business to customer*, ili *b2c*).
[30] ITIL je kratica od eng. *Information Technology Infrastructure Library*. Više o ovom skupu najbolje prakse cf. poglavlje 3.3.3. doktorske disertacije.

2.3.3. Upravljanje životnim ciklusom podataka i informacija

Klasifikacija informacijskog kapitala predstavlja temeljni preduvjet za uvođenje koherentnog sustava upravljanja životnim tijekom informacija. Bez klasifikacije podataka ono ne može biti konzistentno. Upravljanje životnim tijekom informacijskog kapitala omogućuje troškovnu efikasnost, optimizaciju kapitalnih i operativnih ulaganja u računalne resurse koji se koriste za spremanje i obradu informacija, poboljšava informacijsku sigurnost i podupire poslovne ciljeve.

Upravljanje životnim ciklusom podataka je u biti održiva **strategija pohrane** podataka koja mora biti prilagođena održavanju balansa između **troška** pohrane podataka i njihove **vrijednosti** za poslovne procese u poduzeću, koja se konstantno mijenja pod utjecajem promjene uvjeta unutar i izvan poduzeća. Prema tome, klasifikacija podataka pruža praktičnu metodologiju za usklađivanje troškova skladištenja informacijskog kapitala poduzeća sukladno prioritetima poslovne politike. Kako bi se uspostavio efikasni sustav klasifikacije podataka, procedure upravljanja promjenama već moraju biti uspostavljene. Moderni informacijski sustavi poduzeća imaju vrlo kompleksnu organizacijsku strukturu i pravovremena uspostava sustava klasifikacije te upravljanja životnim ciklusom informacija prema svim zainteresiranim stranama je kritični čimbenik. Klasifikacija podataka je rijetko statička i mijenja se s korištenjem. (Mogull, 2013) Tijekom odvijanja procesa upravljanja životnim tijekom podataka mijenjaju se i razine usluga.[31] Postoje mnogi uzroci promjena u klasifikaciji informacijskog kapitala poduzeća, a tri od njih su dominantni u velikim sustavima. Često ih uzrokuju vanjski okidači koji mogu ali i ne moraju biti određeni unaprijed, no u svakom slučaju, oni otežavaju klasifikaciju podataka. Mogu se kategorizirati na sljedeći način: (Tijan, 2009, p. 565)

1. **Promjene u klasifikaciji ili servisnoj razini.** Klasifikacija i dogovorene razine usluga ponekad u sebi sadrže unaprijed dogovorene okidače koji mijenjaju klasifikaciju informacija. Osim toga, vremenski tijek kreira aspekte upravljanja koji su vremenski određeni i odnose se na mjesečne cikluse obrade informacija, kvartalne akcije ili obradu podataka krajem godine. To također ima utjecaj na zahtjeve za razinama usluga i trebalo bi biti reprezentirano unutar klasifikacijskog sistema.
2. **Promjena svrhe ili uporabe podataka.** Kako se mijenja način uporabe informacijskog kapitala, tako se informacije mogu klasificirati na različite načine. U velikim poduzećima, tipični scenarij kod kojega se mijenja svrha i način uporabe podataka je primjena modela poslovne inteligencije i migriranje ulaznih podataka iz transakcijskog sustava u sustav skladišta podataka. Isto tako moguće je i da podaci koji su sadržani i arhivirani unutar transakcijskog sustava naknadno postanu kritično važni za poduzeće. Tako npr. podaci o

[31] Zbog potrebe za klasifikacijom podataka koja se može adaptirati i mijenjati koristi se i izraz „*dinamička klasifikacija podataka*."

dobavljačima s kojima više nema poslovnog odnosa mogu u određenoj točki prestati biti relevantni, ali kasnije, nakon što se s tim dobavljačima obnove poslovni odnosi, moguće je da informacije koje su prije bile nevažne opet postanu kritične i važne za poslovanje.

3. **Promjena klasifikacijske taksonomije.** Realistično je očekivati da vanjski događaji poput promjena zakonskih propisa, strukture i organizacije poduzeća i broja uključenih klijenata, promjene u tehnologijama ili poslovnoj strategiji mogu promijeniti temeljnu strukturu klasifikacije informacija. Način na koji je organiziran sustav upravljanja promjenama tijekom razvoja klasifikacijske taksonomije je kritičan za dugovječnost klasifikacije informacijskog kapitala. Veća vjerojatnost promjena indicira veću potrebu za prilagodljivim i fleksibilnim sustavom klasifikacije podataka. Taj proces trebao bi predvidjeti promjene i projekt bi se na početku trebao fokusirati na adaptivnu klasifikaciju koja bi bila prilagođena stvarnim zahtjevima poslovnog sustava i poslovne logike. Korisnici informacijskog kapitala morali bi biti u potpunosti svjesni fundamentalnih promjena u propisima, poslovnoj strategiji i strukturi poduzeća kako bi se osiguralo da je klasifikacijska taksonomija prilagođena poslovnim zahtjevima. Tome pomaže formalni mehanizam odobravanja i nadzora od strane uprave poduzeća kakav je prisutan u okviru mnogih klasičnih sustava upravljanja kvalitetom. Samo takav mehanizam može osigurati da je klasifikacijska taksonomija usklađena i s internim poslovnim zahtjevima i s eksternim čimbenicima.

Taksonomija klasifikacije podataka je temeljni proces koji se sastoji od dodjele vrijednosnog atributa informacijama koje su pohranjene ili u tranzitu. Najčešće korišteni model je razvijen od strane *Bella i LaPadule*[32] i oslanja se na klasični koncept integriteta, raspoloživosti i povjerljivosti. (Bell, 2005, p. 2) Postoje i drugi modeli koji su obično razvijeni u okviru informacijske sigurnosti koji se mogu djelomično ili posve iskoristiti u procesu izrade sustava klasifikacije informacija, kao na primjer: (Tijan, 2009, p. 559)

1. **Graham-Denningov** model. (Huffmire, et al., 2010, p. 30) Može se koristiti kako bi se osiguralo kreiranje i brisanje informacijskih objekata koji će ući u shemu klasifikacije podataka. Koristeći ovaj model osigurava se i dodjeljivanje adekvatnih prava pristupa. Njegova upotreba je od koristi kada se pristup podacima mora osigurati kroz više distribuiranih sustava. Upotreba Graham-Denning modela opisuje i primjenjuje definiciju osnovnih prava kojima se dozvoljava autoriziranim subjektima da izvršavaju sigurnosnu funkciju na objektu. Model ima osam temeljnih prava zaštite koja opisuju (Tijan, 2009, p. 560):

- Kako se sigurno kreira objekt?

[32] Bell-LaPadula model (*BLP*) je model razvijen od strane David Elliott Bella i Leonarda J. LaPadule u svrhu formaliziranja višerazinske sigurnosne politike koju je donijelo američko Ministarstvo obrane. Radi se o matematičkom izrazu stanja informacijske sigurnosti sustava koji je razvijen u okviru njihovog rada u The Mitre Corporation s početkom 1972. godine.

- Kako se sigurno kreira subjekt?
- Kako se sigurno briše objekt?
- Kako se sigurno briše subjekt?
- Kako se osigurava dodjela prava čitanja informacija?
- Kako se osigurava dodjela prava pristupa informacijama?
- Kako se osiguravaju prava brisanja informacija?
- Kako se osiguravaju prava transfera?

Kako bi se osigurala konzistencija, svaki informacijski objekt ima vlasnika s posebnim dodijeljenim pravima i svaki subjekt ima drugog subjekta koji ima posebna prava nad njim.[33] Tipični primjer praktične primjene Graham-Denning modela je razvoj sustava upravljanja dokumentima unutar poduzeća.

1. **Clark-Wilson model integriteta.** (Dollinger, 2004, p. 315) Clark-Wilsonov model pruža osnovu za specifikaciju i analizu politike integriteta baze podataka ili sustava obrade podataka. Taj model formalizira informacijski integritet što se postiže sprečavanjem korupcije podataka iz bilo kojeg razloga (sistemska ili korisnička pogreška ili namjerno činjenje). Politika integriteta koja se koristi u ovom modelu specificira kako treba podatke skladištiti unutar sustava kako bi se održala njihova konzistencija tijekom prolaska kroz sustav i specificira sposobnosti pojedinih elemenata transakcije. Provođenje ovog modela i pravila certifikacije definira podatke i procese koji su osnova za kreiranje politike integriteta. Prema tome, temelj ovog modela je baziran na pojmu transakcije. Bavećі se integritetom transakcije, ovaj model koristi niz operacija koje mijenjaju stanje sustava iz jednog u drugo, s time da u oba slučaja zajednički temelj mora biti konzistentnost sustava. U ovom modelu, certifikacijska i implementacijska tijela su odvojena, što osigurava odvajanje dužnosti.

2. **Biba model integriteta.** (Krause & Tipton, 2005, p. 112) Biba model integriteta razvijen je 1977. godine. [34] U svom formalnom stanju radi se o tranzicijskom sustavu politike računalne sigurnosti koji upisuje skup kontrola pristupa koje su kreirane kako bi se osigurao integritet informacija. Podaci i subjekti grupirani su u hijerarhijskim razinama koji odgovaraju njihovom integritetu. Subjekt ne može mijenjati podatke na razinama koje su više od njega samoga, niti se može mijenjati putem podataka s razine koja je niža od subjektove. Općenito govoreći, očuvanje integriteta podataka za cilj ima prevenciju neautoriziririrane promjene podataka od autoriziranih ili neautoriziranih korisnika informacija i održavanju konzistentnosti

[33] Subjekt s ovakvim specifičnim pravima naziva se „*kontroler više razine*".
[34] Autor ovog modela je Kenneth J. Biba, također zaposlenik The Mitre Corporation. Za više detalja cf. Biba, K. J. "**Integrity Considerations for Secure Computer Systems**", MTR-3153, The Mitre Corporation, April 1977.

podataka. Ovaj sigurnosni model je usmjeren više ka očuvanju integriteta nego povjerljivosti, što je protivno Bell LaPadula modelu koji je orijentiran više ka povjerljivosti i raspoloživosti. U Biba modelu korisnici mogu mijenjati informacije samo na njihovoj istoj razini ili ispod nje, dok sadržaj informacija mogu pregledavati samo ako je na njihovoj ili višoj razini.

3. **Obavezna kontrola pristupa.** (FREE BSD, The Power to Serve, 2013) Obavezna kontrola pristupa je podvrsta kontrole pristupa pomoću koje sustav upravljanja dokumentima, operacijski ili aplikacijski sustav ograničava mogućnost subjekta ili drugog inicijatora za pristupom ili općenito, bilo kojom drugom operacijom na zadanom objektu. U širem smislu, subjekt je obično proces ili nekoliko procesa dok su objekti tehničke prirode i obično su to datoteke, direktoriji, baze podataka ili transakcijski sustavi. Subjekti i objekti imaju dodijeljen skup sigurnosnih atributa. Kada subjekt treba pristupiti određenom objektu, uključeno pravilo autorizacije koje provodi sam sustav provjerava sigurnosne atribute i donosi odluku hoće li pristup biti dozvoljen. Bilo koja operacija od bilo kojeg subjekta na bilo kojem objektu bit će prvo uspoređena sa skupom pravila kako bi se odlučilo je li operacija dozvoljena.[35]

4. **Diskrecijska kontrola pristupa.** (Curphey, 2013) Definira je način ograničavanja pristupa određenim objektima utemeljeno na identitetu subjekta i grupe kojima pripadaju. Kontrole su diskrecijske u tom smislu da subjekt s određenim pravima pristupa može prenijeti ta prava na bilo koji drugi subjekt. Iznimka nastupa kada obavezna kontrola pristupa zabranjuje takav pristup. Diskrecijska kontrola pristupa obično je komplementarni koncept obaveznoj kontroli pristupa (nediskrecijskoj kontroli pristupa). Ponekad se izraz „*diskrecijski*“ koristi kako bi se naglasilo da određeni informacijski sustav nije u potpunosti sukladan pravilima obavezne kontrole pristupa. Međutim, diskrecijska i obavezna kontrola pristupa mogu se međusobno primjenjivati i transferirati unutar istog sustava. U takvom sustavu, diskrecijska kontrola pristupa odnosi se na one kontrole koje subjekti mogu prenositi između sebe dok se obavezna kontrola pristupa odnosi na drugu kategoriju kontrola pristupa koja postavlja ograničenja putem diskrecijskog skupa pravila.

5. **Sigurnost na više razina.** (Samarati & de Capitani di Vimercati, 2007, p. 148) Model sigurnosti na više razina predstavlja primjena kompjutorskog sustava u obradi informacija različite osjetljivosti na različitim sigurnosnim razinama što omogućava istovremeni pristup korisnika koji imaju različite sigurnosne ovlasti i posljedično sprečava korisnike od pristupa informacijama ukoliko nemaju prikladnu razinu autorizacije. Ovakav model sigurnosti omogućava jednostavan pristup manje osjetljivim informacijama od strane osoba koje imaju visoke razine autorizacije i razmjenu informacija s osobama koje imaju niže razine sigurnosne

[35] Ovaj skup pravila obično se naziva *politikom*. Obavezna se kontrola pristupa često koristi kod sustava autorizacije pristupa pojedinim resursima mrežnih ili aplikativnih sustava, npr. kod korištenja *Microsoft Windows Active Directory* sustava administracije kod kojega se ova politika naziva grupnom politikom (eng. *group policy*). Za više detalja cf. tehnička dokumentacija, **http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx** (14.06.2013.)

autorizacije. Nadalje, ovaj model se može iskoristiti za kreiranje „*čistih*“ inačica dokumenata i informacija koje ne sadrže informacije kojima nemaju pristup osobe s nižim razinama autorizacije pristupa.

2.3.4. Planiranje organizacijskih mjera informacijske sigurnosti

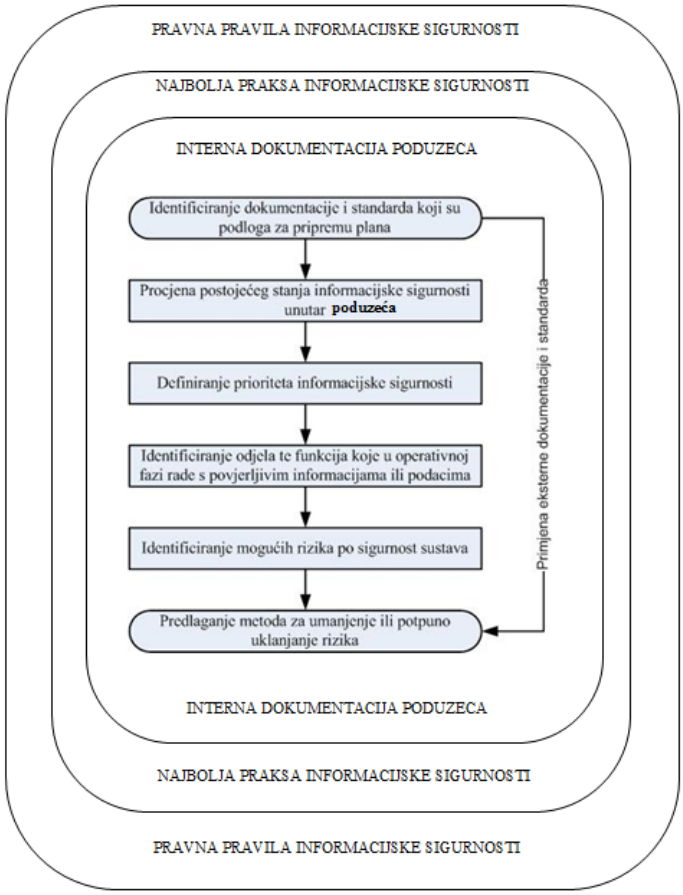
U današnje doba nužno je da uprava poduzeća prepozna važnost upravljanja informacijskom sigurnosti kao odlučujućim čimbenikom odvijanja poslovne aktivnosti. U tom smislu, potrebno je proizvesti niz dokumenata koji će na jasan način definirati generalne kriterije, uloge, rizike, funkcije te odgovornosti za osiguranje sigurnosti informacijskog kapitala i informacija koje se prikupljaju i obrađuju tijekom odvijanja poslovne aktivnosti. Kako bi uprava poduzeća mogla ispuniti ove zadaće, moraju se primijeniti razne sigurnosne procedure koje će zaštititi povjerljivost podataka i informacija i na taj način pridonijeti kontinuitetu odvijanja poslovne aktivnosti.

Osnovni dokument koji definira kritične čimbenike upravljanja informacijskom sigurnošću naziva se plan informacijske sigurnosti. (SANS Institute, 2004, p. 7) Taj plan mora biti prilagođen organizaciji na koju se primjenjuje i stoga može posjedovati različite razine kompleksnosti. U okviru njega se istražuju rizici koji se mogu pojaviti a imaju utjecaj na poslovni sustav te predložiti određene akcije koje se mogu poduzeti kako bi se oni minimizirali ili u potpunosti izbjegli. Plan informacijske sigurnosti razvija se sukladno internoj dokumentaciji organizacije ili poduzeća koja je identificirana kao osnova za pripremu plana i relevantna je za odvijanje poslovnih procesa.

Nakon identifikacije potrebne dokumentacije (standarda, smjernica i sigurnosnih politika) propagiranih s vrha upravljanja poduzećem, definira se metodologija koju se slijedi tijekom izrade plana[36], prikazana na shemi 3 na sljedećoj stranici. (Aksentijević, 2008, p. 91)

[36] Navedena metodologija korištena je kod uspostavljanja sustava upravljanjem informacijskom sigurnošću u poduzeću Saipem Mediteran Usluge d.o.o., Rijeka, a izloženo kao u neobjavljenom završnom radu poslijediplomskog specijalističkog studija „*Inteligentno elektroničko poslovanje*“, Ekonomskog fakulteta u Rijeci, 08.06.2008. godine, kandidata Saše Aksentijevića., pod naslovom „*Integralna zaštitna funkcija unutar poduzeća i sustav upravljanja informacijskom sigurnošću – Saipem Mediteran Usluge d.o.o, R*ijeka“

Shema 3: Koraci pripreme plana informacijske sigurnosti



Izvor: Aksentijević, S.: **"Integralna zaštitna funkcija unutar poduzeća i sustav upravljanja informacijskom sigurnošću – Saipem Mediteran Usluge d.o.o, Rijeka"**, završni rad poslijediplomskog specijalističkog studija, Ekonomski fakultet, Rijeka, 2008, p.91. (neobjavljen)

Plan informacijske sigurnosti ujedno je i centralni dokument koji definira sve aktivnosti vezane uz informacijsku sigurnost u poduzeću. Razlog za izradu plana informacijske sigurnosti[37] je činjenica da poduzeće koje je dio velikog sustava ne može izdavati smjernice odnosno standarde, to može činiti samo središnjica poduzeća, te se iz tog razloga odabire ovaj oblik dokumenta, iako suštinski, operativni plan informacijske sigurnosti predstavlja daleko više od obične radne upute. U dokumentu se inicijalno izlaže jasna izjava o ovisnosti procesa unutar poduzeća o informacijskom kapitalu uskladištenom na razne načine, od papirnate dokumentacije do magnetoptičkih medija, te volja uprave poduzeća za uvođenjem dokumentirane procedure koja će promovirati sigurnosnu funkciju unutar tvrtke.

Plan informacijske sigurnosti definira i njene ključne organizacijske pozicije. Inicijalno se definira potreba za povjerljivošću, raspoloživošću i integritetom informacijskog kapitala u

[37] Plan informacijske sigurnosti može biti izrađen u formi politike, ali i radne upute ili standarda u okviru sustava upravljanja kvalitetom u poduzeću.

poslovnom kontekstu. Nakon toga se izlaže potreba za diseminacijom (širenjem) informacija po principu nužne potrebe te pravila dobrog ponašanja kod obrade informacija i općenito, tretmana informacijskog kapitala. U tom kontekstu definiraju se korištene razine diskrecije (npr. prema Bell-LaPadulla modelu) koje je moguće koristiti kod klasificiranja informacija. Po identificiranju svih rizika, predlažu se modeli za njihovo smanjivanje ili potpuno uklanjanje, među kojima se osobito ističe potreba za stalnim usavršavanjem i edukacijom zaposlenika po pitanju informacijske sigurnosti, postavljanje zahtjeva i provjera izvršenja zahtjeva informacijske sigurnosti prema trećim stranama te izrada odjelnih planova informacijske sigurnosti koje mogu izrađivati ključni korisnici. Na samom kraju identificiraju se ključni korisnici (obično rukovoditelji odjela ili organizacijskih jedinica, odnosno projekata) odgovorni za praćenje i provođenje plana informacijske sigurnosti unutar svojih odjela, odnosno područja odgovornosti, te vrste informacija kojih su oni vlasnici, a koje se smatraju osobito osjetljivim, odnosno povjerljivim.

2.4. KLJUČNI ČIMBENICI USPJEHA I PRETPOSTAVKE USPJEŠNE PRIMJENE MJERA INFORMACIJSKE SIGURNOSTI

Mjerama integralne i informacijske sigurnosti se osiguravaju prikupljanje i procjena informacija koje se tiču širokog raspona događaja vezanih uz sigurnost organizacije i razne operacije koje mogu negativno utjecati na sigurnost zaposlenih te profitabilnost, odnosno reputaciju organizacije. Jedan od ključnih čimbenika uspješne primjene mjera integralne i informacijske sigurnosti je fokusiranost mjera i napora informacijske sigurnosti u jednoj, točno određenoj funkciji u poduzeću. Ona mora biti sposobna na logičan način odrediti mogućnost nastupa incidenata informacijske sigurnosti, te razviti adekvatne preventivne strategije koje su sukladne poslovnoj procjeni i internim kontrolama. Informacije o razvoju te procjene i preventivne strategije mogu doći iz različitih izvora, uključujući podatke uskladištene u samom poduzeću, te vladine organizacije. **CISO** mora biti sposoban povezivati razne informacije koje često potiču iz različitih izvora, te razumjeti njihovu važnost po sigurnost poduzeća. CISO treba poznavati kakve osobine moraju imati ljudi s kojima surađuje te kakva je priroda potrebne tehnološke potpore koja će omogućiti nesmetano odvijanje ovog procesa i posjedovati konceptualno razmišljanje i kritičnu sposobnosti postavljanja rizika po prioritetima, odnosno razvijati adekvatne preventivne strategije kroz čitavu organizaciju. (Glynn, 2012.)

CISO je odgovoran za osiguravanje pripremljenosti poduzeća za mogućnost napada, katastrofalnog događaja ili povezanog sigurnosnog incidenta (prijevara, maliciozne promjene planova i poslovnih procesa, odnosno proizvoda). To uključuje razvoj i administraciju planova

internih treninga i programa. Proces regularnih periodičkih provjera i evaluacija organizacijske spremnosti u slučaju napada ili nastupa nekog sigurnosnog događaja su ključne odgovornosti upravljanja informacijskim kapitalom.

Sljedeća ključna pretpostavka uvođenja mjera informacijske sigurnosti je **analiza** informacija te **koordinacija** aktivnosti s osobama unutar i izvan organizacije na prevenciji napada i katastrofalnih događaja. To implicira sposobnost uspješnog samostalnog rada u matrično organiziranoj okolini podložnoj stalnim promjenama, te zahtijeva visoku toleranciju na različitosti i diplomatsku sposobnost usmjeravanja programa i projekata ka dovršavanju. U okviru ovih mjera, moraju se identificirati i razumjeti priroda sigurnosnih rizika u poslovnom okruženju i primjena odgovarajućih financijskih i rukovodećih kontrola za smanjivanje rizika. Pretpostavka integriranosti sustava informacijske sigurnosti u zaštiti informacijskog kapitala je primjerena koordinacija mjera rukovođenja rizikom, interne revizije, vanjskih resursa, odjela pravnih poslova, odjela rukovođenja ljudskim resursima i ostalih funkcija koje mogu biti uključenje u smanjenje poslovnih rizika i osiguravanje informacijske sigurnosti.

U slučaju nastupa incidenta, napada ili katastrofe, mjere informacijske i integralne sigurnosti su odgovorne za koheziju napora unutar organizacije kako bi se oporavili kritični sustavi i pružila osnova za funkcioniranje organizacije. Njima se mora koordinirati unutrašnje i vanjske resurse kako bi osigurala adekvatna medicinska, financijska ali i emocionalna podršku zaposlenicima, korisnicima usluga i ostalima uključenima u katastrofalni događaj ili napad na poduzeće, te po potrebi vršiti koordinaciju s lokalnim, državnim i međunarodnim agencijama. Primjena mjera informacijske sigurnosti mora biti usmjerena ka koordinaciji s odgovornima za odnose s javnošću i investitorima, financijama, ljudskim resursima, operacijama i odnosima s državnim tijelima.

Ključne aktivnosti uspješne primjene mjera informacijske sigurnosti su sljedeće: (O'Bryan, 2006, p. 2)

1. Interakcija i komunikacija s visokim menadžmentom, upravom i operativnim odborima,
2. Razumijevanje strateških ciljeva poslovne okoline te kako umetnuti potrebe za informacijskom sigurnošću unutar ciljeva organizacije. To podrazumijeva sposobnost uspostavljanja vizije globalnih i individualnih poslovnih sigurnosnih programa te izgradnja podrške za njihovu implementaciju i razvoj,
3. Razumijevanje i ocjenjivanje utjecaja promjena u područjima ekonomije, geopolitike, organizacijskog dizajna i tehnologije, te kako se oni odnose prema potencijalnim rizicima i prijetnjama organizaciji,

4. Osiguravanje da su sigurnosni incidenti i srodna etička pitanja istraženi te riješeni bez daljeg odugovlačenja i prekida odvijanja poslovne aktivnosti i da su poduzete mjere u skladu s temeljnim vrijednostima poduzeća i uvriježenim načinima ponašanja,
5. Korištenje tehnika tradicionalnog i naprednog planiranja u procjeni rizika i prijetnji organizaciji,
6. Razumijevanje uspješne suradnje i razvoja odnosa sa ključnim osobama i osobljem na raznim razinama hijerarhije unutar organizacije,
7. Realističnost i razumijevanje potrebe za procjenom utjecaja bilo kojeg plana ili prijedloga na financije, zaposlenike, klijente i organizaciju u cjelini,
8. Funkcioniranje kao dio integralnog tima starijeg rukovodstva po pitanju planiranja i kapitalnih izdataka,
9. Razvijanje svjesnost o potrebi održavanja funkcije sigurnosti u čitavom poduzeću, u sukladnosti s poslovnim potrebama i kulturom organizacije.

Iz navedenog proizlazi kako je temeljna pretpostavka uvođenja uspješnih mjera informacijske sigurnosti zapravo u **organizacijskom** području, a ne, kako se to obično misli, u tehnološko-informatičkom području.

2.5. SPECIFIČNOSTI SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA

Razlike u organizaciji i provođenju informacijske sigurnosti u velikim u odnosu na mala i srednja poduzeća sistematizirane su u tablici 1. Velike poduzeća su orijentirana na svoju unutrašnju organizaciju prema principu implementacije mjera informacijske sigurnosti kroz sve poslovne funkcije i to najčešće u vertikali ili mrežno, ukoliko se radi o projektnoj organizaciji. U pravilu podatke i informacije za svoje vlastite poslovne funkcije kontroliraju rukovoditelji tih poslovnih funkcija te oni mogu razvijati i odjelne planove sigurnosti informacija koji su sukladni politici informacijske sigurnosti, a sve pod nadzorom i koordinacijom odjela i funkcija zaduženih za provođenje informacijske sigurnosti u poduzećima. Organizacija upravljanja sustavom informacijske sigurnosti u velikim poduzećima je stoga posljedica metodološke procjene rizika koja je primarno orijentirana ka tehničkim mjerama i načinima uklanjanja ili umanjenja nastupa rizika informacijske sigurnosti, a u manjoj mjeri ka procjeni financijskih učinaka ulaganja u informacijsku sigurnost. Ona je stoga nužno posljedica korištenja sustava najbolje prakse jer velika poduzeća zbog kompleksnosti informacijskih sustava moraju koristiti sustave najbolje prakse koji propisuju načine organizacije te poslovne funkcije koji su utemeljeni na isporuci usluga i rukovođenju poslovnom funkcijom informatike koje je

usklađeno s temeljnom poslovnom djelatnošću i poslovnom politikom poduzeća. Velika poduzeća često izdvajaju odjele za upravljanje informacijskom sigurnošću od odjela za upravljanje poslovnom funkcijom informatike, a sve iz razloga izbjegavanja sukoba interesa jer bi u protivnom rukovodstvo poslovne funkcije informatike nadziralo i revidiralo vlastite odluke. (Itillious, 2013) Na čelo takvih odjela obično se imenuju osobe s posebnim ovlastima, a koje su zadužene za donošenje vrhovnih politika, standarda, kriterija, radnih uputa i standardnih operativnih procedura povezanih uz informacijsku sigurnost poduzeća. Temeljne razlike u organizaciji i provođenju informacijske sigurnosti između poduzeća prikazane su u tablici 1.

Tablica 1: Razlike u organizaciji i provođenju informacijske sigurnosti u velikim u odnosu na mala i srednja poduzeća

Velika poduzeća	Mala i srednja poduzeća
Orijentacija na unutrašnju organizaciju, implementacija mjera informacijske sigurnosti kroz sve poslovne funkcije, sukladno procjeni rizika i formalnim zahtjevima najbolje prakse	Orijentacija na tržište (kupce), povećanje prihoda, opstanak i temeljni razvoj
Inkorporiranje upravljanja informacijskom sigurnošću kroz odjel informatike, odjel upravljanja informacijskom sigurnošću i funkciju CISO	Rukovodstvo i vlasnici orijentirani na Paretov princip: informacijska sigurnost se nalazi „izvan prvih 80%"
Izazovi: eksternalizacija, ubrzani ciklus izmjene tehnologije, gubljenje granica interno-eksterno	Izazov: Rukovodstvu nejasan i teško mjerljiv utjecaj IS na poslovne rezultate
Rukovodstvo uključeno u proces informacijske sigurnosti na svim razinama	Nastup svakog incidenta IS može imati direktan utjecaj na opstanak poduzeća

Izvor: priredio autor

Činjenica da se u provođenju informacijske sigurnosti koriste normalizirani sustavi i najbolja praksa utječe na to da je rukovodstvo na svim razinama uključeno u provođenje informacijske sigurnosti, počevši od Uprava, direktora i predstavnika vlasnika koji moraju donositi ključne odluke i biti uključeni u reviziju i analizu sustava upravljanja informacijskom sigurnošću, pa do razine direktora, rukovoditelja sektora ili odjela i srednjeg menadžmenta. Naposljetku, velika su poduzeća postavljena pred izazove **eksternalizacije** čitavih podsustava poslovne informatike uslijed naglog povećanja broja takvih podsustava, njihove kompleksnosti i manjka internih resursa sposobnih raditi na njihovom uvođenju, korištenju i održavanju. Osim toga, uslijed korištenja paradigme računalstva u oblaku te tehnologija poput *BYOD*[38], ubrzano se gube granice perimetara okoline poduzeća i informacijskih sustava samog poduzeća. Velika poduzeća

[38] *BYOD* je kratica od eng. „*Bring Your Own Device*", a odnosi se na politiku dozvole zaposlenicima da u poslovne svrhe koriste vlastita računala, tablete ili pametne telefone, uključujući pristup podacima i aplikacijama poduzeća putem korištenja vlastitih pristupnih uređaja. Najveća penetracija ovog sustava je u Ruskoj Federaciji, Indiji, Ujedinjenim Arapskim Emiratima, Maleziji i Brazilu (oko 75 %), te na Bliskom Istoku (oko 80 %). Više o tome, cf. Ovum's multi-market Q4 2012 BYOD survey, **http://cxounplugged.com/2012/11/ovum_byod_research-findings-released/** (14.08.2013.)

na ovo nisu spremna jer je jedna od osnova tehnološkog provođenja informacijske sigurnosti jasna distinkcija između okoline i unutrašnjosti poduzeća.

Pokretači informacijske sigurnosti u malim i srednjim poduzećima su značajno drugačiji i iako su ciljevi informacijske sigurnosti nazivno isti – radi se o osiguravanju informacijskih sustava i informacija od neovlaštenog pristupa, gubitka povjerljivosti, integriteta i raspoloživosti, te izbjegavanju nastupa sigurnosnih incidenata koji u konačnici rezultiraju financijskim utroškom - mala i srednja poduzeća često nemaju jasno diferencirane poslovne funkcije ili više njih obavlja samo jedna osoba ili funkcija, a ponekad čak niti jasan smjer kretanja što se tiče temeljne poslovne aktivnosti. Mala su poduzeća stoga izrazito orijentirana na tržište odnosno na povećanje broj kupaca i posljedično, povećanje prihoda poduzeća, osobito u samim počecima poslovanja kada su sredstva investirana te je stoga novčani tijek negativan, dok je povrat investicije u samim začecima, odnosno pozitivni novčani tijekovi se još nisu počeli ostvarivati ili su u svojim inicijalnim fazama. Mala i srednja poduzeća, ukoliko se nalaze u fazi rasta, često moraju s ograničenim resursima, kako vremenskim, tako i financijskim i ljudskim, osigurati ostvarenje poslovne vizije vlasnika i rukovoditelja. Prema tome, povećanje prihoda i adekvatno praćenje organskog rasta često su glavni pokretači malih i srednjih poduzeća. (Heggeseth & Lome, 2012, p. 5)

U takvim okolnostima, u kojima su raspoloživi resursi vrlo oskudni, vlasnici i rukovoditelji poduzeća se ponašaju racionalno, te sukladno Paretovom principu koncentriraju svoje napore na način da oni rezultiraju maksimizacijom dobrobiti po poduzeće. Budući da je informacijska sigurnost, pa i sama poslovna informatika rijetko u fokusu interesa poduzeća, a osobito uslijed činjenice da je često nejasna i zamagljena povezanost tih poslovnih funkcija s poslovnim rezultatom poduzeća, rukovoditelji i vlasnici biraju investicije i troškove za koje znaju da rezultiraju povećanjem prihoda, čak i ukoliko to znači prihvaćanje nerazumno visokih razina rizika uslijed mogućeg nastupa incidenata informacijske sigurnosti. Ovo dovodi do problema da samo jedan ozbiljan incident informacijske sigurnosti može imati tako ozbiljne posljedice po malo ili srednje poduzeće, da ono može prestati postojati.

Pokretači malih i srednjih poduzeća po pitanju poslovne funkcije informacijske sisgurnosti se svrstavaju u tri skupine a vezani su uz **prodaju** odnosno povećanje prihoda poduzeća, **prijetnje** koje poduzeću prijete u slučaju nastupa incidenata informacijske sigurnosti te **zahtjeve** koji se pred poduzeće postavljaju iz njegove **okoline**, a da su povezani uz informacijsku sigurnost.

Po pitanju **prodaje**, mala i srednja poduzeća su u obvezi prepoznati zahtjeve i stremljenja klijenata, te može li informacijska sigurnost biti sredstvo konkurentske prednosti kojim će ti zahtjevi biti zadovoljeni, čak i ukoliko se sama poduzeća ne bave informatikom, visokom

tehnologijom ili uslužnim djelatnostima. Osim toga, njihova orijentacija treba biti takva da prepoznaju predstavlja li izostanak mjera informacijske sigurnosti nedostatak, jer uslijed nastupa incidenta informacijske sigurnosti mogu izgubiti postojeće klijente i samim time ostvariti gubitak osiguranog prihoda, ili propustiti nove akvizicije, uslijed čega trebaju takvu situaciju tretirati zasigurno kao trošak propuštene dobiti. Po pitanju prijetnji, radi se o klasičnom nastupu incidenata informacijske sigurnosti koji mogu rezultirati gubicima i troškovima. Njihove posljedice mogu biti blage, u obliku kraćih prekida poslovnih procesa, pa sve do nastupa onih incidenata koji mogu rezultirati značajnim financijskim gubicima.

Kao i kod velikih poduzeća, i kod malih poduzeća prisutna je latentna prijetnja troška gubitka reputacije među dobavljačima, poslovnim partnerima i klijentima. Naposljetku, treća skupina zahtjeva postavljenih pred mala i srednja poduzeća povezana je uz razne formalne zahtjeve. Radi se o zakonskim zahtjevima koji predstavljaju obligatornu zakonsku regulativu države ili država u kojima poduzeće posluje, a koja mora biti zadovoljena kako bi poduzeće bilo sukladno tim zakonskim propisima.

Drugi zahtjevi sukladnosti vezani su uz **profesionalne certifikacije** vezane uz informacijsku sigurnosti, a radi se onim zahtjevima koje poduzeće mora zadovoljiti kako bi uspostavilo i održalo poslovnu suradnju.[39] Naposljetku, skup zahtjeva koji je kod malih i srednjih poduzeća najčešće zanemaren odnosi se na profesionalne sustave i sustave najbolje prakse koji, ukoliko su zadovoljeni, mogu pozitivno utjecati na status poduzeća u poslovnoj utrci u odnosu na ona poduzeća koja takve zahtjeve najbolje prakse ne zadovoljavaju.

Prema tome, moguće je identificirati pokretače, odnosno motivatore malih i srednjih poduzeća u organizaciji i provođenju informacijske sigurnosti koji su prikazani u tablici 2.

Tablica 2: Pokretači (motivatori) malih i srednjih poduzeća u organizaciji i provođenju informacijske sigurnosti

PRODAJA	PRIJETNJE	ZAHTJEVI
zahtjevi klijenata	prekid poslovnih procesa	zakonski zahtjevi
potencijalni gubitak klijenta (propuštanje realizacije)	financijski gubici	zahtjevi sukladnosti
mogućnost nove realizacije	trošak gubitka reputacije	odnos prema konkurenciji

Izvor: priredio autor

[39] npr. Certifikacija za korištenje *POS* (eng. *Point of Sale*) terminala za prodaju usluga, potrebne formalne certifikacije za sudjelovanje u poslovima javne nabave ili certifikacijski zahtjevi vezani uz poslovanje s državom na području razvoja visokotehnoloških informacijsko-sigurnosnih rješenja.

Prema tome, u izgradnji novog modela potrebno je uzeti u obzir **četiri skupa čimbenika** s makro razine:

1. Mala i srednja poduzeća koja već obavljaju poslovnu djelatnost posjeduju stanovitu, već **dostignutu razinu kulture i načina upravljanja** investicijama u informacijsku sigurnost, prema odrednicama objašnjenim anketnim istraživanjem,
2. Velika poduzeća su **lideri u upravljanju** informacijskom sigurnošću, no načini upravljanja tom poslovnim funkcijom nisu direktno primjenjivi u malim i srednjim poduzećima,[40]
3. Mala i srednja poduzeća imaju različite **pokretače** poslovne djelatnosti i upravljanja[41],
4. Mala i srednja poduzeća imaju apsolutno i relativno **manje resurse** na raspolaganju za postizanje ciljeva upravljanja informacijskom sigurnošću od velikih poduzeća.

[40] U velikim poduzećima uobičajen je slijed: 1. proces identifikacije informacijske imovine->2.proces identifikacije prijetnji->3.proces identifikacije rizika->proces primjene mjera otklanjanja rizika.
[41] Cf. tablica 2.

3. NORMIRANJE SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU PODUZEĆA

Normiranje sustava upravljanje informacijskom sigurnošću poduzeća je aktivnost kojom se osigurava sukladnost poslovne funkcije informacijske sigurnosti s pravnim propisima i zahtjevima koje postavljaju profesionalni standardi i sustavi najbolje prakse. U okviru navedenog, u ovoj glavi doktorske disertacije izučavaju se sljedeće cjeline: **1) Pravno reguliranje informacijske sigurnosti u Republici Hrvatskoj 2) Pravno reguliranje informacijske sigurnosti u ostalim državama od značaja za poslovanje hrvatskih poduzeća 3) Primjena smjernica, standarda i najbolje prakse u korištenju sustava upravljanja informacijskom sigurnošću.**

3.1. PRAVNO REGULIRANJE INFORMACIJSKE SIGURNOSTI U REPUBLICI HRVATSKOJ

U Republici Hrvatskoj postoji veći broj zakona i podzakonskih propisa koji reguliraju područje sigurnosti informacijskih sustava. Međutim, ne postoji jedinstveni zakon ili zakonski propis koji bi u cjelokupnosti regulirao to područje. Iz tog razloga, odgovorne osobe u poduzećima moraju se snalaziti u nizu propisa tražeći one koji se odnose direktno na njihovo poslovanje. Najbolje regulirano je područje financijskog sektora, osobito bankarskog i osiguravateljnog. Donošenjem podzakonskih akata temeljem Zakon o informacijskoj sigurnosti pred tijela državne uprave ali i sve ostale organizacije koje imaju pristup povjerljivim državnim podacima postavlja se niz vrlo detaljno opisanih obaveza. Ovaj sadržaj zahtijeva razradu sljedećih tematskih cjelina: **1) Zakon o zaštiti osobnih podataka, 2) Zakon o informacijskoj sigurnosti, 3) Uredbe i pravilnici koji reguliraju rad financijskog sektora i 4) Ostali vezani pravni akti.**

3.1.1. Zakon o zaštiti osobnih podataka

Osnovna zakonska regulativa u Republici Hrvatskoj na temu informacijske sigurnosti je **Zakon o zaštiti osobnih podataka**. (Narodne novine 106., 2012) U temeljnim odredbama tog zakona se definira kako je svrha zaštite osobnih podataka zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Hrvatski je Zakon o zaštiti osobnih podataka usklađen sa direktivom 95/46/EZ Europskog Parlamenta i Vijeća (Official Journal of the European Union 281., 1995) o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom prijenosu takvih podataka[42].

[42] Kod navedene direktive je CE LEX 31995L0046, a donesena je 24. listopada 1995. godine.

Odredbe ovog zakona primjenjuju se na obradu osobnih podataka od strane državnih dijela, tijela lokalne i područne (regionalne) samouprave te pravnih i fizičkih osoba predstavništava i podružnica stranih pravnih osoba i predstavnika stranih pravnih i fizičkih osoba koje obrađuju osobne podatke. Međutim, ovaj se zakon primjenjuje i u slučaju ukoliko voditelj zbirke osobnih podataka nema prebivalište ili sjedište u jednoj od država članica Europske unije, a za potrebe obrade osobnih podataka koristi automatiziranu ili drugu opremu koja se nalazi na području Republike Hrvatske, osim ako tu opremu koristi samo za prijenos osobnih podataka preko teritorija Europske unije, te je u tom slučaju voditelj zbirke osobnih podataka dužan imenovati zastupnika na području Republike Hrvatske koja će ga zastupati u svezi s obradom osobnih podataka. Zakon se primjenjuje na sve zbirke osobnih podataka neovisno o tome jesu li predmet automatske ili ručne obrade podataka, ali se ne primjenjuju na obradu osobnih podataka koju provode fizičke osobe isključivo za osobnu primjenu ili za potrebe kućanstva.

Zakonom se osobito štiti prikupljanje i daljnja obrada osobnih podataka koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život i osobne podatke o kaznenom ili prekršajnom postupku na način da se definiraju iznimke pod kojim uvjetima se ti podaci mogu prikupljati i obrađivati.

Voditelj zbirke podataka za svaku zbirku osobnih podataka koju vodi i uspostavlja mora voditi **evidenciju** koja se sastoji od:

1. Naziva zbirke,
2. Naziva, odnosno osobnog imena voditelja zbirke i njegovog sjedišta, odnosno adrese,
3. Svrhe obrade,
4. Pravnog temelja uspostave zbirke podataka,
5. Kategorije osoba na koje se podaci odnose,
6. Vrste podataka sadržanih u zbirci podataka,
7. Načina prikupljanja i čuvanja podataka,
8. Vremenskog razdoblja čuvanja i uporabe podataka,
9. Osobnog imena, odnosno naziva primatelja zbirke, njegove adrese, odnosno sjedišta,
10. Naznake unošenja, odnosno iznošenja podataka iz Republike Hrvatske s naznakom države. odnosno međunarodne organizacije i inozemnog primatelja osobnih podataka te svrhe za to unošenje, odnosno iznošenje propisano međunarodnih ugovorom, zakonom, ili drugom propisom, odnosno pisanim pristankom osobe na koju se podaci odnose,
11. Naznake poduzetih mjera zaštite osobnih podataka.

Važno je napomenuti kako se u glavi VIII. Zakona[43] detaljno definiraju prava osoba čiji se podaci obrađuju[44], te njihovih zakonskih zastupnika i punomoćnika, definiraju se dužnosti voditelja zbirke podataka po pitanju pružanja informacija o tome koja se vrsta podataka obrađuje i na koji način se te informacije pružaju te kriteriji i način izmjene i brisanja podataka iz zbirke podataka. Za poslove obavljanja nadzora nad obradom osobnih podataka, tim se Zakonom osniva Agencija za zaštitu osobnih podataka koja je samostalna i odgovara Hrvatskom saboru. Osobe koje smatraju da im je obradom podataka povrijeđena privatnost mogu tražiti zaštitu Agencije. U kaznenim odredbama[45] definiraju se kazne za prekršaje iz domene ovog zakona, a koje se kreću u iznosu od 20.000 do 40.000 kuna za voditelje zbirki osobnih podataka i izvršitelje obrade podataka.

3.1.2. Zakon o informacijskoj sigurnosti

Zakon o informacijskoj sigurnosti (Narodne novine 79., 2007) obvezuje sva tijela državne uprave, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima koje u svom djelokrugu koriste klasificirane i neklasificirane podatke, te pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim ili neklasificiranim podacima na provođenje mjera informacijske sigurnosti što uključuje ne samo ulaganje u informacijsku tehnologiju nego i obrazovanje, odnosno imenovanje stručnjaka odgovarajućeg profila, prema tome predviđaju se ne samo tehnološke nego i organizacijske promjene. U osnovnim odredbama Zakona definiraju se pojmovi uglavnom na način koji je sukladan strukovnom i znanstvenom definiranju tih pojmova, a radi se o pojmovima informacijske sigurnosti, mjera informacijske sigurnosti, standardima informacijske sigurnosti, područjima informacijske sigurnosti, i sigurnosnoj akreditaciji informacijskog sustava.

Mjerama i standardima informacijske sigurnosti utvrđuju se minimalni kriteriji zaštite klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama koji su obveznici ovog zakona. Oni se utvrđuju za klasificirane i neklasificirane podatke sukladno stupnju tajnosti, broju, vrsti i ugrozama klasificiranih i neklasificiranih podataka. Mjere i standardi informacijske sigurnosti obuhvaćaju nadzor pristupa i postupanja s klasificiranim podacima, postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka, planiranje mjera prilikom izvanrednih situacija i ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj, odnosno za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.

[43] Glava VIII. – „*Prava ispitanika i zaštita prava"*
[44] Ovo osobe zakon naziva „*ispitanicima*".
[45] Kaznene odredbe nalaze se u glavi X. Zakona o informacijskoj sigurnosti.

Područja informacijske sigurnosti koje predviđa ovaj zakon, a za koja se propisuju mjere i standardi informacijske sigurnosti su:

1. Sigurnosna provjera,
2. Fizička sigurnost,
3. Sigurnost podatka,
4. Sigurnost informacijskog sustava,
5. Sigurnost poslovne suradnje.

U IV. glavi Zakona definiraju se središnja državna tijela zadužena za informacijsku sigurnost. To su:

1. **Ured Vijeća za nacionalnu sigurnost**[46], koji je središnje državno tijelo za informacijsku sigurnost koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija,
2. **Zavod za sigurnost informacijskih sustava**[47], odnosno središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama, obveznicima ovog zakona,
3. **Nacionalni CERT**[48], tj. nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti informacijskih sustava u Republici Hrvatskoj koja je ustrojena u okviru Hrvatske akademske i istraživačke mreže (CARNet)[49], a koji usklađuje postupanja u slučaju nastupa sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalim u Republici Hrvatskoj ili u drugim zemljama i organizacijama povezanim s Republikom Hrvatskom.

CERT i Zavod za sigurnost informacijskih sustava surađuju na prevenciji i zaštiti od računalnih ugroza sigurnosti informacijskih sustava te sudjeluju u izradi preporuka i normi u Republici Hrvatskoj iz područja sigurnosti informacijskih sustava. Ovim zakonom definirana je provedba informacijske sigurnosti te nadzor informacijske sigurnosti. Naime, u slučaju da tijela i pravne osobe nemaju odgovarajuće informatičke i tehničke mogućnosti, mjere i standarde informacijske sigurnosti primijenit će središnje tijelo državne uprave nadležno za razvoj informacijskog sustava, dok u području obrazovnog i akademskog sektora mjere i standarde primjenjuje središnje tijelo državne uprave nadležno za znanost i obrazovanje. Poslove nadzora informacijske sigurnosti koji se sastoje od nadzora organizacije, provedbe i učinkovitosti

[46] Za više detalja cf. **http://www.uvns.hr/** (14.07.2013.)
[47] Za više detalja cf. **http://www.zsis.hr** (14.07.2013.)
[48] Za više detalja cf. **http://www.cert.hr/** (14.07.2013.)
[49] *CARNet* je kratica od eng. *Croatian Academic and Research Network*. Hrvatska akademska i istraživačka mreža je nacionalna istraživačka i obrazovna mreža Republike Hrvatske osnovana 1991.kao projekt Ministarstva znanosti i tehnologije Republike Hrvatske i financirana iz državnog proračuna. Za više detalja cf. **http://www.carnet.hr/** (14.07.2013.)

propisanih mjera i standarda informacijske sigurnosti obavljaju savjetnici za informacijsku sigurnost koji o tome moraju podnijeti izvješće čelniku tijela ili pravne osobe te središnjem državnom tijelu zaduženom za informacijsku sigurnost.

Vlada Republike Hrvatske je donijela Uredbu o mjerama informacijske sigurnosti[50] (Narodne novine 46., 2008) kojom se utvrđuju mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podacima koja se primjenjuje na ista tijela, pravne i fizičke osobe kao i Zakon o informacijskoj sigurnosti.

Ovom Uredbom definiraju se:

1. Mjere informacijske sigurnosti za područje sigurnosne provjere,
2. Mjere informacijske sigurnosti za područje fizičke sigurnosti,
3. Mjere informacijske sigurnosti za područje sigurnosti podataka,
4. Mjere informacijske sigurnosti za područje sigurnosti informacijskog sustava,
5. Mjere informacijske sigurnosti za područje sigurnosti poslovne suradnje,
6. Upravljanje rizikom informacijske sigurnosti, i
7. Nadzor mjera i standarda informacijske sigurnosti.

Naposljetku, temeljem Uredbe o mjerama informacijske sigurnosti, donesen je niz pravilnika od kojih je Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost (Narodne novine 30., 2011) jedini objavljen u Narodnim novinama, dok su svi ostali označeni oznakom „Neklasificirano“, te se stoga koriste u službene svrhe i ne objavljuju se u Narodnim novinama. Pravilnikom o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost[51] utvrđeni se kriteriji i uvjeti za raspored na radno mjesto savjetnika. Odredbama ovog Pravilnika, državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima koja u svom djelokrugu stvaraju ili koriste klasificirane podatke dužna su ustrojiti radno mjesto savjetnika, sukladno kriterijima navedenim u tom Pravilniku. Uredbom se dodatno definiraju uvjeti za raspored na radno mjesto savjetnika, odgovornost i poslovi savjetnika, te nadzor mjera i standarda informacijske sigurnosti.

Pravilnici koji nisu objavljeni u Narodnim novinama, s datumom donošenja, su sljedeći:

1. Pravilnik o standardima sigurnosne provjere (Ured Vijeća za nacionalnu sigurnost, ožujak 2011., Neklasificirano),

[50] Temeljem članka 7. Zakona o informacijskoj sigurnosti (Narodne novine 79., 2007.)
[51] U nastavku odlomka, „*Pravilnik“*

2. Pravilnik o standardima fizičke sigurnosti (Ured Vijeća za nacionalnu sigurnost, ožujak 2011., Neklasificirano),
3. Pravilnik o standardima sigurnosti podataka (Ured Vijeća za nacionalnu sigurnost, svibanj 2011., Neklasificirano),
4. Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava (Ured Vijeća za nacionalnu sigurnost, svibanj 2008, Neklasificirano),
5. Pravilnik o standardima sigurnosti poslovne suradnje (Ured Vijeća za nacionalnu sigurnost, svibanj 2008, Neklasificirano)

3.1.3. Uredbe i pravilnici koji reguliraju rad financijskog sektora

Cilj djelovanja Bazelskog komiteta za nadzor banaka[52] je svrha stvaranje internacionalnog standarda koji nacionalni zakonodavci mogu koristiti pri kreiranju zakonske regulative koja definira koliko kapitala treba biti izdvojeno u obavezne rezerve kako bi se pokrili financijski i operativni rizici banaka. **Basel II** je drugi od bazelskih sporazuma, inicijalno izdan 2004. godine, a njegov je temeljni cilj kreiranje međunarodnog standarda koji bi trebao otkloniti mogućnost da preuzimanje većih razina neutemeljenog bankovnog rizika postane načinom tržišnog natjecanja. (Bank for International Settlements, 2005) Aktualna verzija bazelskih standarda je **Basel III** koji je dogovoren tijekom 2010. i 2011. godine s nakanom implementacije u periodu od 2013. do 2015. godine, no naknadno je njihova implementacija odgođena do 2019. godine. (Bank for International Settlements, 2011)

Svrha primjene ovog internacionalnog standarda je zaštita financijskih institucija od problema koji bi mogli nastati ukoliko jedna banka ili niz banaka ode u stečaj kroz postavljanje zahtjeva za upravljanje kapitalom i rizikom na način da banke posjeduju adekvatan kapital kako bi se zaštitile tijekom cijelog procesa posuđivanja novca i, odvojeno, investiranja. Logično, čim je veći rizik kojemu je banka izložena, veća je količina pričuvnog kapitala koji banka mora zadržati kako bi osigurala solventnost[53] i općenitu ekonomsku stabilnost.

Hrvatski zakonodavac u **Zakonu o bankama** (Narodne novine 84., 2002) definira i operativni rizik koji proizlazi iz neadekvatnog upravljanja informatičkim i pridruženim tehnologijama. Hrvatska Narodna Banka izdala je **Smjernice za upravljanje informacijskim sustavom** u cilju smanjenja operativnog rizika u ožujku 2006. u kojima vrlo detaljno propisuje načine na koje je moguće implementirati upravljanje informacijskom sigurnošću banke, čime je dala do znanja da

[52] eng. *Basel Committee*, za detalje cf. Bank for International Settlements, http://www.bis.org/bcbs/about.htm (14.08.2013.)
[53] Pojam protivan solventnosti banke je njena insolventnost koja se definira kao negativna vrijednost banke kada su obveze iznad vrijednosti njezine imovine. Za detalje cf. Hefferna, S.: „**Modern Banking in Theory and Practice**“, John Wiley&Sons Ltd., Chicester 1996, p.165.

se većina operativnog rizika nalazi u radu informacijskih sustava, te da su mjere zaštite informacija najbolji način umanjenja tog rizika.

Temeljna **poglavlja** koja razmatra taj dokument su sljedeća:

1. Temeljna načela sigurnosti informacijskog sustava te elementi upravljanja rizikom,
2. Upravljanje informacijskim sustavom,
3. Upravljanje rizikom informacijskog sustava,
4. Unutarnja revizija,
5. Sigurnost informacijskog sustava,
6. Održavanje informacijskog sustava,
7. Planiranje kontinuiteta poslovanja,
8. Razvoj sustava i eksternalizacija,
9. E-bankarstvo, rizici i upravljanje rizicima,
10. Zaključci i preporuke.

Temeljem Smjernica, Hrvatska Narodna Banka izdala je i **Odluku o primjerenom upravljanju informacijskim sustavom** (Narodne novine 80., 2007), u kojemu se uz provedbene rokove definira i obveza provođenja onoga što je u Smjernicama naznačeno.

3.1.4. Ostali vezani pravni akti

Prema preporuci Hrvatske agencije za zaštitu podataka Vlada Republike Hrvatske je donijela **Uredbu o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka**. (Narodne novine 139., 2004) Tom se uredbom propisuje niz mjera koje su sukladne zahtjevima norme ISO 17799, odnosno ISO 27002[54], te aneksu A standarda ISO 27001. Važan iskorak prema prihvaćanju standardizacije napravljen je pozivanjem na sam standard unutar uredbe.

Ovom Uredbom propisuju se:

1. Obveza uporabe uređaja za neprekidno napajanje (UPS)[55],
2. Korištenje modemskih priključaka za pristup sustavu,
3. Smještanje, postavljanje i ugradnja računala i računalne mreže,
4. Način priključenja računala i ostale informatičke opreme,

[54] ISO/IEC 27002 je standard informacijske sigurnosti naslovljen s eng. „Information technology – Security Techniques – Code of practice for information security managament“. Razvijen je iz britanskog standarda BS7799 te pruža smjernice najbolje prakse u započinjanju, implementaciji i održavanju sustava upravljanja informacijskom sigurnošću. Za detalje cf.
http://www.iso.org/iso/catalogue_detail?csnumber=50297 (12.08.2013.)

[55] UPS je kratica od eng. *„Uninterruptible Power Supply*“. Radi se o uređajima koji nadomještaju funkciju prekinutog izvora vanjskog električnog napajanja a koji su uobičajeni u serverskim sobama.

5. Način osiguranja posebnih kategorija osobnih podataka,
6. Pristup prostorijama s računalnom i telekomunikacijskom opremom,
7. Pristup podacima pohranjenim u sustavu,
8. Fizički pristup aplikacijama, računalima i telekomunikacijskom sustavu,
9. Obveza uporabe jedinstvenih korisničkih imena i lozinki,
10. Evidencija i praćenje neovlaštenih pokušaja pristupa,
11. Obveza pohranjivanja zapisa,
12. Sustav kriptološkog osiguranja podataka,
13. Tjedne, mjesečne i godišnje provjere funkcioniranja sustava,
14. Mjere zaštite od požara,
15. Mjere zaštite od električnog i magnetskog polja; ionizirajućeg zračenja; elektrostatičkog elektriciteta; vlage, hladnoće i topline; nagrizajućih i lakohlapljivih tekućina, eksplozivnih sredstava i sličnih tvari; prašine,
16. Mjere zaštite u slučaju potresa ili drugih elementarnih nepogoda, rata i neposredne ratne opasnosti,
17. Obveza pohranjivanja podataka (dnevno, tjedno, mjesečno i godišnje),
18. Ovlasti za provedbu pohranjivanja podataka,
19. Udaljenost spremanja pohranjenih podataka,
20. Mjesto i opremu za pohranu sigurnosnih kopija,
21. Način prenošenja medija s pohranjenim zbirkama,
22. Provjeru ispravnosti sigurnosnih kopija,
23. Vremenske razmake provjere kakvoće medija,
24. Osobe ovlaštene za izradu sigurnosnih kopija i povrat podataka,
25. Osobe ovlaštene za iznošenje i unošenje prenosivih informatičkih medija i dodjeljivanje korisničkih imena i propusnica,
26. Kriptološko osiguranje posebnih kategorija osobnih podataka u prijenosu informatičkim i telekomunikacijskim sustavom; ovjeru podataka koji se prenose; provjeru izvornosti; provjeru utvrđenih mjera, postupaka i osoba ovlaštenih za osiguranje, pohranjivanje i zaštitu sustava,
27. Održavanje i popravak opreme sustava.

U **Zakonu o osiguranju** (Narodne novine 151., 2005) neizravno se propisuje potreba za sustavom upravljanja informacijskom sigurnošću, ali se i direktno nominiraju obveze i odgovornosti po pitanju zaštite podataka te njihove privatnosti koje se odnose na zaposlenike osiguravajućih društava, njihove dioničare te povezane osobe. Postavlja se i zahtjev obavljanja unutarnje revizije sigurnosti informacijskog sustava te se taj proces stavlja u direktan odnos s umanjivanjem rizika poslovanja osiguravajućih društava. U **Pravilniku o detaljnom obliku i**

najmanjem opsegu te sadržaju revizorskog prijedloga i revizorskog izvješća s obzirom na specifičnosti poslova osiguranja i reosiguranja (Narodne novine 119., 2009) naglasak je stavljen na upravljanje svim vrstama rizika, detaljno je naznačeno da izvješće mora obuhvatiti i kvalitetu informacijskog sustava osiguravajućeg društva te politiku i organizaciju sigurnosti i zaštite informacijskog sustava, odnosno primjerenost vanjskih, sistemskih i ostalih kontrola.

Zakon o zaštiti na radu (Narodne novine 143., 2012) propisuje samoizvođenje evakuacijskih vježbi najmanje svake dvije godine, te propisuje da sve pravne osobe moraju pravovremeno planirati i poduzimati mjere po pitanju planiranja otklanjanja posljedica katastrofa. Još jednom valja dodati kako se financijske institucije i banke nalaze izvan definicije[56] prema broju zaposlenih, prihoda i bilance, odnosno financijske institucije i banke se ne nalaze u obuhvatu navedene definicije.

Povezano uz odnose Republike Hrvatske s Europskom unijom i tretman informacijske sigurnosti tijekom odvijanja tih odnosa, značajna su još **dva dokumenta**:

1. Zakon o potvrđivanju ugovora između Republike Hrvatske i Europske unije o sigurnosnim postupcima za razmjenu tajnih podataka (Međunarodni ugovori 9., 2006)
2. Memorandum o razumijevanju između Republike Hrvatske i europske zajednice o sudjelovanju Republike Hrvatske u programu Zajednice o interoperabilnom pružanju europskih prekograničnih elektroničkih usluga javne vlasti javnim upravama, poduzetnicima i građanima (IDABC)[57] (Međunarodni ugovori 2., 2007)

3.2. PRAVNO REGULIRANJE INFORMACIJSKE SIGURNOSTI U OSTALIM DRŽAVAMA OD ZNAČAJA ZA POSLOVANJE HRVATSKIH PODUZEĆA

Mala i srednja poduzeća u Republici Hrvatskoj obavljaju svoju poslovnu djelatnost u stanovitim relacijama i interakcijama u odnosu na svoje referentno okruženje, a prema u nastavku izloženom, osobito prema nekim trgovinskim i strateškim partnerima koji pripadaju odgovarajućim geopolitičkim i ekonomskim područjima. Iz tog razloga, u ovom poglavlju izučavaju se sljedeće cjeline s obzirom na pravno reguliranje informacijske sigurnosti u njima: **1) Europska unija 2) Sjedinjene Američke Države 3) Zemlje jugoistočne Europe.**

[56] Odnosno, izvan predmetne klasifikacije.

[57] IDABC je kratica od eng. *„Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens"*. Navedeni je program dovršen 2009. godine. Za detalje cf. *EIF* - European Interoperability Framework for pan-European eGovernment services, **http://ec.europa.eu/idabc/en/document/2319/5644.html** (14.07.2013.)

3.2.1. Europska unija

Pravno reguliranje informacijske sigurnosti u Europskoj uniji izvodi se iz i odnosi na koncept jedinstvenog **europskog informacijskog prostora**.[58] Radi se o inicijativi koju je započela Europska komisija još 2005. godine, čiji je cilj pružanje širokopojasnih komunikacijskih usluga u okviru regulatornog okvira koji je tržišno orijentiran. Jedinstveni europski informacijski prostor omogućuje institucijama, pružateljima usluga i građanima suradnju ili korištenje raspoloživih podataka bez tehničkih ograničenja. Taj je prostor utemeljen na istraživačkoj viziji informacijsko-komunikacijskih tehnologija usmjerenoj ka:

1. Vezi u realnom vremenu između heterogenih informacijskih resursa,
2. Omogućavanju pretraživanja sistema bez ograničenja,
3. Omogućavanju multidisciplinarnog pristupa i dijeljenja podataka neovisno o granicama.

Ova je inicijativa zaživjela do 2010. godine te je bila logičan nastavak razvoja tehničkih, informacijskih i zakonskih zahtjeva postavljenih pred dionike koji su zaduženi za upravljanje informacijskom imovinom. Razvoj ovog procesa prikazan je na shemi 4. Još od razvoja prvotnih sustava upravljanja informacijama tijekom 2. svjetskog rata pa do početka 70-tih godina prošlog stoljeća postojala je klasična podjela informacija na one koje su javno dostupne i one, počesto strateškog, vojnog ili politekonomskog značaja koje su tajne. Takvim su informacijama uglavnom upravljala tijela koja su za to zadužena od strane države. Povećanjem broja obrađivanih podataka po bilo kojoj osnovi u državnim tijelima, ali i poduzećima, a sve uslijed jakog razvoja uslužnog sektora, od početka 80-tih godina prošlog stoljeća te osobito s adaptiranjem modernih informacijsko-telekomunikacijskih tehnologija u svakodnevno poslovanje (prvo u uredsko poslovanje i industrijsku proizvodnju, a zatim i u svim granama i na svim razinama nacionalnih industrija), dolazi do pojave informacijskog prostora kao novog entiteta. U sljedećih 10-15 godina, do 90-tih godina, u okviru informacijskog društva egzistira podjela, odnosno jasno razgraničenje **informacijskih domena** na (grafički prikaz na shemi 4.):

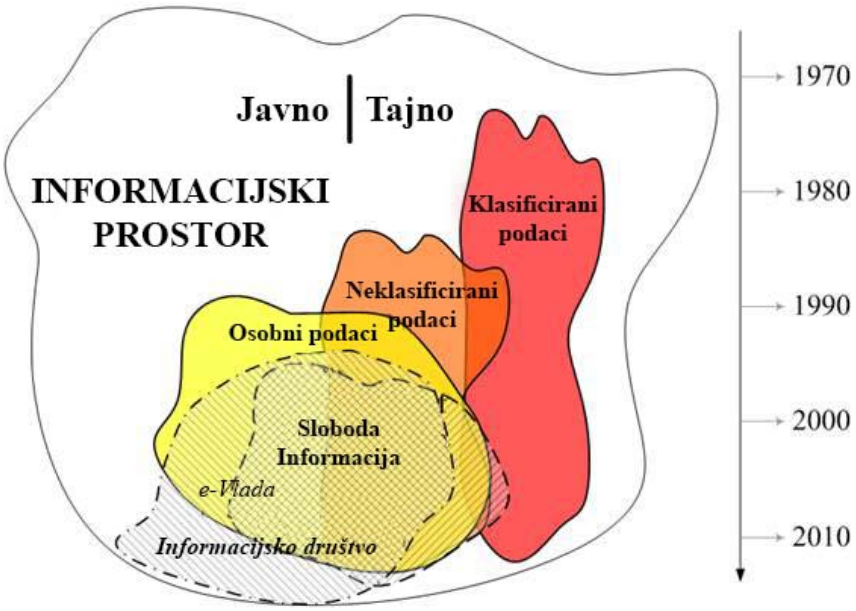
1. **Klasificirane** informacijske domene, karakterizirane tajnošću, čiji su nositelji pravne osobe iz domene vlasti i vojske a glavni im je čimbenik povjerljivost obrađenih informacija,
2. **Neklasificirane** informacijske domene čiji su nositelji pravne osobe, a karakterizirane su privatnošću kao glavnim zahtjevom kontrole,
3. **Domene osobnih podataka**, čiji su nositelji fizičke osobe a karakterizirane su privatnošću kao glavnim kontrolnim zahtjevom,

[58] SISE je kratica od eng. „*Single Information Space in Europe*“. Za specifične akcije i ciljeve SISE programa, cf. EUbusiness - Single European Information Space, **http://www.eubusiness.com/topics/internet/i2010** (14.11.2012.)

4. **Javne informacijske domene**, koje sadrže informacije čije otkrivanje nije dobrodošlo ali ono ne rezultira negativnim rezultatima.

Od kraja devedesetih godina, djelomično uslijed razvoja Interneta kao platforme pogodne za implementaciju novih tehnološko-organizacijskih obrazaca, ali i zbog same količine i prirode prikupljenih podataka u bazama raznih nosioca, došlo je do promjene ove vrste razgraničenja informacijskih domena korištenjem koncepata slobode informacija, te otvorenih vlada (*e-Government*)[59], koje vode u smjeru stvaranja **informacijskog društva**. (Hai, 2007, p. 14) No, valja pritom uočiti kako neovisno o ovom procesu i dalje egzistira potreba za zaštitom informacija od neovlaštenog pristupa, korištenja, umanjenja raspoloživosti, povjerljivosti ili njihovog integriteta. Svi napori Europske unije po pitanju informacijske sigurnosti zapravo su usmjereni ka naizgled suprotstavljenim ciljevima: omogućiti sigurnost informacija, ali i neometan pristup njima od strane svih kojima informacije sadržane u bazama podataka mogu biti od koristi u istraživačke, znanstvene, ekonomske ili privatne svrhe.

Shema 4: Prikaz povijesnog razvoja paradigme informacijske sigurnosti u Europi



Izvor: prilagodio autor prema prezentaciji Klaić, A.: **„EU's information security expectations“**, konferencija infosecweek, Zagreb, 14-18. svibanj 2007., p.5. (neobjavljeno)

Paradigma razvoja informacijskog društva u Europskoj uniji nužno uključuje korištenje privatne informacijske i telekomunikacijske infrastrukture u svrhu razvoja *e-Government* sustava, a posve logična posljedica te činjenice su dodatni izazovi koji se postavljaju pred dionike:

[59] e-Vlada (eng. *e-Government*) predstavljena je digitalnom interakcijom između vlasti i građana, ali i poslovnog sektora, zaposlenika te unutar same vlade i vladinih agencija.

osigurati informacije, sustave i usluge koji mogu biti povjerljive prirode, a koji se, pak, služe privatnim resursima za svoju pohranu i eksploataciju. Prema tome, dobrim dijelom se pravno reguliranje informacijske sigurnosti poduzeća koja posluju u Europskoj uniji oslanja, odnosno izvodi iz načina na koji se razvijala tehnička, organizacijska i logička infrastruktura paradigme *e-Government* u Europskoj uniji.

U **eksplicitnu** legislativu spadaju sljedeće direktive Europske unije:

1. Odluka Vijeća Europe 92/242/EEC u području sigurnosti informacija (Official Journal of the European Union 123., 1992)
2. Rezolucija Vijeća Europe o zajedničkom pristupu i specifičnim akcijama u području sigurnosti mreža i informacija (Official Journal of the European Union 43., 2002)
3. Direktiva 95/46/EC o zaštiti osoba s obzirom na obradu osobnih podataka i slobodno kretanje takvih podataka (Official Journal of the European Union 281., 1995)
4. Direktiva o zaštiti telekomunikacijskih podataka 97/66/EC (Official Journal of the European Union 24., 1998)
5. Direktiva 2002/58/EC o privatnosti i elektroničkim komunikacijama (Official Journal of the European Union 201., 2002)
6. Direktiva o zadržavanju podataka 2006/24/EC (Official Journal of the European Union 105., 2006)
7. Objava Vijeća o mjerama protiv spama (COM (2004) 28 final) (Commission of the European Communities, 2004.)
8. Rezolucija Vijeća 2000/C 293/02 o organizaciji i upravljanju Internetom (Official Journal of the European Union 43., 2000)
9. Odluka Europskog parlamenta i Odluka Vijeća Europe 854/2005/EC o promociji sigurnijeg korištenja Interneta (Official Journal of the European Union 149., 2005)
10. Odluka 1151/2003/EC o borbi protiv ilegalnog i štetnog sadržaja na globalnim mrežama (Official Journal of The European Union 162., 2003)
11. Program "*Safer Internet Programme*" (Europe's Information Society Thematic Portal, 2013)

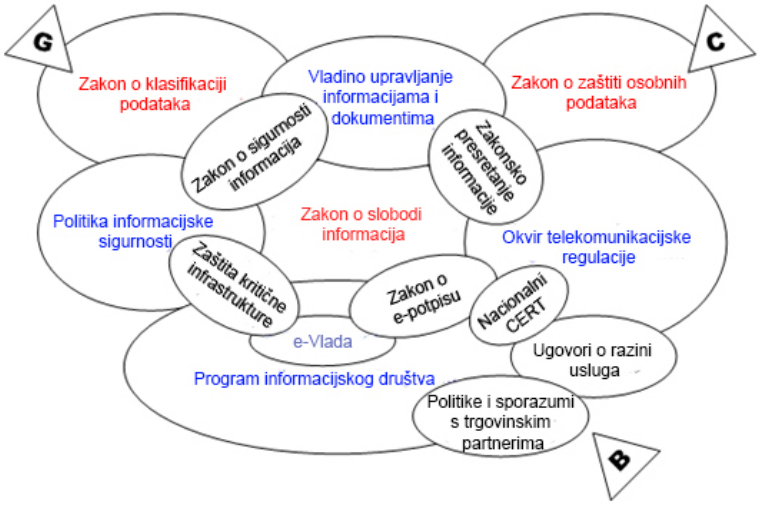
U Europskoj uniji, regulacija područja informacijske sigurnosti ostvaruje se eksplicitnim **zakonskim zahtjevima** te implicitnim **regulatornim zahtjevima**. Eksplicitni zakonski zahtjevi mogu se podijeliti na općenite zakonske zahtjeve (npr. one koji postoje u okviru nacionalnih zakonodavstava poput zakona o zaštiti podataka i sl.), te na specifične zakonske zahtjeve poput

Sarbanes-Oxley zakona i sl. Osim toga, postoje i specifične vezane direktive koje države-pristupnice moraju poštovati prije pristupanja Europskoj uniji. [60]

Implicitni zahtjevi, odnosno zahtjevi sigurnosnih politika, drugi su oblik formalnih zahtjeva koji se postavljaju u području informacijske sigurnosti. Primjer takvih politika su npr. sigurnosna politika 2001/264/EC (Official Journal of the European Communities 101., 2011), inicijative stručne zajednice (npr. i2010-COM(2005)229) (Commission of the European Communities, 2005) te specifični sektorski zahtjevi između kojih su najznačajniji sustavi u financijskoj zajednici poznati kao Basel II i Basel III.

Kompleknost i međudjelovanje svih navedenih zahtjeva prikazuje shema 5. Iz te sheme je vidljivo kako se u centru interesa regulacije nalazi zapravo – sloboda korištenja informacija, reprezentirana s „*Freedom of access to information*“, sukladno direktivi 2003/4/EC (Official Journal of the European Union 41., 2003) prema kojoj je jedan od zahtjeva *e-Vlade* u državama članicama slobodan pristup javnosti podacima koje čuvaju i obrađuju tijela pojedinih država. Dionici u opisanom postupku su vlade i tijela država[61], privatne (fizičke) osobe[62] te poduzeća i poslovni subjekti.[63]

Shema 5: Grafički prikaz kompleksnosti domena i zahtjeva informacijske sigurnosti u Europskoj uniji



Izvor: priredio autor

[60] Ovakav primjer je direktiva 1999/93/EC koja definira zajednički okvir za primjenu elektroničkog potpisa. Za detalje cf. **„Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures**“, Official Journal of the European Union 13., 19.01.2000.
[61] Reprezentirani u gornjem lijevom kutu slovom „G“ – kratica od eng. „*government*“
[62] Reprezentirane u gornjem desnom kutu slovom „C“ – kratica od eng. „*customers*“
[63] Reprezentirani u donjem desnom kutu slovom „B“ – kratica od eng. „*business*“

Iz sheme 5. vidljivo je kako zakoni djelomično reguliraju područje informacijske sigurnosti u domenama koje se odnose na državne informacijske sustave, dok je situacija slična u odnosu na građane, odnosno fizičke osobe, na koje se odnose skupovi zakona vezanih uz zaštitu osobnih podataka. Međutim, u slučaju poduzeća i poslovnog sektora, u pravilu ne postoje specifični zakoni koji bi bili orijentirani ka informacijskoj sigurnosti sustava u tom segmentu. Poslovni se sektor stoga u tu svrhu koristi **ugovorima** o razinama usluga[64], ugovorima i **politikama** odnosa s poslovnim partnerima, zakonom koji regulira korištenje elektroničkih potpisa, dok se za sigurnost dijela infrastrukture koriste uslugama nacionalnog CERT-a.

Glavno tijelo Europske unije s ulogom poboljšanja sigurnosti mreža i informacija u Europskoj uniji je agencija[65] ENISA[66], kreirana 2004. godine, sa sjedištem u Heraklionu na otoku Kreti u Grčkoj. ENISA je osnovana kako bi poboljšala funkcioniranje unutrašnjeg tržišta Europske unije, te je centar ekspertize informacijske sigurnosti zemalja članica, i posljedično, poslovne zajednice, te mora konstantno pomagati u ispunjavanju zahtjeva postojećih, ali i novih zakona i propisa vezanih uz informacijsku sigurnost. Izvorno, ENISA je formirana sukladno Uredbi Europske komisije Br. 460/2004, (Official Journal of the European Union 77., 2004) mandat joj je produžen Uredbom Br. 1007/2008, (Official Journal of the European Union 293., 2008) a poslijednja Uredba kojom se regulira funkcioniranje ENISE je Uredba Br. 526/2013. (Official Journal of the European Union 165., 2013), kojom se ukida prethodna Uredba iz 2004. godine.

3.2.2. Sjedinjene Američke Države

Između 2000. i 2002. godine u Sjedinjenim Američkim Državama došlo je do otkrivanja većeg broja korporacijskih skandala i prijevara među kojima su najpoznatiji bili skandali vezani uz poslovanje i korporativno upravljanje korporacijama Enron, WorldCom i Tyco.[67] Kumulativno, pad vrijednosti tih tvrtki po otkrivanju skandala iznosio je oko pola trilijuna američkih dolara. Analiza kompleksnog načina na koji je došlo do tih prijevara dovela je do donošenja **Sarbanes-Oxley** zakona. (University of Cincinnati, College of Law, 2002) Nedostatak odgovarajućih kontrolnih mehanizama, sukob interesa prisutan kod velikih revizorskih tvrtki koje su

[64] Ugovori o razinama usluga poznati su i kao *SLA* – kratica od eng. *„Service Level Agreements"*.
[65] Europska unija ima više od 30 agencija u različitim državama. Europske agencije imaju važnu ulogu u implementiranju politika Europske unije, a osobito kada su u implementiranje politika uključeni zadaci tehničke, znanstvene, operativne ili regulatorne prirode. Ovakav način funkcioniranja oslobađa druge institucije Europske unije, a osobito Europsku komisiju od operativnih zadaća i omogućuje koncentraciju na izradu politika. Europske agencije podržavaju kooperaciju Europske unije i nacionalnih vlada koncentriranjem tehničke i specijalističke ekspertize iz nacionalnih institucija i same Europske unije. Decentralizirane su agencije nezavisni pravni entiteti, odvojeni od institucija Europske unije poput Vijeća, Parlamenta ili Komisije.
[66] ENISA je kratica od eng. *„European Netwok and Information Security Agency*".
[67] Za detalje oko ovog skandala cf. Forbes, **http://www.forbes.com/2002/07/01/0701topnews.html** (01.06.2013.)

istovremeno nastupale kao konzultanti i revizori koji bi trebali dati nezavisno mišljenje i tako dati investitorima adekvatne cjenovno osjetljive informacije, praksa hvaljenja nekih tehnoloških dionica od strane menadžera investicijskih fondova koji bi ih zatim potiho prodavali, nesposobnost uprava da razumiju i shvate sve poslovne procese i koriste svoja ovlaštenja, tretiranje opcija i dionica kao vaninstitucionalnog načina kompenzacije menadžerima te sve veći pritisak na uprave poduzeća da produciraju opipljivu dobit u točno određenom iznosu vidljivu u financijskim izvješćima dovela je do korporacijskih skandala, prijevara, falsificiranja financijskih izvješća i krize, primarno u sektoru informatičkih tehnologija, a onda u manjoj mjeri i na cjelokupnom financijskom tržištu.

Puni naziv Sarbanes-Oxley zakona je „*Public Company Accounting Reform and Investor Protection Act of 2002*“, (Addison-Hewitt Associates, B2B Consultancy, 2002)[68]. Zakon postavlja nove i poboljšava postojeće standarde za poslovanje svih računovodstvenih tvrtki i američkih dioničkih društava, no ne odnosi se na tvrtke koje se nalaze u privatnom vlasništvu. Po tom zakonu osnovane su i nove, djelomično javne agencije koje nadziru, reguliraju, vrše inspekciju te kažnjavaju računovodstvene i konzultantske tvrtke koje revidiraju financijska izvješća javnih dioničkih društava.

Utjecaj ovog zakona na tvrtke koje kotiraju na američkih burzama ovisi o tome kakav je stupanj regulatorne kontrole u njihovim domicilnim državama. Utjecaj Sarbanes-Oxley zakona na tvrtke čije je sjedište u državama s labavom legislativom je pozitivan i nadilazi novčana sredstva koja je potrebno uložiti u implementiranje dodatnih kontrola. Američka komisija za nadzor financijskih tržišta definira da je metodologija za postizanje sukladnosti sa Sarbanes-Oxley zakonom – **COSO**[69]. COSO predstavlja zajedničku definiciju internih kontrola, standarda i kriterija prema kojima poduzeća mogu procijeniti vlastite kontrolne sustave, izdan je 1985. godine i predstavlja inicijativu privatnog sektora. COSO definira pet glavnih komponenti internih kontrola koje pomažu podržati zahtjeve koje postavlja zakon Sarbanes-Oxley. (Committee of sponsoring organizations of the Treadway Commission, 2013) Tih pet područja i njihov utjecaj na odjele informatičke podrške su sljedeći:

1) **Procjena rizika**. Prije nego što su primijenjene potrebne kontrole, rukovoditelji informatičkog sektora moraju procijeniti i shvatiti područja rizika koja utječu na kompletnost i ispravnost financijskih izvješća. Stoga se mora utvrditi kako se koriste sustavi poduzeća i koja

[68] U prijevodu, naziv ovog zakona je „*Reforma računovodstva javnih dioničkih društava i zakon o zaštiti investitora iz 2002 godine*“. Sarbanes-Oxley zakon je obvezujući za sva poduzeća i organizacije neovisno o veličini. Za razmatranje informacijske sigurnosti, važno je postizanje sukladnosti sa njegovim člancima broj 302, 401, 404, 409 i 802.

[69] skraćenica od eng. *„Committee of Sponsoring Organizations of the Treadway Commission.“*

je razina točnosti trenutačno postojeće dokumentacije. Područja identificiranog rizika definiraju preostale četiri komponente COSO radnog okvira.

2) **Kontrolna okolina**. Ona utječe na svijest potrebe za kontrolom koju bi trebali imati svi zaposleni u poduzeću i predstavlja osnovu svih drugih komponenti interne kontrole pružajući potrebnu strukturu. Čimbenici kontrolne okoline uključuju integritet, etičke vrijednosti i znanja te sposobnosti zaposlenih, filozofiju uprave te operativni stil, odnosno način na koji uprava dodjeljuje odgovornosti i autoritet upravljanja te organizira i razvija ljudske resurse.

3) **Kontrolne aktivnosti.** To su politike i procedure koje osiguravaju da će upute uprave biti izvršene. One pomažu osigurati poduzimanje potrebnih akcija kako bi se smanjili rizici ostvarenja ciljeva organizacije. Pojavljuju se u cijeloj organizaciji, na svim razinama i funkcijama te uključuju niz aktivnosti u koja spadaju autorizacije, provjere operativnih procedura, sigurnosti imovine te podjele dužnosti. U informatičkom okruženju, kontrolne aktivnosti tipično uključuju opće kontrole, poput kontrola pristupa programima, promjenama programa i zahvatima na računalnim sustavima.

4) **Nadzor.** Proces i raspored revizije trebaju biti razvijeni na način da primarno smanjuju područja visokog rizika unutar informacijskih sustava. Zaposleni u informatičkim odjelima trebali bi često činiti interni nadzor, no nadzori i revizije trebaju biti vršeni i od strane vanjskih revizora po rasporedu koji odgovara razinama percipiranog rizika. Za rezultate takvih revizija uprava mora imati jasnu odgovornost.

5) **Informiranje i komuniciranje**. Bez pravovremenih i točnih informacija, rukovoditelji informatičkih službi teško mogu proaktivno identificirati i pratiti područja rizika. Moguć je i izostanak reakcije na novonastale probleme. Rukovoditelji moraju pokazati razumijevanje svih mjera koje je potrebno poduzeti da bi se bilo u sukladnosti sa Sarbanes-Oxley zahtjevima i načinima postizanja te sukladnosti. Značajan izvor kontrola informacijske sigurnosti predstavljaju i informacijsko-sigurnosni standardi američke federalne vlade.[70] Prema posebnoj publikaciji NIST-a, **SP800-53** (NIST, 2013), u posljednjoj, četvrtoj reviziji tog dokumenta navodi se 18 glavnih kontrola informacijske sigurnosti. Ove kontrole prikazane su u tablici 3.

Tablica 3: Kontrole informacijske sigurnosti prema publikaciji SP800-53 revizija 4

Redni broj.	Kratica kontrole informacijske sigurnosti	Naziv kontrole informacijske sigurnosti
1.	AC	Kontrola pristupa
2.	AT	Trening i osvješćivanje informacijske sigurnosti
3.	AU	Revizija i odgovornost za informacijsku sigurnost
4.	CA	Certifikacija, akreditacija i procjena informacijske sigurnosti
5.	CM	Upravljanje konfiguracijom
6.	CP	Planiranje rezervnih informacijskih resursa
7.	IA	Identifikacija i autentikacija

[70] eng. *„U.S. Federal Government information security standards"*

8.	IR	Odgovor na incidente informacijske sigurnosti
9.	MA	Održavanje
10.	MP	Zaštita nosioca podataka
11.	PE	Fizička zaštita i zaštita okoline
12.	PL	Planiranje
13.	PS	Sigurnost osoblja
14.	RA	Procjena rizika
15.	SA	Nabava sustava i usluga
16.	SC	Zaštita sustava i komunikacija
17.	SI	Integritet sustava i informacija
18.	PM	Upravljanje programom informacijske sigurnosti

Izvor: prilagodio autor prema U.S. Department of Commerce**: „Recommended Security Controls for Federal Information Systems and Organizations – NIST Special Publication 800-53“**, National Institute of Standards and Technology, Gaithersburg, kolovoz 2009.

Prema uputama američkog ministarstva obrane 8500.2 (Department of Defense, 2003), moguće je identificirati osam različitih područja osiguranja informacija[71], a njihove kontrole se u jeziku tih uputa nazivaju kontrolama osiguranja informacija. Popis tih osam kontrola prikazuje tablica 4.

Tablica 4: Područja osiguranja informacija američkog ministarstva obrane

Redni broj.	**Kratica kontrole informacijske sigurnosti**	**Naziv kontrole informacijske sigurnosti**
1.	DC	Dizajn sigurnosti i konfiguracija informacijskog sustava
2.	IA	Identifikacija i autentikacija
3.	EC	Enklave i računalno okruženje
4.	EB	Zaštita granice enklave
5.	PE	Fizička zaštita i zaštita okruženja
6.	PR	(zaštita) osoblja
7.	CO	(osiguranje) kontinuiteta (informacijskih usluga)
8.	VI	Ranjivosti i upravljanje sigurnosnim incidentima

Izvor: prilagodio autor prema **„Instruction Number 8500.2: Information Assurance (IA) Implementation“**, Department of Defense, Sjedinjene Američke Države, 6.2.2003.

Interesantno je kako ova uputa definira pojam koji inače nije uvriježen u upravljanju informacijskom sigurnošću, a to je pojam **informacijske enklave**. Ona se definira[72] kao zbirka računalnih okruženja koja je povezana s jednom ili više unutarnjih mreža koje se nalaze pod kontrolom istog tijela i iste politike informacijske sigurnosti, uključivo sigurnost osoba i fizičku sigurnost. Prema tome, unutar informacijskih enklava postoje zajedničke potrebe za informacijskom sigurnošću. U okviru informacijskih enklava štite se granice vlastitog sustava, detektiraju incidenti informacijske sigurnosti, upravlja informacijskom sigurnošću i odgovorom

[71] eng. *„Information Assurance Areas“*
[72] Definicijase nalazi u točki E2.1.17.2 predmetne upute.

na incidente informacijske sigurnosti, te se korisnicima pružaju uobičajene informatičke usluga poput uredskih aplikacija, poslovnih informacijskih sustava ili elektroničke pošte.

3.2.3. Zemlje jugoistočne Europe

U okviru ovog poglavlja, razmotrit će se oni zakonski propisi država okruženja u okviru kojih se tretira područje informacijske sigurnosti, a osobito s obzirom na sigurnost informacija. Način na koji države iz okruženja tretiraju područje informacijske sigurnosti važan je za mala i srednja poduzeća u Republici Hrvatskoj. Prema raspoloživim podacima, Bosna i Hercegovina je drugi najveći hrvatski izvozni partner, Srbija šesti, Crna Gora deseti a Makedonija dvadeset i treći. Na strani uvoza, Bosna i Hercegovina je osmi, Srbija šesnaesti, a Crna Gora dvadeset i deveti te trideseti najveći partneri. (Hrvatska gospodarska komora, 2013, pp. 66,67) Navedeni podaci impliciraju kako između Republike Hrvatske i zemalja jugoistočne Europe koje su tvorile SFRJ postoji značajan opseg ekonomske aktivnosti, a uzme li se u obzir kako mala i srednja poduzeća sudjeluju u kreiranju točno pola bruto nacionalnog proizvoda i zapošljavaju točno dvije trećine zaposlenih u Republici Hrvatskoj (CEPOR - Centar za politiku razvoja malih i srednjih poduzeća i poduzetništva, 2012), jasno je kako je tretman područja informacijske sigurnosti u tim poduzećima od velikog značaja i za partnere iz Republike Hrvatske, i obrnuto. Unutar Europske unije postoji princip u odnosu na informacijsku sigurnost prema kojemu se uzima da druge države članice imaju minimalno istu dostignutu razinu informacijske sigurnosti kao neka referentna država ili višu: takvo implicitno davanje vjere omogućuje da kod razmjene informacija koje Republika Hrvatska daje na korištenje drugim državama razina dostignute informacijske sigurnosti bude ista ili bolja nego u Republici Hrvatskoj. Kao što će se pokazati u nastavku, u drugim odabranim državama jugoistočne Europe situacija nije takva i iako postoje zakonski propisi koji tretiraju ovu problematiku, zakonodavni okvir nije toliko razvijen kao u državama Europske unije te samim time ne pruža jednaku razinu zaštite poslovnih informacija malim i srednjim poduzećima koje posluju u tim državama kao što je to u Republici Hrvatskoj ili ostalim državama Europske unije.

U Bosni i Hercegovini, moguće je identificirati kako je temeljni zakonski propis koji tretira područje informacijske sigurnosti **Zakon o zaštiti ličnih podataka** (Službeni glasnik BiH 49., 2006) . Cilj ovog Zakona je[73] da se na teritoriji države svim osobama neovisno o državljanstvu ili prebivalištu osigura zaštita ljudskih prava i osnovnih sloboda a osobito pravo na tajnost u pogledu obrade osobnih podataka koji se na njih odnose. Ovim se Zakonom osniva i **Agencija za zaštitu ličnih podataka**[74] u Bosni i Hercegovini te utvrđuju njena nadležnost, organizacija i

[73] Prema čl. 1.
[74] Za detalje cf. Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, **http://www.azlp.gov.ba/** (19.08.2013.)

upravljanje. Opseg ovog Zakona čine osobni podaci koje obrađuju javna tijela, fizičke i pravne osobe, osim u slučaju obrade fizičkih osoba isključivo u privatne svrhe. Na ovaj zakonski propis oslanjaju se i četiri sljedeća pravilnika, te jedna uredba:

1. Pravilnik o načinu vođenja i obrascu evidencije o zbirkama ličnih podataka (Službeni glasnik BiH 52., 2009),
2. Pravilnik o načinu čuvanja i posebnim mjerama tehničke zaštite ličnih podataka (Službeni glasnik BiH 67., 2009),
3. Pravilnik o inspekcijskom nadzoru u oblasti zaštite ličnih podataka (Službeni glasnik BiH 51., 2009),
4. Pravilnik o postupku po prigovoru nosioca podataka u Agenciji za zaštitu ličnih podataka u Bosni i Hercegovini (Službeni glasnik BiH 51., 2009),
5. Instrukcija o načinu provjere obrade ličnih podataka prije uspostavljanja zbirke ličnih podataka (Službeni glasnik BiH 76., 2009).

Donošenjem ovog Zakona Bosna i Hercegovina pridružila se većini zemalja svijeta koje u svom zakonskom sustavu posjeduju usporediv zakon.

U Republici Srbiji, u **Krivičnom Zakoniku** Republike Srbije (Službeni glasnik Republike Srbije 85.,88., 2005., ispr. 107/2005., 72/2009., 111/2009., 121/2012.) nalazi se čitav niz članaka zakona koji se odnose na informacijsku sigurnost, i to u slučaju objave informacija putem novina ili drugih sredstava javnog informiranja[75],vezano uz elektronske informacije o autorskom i srodnim pravima [76], te vezano uz terorističke činove i uništenje infrastrukture uključivo informacijske sustave[77]. U uvodnim odredbama osobito se definiraju računalni podatak, mreža, sistem, program i virus, što znači da zakonodavac prepoznaje temeljne pojmove i neke ugroze informacijskih sustava. Osim toga, prepoznat je oblik krivičnog djela „*Iskorišćivanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu*“[78] i neovlaštenog iskorištavanja autorskog djela ili predmeta srodnog prava[79]. U glavi dvadeset i sedmoj naslovljenoj „*Krivična dela protiv bezbednosti računarskih podataka*“, prepoznaju se oblici krivičnih djela „*Oštećenje računarskih podataka i programa*“[80], „*Računarska sabotaža*“,[81] „*Pravljenje i unošenje računarskih virusa*“[82], „*Računarska prevara*“[83], „*Neovlašćeni pristup zaštićenom računaru,*

[75] Prema čl. 38.-40.
[76] Prema čl. 200.
[77] Prema čl. 391.
[78] Prema čl. 185a i 185b.
[79] Prema čl. 199.
[80] Prema čl. 298.
[81] Prema čl. 299.
[82] Prema čl. 300.
[83] Prema čl. 301.

računarskoj mreži i elektronskoj obradi podataka"[84], „*Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži*"[85], „*Neovlašćeno korišćenje računara ili računarske mreže*"[86] te „*Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka*"[87]. Iz navedenog je

jasno kako je zakonodavac posljednjim promjenama Krivičnog zakona[88] prepoznao nove oblike kaznenih djela te ih uvrstio u Krivični zakon.

Zakon o telekomunikacijama (Službeni glasnik Republike Srbije 44., 2003) definira[89] kako je za kontrolu nad obavljanjem djelatnosti u oblasti telekomunikacija i nad korištenjem radiofrekvencijskog spektra zadužena Republička agencija za telekomunikacije[90], uključivo sigurnost informacija. Agencija može izmijeniti uvjete iz koncesije za javne telekomunikacijske mreže i javne telekomunikacijske usluge ukoliko to zahtijeva javni interes, kao što su potrebe obrane zemlje, državne i javne sigurnosti i sl.[91] Zakon vrlo detaljno obrađuje tematiku privatnosti i sigurnosti informacija[92] po pitanju obaveza javnih telekomunikacijskih operatera o čuvanju informacija o sadržaju, činjenicama i uvjetima prijenosa poruka, te zakonske obaveze po pitanju tehničkih uvjeta za podsustave, uređaje, opremu i instalacije za zakonom ovlašteni nadzor nekih telekomunikacija. Pod kaznenim odredbama[93] definiraju se i novčane kazne za one koji krše neke odredbe ovog Zakona.

Zakon o zaštiti podataka o ličnosti (Službeni glasnik Republike Srbije 97., 2008) sadrži uobičajene odredbe vezane uz zaštitu podataka o osobama, kao i u Republici Hrvatskoj ili Bosni i Hercegovini.

Naposljetku, **Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminaliteta** (Službeni glasnik Republike Srbije 61., 2005) utvrđuje obrazovanje, organizaciju, nadležnost i ovlaštenja posebnih organizacionih jedinica državnih organa radi otkrivanja, kaznenog progona i suđenja za kaznena djela iz područja visokotehnološkog kriminala. Ona su definirana činjenjem kaznenih djela kod kojih se kao objekt ili sredstvo izvršenja pojavljuju računala, računalne mreže, računalni podaci te njihovi proizvodi u materijalnom ili elektronskom obliku, dok se proizvodima osobito

[84] Prema čl. 302.
[85] Prema čl. 303.
[86] Prema čl. 304.
[87] Prema čl. 304a.
[88] Iz travnja 2013. godine.
[89] Prema čl. 24.
[90] Za detalje, cf. RATEL, Republička agencija za elektronske telekomunikacije, **www.ratel.rs** (08.08.2013.)
[91] Prema čl. 40.
[92] Prema čl. 54. i 55.
[93] U glavi X.

podrazumijevaju računalni program i autorska djela u elektronskom obliku. Zakonom se predviđa osnivanje posebnog Državnog odvjetništva za visokotehnološki kriminalitet a primjenjuje se radi otkrivanja, kaznenog progona i suđenje za kaznena djela protiv sigurnosti računalnih podataka određenih kaznenim zakonom te intelektualnog vlasništva.[94]

Zakon o informacionoj bezbjednosti Republike Crne Gore (Službeni list Crne Gore 14., 2010) definira osnovne mjere i standarde informacijske sigurnosti, sukladno C-I-A trijadi. Obveznici tog zakona su državna tijela, tijela državne samouprave, organi jedinica lokalne samouprave, pravne osobe s javnim ovlastima, ali i druge pravne i fizičke osobe koje ostvaruju pristup ili koriste podatke. Zanimljivo je da se taj zakon ne primjenjuje u odnosu na one podatke čija se informacijske sigurnost osigurava sukladno propisima o tajnosti podataka. Zakon definira mjere koje se koriste za osiguranje osnovne zaštite podataka na fizičkoj, tehničkoj i organizacijskoj razini, a one obuhvaćaju fizičku zaštitu, zaštitu podataka i zaštitu informacijskih sustava. Uloga koordinacije prevencije i zaštite ovim je zakonom dodijeljena nacionalnoj organizacijskoj jedinici – CIRT[95]. Ostali zakonski propisi u Crnoj Gori koji se odnose svojim odredbama na područje informacijske sigurnosti su **Zakon o elektronskom potpis**u (Službeni list Republike Crne Gore 31., 2005), uključujući **Zakon o izmjenama i dopunama zakona o elektronskom potpisu** (Službeni list Republike Crne Gore 21., 2008), **Zakon o elektronskom dokumentu** (Službeni List Republike Crne Gore 5., 2008.) i **Zakon o elektronskoj trgovini** (Službeni List Republike Crne Gore 80., 2004).

U Republici Makedoniji moguće je identificirati nekoliko zakona koji definiraju područje informacijske sigurnosti. **Zakonom o slobodnom pristupu informacijama od javnog značaja**[96] u uvodnom dijelu – predmetu zakona (Služben vesnik 13., 2006) - uređuju se uvjeti, načini i postupci za ostvarivanje prava na slobodan pristup informacijama od javnog značaja kojima raspolažu tijela državne vlasti i druge ustanove i institucije, općine, glavni grad, javne ustanove i službe, te pravne i fizičke osobe koje obavljaju javne dužnosti u javnom interesu, a koje su utvrđene zakonom. Zakon definira i osnivanje Komisije za zaštitu prava na slobodan pristup informacijama od javnog značaja čiji je temeljni akt Uputstvo za način i postupanje provođenja ovog zakona. Zakonom se jamči slobodan pristup informacijama svim fizičkim i pravnim osobama.

[94] Zanimljivo je kako je zakonodavac definirao da se odredbe ovog Zakona primjenjuju samo ukoliko je broj primjeraka veći od 400 ili materijalna šteta prelazi iznos od 850.000 dinara.
[95] Za detalje o crnogorskom nacionalnom CIRT-u, cf. CIRT, **http://www.cirt.me/** (18.08.2013.)
96 Izvorni naziv zakona je (transkribiran na latinično pismo) - *„Zakon za sloboden pristap do informacii od javen karakter"*

Zakonom o zaštiti osobnih podataka[97] uređuje se zaštita osobnih podataka za koje zakon (Služben vesnik 103., 2008) prepoznaje kako pripadaju temeljenim slobodama i pravima fizičkih osoba, a osobito pravima na privatnost tijekom obrade osobnih podataka. Ovaj zakon se primjenjuje i na potpunu ili djelomično automatiziranu obradu osobnih podataka.

Zakon o elektroničkim komunikacijama[98] definira uvjete i način postupanja u području elektronskih komunikacija u Republici Makedoniji (Služben vesnik 13., 2005) na način da predviđa osnivanje Agencije za elektroničke komunikacije[99], te izgradnju, održavanje, sigurnost, nadzor i korištenje komunikacijskih mreža i usluga, interkonekcija i pristup elektroničkim komunikacijama, osiguranje univerzalne usluge, osiguranje tržišnog natjecanja (konkurencije), korištenje i kontrolu radio-spektra, numeraciju, odnose među pružateljima usluga, upravljanje, i zaštitu tajnosti elektroničkih komunikacija.

Zakonom o klasificiranim informacijama[100] uređuje se klasifikacija informacija, uvjeti, kriteriji, mjere i aktivnosti koje se poduzimaju s ciljem osiguravanja zaštite, prava i definiranja odgovornosti pružatelja i korisnika klasificiranih informacija i njihova međunarodna razmjena. Cilj ovoga zakona (Služben vesnik 9., 2004) je osiguravanje zakonskog korištenja klasificiranih informacije i onemogućavanje bilo kojeg oblika nezakonitog pristupa takvim informacijama. Za provođenje utvrđene politike zaštite klasificiranih informacija i međunarodnih standarda, realiziranje njihove razmjene te obavljanje drugih radnji, ovim zakonom osnovana je Direkcija za sigurnost klasificiranih informacija.

3.3. PRIMJENA SMJERNICA, STANDARDA I NAJBOLJE PRAKSE U KORIŠTENJU SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

Osim zakonskih propisa koji definiraju koje mjere informacijske sigurnosti se moraju provoditi kako bi se postigla sukladnost sa nacionalnom ili nadnacionalnom regulativom, mala i srednja poduzeća obavljaju svoju djelatnost u profesionalnom okruženju koje postavlja posebne zahtjeve po pitanju politike, mjera i procesa informacijske sigurnosti. Zbog navedenog razloga u ovom poglavlju se iznose temeljne karakteristike takvih sustava a to su: **1) ISO 9001, 2) ISO:IEC 27001:2005 i vezani standardi, 3) ITIL 4) PRINCE2 i 5) COBIT.**

97 Izvorni naziv zakona je (transkribiran na latinično pismo) - *„Zakon za zaštita na lični podatoci“*
98 Izvorni naziv zakona je (transkribiran na latinično pismo) - „*Zakon za elektronskite komunikacii*“
99 Za detalje cf. Agencija za elketronski komunikacii, **http://www.aec.mk/** (18.08.2013.)
100 Izvorni naziv zakona je (transkribiran na latinično pismo) - *„Zakon za klasificirani informacii“*

3.3.1. ISO 9001

ISO 9000 obitelj standarda je zasigurno jedna od međunarodnih normi prema kojoj je certificiran najveći broj organizacija u svijetu.[101] Ova obitelj standarda utemeljena je na BS 5750 seriji standarda osiguranja kvalitete izdanih 1979. godine (BSS 5750 (PUBMed, 1995), koji su samu utemeljenu na standardu, odnosno publikaciji Ministarstva obrane USA iz 1959. godine, **MIL-Q-9858** (ASQ, 1959)). Prva inačica ISO 9000 standarda izdana je 1987. godine, druga 1994., treća 2000., a četvrta i trenutačno važeća, 2008. godine, pa se prema njoj standard i naziva ISO 9001:2008[102].

ISO 9000 opisuje osnove sustava upravljanja kvalitetom, uključujući osam temeljnih principa upravljanja na kojima se temelji ova obitelj standarda. S druge strane, ISO 9001 izlaže zahtjeve koje mora ispuniti organizacija koja želi biti certificirana sukladno standardu.

Globalno prihvaćanje korištenja ovog standarda može se pripisati nizu čimbenika. Većina velikih kupaca materijala i usluga zahtijeva da ponuditelji, odnosno dobavljači, posjeduju ovaj certifikat. Način na koji ISO 9001 certifikacija poboljšava rezultate poduzeća, odnosno utječe na kvalitetu je i dalje predmet istraživanja. Prema nekim autorima, operativna poboljšanja (redukcija u obrtaju zaliha, roba, novca) rezultat su certifikacije. (Lo, et al., 2007, pp. 35-40) Prema drugim autorima, iako postoji korelacija, kauzalnosti nema, već su sva poboljšanja posljedica činjenice kako poduzeća s boljim poslovnim rezultatima provode proces certifikacije. (Heras, et al., 2002, p. 774)

Najveći broj poduzeća s ISO 9001:2008 certifikacijom je u Kini, na koju otpada jedna trećina ukupnog broja izdanih certifikata. Broj izdanih ISO 9001:2008 certifikata prema državama prikazuje tablica 5.

Tablica 5: Deset svjetskih država s najvećim brojem ISO 9001 certifikata

Redni broj	Država	Broj certificiranih organizacija
1	Kina	328213
2	Italija	171947
3	Japan	56912
4	Španjolska	53057
5	Njemačka	49540
6	Velika Britanija	43564
7	Indija	29574
8	Francuska	29215

[101] Više od milijun ISO 9001:2008 certifikata je izdano do 2009.. godine, podaci najnovije raspoložive studije studije ISO Survey 2011. koja se slobodno može preuzeti s Internet stranica ISO organizacije pokazuju kako je taj broj u prosincu 2011. dostigao 1,111,698 certificiranih organizacija.

[102] ISO standardi nisu javno besplatno objavljeni, te iz navedenog razloga nije moguće direktno se referencirati na konkretan sadržaj pojedinih ISO standarda.

9	Brazil	28325
10	Južna Koreja	27284

Izvor: prilagodio autor prema ISO:**„The ISO Survey of Management System Standard Certifications (1993.-2011.)**“, www.iso.org (11.07.2013.)

ISO 9001 „*Sustavi upravljanja kvalitetom – zahtjevi*“[103] je dokument koji prate dva druga standarda: ISO 9000:2005 („*Sustavi upravljanja kvalitetom – temeljne postavke i rječnik*[104]) te ISO 9004:2009 („*Upravljanje za održivi uspjeh organizacije – pristup upravljanja kvalitetom*“[105]). **Sadržaj ISO 9001** standarda je sljedeći:

1. Predgovor,
2. Uvod,
3. Zahtjevi,
    - Opseg,
    - Normativne reference,
    - Pojmovi i definicije,
    - Sustav upravljanja kvalitetom,
    - Odgovornost rukovodstva,
    - Upravljanje resursima,
    - Kreiranje proizvoda,
    - Mjerenje, analiza i poboljšanje,
5. Usporedne tablice između ISO 9001 i ostalih standarda,
6. Popis literature.

Prije nego certifikacijsko tijelo može izdati ili obnoviti certifikat, revizor mora biti uvjeren kako je organizacija implementirala zahtjeve.[106] Neka poglavlja standardanisu predmetom revizije[107], ali se uzimaju u razmatranje budući da ona pružaju kontekst i definicije za ostatak standarda. Standard specificira kako svaka sukladna organizacija mora izdati i održavati šest **dokumentiranih procedura**:

1. Kontrola dokumenata,
2. Kontrola zapisa,
3. Interna revizija,
4. Kontrola nesukladnih proizvoda/usluga,

[103] izvorni naslov eng. *„ISO 9001:2008 Quality management systems — Requirements“*
[104] izvorni naslov eng. *„ISO 9000:2005 Quality management systems — Fundamentals and vocabulary“*
[105] izvorni naslov eng. *„ISO 9004:2009 Managing for the sustained success of an organization — A quality management approach“*
[106] Obvezni zahtjevi standarda prikazani su u poglavljima 4.-8.
[107] Radi se o poglavljima 1.-3.

5. Korektivne akcije,
6. Preventivne akcije.

Osim navedenih procedura, ISO 9001:2008 standard zahtijeva da organizacije dokumentiraju sve druge procedure koje mogu biti zahtijevane za efikasno upravljanje kvalitetom. Standard također zahtijeva da organizacije izdaju dokumentiranu politiku kvalitete i da održavaju ostale zapise specificirane u samom standardu.

ISO 9001 certifikat nije izdan jednom zauvijek, već mora biti obnovljen u regularnim intervalima koje predlaže certifikacijsko tijelo, a obično se radi o procesu recertifikacije svake tri godine. Ne postoji kvantitativna gradacija uspješnosti poduzeća, odnosno ona su ili certificirana sukladno standardu, tj. predana metodama upravljanja kvalitetom na način na koji je to opisano u standardu, ili nisu certificirana, odnosno sukladna.

ISO 9001 je u malim i srednjim poduzećima često prisutan, ali vrlo rijetko ispravno korišten alat u postizanju ciljeva informacijske sigurnosti. Ispravno korištena, ta certifikacija može biti vrlo uspješno sredstvo za osiguravanje sigurnosti informacija u malim i srednjim poduzećima u željenom opsegu. Naime, općenita efikasnost implementiranog ISO sustava ovisi o nizu **čimbenika**, od kojih su najvažniji:

1. Dostignuta **razina** vještine kojom revizor pronalazi i predlaže područja za poboljšanje. Naime, revizori u okviru ISO sustava nisu konzultanti, oni isključivo mogu predlagati područja u kojima je vidljivo kako organizacija može postići poboljšanje. Postoje dva načina na koje revizori mogu komunicirati s klijentom: jedan način je puko indiciranje sukladnosti ili nesukladnosti s pojedinim zahtjevima standarda, što teško da može voditi ka znatnim poboljšanjima u sustavu upravljanja kvalitetom. Drugi način je obraćanje rukovoditeljima u terminima konkretne poslovne djelatnosti poduzeća. Upravljanje poslovnom informatikom te osobito informacijskom sigurnošću u malim i srednjim poduzećima, počesto je strano i nepoznato ne samo revizorima, već i samom rukovodstvu poduzeća[108], tim više što se ta poslovna djelatnost u svim poduzećima koja nisu visokotehnološka, ili se ne bave izradom rješenja iz područja informacijske sigurnosti, smatra potpornom djelatnošću, a samim time uglavnom se nalazi izvan opsega certifikacije, odnosno smatra potpornom djelatnošću.
2. Način na koji je ISO certifikacija **integrirana** u postojeću poslovnu praksu. Ukoliko je od samog početka procesa certifikacije sigurnost sustava poslovnih informacija jedan od

[108] Iz razloga što je upravljanje informacijskom sigurnošću vrlo kompleksno i često strano rukovoditeljima i vlasnicima, u profesionalnom se smislu velika pažnja poklanja tome da zaduženi za informacijsku sigurnost aktivno rade na tome da se unutar onih koji odlučuju podigne svijest o važnosti ove poslovne funkcije. Taj se postupak u korporativnom žargonu naziva eng. „*buy in*“. Za formalnu definiciju, cf. Cambridge Dictionaries, **http://dictionary.cambridge.org/dictionary/business-english/buy-in** (18.08.2013.)

procesa koji je obuhvaćen opsegom certifikacije, u svim budućim koracima on će biti uključen u procese poboljšanja i recertifikacije. Najboljom praksom pokazalo se uključivanje informacijske sigurnosti u malim i srednjim poduzećima u proces izrade priručnika upravljanja kvalitetom, uz dodavanje novih vezanih procesa koje je potrebno pratiti i unaprjeđivati na način i dinamikom kako se to pokaže potrebnim.

3. Budući da su sustavi upravljanja kvalitetom fokusirani na iskustvo klijenta, mala i srednja poduzeća trebala bi se **fokusirati** na klijente dok uključuju informacijsku sigurnost u svoj sustav upravljanja kvalitetom. Ukoliko je sigurnost informacija jedna od ključnih funkcija za dostizanje razine očekivanja koja je postavljena od strane klijenata, i mala i srednja poduzeća imaju opravdanje za angažiranje dodatnih resursa u smjeru inkorporiranja informacijske sigurnosti u sustav upravljanja kvalitetom.
4. Najvažniji način na koji se može iskoristiti ISO 9001 certifikacija u malim i srednjim poduzećima je **skretanje** pažnje vlasnika i rukovoditelja na poslovnu funkciju osiguranja informacijske sigurnosti. Rukovoditelji poduzeća i vlasnici su u procesu stjecanja i održavanja certifikacije direktno uključeni u praćenje, kontrolu i poboljšanje upravljanja kvalitetom.

Ključni korak u inkorporiranju procesa informacijske sigurnosti u sustav upravljanja kvalitetom je definiranje godišnjih **ciljeva** u okviru kojih je moguće pratiti i ciljeve informacijske sigurnosti[109]. Postavljane i praćenje tih ciljeva može biti početna točka za strukturirano širenje utjecaja poslovne funkcije informacijske sigurnosti unutar malih i srednjih poduzeća, osobito u situaciji u kojoj je ISO 9001 certifikacija sve češće dio njihove poslovne prakse. Implementiranje certificiranog sustava upravljanja kvalitetom u tom smislu, kao i u općenitom smislu (Sroufe & Curkovic, 2008, p. 507), rezultirati će sljedećim komparativnim **prednostima** po certificirana mala i srednja poduzeća:

1. Kreiranje efikasnijeg i produktivnijeg sustava upravljanja informacijskom sigurnošću,
2. Povećanje zadovoljstva klijenata i njihovo zadržavanje,
3. Smanjenje potreba za revizijama poslovanja i provođenjem unutarnjih kontrola,
4. Poboljšanje efikasnosti marketinških akcija poduzeća,
5. Poboljšanje motivacije zaposlenika i njihove svjesnosti o važnosti sigurnosti informacija u svakodnevnom radu,
6. Poboljšanje imidža poduzeća u odnosu na poslovne partnere,
7. Smanjenje troškova uslijed nastupa sigurnosnih incidenata i samim time povećanje dobiti poduzeća,

[109] Neki od mogućih ciljeva informacijske sigurnosti koje je moguće periodički pratiti su npr. broj sigurnosnih incidenata, vrijeme raspoloživosti informatičkih usluga, utrošak na rješavanje posljedica sigurnosnih incidenta i sl. Pri definiranju ovih ciljeva treba se voditi uobičajenom metodologijom definiranja ključnih pokazatelja (KPI – eng. „*Key Performance Indicators*“). Za detalje cf. Meyer, Paul J.: „**Attitude is Everything**“, The Leading Edge Publishing, Merced, CA, 2006., p. 6.-24.

8. Kreiranje jedinstvenog alata za standardizaciju napora organizacije (poduzeća) u postizanju ciljeva informacijske sigurnosti.

3.3.2. ISO/IEC 27001:2005 i vezani standardi

ISO/IEC 27001 je ISO [110] **norma** koja je krajem 2005 godine naslijedila staru britansku normu BS 7799-2. To je standard koji se bavi sustavom upravljanja informacijskom sigurnošću a namijenjen je za korištenje zajedno s ISO/IEC 27002, prije poznat kao ISO/IEC 17799, što je praktični kodeks koji definira ciljeve sigurnosnih kontrola i preporuča određeni praktični raspon istih. On pruža praktičan model za uspostavljanje, primjenu, korištenje, praćenje, održavanje i konstantno poboljšavanje sustava za upravljanje informacijskom sigurnošću, pri čemu su dizajn i primjena pod utjecajem ciljeva poduzeća ili organizacije, procesa koji se odvijaju, te veličine i strukture same organizacije. One organizacije koje u svom svakodnevnom poslovanju koriste ISO/IEC 27002 pri procjeni svog sustava upravljanja informacijskom sigurnošću vrlo vjerojatno će biti u sukladnosti sa normama ISO/IEC 27001.

Certifikaciju prema ovoj normi čine akreditacijska tijela koja često funkcioniraju na nacionalnoj ili međunarodnoj razini. Sam proces certifikacije izvode certificirani vodeći revizori. On se obično sastoji od tri osnovne međusobno povezane faze: (The ISO 27000 Directory, 2013)

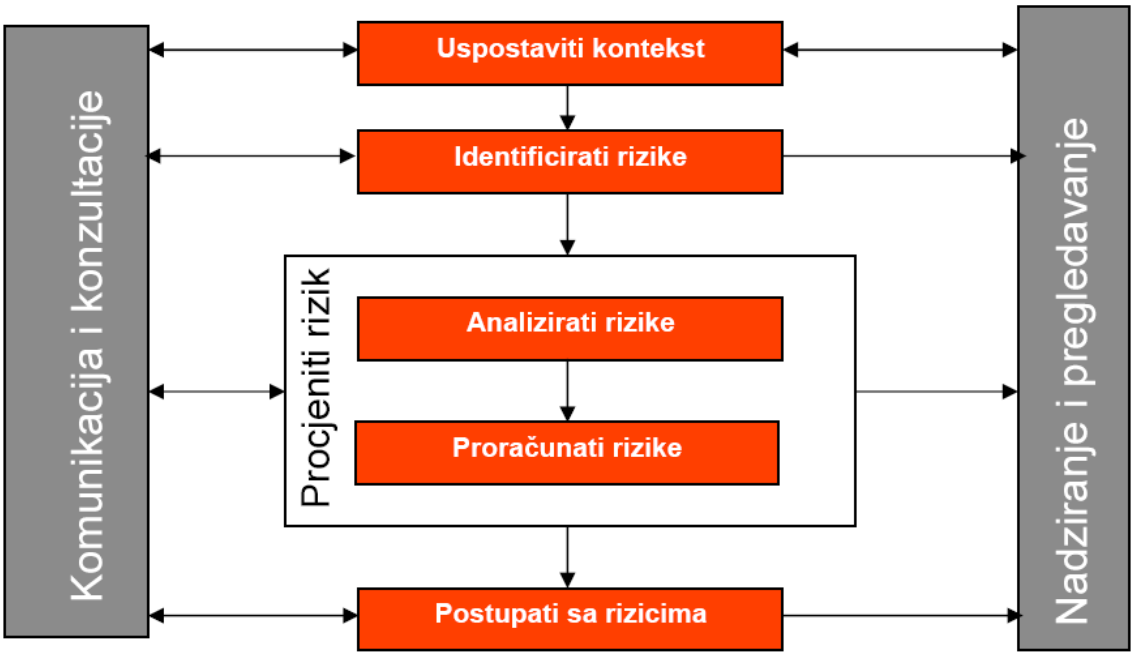
1. Provjera postojanja i potpunosti **ključne dokumentacije** potrebne za uvođenje sustava upravljanja informacijskom sigurnošću, a radi se o sigurnosnoj politici organizacije, izjave o primjenjivosti kontrola[111], te planu tretmana rizika[112],
2. **Dubinsko snimanje i revizija** koji testiraju postojanje i efikasnost kontrola informacijske sigurnosti koje se navode u izjavi o primjenjivosti kontrola te planu tretmana rizika, uključujući potpornu dokumentaciju. Sam proces procjene i upravljanja rizikom informacijske sigurnosti je kontinuiran a ne jednokratan proces, baš kao što se teoretski smatra da sustav upravljanja informacijskom sigurnošću nikada nije u potpunosti uveden već se radi o konstantnom procesu evaluacije te traženja mogućih nesukladnosti i njihovog ispravljanja,
3. Treća faza je **ponovljena procjena**, odnosno naknadna revizija, kojom se provjerava da li su poduzeće ili organizacija koji su prvobitno certificirani u skladu sa standardom i dalje u sukladnosti s njim. Ona se odvija periodički kako bi se potvrdilo da sustav upravljanja informacijskom sigurnošću funkcionira kako je zamišljeno i dokumentirano.

[110] *ISO* je kratica od eng. „*International Organization for Standardization*“, organizacija koja se bavi kreiranjem i izdavanjem međunarodnih standarda. .Više detalja o poslovanju organizacije moguće je naći na Internet stranicama, cf. ISO, **http://www.iso.org/iso/about.htm** (19.05.2013.)
[111] Kratica od eng. *SoA* - "*Statement of Applicability"*
[112] Kratica od eng. "*Risk Treatment Plan*".

Sam standard strukturiran je tako da ga je moguće uvesti u svaku organizaciju, bila ona profitna ili neprofitna te neovisno o njenoj veličini. U samoj srži standarda podržan je osnovni zahtjev informacijske sigurnosti izražen u već opisanoj C-I-A trijadi (Stamp, 2006, p. 2), prema kojemu je dohvat informacijama dozvoljen samo onima koji su autorizirani za njihovo korištenje, informacije moraju biti točne i potpune te da je pristup njima neprekinut, odnosno dozvoljen u kontinuitetu kada je to potrebno.

Standardi ISO/IEC 27001 i ISO/IEC 17799 definiraju sljedeće faze (korake) procesa procjene i upravljanja rizikom informacijske sigurnosti, a koje prikazuje shema 6. Ovi se **koraci** detaljno objašnjavaju u nastavku. (Hlača, et al., 2008, pp. 250-251)

Shema 6: Proces procjene i upravljanja rizikom



Izvor: Košutić, D.: **"Elementi procjene i upravljanja informacijskim rizicima"**, Kvadra Savjetovanje d.o.o, Zagreb, 2007., p.2. (neobjavljeno)

1) **Definiranje pristupa procjeni rizika**. Sastoji se od identificiranja metodologije procjene koja je odgovarajuća za sustav upravljanja organizacijom, te zakonskih i ostalih zahtjeva, a cilj joj je razvijanje kriterija za prihvaćanje rizika i identifikaciju prihvatljive razine rizika,

2) **Identificiranje rizika**. Identificira se informacijska imovina unutar opsega procjene te vlasnike dotične imovine moguće prijetnje toj imovini, ranjivosti koje bi te prijetnje mogle iskoristiti za nanošenje štete i identificiranje utjecaja koji bi mogli imati gubitak raspoloživosti, povjerljivosti i dostupnosti po tu imovinu, (Tipton & Nozaki, 2006, p. 433),

3) **Analiziranje i procjena rizika.** Radi se o procjeni utjecaja na poslovanje organizacije do kojih bi moglo doći zbog sigurnosnih incidenata, procjeni vjerojatnosti da će doći do sigurnosnih incidenata u svjetlu ranjivosti i prijetnji, te postojećih mjera zaštite i procjeni prihvatljivosti rizika te zahtijevaju li oni tretman korištenjem kriterija za prihvaćanje rizika,

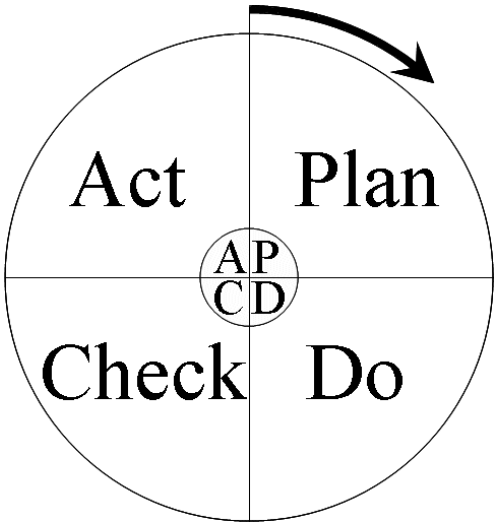
4) Identificiranje i ocjena **mogućnosti tretmana rizika**. Rizik se može tretirati primjenom adekvatnih mjera zaštite, prihvaćanjem rizika, njegovim izbjegavanjem ili prebacivanjem na treću stranu (npr. osiguravatelj ili dobavljač),

5) **Odabir ciljeva** za mjere zaštite i određivanje pojedinih mjera zaštite za tretman rizika. Za one rizike kod kojih je organizacija odlučila primijeniti adekvatne mjere zaštite, mora se osigurati smanjivanje rizika na prihvatljivu razinu uzimajući u obzir zahtjeve domaće i internacionalne regulative, ciljeve organizacije, operativne potrebe i ograničenja, cijenu implementacije u odnosu na visinu rizika koji se umanjuje i potrebu balansiranja investicija u implementaciju u odnosu na potencijalnu štetu od nastupa sigurnosnog incidenta (Blakley, et al., 2001, pp. 98,99),

6) **Dobivanje dozvole uprave** za implementaciju mjera zaštite, ali i eventualno prihvaćanje rizika.

Sam standard utemeljen je na PDCA[113] modelu koji se primjenjuje na sve strukture procesa sustava za upravljanje informacijskom sigurnošću, a prikazuje ga shema 7.

Shema 7: PDCA ciklus



Izvor: Hlača, B., Aksentijević, S., Tijan, E**.:"Influence of ISO 27001:2005 on the Port of Rijeka security"**, Pomorstvo, Pomorski fakultet, Rijeka, god. 22, br. 2, 2008., p. 247.

Sastavni elementi PDCA ciklusa navode se na sljedećoj stranici.[114]

[113] PDCA je kratica od eng.izraza "*Plan-Do-Check-Act*", odnosno "*planiraj-učini-provjeri-primijeni*". Radi se o cikličkom procesu koji je temelj većine sustava upravljanja kvalitetom te isporukom usluga.

1) **Planiranje uspostavljanja ISMS-a**[115]. U ovoj fazi potrebno je uspostaviti politiku informacijske sigurnosti, ciljeve, procese i procedure koje su potrebne za upravljanje rizikom i poboljšanje informacijske sigurnosti te koji doprinose ostvarivanju cjelokupnosti ciljeva organizacije,
2) **Implementacija** (primjena i korištenje ISMS-a). Uvode se i operativno koriste politika, kontrole, procese i procedure koje se tiču sustava upravljanja informacijskom sigurnošću,
3) **Provjera** (praćenje i revizija ISMS-a). Tijekom faze provjere mjeri se funkcioniranje sustava informacijske sigurnosti u praksi te uspoređuje s politikama, ciljevima i praktičnim iskustvom te se potom dobiveni rezultati predočavaju upravi,
4) **Primjena** (održavanje i poboljšavanje ISMS-a). Nakon provjere poduzimaju se korektivne i preventivne akcije na osnovi rezultata interne revizije sustava, kako bi se uspostavilo konstantno poboljšavanje sustava upravljanja informatičkom sigurnošću.

Standard zahtijeva da dio procedura bude u dokumentiranom obliku, dok za operativne procedure zahtijeva postojanje, no ne moraju biti dokumentirane. Zahtjev za **dokumentacijom** vezano uz sustav upravljanja informacijskom sigurnošću je sljedeći: (Aksentijević, 2008, p. 29)

1. Politika i ciljevi upravljanja informacijskom sigurnošću,
2. Opseg ISMS-a,
3. Procedure i kontrole koje podržavaju ISMS,
4. Opis metodologije procjene rizika,
5. Izvještaj o procjeni rizika,
6. Plan tretmana rizika,
7. Dokumentirane procedure kojima organizacija osigurava efikasno planiranje, provođenje i kontrolu procesa informacijske sigurnosti te opis efikasnosti kontrola,
8. Dokumentirane procedure koje opisuju način čuvanja zapisa,
9. Izjava o primjenjivosti kontrola,
10. Dokumentirana odgovornost instanci odlučivanja za planiranje i provođenje revizije, izvještavanje i čuvanje rezultata revizije,
11. Dokumentiranje procedura o poduzimanju korektivnih te preventivnih akcija.

[114] W. Edwards Deming je 1950-tih godina predložio da se poslovni procesi analiziraju i mjere kako bi se identificirali izvori varijacija koji uzrokuju da se proizvodi i usluge razlikuju od zahtijeva klijenata. U okviru tog prijedloga razvio je jednostavni model kojim rukovoditelji mogu identificirati i promijeniti one dijelove procesa koje treba unaprijediti. Za više informacija cf. Balanced Scorecard Institute, **http://balancedscorecard.org/?TabId=112** (17.08.2013.)

[115] ISMS je kratica od eng. *„Information Security Management System"*, odnosno sustav upravljanja informacijskom sigurnošću.

ISO standard 27001:2005[116], preporučuje ukupno 133 kontrole koje reguliraju preko svojih podvrsta svoja zasebna područja. (Praxiom Research Group limited, 2013) Kontrole informacijske sigurnosti s objašnjenjem prikazane su u tablici 6.

Tablica 6: Kontrole informacijske sigurnosti sukladno standardu ISO 27001:2005 (aneks „A" – ISO 27002)

Oznaka	Naziv skupine kontrola
1.	Procjena i tretman rizika – analiza informacijskih rizika poduzeća
2.	Politika sigurnosti – pogled rukovoditelja
3.	Organizacija informacijske sigurnosti – upravljanje informacijskom sigurnošću
4.	Upravljanje informacijskom imovinom – inventar i klasifikacija informacijske imovine
5.	Sigurnost ljudskih resursa – sigurnosni aspekti zapošljavanja, transfera i prestanka radnog odnosa zaposlenika
6.	Fizička sigurnost i sigurnost okoline – zaštita prostora s informacijskom imovinom
7.	Upravljanje komunikacijama i operacijama – upravljanje kontrolama tehničke sigurnosti u informacijskim sustavima i mrežama
8.	Kontrola pristupa – ograničenje prava pristupa mrežama, sustavima, aplikacijama, funkcijama i podacima
9.	Nabava, razvoj i održavanje informacijskih sustava – ugrađivanje sigurnosti u računalne aplikacije
10.	Upravljanje incidentima informacijske sigurnosti – predviđanje i adekvatni odgovor na sigurnosne incidente
11.	Upravljanje poslovnim kontinuitetom – zaštita, održavanje i povrat sustava i procesa kritičnih za odvijanje poslovne aktivnosti
12.	Sukladnost – osiguravanje sukladnosti s politikama informacijske sigurnosti, standardima, zakonima i propisima

Izvor: prilagodio autor prema **„ISO/IEC 27001 Information Security Management standard"**, BSI, London, Velika Britanija, 2013.

Kontrole ili mjere zaštite su načini kojima se upravlja informacijskim rizicima. U svojoj osnovi uključuju procese, politike, standarde, postupke, smjernice, prakse, organizacijske strukture i druge elemente koji mogu biti administrativne, upravljačke, pravne ili tehničke naravi. Temeljna svrha mjera zaštite odnosno kontrola je smanjiti rizike po funkcioniranje sustava upravljanja informacijskom sigurnošću koji su identificirani kroz procjenu rizika.

3.3.3. ITIL

ITIL[117] je **skup tehnika** (odnosno koncepata i najbolje prakse) za rukovođenje infrastrukturom informacijskih tehnologija, njihovim razvojem i funkcioniranjem. Izdan je u obliku serije knjiga koje pokrivaju tematiku rukovođenja informatičkim tehnologijama. Sama imena ITIL te IT

[116] U okviru navedenog sustava, kontrole se nalaze u njegovom zasebnom dijelu, aneksu A. Taj je aneks kasnije proširen i izdan u obliku zasebnog standarda ISO 27002 – *„Information technology – Security techniques – Code of practice for information security management."*

[117] *ITIL* je kratica od eng. *„Information Technology Infrastructure Library",* za formalno objašnjenje značenja i opsega *ITIL-a* cf. službene Internet stranice na adresi **http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp** (19.05.2013.)

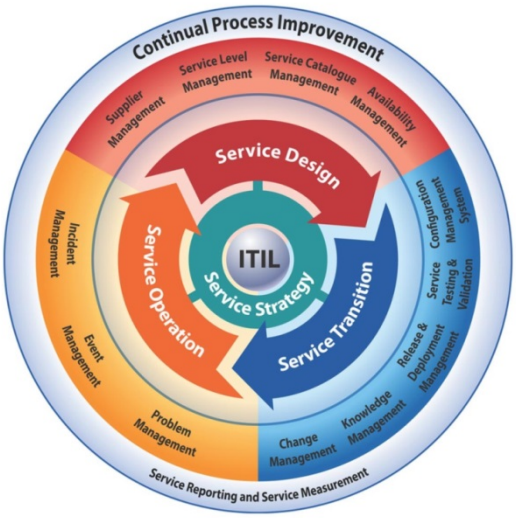
Infrastructure Library su registrirana i zaštićena u Velikoj Britaniji. ITIL daje detaljan opis niza važnih postupaka u upravljanju s detaljnim listama provjera, zadacima i procedurama koje mogu biti prilagođene bilo kojoj organizaciji. Slično kao i mnoge druge metode projektne i informatičke organizacije, ITIL je izgrađen oko Demingovog PDCA ciklusa (Arveson, 2013). Početnih 30 knjiga koje su nastale u periodu od 1989. do 1996. godine, 2001. godine je sabrano u devet logički grupiranih tomova koji obuhvaćaju sve aspekte upravljanja poslovnom informatikom, aplikacijama i uslugama. Najšire distribuiran i najčešće korišten je upravo skup vezan uz upravljanje uslugama[118]. Trenutačno važeća inačica je izdana 2007. godine i nosi naziv „v3“[119] i sastoji se od 26 procesa i funkcija grupiranih u pet tomova i uređenih oko koncepta životnog vijeka servisnih informatičkih usluga. Certifikacija prema prethodnom, v2 sustavu, ne provodi se od 2009. godine. **Pet tomova** ITIL v3. koncepata i najbolje prakse su (itSMF - The IT Service Management Forum, 2007):

1. **Strategija informatičkih usluga**[120] (itSMF - The IT Service Management Forum, 2007, p. 12),
2. **Dizajn informatičkih usluga**[121] (itSMF - The IT Service Management Forum, 2007, p. 18),
3. **Tranzicija usluga**[122] (itSMF - The IT Service Management Forum, 2007, p. 24),
4. **Pružanje informatičkih usluga**[123] (itSMF - The IT Service Management Forum, 2007, p. 29),
5. **Kontinuirano poboljšanje usluga**[124] (itSMF - The IT Service Management Forum, 2007, p. 35).

Izvorni **dijagram procesa** ITIL v3 sustava prikazan je na shemi 8. na sljedećoj stranici.

[118] eng. *„The Service Management set – Service Support and Service Delivery“*
[119] *„v3“* je u svijetu informatike uobičajena oznaka za treću inačicu.
[120] eng. „*ITIL Service Strategy*“
[121] eng. „*ITIL Service Design*“
[122] eng. „*ITIL Service Transition*“
[123] eng. „*ITIL Service Operation*“
[124] eng. „*ITIL Continual Service Improvement*“

Shema 8: Procesi ITIL v3 sustava



Izvor: NoxGlobe, **http://www.noxglobe.com/blog/itil/itil-v3-processes/** (04.08.2013.)

Svi procesi ITIL-a su podvrgnuti procesu kontinuiranog poboljšanja (vanjski svijetloplavi krug). Unutar njega, crvenom bojom je prikazan dizajn usluga, tamnoplavom tranzicija usluga a narančastom pružanje informatičkih usluga. U središtu interesa ITIL-a nalazi se strategija pružanja usluga (sivo). Dizajn usluga, tranzicija usluga i pružanje usluga dalje se dijele na svoje **domene.** One su prikazane u tablici 7.

Tablica 7: Procesi i domene ITIL-a

Dizajn usluga	Pružanje usluga	Tranzicija usluga
Upravljanje dobavljačima	Upravljanje incidentima	Upravljanje promjenama
Upravljanje razinama usluga	Upravljanje događajima	Upravljanje znanjem
Upravljanje katalogom usluga	Upravljanje problemima	Upravljanje početnom isporukom usluga
Upravljanje raspoloživošću usluga		Provjera i testiranje usluga
		Sustav upravljanja konfiguracijom

Izvor: priredio autor

Glavna zamjerka ITIL-ovom aspektu upravljanja informacijskom sigurnošću je činjenica kako su ITIL kontrole bogate kontrolama fizičke sigurnosti informacijskih sustava ali siromašne u pogledu aplikacijske, programske i logičke sigurnosti informatičkih sustava. Isto tako, ITIL

sustav je zatvoren, odnosno njegove publikacije nisu raspoložive javnosti usprkos pokušajima da se one izdaju pod nekom od slobodnih kreativnih licenci. (ITSM, 2013)

3.3.4. PRINCE2

PRINCE2[125] je **metodologija menadžmenta** i **upravljanja projektima**. PRINCE2 je razvijen iz prethodne verzije PRINCE tehnike[126], kao standard za upravljanje projektima u informatičkom sektoru, međutim, od tada je metodologija toliko zaživjela da je postala praktični standard općeg projektnog upravljanja u Ujedinjenom Kraljevstvu i još pedeset drugih država svijeta. PRINCE2 metodologija je revidirana 2009. godine no radi vjernosti izvornome konceptu, zadržan je isti naziv. Temeljni razlog revizije PRINCE2 metodologije je pojednostavljenje i bolja integracija s drugim metodologijama koje se odnose na upravljanje informatikom i informacijskom sigurnošću.

PRINCE2 ne pruža direktan okvir za procjenu i podržavanje sigurnosti informacijskog sustava, no njegova je specifičnost, za razliku od ostalih metodologija, omogućavanje originalnog **pristupa riziku**, budući da se radi o općoj metodologiji upravljanja projektima koja nije striktno vezana samo uz informacijsku tehnologiju. Naime, u klasičnom projektnom upravljanju, pristup riziku nije isključivo negativistički, odnosno ne promatra se samo *„loša"* strana rizika koja može imati negativan utjecaj po ciljeve organizacije, već i pozitivan rizik, koji može rezultirati neočekivanom dobiti po organizaciju. Većina ostalih metodologija promatra samo kako ukloniti nastup neželjenih događaja, no PRINCE2 strukturiran je na način da reducira utjecaj prijetnji ali i iskorištavanja nastupa pozitivno naklonjenih mogućnosti koje se otvaraju tijekom poslovanja. Temeljne **faze vođenja projekata** prema PRINCE2 metodologiji objašnjavaju se na sljedećoj stranici.

1. **Prethodni koraci započinjanja projekta**.[127] U ovoj fazi nominira se projektni tim i definiraju se projektni ciljevi. Također, u ovoj se fazi određuje rukovoditelj projekta. U okruženju malih i srednjih poduzeća, za očekivati je kako će rukovoditelj projekta uspostavljanja sustava informacijske sigurnosti biti vlasnik poduzeća ili osoba nominirana od njihove strane, odnosno zadužena za informacijsku sigurnost,

[125] *PRINCE2* je kratica od eng. „*Projects in Controlled Environments*".
[126] *PRINCE* tehnika izdana je od strane *CCTA* agencije[126] 1989. godine. *CCTA* je kratica od eng. „*The Central Computer and Telecommunications Agency"*. Agencija je osnovana 1957. godine pod nazivom *TSU* (eng. „*Technical Support Unit*") a 2000. godine je postala dijelom *OGC* (eng. *„Office of Government Commerce*").
[127] U *PRINCE2* metodologiji ovi koraci poznati su kao „*SU*", što je kratica od eng. „*Starting up a project*)".

2. **Započinjanje projekta**.[128] U drugoj fazi definira se upravljanje kvalitetom projekta, načini kontrole projekta i dokumenti kojima će se projekt kontrolirati,

3. **Usmjeravanje projekta**[129]. U trećoj fazi projektni direktor ili odbor odobravaju projekt, definiraju pravila za upravljanje iznimkama i način dovršetka projekta,

4. **Kontroliranje faze projekta**.[130] Prema PRINCE2 metodologiji projekt se dijeli na više faza i ti procesi određuju način kontrole svake od tih faza. Ključne su aktivnosti odobravanje projektnih faza, napretka, izvješćivanje, primjena korektivnih akcija i kriteriji dovršavanja projektnih faza,

5. **Upravljanje granicama projekta.**[131] U ovoj fazi definiraju se obavezni koraci koje je potrebno poduzeti pri kraju izvođenja projekta. U njoj se unose nove informacije o projektu i novim rizicima u dokumentaciju, izvješća i plan iznimki koje su se pojavile tijekom projekta.

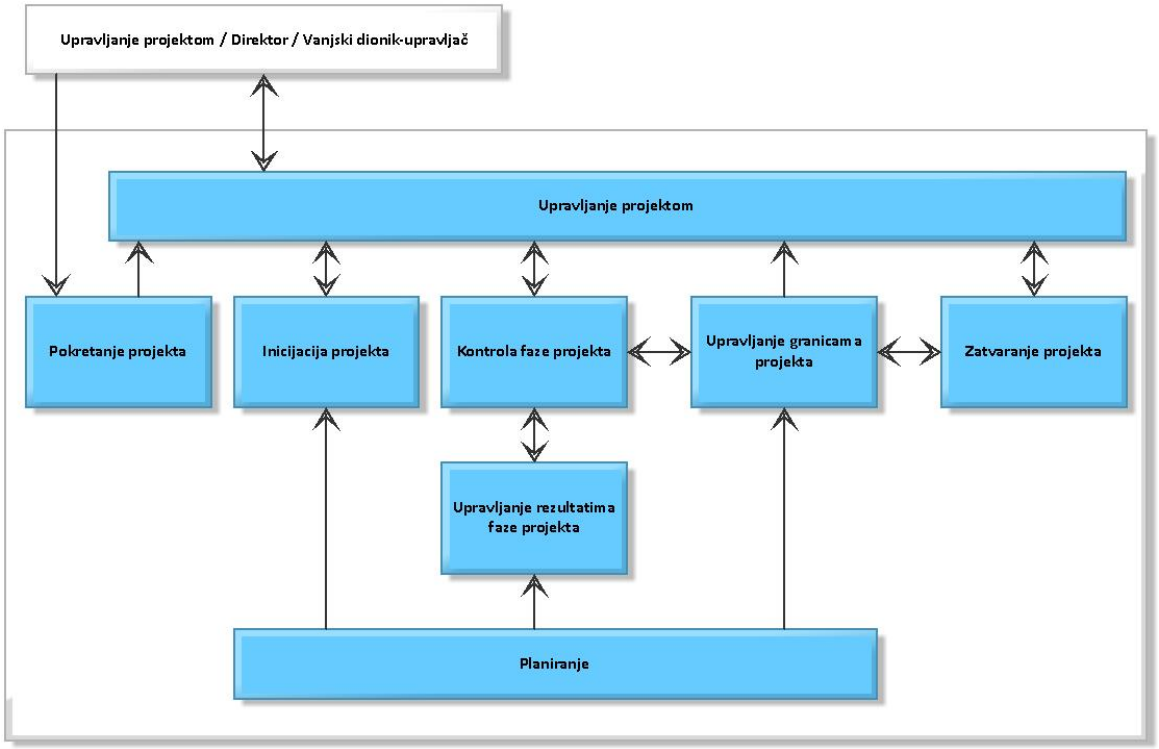
6. **Upravljanje rezultatima projekta**.[132] U ovoj fazi projekta uspostavlja se formalna veza između rukovoditelja projekta i voditelja timova koji rade na implementaciji kroz postavljanje formalnih zahtjeva za prihvat i izvođenje projektnih radova. Ciljevi ovog procesa su osiguranja autorizacija obavljenih aktivnosti unutar tolerancija vremena, troškova i kvalitete,

7. **Zatvaranje (dovršenje) projekta**.[133] U posljednjoj fazi vođenja projekata resursi zauzeti izvođenjem projekata se oslobađaju te se definiraju akcije i metode naknadne procjene uspješnosti projekta.

Tijek informacija i međusobnog odnosa pojedinih **faza** projektne metodologije PRINCE2 prikazani su na shemi 9. na sljedećoj stranici.

[128] Kratica „*IP*“, od eng. *„Initiating a project“*.
[129] Kratica „*DP*“ od eng. „*Directing a project“*.
[130] Kratica „*CS*“ od eng. „*Controlling a stage*“.
[131] Kratica „*SB*“ od eng. "*Managing stage boundaries*".
[132] Kratica „*MP“* od eng. "*Managing product delivery*".
[133] Kratica *„CP“* od eng. "*Closing a project*".

Shema 9: Tijek informacija i odnosa faza PRINCE2 metodologije



Izvor: priredio autor

Kao i kod mnogih formalnih sustava, glavna zamjerka PRINCE2 metodologiji je činjenica kako tvorci sustava proklamiraju mogućnost korištenja metodologije **neovisno o veličini** organizacije ili projekta, no sama projektna metodologija očito zahtijeva veći broj uloga te je stoga teško primjenjiva u svom izvornom obliku u manjim organizacijama. Međutim, pojedini procesi PRINCE2 sustava mogu biti adaptirani i za okruženje uvođenja sustava upravljanja informacijske sigurnosti u malim i srednjim poduzećima, a osobito u dijelu segmentiranja projekta na više manjih makro-procesa, kontroli provođenja i isporuke pojedinih faza te planiranju. Glavna **razlika** PRINCE2 metodologije i upravljanja informacijskom sigurnošću neovisno o veličini organizacije u činjenici je da informacijska sigurnost nikada nije postigla svoje ciljeve, već se radi o poslovnoj funkciji koja se neprestano i kontinuirano nalazi u procesu uvođenja i ponovne evaluacije, odnosno radi se o cikličkoj funkciji, dok projekti tipično imaju točno određeno trajanje, ciljeve i isporuku rezultata.

3.3.5. COBIT

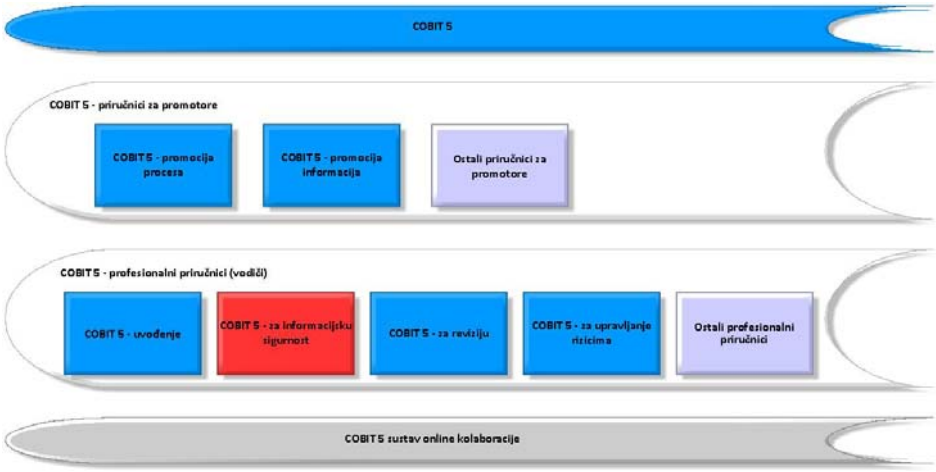
COBIT[134] je skup pravila **(okvir) za upravljanje** informacijskom tehnologijom kreiran od strane organizacija ISACA [135] i ITGI[136] 1992. godine. COBIT pruža rukovoditeljima, revizorima

[134] *COBIT* je kratica od eng. *„Control Objectives for Information and related Technology“,* za detalje cf. **http://www.ezcobit.com/UsingCobit/html/00Intro2.html** (10.08.2013.)

i korisnicima informacijskih sustava skup generalno prihvaćenih mjera, procesa, indikatora i pravila koji im mogu pomoći u maksimizaciji koristi od informacijskog sustava, ali i odgovarajuće upravljanje informacijskim resursima te kontrolu unutar poduzeća. Izdan je 1996. godine, a njegova je misija istraživanje, razvoj, publiciranje i promoviranje autoritativnog, aktualnog i međunarodnog skupa općenito prihvaćenih kontrolnih ciljeva koje koriste rukovoditelji i revizori informacijskih sustava. Koristi koje oni imaju od razvoja COBIT-a su primarno razumijevanje informacijskog sustava te razina sigurnosti i kontrola potrebnih za zaštitu poslovanja tvrtke, odnosno predmetne organizacije. COBIT pruža osnovu na temelju koje se mogu donositi odluke o investicijama u informacijsku infrastrukturu. Sastoji se od 34 procesa koji pokrivaju 210 kontrola koje su kategorizirane u četiri **glavne skupin**e, a to su: 1. *Planiranje i organizacija*, 2. *Dobava i primjena*, 3. *Isporuka i podrška*, i 4. *Praćenje i procjena*.

Priručnici i domene COBIT-a prikazani su na shemi 10.

Shema 10: Priručnici i domene COBIT-a



Izvor: priredio autor

Cjelokupan COBIT sustav sastoji se od šest **publikacija**: (ITSM Partner d.o.o., 2007)

1. **Izvještaj Upravi.** Poslovne odluke koje poboljšavaju poziciju organizacije moraju biti temeljene na pravovremenim, relevantnim i konciznim informacijama. COBIT-ov izvještaj Upravi pruža osnovne principe i ključne koncepte a uključuje i skraćenu inačicu okvirnih pravila koja pružaju njihovo detaljnije razumijevanje, identificirajući osnovne COBIT-ove domene i 34 procesa operativnog provođenja informacijskih tehnologija.
2. **Radni okvir.** Budući da se uspješna organizacija bazira na ispravnom postavljanju poslovne filozofije, te ispravnim i pravovremenim informacijama, radni okvir COBIT-a

[135] *ISACA* je kratica od eng. *"Information Systems Audit and Control",* pobliža struktura organizacije opisana na Internet stranicama, cf. **http://www.isaca.org/** (19.05.2013.)
[136] *ITGI* je kratica od eng. *„IT Governance Institute",* sjedište instituta je u Rolling Meadows, Illinois, Sjedinjene Američke Države, cf**. http://www.itgi.org/** (10.08.2013.)

objašnjava način na koji procesi informacijske tehnologije pružaju informacije koje poslovni procesi trebaju za postizanje svojih ciljeva. On identificira koji od sedam informacijskih kriterija (efektivnost, efikasnost, povjerljivost, integritet, raspoloživost, pouzdanost i sukladnost), ali i informacijsko tehnoloških resursa (ljudi, aplikacije, informacije i infrastruktura) su bitni informacijskim procesima kako bi oni u potpunosti mogli podupirati odvijanje poslovnih procesa.

3. **Kontrolni ciljevi.** Ključni čimbenik za održavanje profitabilnosti u okolini koja se tehnološki neprestano mijenja je način održavanja kontrole. COBIT-ovi kontrolni ciljevi pružaju kritični uvid potreban kako bi se definirala jasna politika i praksa kontrola informacijskih ciljeva.

4. **Smjernice revizije.** Željeni ciljevi mogu se postići samo ako se konstantno i konzistentno revidiraju i prate procedure koje su primijenjene unutar poduzeća. Smjernice revizija opisuju i predlažu aktivnosti koje je potrebno provesti prema svakoj od 34 vrhovne kontrole, čime se smanjuje rizik neispunjenja kontrolnih ciljeva. [137]

5. **Alati za primjenu.** Alati za primjenu COBIT-a sadrže dijagnostiku, vodič za primjenu, često postavljana pitanja, primjere drugih organizacija koje su uvele i prihvatile COBIT u svom svakodnevnom poslovanju te misiju koju je definirala Uprava poduzeća.

6. **Smjernice Upravi.** Rukovođenje uspješnim poduzećem podrazumijeva efikasno upravljanje sinergijom između poslovnih i informacijskih procesa. Smjernice Upravi sastoje se od modela koji pomažu usporediti faze procesa i očekivane koristi od uvođenja kontrola s industrijskim prosjecima i normama, kritične čimbenike uspjeha koji identificiraju najvažnije akcije koje je potrebno poduzeti kako bi se postigla kontrola nad procesima informacijskih tehnologija, te ključne indikatore uspješnosti i ključne indikatore ciljeva, kako bi se moglo izmjeriti postižu li kontrolni procesi svoje ciljeve.

Procesi COBIT-a mogu se podijeliti u četiri **domene**:

1. Praćenje, .
2. Operacije,
3. Planiranje, i
4. Upravljanje izgradnjom.

Navdeni **procesi** prikazani su u tablici 8. na sljedećoj stranici.

[137] Smjernice revizije su vrijedan alat primarno revizorima informacijskih sustava, a koji pružaju Upravi sigurnost u već implementirane mjere i smjernice, odnosno daju savjete za njihovo poboljšanje.

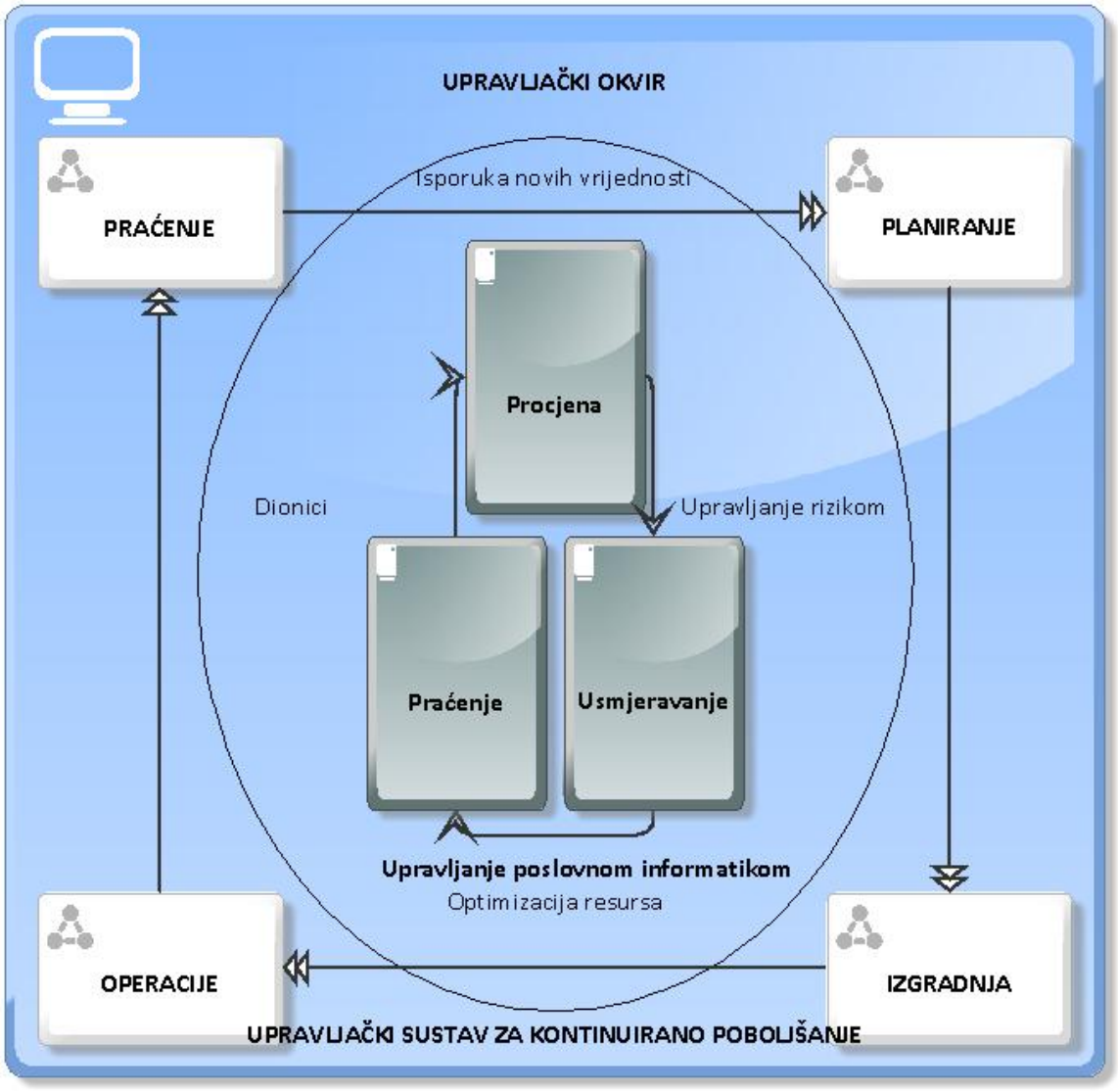
Tablica 8: Procesi COBIT sustava

1. Praćenje	**2. Operacije**
8. Praćenje i procjena sukladnosti i performansi sustava 9. Praćenje sustava internih kontrola 10. Praćenje i procjena sukladnosti s vanjskih zahtjevima	11. Upravljanje operacijama 12. Upravljanje imovinom 13. Upravljanje konfiguracijom 14. Upravljanje servisnim zahtjevima i incidentima 15. Upravljanje problemima 16. Upravljanje kontinuitetom poslovanja 17. Upravljanje sigurnošću 18. Upravljanje kontrolama poslovnog procesa
3. Planiranje	**4. Upravljanje izgradnjom**
19. Definiranje upravljačkog okvira 20. Definiranje strategije 21. Upravljanje poslovnom arhitekturom 22. Upravljanje inovacijama 23. Upravljanje portfoliom rješenja 24. Upravljanje proračunom i troškovima 25. Upravljanje ljudskim resursima 26. Upravljanje odnosima 27. Upravljanje razinama usluga 28. Upravljanje dobavljačima 29. Upravljanje kvalitetom 30. Upravljanje rizicima	31. Upravljanje programima i projektima 32. Definiranje zahtjeva 33. Identificiranje i izgradnja rješenja 34. Upravljanje raspoloživošću i kapacitetima 35. Omogućavanje organizacijskih promjena 36. Upravljanje promjenama 37. Prihvaćanje i upravljanje tranzicijom 38. Upravljanje znanjem

Izvor: priredio autor prema ISACA, **http://www.isaca.org/COBIT/Pages/default.aspx** (14.06.2013.)

Vrhovni **ciklički procesi** COBIT-a prikazani su na shemi 11. na sljedećoj stranici. U interakciji praćenja i planiranja, isporučuju se nove vrijednosti. U odnosu između planiranja i izgradnje, procjenjuju se svi rizici izgradnje i upravljanja sustavom poslovne informatike. Između makro upravljačkih procesa izgradnje i operacija ostvaruje se optimizacija korištenih resursa, dok su u aktivnosti operacija i praćenja uključeni svi dionici procesa.

Shema 11: Vrhovni ciklički procesi COBIT-a



Izvor: priredio autor

Prema tome, **procjena, praćenje i usmjeravanje** tri su procesa koji se nalaze u **jezgri** COBIT procesa. U odnosima između procjene i usmjeravanja ostvaruju se ciljevi upravljanja rizika, u odnosima između praćenja i usmjeravanja ostvaruju se ciljevi optimizacije resursa dok izlazne rezultate procesa koriste svi uključeni dionici kroz procese procjene i praćenja aktivnosti.

4. ANALIZA I OCJENA MOGUĆNOSTI PRIMJENE EKONOMSKIH KRITERIJA NA FUNKCIJU UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU MALIH I SREDNJIH PODUZEĆA

Za analizu i ocjenu mogućnosti primjene ekonomskih kriterija na funkciju upravljanja informacijskom sigurnošću malih i srednjih poduzeća u Republici Hrvatskoj, potrebno je obaviti inicijalnu analizu svojstava investicijskih ulaganja u sustav upravljanja informacijskom sigurnošću, nakon čega će se analizirati matrica ukupnosti operativnih troškova sustava upravljanja informacijskom sigurnošću. Na samom kraju, bit će dan pregled svih specifičnosti ekonomske analize ulaganja u sustave upravljanja informacijskom sigurnošću malih i srednjih poduzeća. Iz navedenog razloga, u nastavku se obrađuju sljedeće cjeline: **1) Analiza matrice investicija i troškova sustava upravljanja informacijskom sigurnošću, 2) Analiza investicijskih ulaganja u sustav upravljanja informacijskom sigurnošću, 3) Analiza operativnih troškova upravljanja informacijskom sigurnošću, 4) Specifičnosti ekonomske analize ulaganja u sustave upravljanja informacijskom sigurnošću malih i srednjih poduzeća.**

4.1 Analiza matrice investicija i troškova sustava upravljanja informacijskom sigurnošću

Kod ovakve vrste analize, nužno je inicijalno identificirati sve moguće vrste **investicija** i **troškova** vezanih uz provođenje mjera informacijske sigurnosti. Poduzeća mogu usluge i proizvode iz portfelja vezanog uz informacijsku sigurnost pribavljati ili kao investicije, inkorporiranjem istih u portfelj rješenja kao **kratkotrajne** ili **dugotrajne** imovine, ili mogu odabrati mogućnost tretmana ove vrste proizvoda i usluga kroz **najam** i **leasing**, u slučaju čega se oni razmatraju kao tekući trošak[138]. Ova je činjenica osobito izražena u zadnjem desetljeću, inicijalno putem korištenja paradigme softvera kao usluge,[139] a kasnije i ostalih vezanih pojavnih oblika korištenja informatičkih resursa u obliku usluge.[140] Konvergencijom raznih

[138] U kontekstu upravljanja informatikom, često se koriste izrazi operativni trošak, tekući trošak ili varijabilni trošak za sav trošak održavanja i korištenja pojedinih komponenti informacijskog sustava, iako između tih pojmova postoje razlike u ekonomskoj teoriji. Suprotstavljeni način plaćanja za usluge bile bi investicije u vlastite informatičke resurse i imovinu.

[139] Kartica ovog pojma je "*SaaS*" – eng. „*Software as a Service*". Radi se o isporuci softverskih usluga utemeljenih na daljinskom Web pristupu putem Interneta. Za detalje cf. Webopedia, **http://www.webopedia.com/TERM/S/SaaS.html** (22.08.2013.)

[140] Radi se o paradigmama „*NaaS*" - eng. „*Network as a Service*", „*StaaS*" – eng. „*Storage as a Service*", te IaaS – eng. „*Infrastructure as a Service*", kod kojih se pristup, redom, mrežnim resursima, medijima za

tehnologija došlo je do spajanja svih navedenih mogućnosti uz dodatnu skalabilnost i fleksibilnost korištenjem informatičkih usluga „*u oblaku*“[141]. Navedeni razvoj dovodi do dodatnog kompliciranja različitih pojavnih oblika investicija i troškova vezanih uz poslovnu funkciju informatike, a samim time i informacijske sigurnosti, iako valja napomenuti kako su rukovoditelji i vlasnici poduzeća u značajnom dijelu neskloni korištenju mjera i tehnologije informacijske sigurnosti kroz najam, a osobito ukoliko se razni elementi nalaze pod kontrolom pružatelja usluga zbog problema implicitnog povjerenja. Međutim,i ta se situacija mijenja pod utjecajem narastajućih tehničko-tehnoloških zahtjeva, a osobito uslijed potrebe za usklađenošću sa zakonskim i strukovnim propisima te najboljom praksom. Temeljna **podjela investicija i troškova** u informacijsku sigurnost prikazana je u tablici 9. na sljedećoj stranici.

pohranu podataka te čitavoj informatičkoj infrastrukturi, ostvaruje putem Web servisa, odnosno Interneta, a često je pružatelj usluga druga poduzeće, odnosno entitet. Za više detalja cf. Webopedia, **http://www.webopedia.com/TERM/S/SaaS.html** (22.08.2013.), Telecom Cloud, **http://www.telecom-cloud.net/network-as-a-service**/ (22.08.2013.), te Gartner IT Glossary, **http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas**/ (22.08.2013). Svi navedeni načini pružanja informatičkih usluga jednom kraticom nazivaju se „XaaS“ – eng. „Anything as a Service“, odnosno, „Sve kao usluga“. Za detalje cf. SearchCloudComputing, **http://searchcloudcomputing.techtarget.com/definition/XaaS-anything-as-a-service** (22.08.2013).

[141] Kratica od eng. „*Cloud Computing*“. Radi se o paradigmi korištenja računalnih resursa korištenjem dijeljenih resursa, umjesto vlastitog posjedovanja servera ili uređaja koji pružaju usluge i aplikacije. Za detalje cf. Webopedia, **http://www.webopedia.com/TERM/C/cloud_computing.html** (22.08.2013).

Tablica 9: Struktura investicija i troškova poslovne funkcije informacijske sigurnosti

	KAPITALNO BUDŽETIRANJE	OPIS
1.	1. NAZIV INVESTICIJE	1.1. Kupovina hardvera
		1.2. Kupovina telekomunikacijskih sigurnosnih rješenja
		1.3. Kupovina osnovnog sigurnosnog softvera
		1.4. Kupovina aplikacijskog sigurnosnog softvera
		1.5. Ulaganja u strateške sigurnosne studije/Razvoj sigurnosno-aplik. rješenja
		1.6.Ulaganja u informacijsko-sigurnosnu infrastrukturu
		1.7. Ulaganje u sigurnost telekomunikacijskih i mrežnih sustava
		UKUPNE INVESTICIJE

	TEKUĆI TROŠAK	OPIS TIPA TROŠKA
2.	2.1. IS APLIKACIJE	2.1.1. Strateške sigurnosne studije
		2.1.2. Razvoj sigurnosnih aplikacija
		2.1.3. Trošak upravljanja sigurnosnim aplikacijama
		2.1.4. Održavanje sigurnosno aplikacijskog softvera
		2.1.5. Najam sigurnosno aplikacijskog softvera
		2.1.6. Leasing sigurnosno aplikacijskog softvera
		UKUPNI APLIKACIJSKI TROŠAK
	2.2. INFORMACIJSKO-SIGURNOSNA INFRASTRUKTURA	2.2.1. Razvoj informacijsko-sigurnosne infrastrukture
		2.2.2. Korisnička podrška
		2.2.3.Infrastrukturne usluge za informacijsko-sigurnosna rješenja
		2.2.4. Usluge za sigurnosno-aplikacijske servere
		2.2.5. Usluge za korporativna sigurnosna rješenja
		2.2.6. Usluge sigurnosnog konzaltinga
		2.2.7. Održavanje sigurnosno aplikacijskog hardvera
		2.2.8. Održavanje osnovnog informacijsko-sigurnosnog softvera
		2.2.9. Najam osnovnog informacijsko-sigurnosnog softvera
		2.2.10. Najam i leasing informacijsko-sigurnosnog hardvera
		2.2.11. Kupovina informacijsko-sigurnosnog rješenja (neinvesticijsko)
		UKUPNI TROŠAK INFORMACIJSKO-SIGURNOSNE INFRASTRUKTURE
	2.3. TELEKOMUNIKACIJSKO-SIGURNOSNA INFRASTRUKTURA	2.3.1. Razvoj sigurnosno-telekomunikacijske infrastrukture
		2.3.2. Sigurnosne usluge za lokalnu mrežu (LAN)
		2.3.3. Sigurnosne usluge za fiksnu telefoniju
		2.3.4. Sigurnosne usluge za mobilnu telefoniju
		2.3.5. Sigurnosne usluge prijenosa podataka
		2.3.6. Sigurnosne usluge za korištenje Interneta
		2.3.7. Ostale sigurnosne usluge
		2.3.8. Usluga održavanja sigurnosno telekomunikacijskog hardvera
		2.3.9. Usluga održavanja sigurnosno telekomunikacijskog softvera
		2.3.10. Najam sigurnosno telekomunikacijskih rješenja
		2.3.11.Kupovina telekomunikacijsko sigurnosniih rješenja (neinvesticijsko)
		UKUPAN TROŠAK TELEKOMUNIKACIJSKO SIGURNOSNIH RJEŠENJA
		POD-SUMA INFORMACIJSKO TEHNOLOŠKIH PODRUČJA
	2.4. OSTALO	2.4.1. Trošak potrošnog materijala
		UKUPNI OPERATIVNI TROŠAK
	TROŠAK RADA	Standardizirani trošak stalnog sigurnosnog osoblja
	TROŠAK OSIGURANJA	Godišnji trošak police osiguranja

Izvor: priredio autor

Kao što se vidi iz tablice 9., investicijski utrošci vezani uz informacijsku sigurnost odnose se na razne oblike kupovine hardvera koji ima ulogu osiguravanja informacijske sigurnosti, neovisno o tome radi li se o hardveru koji se odnosi na poslužiteljske sustave ili telekomunikacijske mreže. Osim toga, u investicije informacijske sigurnosti pripadaju još i osnovni sigurnosni softver te aplikacijski sigurnosni softver, te ulaganja u sigurnosno-aplikativna rješenja koja su dugoročnog karaktera, odnosno dugoročni razvojni projekti.

4.2. Analiza investicijskih ulaganja u sustav upravljanja informacijskom sigurnošću

Analizu investicijskih ulaganja u sustav upravljanja informacijskom sigurnošću je potrebno obaviti na način da se obrazlože glavne odrednice pojedinih pojavnih oblika takvih ulaganja. Uslijed navedenog u nastavku se izlažu sljedeće jedinice: **1) Ulaganja u sigurnosnu računalnu infrastrukturu, i 2) Ulaganja u sigurnosne računalne aplikacije.**

4.2.1. Ulaganja u sigurnosnu računalnu infrastrukturu

Ulaganja u sigurnosnu računalnu infrastrukturu dijele **temeljne karakteristike** koje su specifične za općenita ulaganja u hardver. Računalni hardver, a osobito rješenja koja se koriste u osiguravanju informacija, moraju se nužno promatrati kroz koncept ukupnog troška korištenja[142]. Naime, računalni hardver je nužno povezan uz vrlo brzo tehnološko zastarijevanje, visoke operativne troškove održavanja, oportunitetne troškove alternativnih investicija, a osobito je komplicirano usporediti trošak investicije u hardver informacijsko-sigurnosnog rješenja s troškom nastupa rizika. Korištenjem koncepta ukupnog troška korištenja moguće je procijeniti ukupan financijski utjecaj investicije u računalni hardver informacijsko-sigurnosnog rješenja. (Osten & Kanter, 2007, p. 48)

Mala i srednja poduzeća su izložena **višim jediničnim troškovima** investicijske nabave računalnog hardvera iz razloga što ne mogu tijekom procesa nabave derivirati dodatne koristi od povoljne pregovaračke pozicije uslijed malog kupovnog volumena. Iz navedenog razloga, početni investicijski troškovi neovisno o konačno potrebnim kapacitetima za mala i srednja poduzeća su komparativno viši nego za velika poduzeća koja imaju jaču pregovaračku poziciju.

Pri implementiranju većine hardverskih rješenja koja otklanjaju rizike informacijske sigurnosti, poduzeća su izložena dvjema opcijama između kojih se mogu odlučiti, a koje su povezane uz inicijalnu instalaciju i uvođenje u rad. Jedna je mogućnost dobava takve vrste usluge **od strane prodavača rješenja**, odnosno distributera, dok je druga mogućnost **samostalna** instalacija i uvođenje u rad. Kompleksnost takvih rješenja najčešće ne dozvoljava samostalnu instalaciju, a često i održavanje, već su mala i srednja poduzeća izložena nužnosti uključivanja takve usluge koja predstavlja dodatni inicijalni trošak povrh nabavne cijene informacijsko sigurnosnog hardverskog rješenja.

[142] *TCO*, kratica od eng. „*Total Cost of Ownership*“. Radi se o financijskoj procjeni koja računa ukupne direktne i indirektne troškove korištenja nekog računalnog sustava, a ne samo inicijali trošak nabave.

Budući da hardverska rješenja povezana uz informacijsku sigurnost uklanjaju ili umanjuju odgovarajuće rizike, to znači da se ona moraju konstantno poboljšavati najnovijim definicijama, protokolima uklanjanja ugroza ili novim funkcionalnostima. Način na koji se to postiže je primjena **sigurnosnih zakrpa** kojima se na postojećem hardveru implementiraju nove funkcionalnosti. Sigurnosne se zakrpe mogu preuzimati od proizvođača instaliranog hardvera ili od trećih strana koje se bave distribucijom te vrste digitalnih proizvoda. Uobičajeno se kod kupovine informacijsko-sigurnosnih rješenja prva godina ove vrste podrške uključuje u nabavnu cijenu, dok se za svaku sljedeću godinu mora posjedovati sklopljen ugovor o održavanju koji uključuje i ovu vrstu usluge. Naime, bez plaćanja održavanja, efektivno prestaje mogućnost potpunog korištenja svih funkcionalnosti hardvera, podrška od strane proizvođača, odnosno mogućnosti otklanjanja grešaka u radu, nadogradnje na nove verzije softvera koji je implementiran kao operativni sustav informacijsko-sigurnosnog hardvera, mogućnost migracije na druge lokacije ili upotrebe u drugim organizacijskim jedinicama.

Osim navedenog, kod analize implementacije vlastitih hardverskih rješenja kao novih investicija valja uzeti u obzir i sljedeće elemente koji povećavaju **troškove implementacije**, a kasnije i korištenja takvih rješenja:

1. **Trošak dodatnog hardvera** koji može biti potreban za korištenje hardverskih rješenja informacijske sigurnosti,[143]
2. **Trošak potrebne instalacije** operativnih sustava,
3. **Trošak aplikativnih sustava** vezanih uz hardverska rješenja informacijske sigurnosti,
4. **Trošak integracije i prilagođavanja** ostalih sustava u poduzeću.

Često izostavljeni elementi analize investicijskog troška informacijsko sigurnosnih rješenja u malim i srednjim poduzećima su:[144]

1. **Trošak nabave**,
2. **Trošak buduće zamjene** (ostali računalni sustavi u poduzeću mogu biti rekonfigurirani na način da su prilagođeni individualnom informacijsko-sigurnosnom rješenju, što može povećati njihov trošak u budućnosti), i
3. **Trošak povećanja kapaciteta** – u pravilu, hardverska rješenja imaju točno definiranu gornju granicu kapaciteta korištenja i često neko rješenje ne može biti korišteno ukoliko se poveća kapacitet, odnosno traženi broj korisnika. U okviru malih i srednjih poduzeća

[143] npr. osobna računala, prijenosna računala ili enkripcijski uređaji.
[144] Potrebno je primijetiti kako je činjenica da korištenje računalstva u oblaku smanjuje neke od navedenih troškova, ali otvara čitav niz pitanja, a osobito vezanih uz sigurnost podataka i sustava povjerenih vanjskom pružatelju usluga. Osim toga, točka isplativosti eksternalizacije ovisi o vrsti sustava, organizacije, pružatelja usluga te razini zrelosti informacijskog sustava i vlastite informacijske imovine.

s obzirom na ograničenost definicijom, ova činjenica ne bi trebala predstavljati značajniji problem.

4.2.2. Ulaganja u sigurnosne računalne aplikacije

Investicijska ulaganja u izradu sigurnosnih računalnih aplikacija posjeduju većinu karakteristika investicijskih ulaganja u informacijsko sigurnosni hardver. Temeljne **razlike** između ulaganja u informacijsko sigurnosni hardver i sigurnosne računalne aplikacije leži u sljedećim činjenicama:

1. Za razliku od informacijsko sigurnosnog hardvera koji je računovodstveno gledano dio materijalne imovine poduzeća, aplikacije su dio **nematerijalne** imovine poduzeća. To vodi do drugog tretmana imovine od strane rukovoditelja i vlasnika, ali i poreznog razmatranja, osobito vezano uz porez po odbitku,
2. Sigurnosne računalne aplikacije, ukoliko se ukupnost njihovog troška vlasništva, nose značajan kasniji **trošak održavanja**. Ovaj trošak može se, ovisno o vrsti ugovora, odnositi na trošak reinstalacija aplikacije pri transferu s jedne na drugu lokaciju, trošku nadogradnje na manje značajnu ili značajnu, novu inačicu ili pravo korištenja. U današnje doba, iznos održavanja računalnih aplikacija uobičajeno se plaća za prvu godinu korištenja obavezno već kod prvotne kupovine, dok se zatim plaća u godišnjim iznosima kako bi se zadržala ugovorna prava. Ukoliko se posjednik ili vlasnik sigurnosne računalne aplikacije odluči ne plaćati trošak održavanja, izložen je raznim problemima i poteškoćama, od nemogućnosti prijenosa s lokacije na lokaciju, do prestanka rada pojedinih funkcionalnosti. Trošak održavanja u ukupnom trošku eksploatacije softvera iznosi 75 do 80 %, i ova činjenica je uglavnom nepromijenjena već u zadnja tri do četiri desetljeća (Lientz, et al., 1978, p. 466),
3. Korištenje sigurnosnih aplikacija u pojedinim domenama često je povezano uz računalna ili aplikativna **rješenja trećih strana**. Uobičajeno je da pojedina poduzeća koja izrađuju ovakvu vrstu softverskih rješenja koriste definicije[145] od trećih strana koje isključivo pružaju takvu vrstu definicija. Na taj način uspješnost i kvaliteta informacijsko sigurnosnog rješenja ovisi ne samo o algoritmu već i o kvaliteti i brzini izdavanja takvih definicija koje se u obliku zakrpa ili nadopuna preuzimaju putem Interneta.

Neka od tipičnih područja primjene računalnih aplikacija u postizanju ciljeva informacijske sigurnosti su dvofaktorska autentikacija korisnika ili sustava, enkripcija (kodiranje), filtriranje sadržaja na Internetu prema protokolu ili vrsti sadržaja, sigurnost krajnjih točaka vlastitog

[145] npr. definicije (potpisi) virusa, trojanskih konja, obrazaca ponašanja itd.

sustava, antivirusna zaštita, sigurnost telefonskih usluga preko računalne mreže te osobito raširena kategorija računalnih aplikacija koje se koriste u svrhu računalne sigurnosti, a to su računalne aplikacije koje se koriste kako bi se osigurala sukladnost s certifikacijskim, zakonskim zahtjevima i zahtjevima najbolje prakse. (Kilpatrick, 2013)

4.3. Analiza operativnih troškova sustava upravljanja informacijskom sigurnošću

Tekući, a po prirodi **varijabilni trošak** informacijske sigurnosti sastoji se od tri temeljne komponente: 1. Tekući trošak korištenja i održavanja **aplikacijske podrške** informacijske sigurnosti, 2. Tekući trošak korištenja i održavanja **informacijsko-sigurnosne infrastrukture** i 3. Tekući trošak **telekomunikacijsko-sigurnosne infrastrukture**. Tekući trošak korištenja i održavanja aplikacijske podrške informacijske sigurnosti povezan je uz, najam, *leasing*[146], razvoj, i održavanje informacijsko sigurnosnih aplikacija, uključivo strateške studije i tekući trošak upravljanja navedenim aplikacijama. Tekući trošak informacijsko-sigurnosne infrastrukture odnosi se na operativni trošak razvoja informacijsko-sigurnosne infrastrukture, korisničku podršku pri korištenju, usluge konzaltinga, održavanja servera, hardvera, kao i najam i leasing informacijsko-sigurnosnog hardvera i softvera.

Tekući trošak održavanja telekomunikacijsko-sigurnosne infrastrukture odnosi se na tekući trošak razvoja sigurnosno-telekomunikacijske infrastrukture, istovjetnih rješenja koja se koriste za lokalnu mrežu,[147] usluge zemaljske (fiksne) telefonije, mobilne telefonije, prijenosa podataka i korištenja Interneta[148], te održavanja sigurnosno- telekomunikacijskog hardvera, softvera i rješenja.

Tri **izdvojena troška** koji se mogu identificirati a koji su povezani uz izgradnju, razvoj i korištenje sigurnosno-informacijskih poslovnih sustava su trošak **potrošnog materijala**, trošak **rada** i trošak **osiguranja**. Trošak potrošnog materijala se u računovodstvene svrhe obično tretira kao sitni inventar predstavlja one dijelove sigurnosno-informacijskih rješenja koji se po svojoj prirodi troše u roku kraćem od godinu dana i imaju manju vrijednost od 3500 Kn (Narodne novine 30., 2008). Trošak rada, zasebna je kategorija troška koji se rijetko uzima u

[146] *Leasing* je poseban oblik financiranja koji se zasniva na ideji da je objekt leasinga bolje koristiti nego kupiti. Leasing omogućuje korisniku da neku opremu ili nekretninu dobije na korištenje za vrijeme koliko mu je potrebna, umjesto da ju kupi. Pojam leasing dolazi od eng. "*to lease*" što znači iznajmiti, tj. dati u najam. Najam je sporazum na temelju kojeg najmodavac prenosi na korisnika leasinga, kao zamjenu za najamninu, pravo na korištenje nekog sredstva za dogovoreno razdoblje.“ Za detalje cf. Fin-In, **http://www.in-fin.info/krediti-i-leasing/** (21.08.2013.)

[147] *LAN*, kratica od eng. „*Local Area Network*“, za detalje cf. The free dictionary by Farlex, **http://www.thefreedictionary.com/LAN** (21.08.2013.)

[148] *WAN*, kratica od eng. „World Area Network“, za detalje cf. The free dictionary by Farlex, **http://www.thefreedictionary.com/wan** (21.08.2013.)

obzir kada se radi o analizi troškova informacijske sigurnosti, iz razloga što se smatra da je trošak rada relativno fiksan, zadan, iako kod razvoja kompleksnih informacijsko-sigurnosnih rješenja može biti vrlo značajan izdatak. Naposljetku, trošak osiguranja je posebna podvrsta troška povezanog uz uklanjanje ili umanjenje nastupa sigurnosnog incidenta kojim se osiguravajuća kuća obvezuje podmiriti nastalu štetu u odgovarajućem opsegu, dok poduzeće mora platiti odgovarajući iznos police osiguranja. Tržište osiguranja iz područja informacijske sigurnosti u Republici Hrvatskoj nije razvijeno, odnosno ta vrsta transfera rizika trenutačno nije moguća.

4.4. SPECIFIČNOSTI EKONOMSKE ANALIZE ULAGANJA U SUSTAVE UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU MALIH I SREDNJIH PODUZEĆA

Ova se cjelina obrazlaže kroz dvije povezane jedinice: **1) Teorijska razmatranja ekonomske analize poslovne funkcije informacijske sigurnosti**, **2) Mogućnosti primjene metode analitičkih hijerarhijskih procesa pri odlučivanju o ulaganjima u sustave upravljanja informacijskom sigurnošću** i **3) Mogućnosti analize povrata investicije ulaganja u informacijsku sigurnost.**

4.4.1. Teorijska razmatranja ekonomske analize poslovne funkcije informacijske sigurnosti

Kako bi se odgovorilo na pitanje koje su mogućnosti izračuna povrata investicije ulaganja u informacijsku sigurnost, valjalo je inicijalno izučiti literaturu koja se bavi tom problematikom i osobitostima funkcije upravljanja informacijskom sigurnošću. **Ekonomika informacijske sigurnosti** razmjerno je mlada grana ekonomije koja se pojavila prije petnaestak do dvadeset godina[149], kada je uočeno da je broj vrsta rizika informacijske sigurnosti velik, trošak nastupa incidenata informacijske sigurnosti značajan, te da posljedično informacijska sigurnost nije samo tehnička disciplina. Iz navedenog razloga potrebno je na početku svrstati razmatranja ove problematike u nekoliko kategorija.

U okviru razmatranja informacijske sigurnosti kao tradicionalno tehničke discipline, više autora zauzima sukladne stavove, ali uočavaju i potrebu za odmakom od takvog stava. Tradicionalno, informacijska sigurnost je tehnička disciplina čija svrha je pružanje **maksimalne** moguće razine

[149] Jedna od prvih konferencija s temom ekonomike informacijske sigurnosti održana je 2002. godine u Berkeleyu. Radi se o konferenciji „*Workshop on the Economics of Information Security*“ koja se održava svake godine u drugom gradu. Za detalje cf. Workshop on the Economics of Information Security 2013., **http://www.weis2013.econinfosec.org/** (17.07.2013.)

sigurnosti. (McGraw, 2006, p. 89) Procjenu mogućnosti nastupa sigurnosnog incidenta moguće je obaviti korištenjem subjektivnog probabilističkog modela kod kojega se koristi skala od pet koraka (od vrlo male mogućnosti do vrlo velike mogućnosti nastupa sigurnosnog incidenta). Ova vrsta pristupa je djelomično kvantitativna jer koristi kvalitativni pristup za procjenu kvantitativnih procjena vjerojatnosti. (Fahramand, et al., 2003, p. 350)

U procesima provođenja mjera informacijske sigurnosti, upravljanje rizicima informacijske sigurnosti je **ključna** aktivnost. Razmatranje informacijske sigurnosti u okviru financijskih kriterija među prvima promišlja Hoo, koji razvija jedan od prvih analitičkih sustava za donošenje odluka na način da analizira grupu zaštitnih mjera ili politika, a za svaku mjeru ili politiku pokušava se naći kompromis između troškova i dobrobiti. Ovakav postupak zahtijeva identifikaciju i procjenu informacijske imovine i procjenu potencijalnog utjecaja na poslovanje te donošenje odluka temeljem **analize troškova** i koristi informacijske sigurnosti. (Hoo, 2010) Ovaj način razmišljanja je osobito značajan jer se radi o jednom od prvih radova koji naglasak osim na mjere informacijske sigurnosti stavlja i na financijsku analizu vezanih troškova u odnosu na moguće koristi. U tom kontekstu, povećanje kompleksnosti informacijskih sustava i prateće tehnologije zahtijeva sofisticirane **metode** donošenja odluka vezanih uz investicije u informacijsku sigurnost i zaštitu informacijske imovine. (Gordon & Richardson, 2004) Poduzeća poduzimaju mjere informacijske sigurnosti kako bi se osigurali monopoli, kako bi se naplaćivale različite cijene različitim klijentima za istu uslugu i kako bi se **smanjio rizik**, te je takvo ponašanje za velike sustave racionalno. (Anderson, 2001, p. 360) Razmatranje ekonomske komponente informacijske sigurnosti i vezana istraživanja povećavaju se zbog povećanja opsega **ulaganja** u sustave upravljanja informacijskom sigurnošću. (Anderson, 2001, p. 362) Nastavno, promatranje aktivnosti informacijske sigurnosti s **ekonomskog** stajališta može pronaći odgovore na pitanja u kojima striktna tehnička stajališta ne mogu dati adekvatne odgovore. (Gordon & Loeb, 2002, p. 440) Sa ekonomske strane, ali i promatrano subjektivno, poduzećima je optimalno **minimalno ulaganje** u informacijsku sigurnost a povećanje razine ulaganja samo ukoliko su direktno izložena troškovima zbog npr. revizijskih zahtjeva u odnosu na neku mjeru informacijske sigurnosti, pa su tako npr. vatrozidi u širokoj upotrebi ne zato što su jako efikasni, već zato što ih gotovo svi standardi revizije informacijskih sustava zahtijevaju. (Schneier, 2004, p. 205) Međutim, informacijska sigurnost nije samo trošak, već kreira novu **vrijednost** koja omogućuje operacije u *e*-poslovanju poduzeća. (Cavusoglu, 2004, p. 75) Aproksimativna mjera pravog troška sigurnosnog incidenta je **gubitak** u tržišnoj kapitalizaciji poduzeća. (Fahramand, et al., 2003, p. 352) Neki autori investiciju u informacijsku sigurnost promatranju kroz smanjenje rizika uspješnosti napada. Prednosti investiranja u informacijsku sigurnost mjere se kao razlika očekivanih gubitaka u scenarijima kada se odgovarajuća mjera koristi u odnosu na nekorištenje mjera. (Ryan & Ryan, 2006, p. 582) Tako neki autori tehničku

analizu posljedica i implikacija nastupa incidenata informacijske sigurnosti zamjenjenjuju analizom ekonomski **optimalnih** mjera prevencije potencijalnih nastupa incidenata. (Acquisti, et al., 2006) U svojoj studiji ova grupa autora analizira neočekivane[150] povrate investicija u dionička društva nakon nastupa sigurnosnih incidenata o kojima je informacija postala javna. Analizirajući incidente informacijske sigurnosti i kretanje cijena dionica poduzeća nakon što su oni javno objavljeni, autori dolaze i do zaključka da kod relativno promatrano većih poduzeća, utjecaj incidenata informacijske sigurnosti ima manji utjecaj na tržišnu kapitalizaciju.

Naposljetku, zadnjih nekoliko godina pojavljuju se teorije ekonomike informacijske sigurnosti. Ekonomika informacijske sigurnosti je novo područje **ekonomike** koje koristi ekonomsku teoriju i modele u analizi odnosa između uključenih dionika. (Bojanc & Jerman-Blažič, 2007, p. 218) Ekonomika informacijske sigurnosti razvija se u više različitih smjerova. Neki pristupi ekonomici informacijske sigurnosti koriste analizu kratkoročnih i dugoročnih dobrobiti, odnosno materijalnih i nematerijalnih koristi, dok drugi pristupi koriste teoriju **efikasnosti** tržišta ili tržišnu valuaciju poduzeća kako bi kvantificirali troškove. (Bojanc & Jerman-Blažič, 2008, p. 418) Druge teorije promatraju koja je optimalna razina investiranja u mjere informacijske sigurnosti u odnosu na **marginalne troškove** i koristi od takvih ulaganja i troškova. Poduzeće treba investirati u mjere informacijske sigurnosti samo do razine na kojoj su marginalne koristi investiranja jednake marginalnim troškovima. Ako je marginalna **korist** veća od marginalnog **troška**, dodatna investicija je opravdana. (Lawrence & Loeb, 2001, p. 72) Kod analize marginalnog troška informacijske sigurnosti, moguće je da gornji limit investiranja ne bude ispravan kada se model primijeni na sve moguće rizike. (Wilemson, 2006, p. 260) Sigurnost informacija je **inverzija rizika** i stoga treba ustanoviti kvantitativni pristup mjerenju dobrobiti od mjera informacijske sigurnosti kroz mjerenje očekivanog gubitka i rizika. (Ryan & Ryan, 2006, p. 582) Pozitivna razina neto koristi od investiranja u informacijsku sigurnost predstavlja **opravdanu** (atraktivnu) investiciju. Ovaj pristup uključuje sposobnost korištenja **distribucije vjerojatnosti** pojave incidenta informacijske sigurnosti. (Gordon & Loeb, 2001, p. 73)

Jedan od mogućih teoretskih pristupa je i korištenje **teorije igara**. One se mogu koristiti za procjenu investiranja u rješenja informacijske sigurnosti, a u tom slučaju smatra se kako je upravljanje informacijskom sigurnošću **igra** između poduzeća i napadača koji imaju motiv nanijeti štetu poduzeću iz odgovarajućeg razloga. (Cavusoglu, 2004, p. 76) Sustavi i softver moraju biti dizajnirani na način da nastavljaju ispravno funkcionirati čak i u slučaju sigurnosnih napada. Predlažu se tri skupa mjera: a) Primijenjeno upravljanje rizicima, b) Najbolja praksa razvoja informacijskih sustava i c) Znanje. Praktični problem pri korištenju ovog pristupa je u

[150] Točan korišten izraz je „*abnormalne povrate*“.

činjenici kako se informacijski sustavi obično se grade pod premisom da neće biti namjerno **zloupotrebljavani**. (McGraw, 2006, p. 154)

Iz navedenog se može zaključiti kako tehnički pristup organizaciji mjera informacijske sigurnosti nije primjeren malim i srednjim poduzećima jer isključuje ekonomske i financijske učinke. Pristup koji koristi marginalne troškove i investicije kao i teorija igara previše su teorijski i objektivno previše kompliciran za primjenu u okruženjima malih i srednjih poduzeća. Ekonomsko razmatranje investicija i troškova informacijske sigurnosti korištenjem klasične financijske metodologije interne stope povrata, neto sadašnje vrijednosti investicije u informacijsku sigurnost i diskontiranih novčanih tijekova nameće se kao izbor koji je realno provediv u malim i srednjim poduzećima te se detaljno obrazlažu rezultati istraživanja u nastavku.

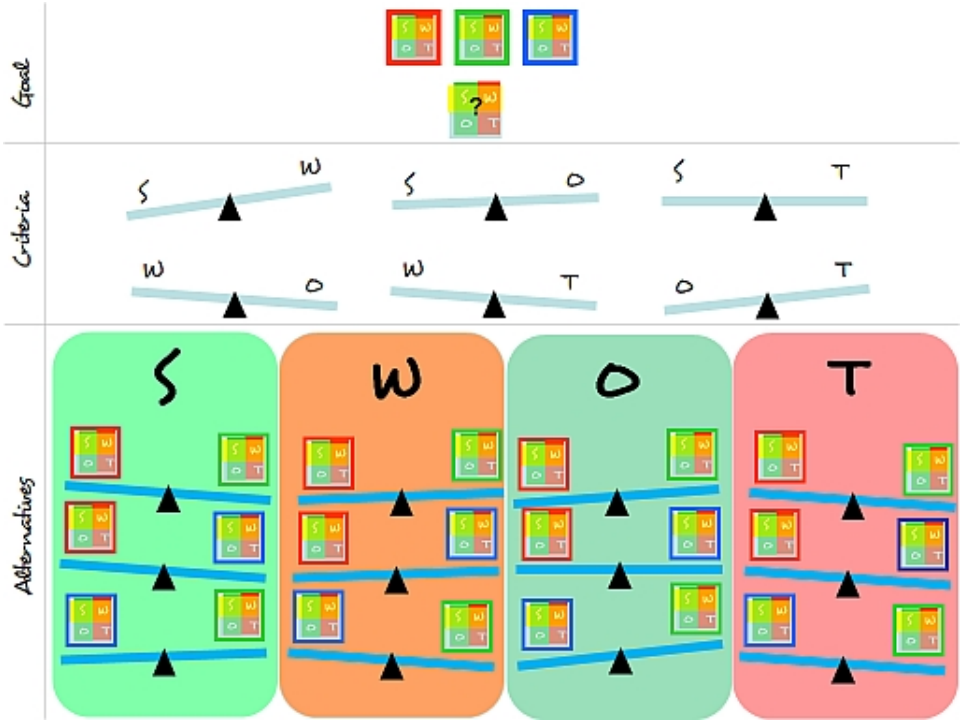
4.4.2. Mogućnosti primjene metode analitičkih hijerarhijskih procesa pri odlučivanju o ulaganjima u sustave upravljanja informacijskom sigurnošću

Jedna od metoda koja se može koristiti pri određivanju sastava portfelja informacijsko-sigurnosnih usluga koje će neko poduzeće koristiti u svom radu je **AHP - metoda analitičkih hijerarhijskih procesa**[151]. Radi se o tehnici organizacije i analize kompleksnih odluka koja je bazirana na kvantitativnim metodama ali sadrži i subjektivni element. (Meixner, 2011, p. 4) Korištenjem AHP metode ne dolazi se do „*idealne*“ odluke, nego se uvažavaju svi kriteriji pri odlučivanju, oni se kvantificiraju čak i kada se međusobno čine nespojivima ili neusporedivima, procjenjuje se njihov utjecaj u odnosu na ukupnost ciljeva koje se želi postići i procjenjuju se alternativna rješenja, a osobno onda kada se pokušava uspostaviti balans između financijskog i subjektivnog, nefinancijskog načina odlučivanja. (Garbin-Praničević & Srića, 2013, p. 213)

Metoda se sastoji od **dekompozicije** problema o kojemu se odlučuje u hijerarhiju problema koji se mogu nezavisno analizirati. Svaki od tih elemenata hijerarhije odnosi se na neki od aspekata problema odlučivanja. Kada je hijerarhija uspostavljena, njeni se elementi uspoređuju u parovima, pri čemu je uspoređivanje subjektivno. Ove se ocjene izražavaju numerički pri čemu se izvodi težinski čimbenik za svaki element hijerarhije. Naposljetku, računaju se numerički prioriteti za svaku alternativu odluke koje predstavljaju relativnu sposobnost alternativa da postignu cilj odlučivanja. Postupak primjene AHP metode slikovito je prikazan na ilustraciji 1. na sljedećoj stranici.

[151] *AHP* je kratica od eng. *„Analytic Hierarchy Process“*

Ilustracija 1: Prikaz postupka primjene AHP metode

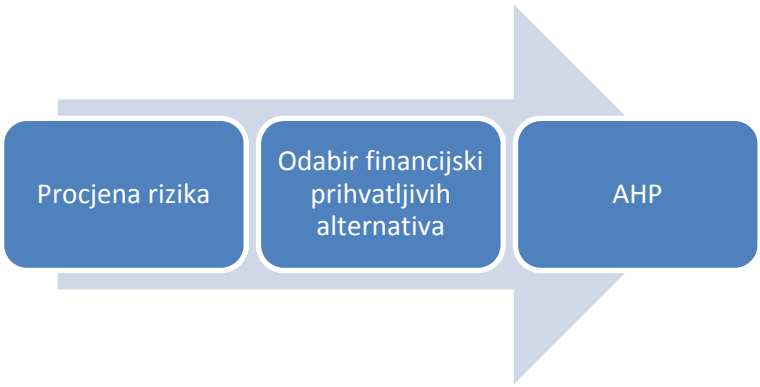


Izvor: 123-AHP, Moj izbor - moja odluka,
http://www.123ahp.com/PrimjerDocs/SWOT_en/SWOT_and_AHP_123ahp.jpg , (24.12.2011.)

Neka od **područja primjene** metode AHP su rješavanje konflikata, upravljanje sustavima kvalitete, sustavno vrednovanje, prioritiziranje, predviđanje, odabiranje i alokacija resursa.

Jedan od temeljnih problema pri odlučivanju o uključivanju nekog sigurnosnog rješenja u portfelj je problem **raspoloživih** financijskih sredstava za financiranje investicije. U praksi se često događa da se tijekom procjene rizika neki rizici nerazmjerno podcjenjuju ili precjenjuju ili se u točki kada rukovoditelji donose odluku o investiciji u neko sigurnosno rješenje preuzimaju previsoki implicitni rizici, odnosno preinvestira se u neka rješenja koja sobom ne donose visoke razine rizika. Metodom AHP moguće je ovaj proces **objektivizirati**. Potencijalna primjena metode AHP u odabiru investicije u informacijsku sigurnost imala bi sljedeće korake, kako je prikazano na shemi br. 12. na sljedećoj stranici.

Shema br. 12.: Smještaj AHP metode u postupku odlučivanja o investiranju u informacijsku sigurnost



Izvor: priredio autor

Jedna od mogućnosti korištenja metode AHP istražena je korištenjem *online* ekspertnog sustava (Init, 2007) „*Moj izbor moja odluka*“.[152] Ulazni **parametri** modela su mogućnosti ulaganja u odgovarajuće oblike osiguravanja informacijske sigurnosti poduzeća koji su odabrani tako da su sukladni kontrolama Aneksa A ISO standarda 27001:2005 koji regulira funkcioniranje sustava upravljanja informacijskom sigurnošću. (SAI GLOBAL, 2007, p. 13) Konkretno, predviđene mogućnosti **ulaganja** su sljedeće:

1. Ulaganja u sigurnost pristupa informacijskim sustavima,
2. Ulaganja u organizaciju informacijske sigurnosti,
3. Ulaganja u sigurnost okruženja,
4. Ulaganja u izradu i provođenje sigurnosnih politika,
5. Ulaganja u sukladnost sa zakonskim propisima,
6. Ulaganja u osiguravanje kontinuiteta poslovanja,
7. Ulaganja u upravljanje informacijskom imovinom,
8. Ulaganja u informacijsku sigurnost zaposlenika,
9. Ulaganja u sigurnost operacija i upravljanja,
10. Ulaganja u sigurnost nabave, razvoja i održavanja sustava.

Definiraju se i kriteriji za koje se uzima da su bitni kod odlučivanja o ulaganju u informacijsku sigurnost. Radi se o proizvoljnim kriterijima koji proizlaze iz poslovnih zahtjeva vezanih uz upravljanje i uvođenje sustava upravljanja informacijskom sigurnošću. U konkretnom slučaju, ti su zahtjevi (**kriteriji**) sljedeći:

1. Umanjenje rizika od sigurnosnog incidenta,

[152] „*Moj izbor-moja odluka*“ hrvatska je inačica online Internet ekspertnog sustava za odlučivanje koji je smješten na Internet adresi **http://www.mojizbormojaodluka.net/,** (20.12.2011.) Ovaj Internet servis omogućuje svima korištenje AHP metode u osobne ili poslovne svrhe.

2. Raspoloživost financijskih sredstava za investiciju,
3. Mjerljivost konkretne koristi,
4. Raspoloživost stručnog osoblja za uvođenje sustava.

Na taj način su definirani ulazni elementi sustava te se pristupa međusobnoj usporedbi elemenata modela pri čemu se osobne **preferencije** izražavaju Saaty-jevom skalom[153] koja ima pet stupnjeva i četiri međustupnja opisanih intenziteta. Saaty-jeva skala prikazana je u tablici br. 10.

Tablica br. 10: Odrednice Saaty-jeve skale

Intenzitet važnosti	**Definicija**	**Objašnjenje**
1	Jednako važno	Obje alternative jednako pridonose cilju
3	Umjereno važnije	Umjerena prednost jedne alternative
5	Strogo važnije	Favoriziranje jedne alternative
7	Vrlo stroga, dokazana važnost	Dominacija jedne alternative dokaziva je u praksi
9	Ekstremna važnost	Favoriziranje jedne alternative potvrđeno je s najvećom sigurnošću
2,4,6,8	Međuvrijednosti	

Izvor: 123-AHP, Moj izbor - moja odluka, prilagodio autor prema h**ttp://www.ahpacus.com/OMetodi.aspx**, (24.12.2011.)

Ukupni prioriteti alternativa dobivaju se izračunom iz lokalnih prioriteta (važnosti), a koji su izračunati iz vlastitih **procjena relativnih** važnosti kriterija i vezanih alternativa u parovima. Tako dobivene rezultate prikazuje tablica br. 11. na sljedećoj stranici.

153 *AHP* metodu je razvio dr. Thomas Saaty 1970-ih godina dok je predavao na *Wharton School of Business*. Metoda je do dan-danas ostala među najcjenjenijima i naširoko upotrebljavanim metodama u procesu odlučivanja. Mnoge institucije i kompanije koriste se njome u donošenju važnih poslovnih odluka.

Tablica br. 11: Izračunati međurezultati odnosa kriterija pri odlučivanju o investiranju u sustave informacijske sigurnosti

međurezultati

odnosi kriterija	Raspoloživost financ. sredstava	Umanjenje rizika od sig. incidenta	Mjerljivost	Raspoloživost stručnog osoblja
Raspoloživost financ. sredstava	1	1/6	**7**	**8**
Umanjenje rizika od sig. incidenta	**6**	1	**7**	**8**
Mjerljivost	1/7	1/7	1	**6**
Raspoloživost stručnog osoblja	1/8	1/8	1/6	1

CI: 0,2638 CR: 0,2964 λ: 4,7914

Raspoloživost financ. sredstava	...u sigurnosne politike	...u organizaciju inf. sigurnosti	...u upravljanje inf. imovinom	...u sigurnost zaposlenika	... u sigurnost okruženja	... u sigurnost operacija i upravljanja	... u sigurnost pristupa sustavima	... u sigurnost nabave, razvoja i odrzavanja sustava	... u sigurnost kontinuiteta poslovanja	... u sukladnost sa zakonskim propisima
...u sigurnosne politike	1	**8**	**8**	**8**	**8**	**8**	**8**	1	**8**	1
...u organizaciju inf. sigurnosti	1/8	1	**8**	**8**	**8**	**8**	**8**	**8**	**7**	1
...u upravljanje inf. imovinom	1/8	1/8	1	**8**	1/8	**5**	1/9	**7**	1	1/8
...u sigurnost zaposlenika	1/8	1/8	1/8	1	1	1/7	1/7	1	1/7	1/8
... u sigurnost okruženja	1/8	1/8	**8**	1	1	**7**	**7**	**6**	1/7	1/8
... u sigurnost operacija i upravljanja	1/8	1/8	1/5	**7**	1/7	1	1/8	**6**	**7**	1/7
... u sigurnost pristupa sustavima	1/8	1/8	**9**	**7**	1/7	**8**	1	**7**	**8**	1
... u sigurnost nabave, razvoja i odrzavanja sustava	1	1/8	1/7	1	1/6	1/6	1/7	1	1	1/7
... u sigurnost kontinuiteta poslovanja	1/8	1/7	1	**7**	**7**	1/7	1/8	1	1	1
... u sukladnost sa zakonskim propisima	1	1	**8**	**8**	**8**	**7**	1	**7**	1	1

CI: 0,8783 CR: 0,5894 λ: 17,9045

Umanjenje rizika od sig. incidenta	...u sigurnosne politike	...u organizaciju inf. sigurnosti	...u upravljanje inf. imovinom	...u sigurnost zaposlenika	... u sigurnost okruženja	... u sigurnost operacija i upravljanja	... u sigurnost pristupa sustavima	... u sigurnost nabave, razvoja i odrzavanja sustava	... u sigurnost kontinuiteta poslovanja	... u sukladnost sa zakonskim propisima
...u sigurnosne politike	1	1/7	1	1/7	1/8	1/8	1/8	1/8	1/8	1/8
...u organizaciju inf. sigurnosti	**7**	1	**7**	**7**	1/5	**5**	1/8	**5**	**6**	**7**
...u upravljanje inf. imovinom	1	1/7	1	1/7	1/7	**4**	1/8	**5**	**4**	**6**
...u sigurnost zaposlenika	**7**	1/7	**7**	1	1/5	1/5	1/6	**3**	1/6	**2**
... u sigurnost okruženja	**8**	**5**	**7**	**5**	1	**5**	1/8	**3**	**4**	**5**
... u sigurnost operacija i upravljanja	**8**	1/5	1/4	**5**	1/5	1	1/5	1/4	**3**	**3**
... u sigurnost pristupa sustavima	**8**	**8**	**8**	**6**	**8**	**5**	1	**7**	**9**	**9**

Izvor: priredio autor korištenjem ekspertnog sustava na Internet stranicama 123-AHP, Moj izbor - moja odluka, **http://www.ahpacus.com**, (16.12.2011.)

Konačni rezultati izračuna pokazuju kako je prema kriteriju koristi u odnosu na trošak **najpoželjnije** ulaganje u sigurnost pristupa sustavima, organizaciju informacijske sigurnosti, sigurnosne politike, sukladnost sa zakonskim propisima i tako redom. Ovakvu prioritizaciju

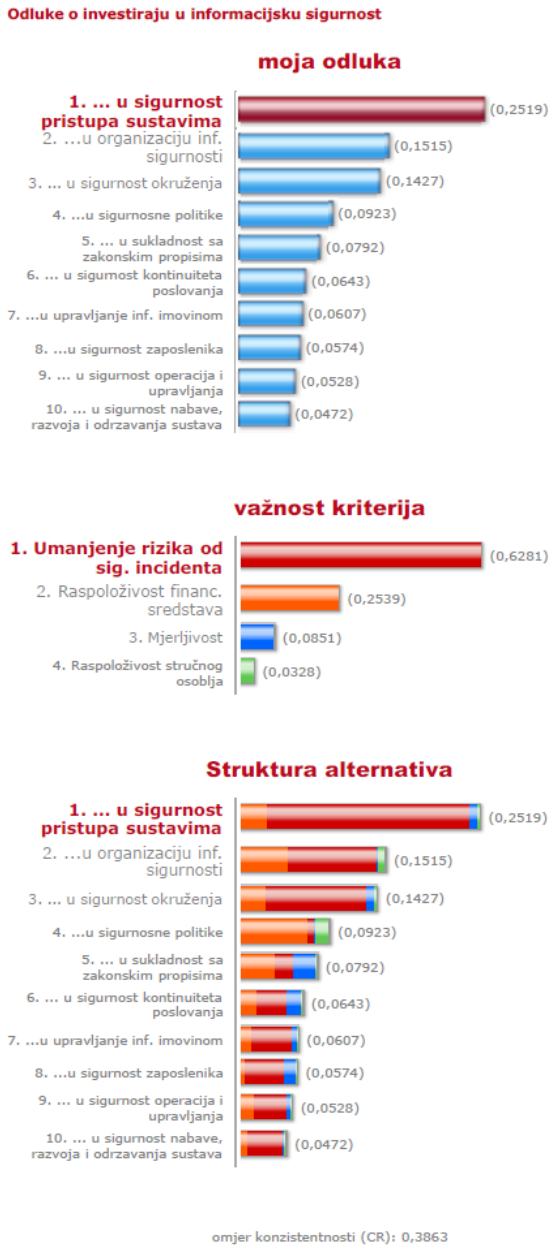
potvrdit će i subjektivno, iskustveno promišljanje ove problematike. Konkretni rezultati prikazani su na grafikonu br. 1.

Grafikon br. 1: Prioriteti odlučivanja o investiranju u informacijsku sigurnost

Izvor: priredio autor korištenjem ekspertnog sustava na Internet stranicama 123-AHP, Moj izbor - moja odluka, **http://www.ahpacus.com**, (16.12.2011.)

Izračunatu važnost kriterija kao i strukturu alternativa prikazuje grafikon broj 2. na sljedećoj stranici.

Grafikon br. 2: Važnost kriterija i struktura alternativa pri donošenju odluke o investiranju u informacijsku sigurnost



Izvor: priredio autor korištenjem ekspertnog sustava na Internet stranicama 123-AHP, Moj izbor - moja odluka, **http://www.ahpacus.com**, (16.12.2011.)

Pri korištenju AHP metode potrebno je obratiti pažnju na **omjer konzistentnosti**[154] kojim se kod AHP metode mjeri konzistentnost subjektivnog odlučivanja. Ukoliko je omjer konzistentnosti manji ili jednak 10 %, nekonzistentnost u odlučivanju je prihvatljiva a ukoliko je omjer konzistentnosti veći od 10 %, u tom slučaju trebalo bi revidirati preferencije pri odlučivanju i odlučivanje o alternativama u postupku nije konzistentno. U konkretnom primjeru

[154] Uobičajena kratica za mjeru konzistentnosti kod korištenja *AHP* metode je *CR*, kratica od eng. *„Consistency Ratio"*.

iako se struktura alternativa subjektivno čini ispravnom, omjer konzistentnosti je veći od 10%. Budući da bi u ovako kompleksnom modelu bilo vrlo kompliciranо iznova ocjenjivati konzistentnost pojedinih međukoraka odlučivanja, ovo upućuje na činjenicu kako bi bilo moguće koristiti metodu AHP pri odlučivanju o ulaganjima u informacijsku sigurnost, no isključivo ukoliko je broj alternativa i kriterija manji, odnosno ukoliko se radi o nekoliko alternativa i kriterija. U praksi bi to bilo moguće očekivati iz razloga što je prikazani primjer razmjerno kompleksan, dok se pri odlučivanju obično radi o nekoliko kriterija i nekoliko alternativa koje se razmatraju, dok se ovdje radilo o deset alternativa i četiri kriterija koji pokrivaju cijeli aneks A ISO 27001:2005 standarda.

4.4.3. Mogućnosti analize povrata investicije ulaganja u informacijsku sigurnost

Obrada ove problematike nameće potrebu da se detaljno prouče sljedeće tematske cjeline: **1) specifičnosti ekonomskog toka, 2) specifičnosti novčanog toka, 3) problemi pri korištenju metode interne stope prinosa, 4) odlučivanje o zamjeni implementiranog sigurnosnog rješenja,** te **5) ostale mogućnosti korištenja financijskih metoda pri odlučivanju o ulaganju u sustave upravljanja informacijskom sigurnošću.**

4.4.3.1. Specifičnosti ekonomskog toka

Kod analize **ekonomskog toka** sigurnosnog rješenja upravljanja sustavom informacijske sigurnosti zanemaruje se struktura izvora financiranja.[155] Razlog za to je činjenica što kamate po uzetim kreditima ne smanjuju ekonomski potencijal rješenja u koje je investirano ili imovinu, nego smanjuju financijski potencijal poduzeća.

Klasična analiza ekonomskog toka investicije, a u promatranom slučaju investicije u informacijsko-sigurnosnu infrastrukturu zahtijeva inicijalnu procjenu učinaka koji su svedeni na tržišne cijene iz **prve godine** eksploatacijskog vijeka mjere informacijske sigurnosti. Izdacima se pritom smatraju one stavke koje smanjuju ekonomski potencijal projekta ili rješenja.

U ovom kontekstu, **izdacima** bi se mogli smatrati:

1. Inicijalna investicija u informacijsko sigurnosno rješenje ili projekt,
2. Trošak održavanja promatranog rješenja ili projekta,
3. Materijalni troškovi korištenja promatranog rješenja[156],
4. Troškovi vanjskih usluga pri korištenju promatranog rješenja[157]

[155] npr. vlastita sredstva ili kredit, odnosno financijska poluga.
[156] npr. struja, klimatizacija

5. Troškovi edukacije stalnih zaposlenika pri uvođenju,
6. Troškovi edukacije stalnih zaposlenika u korištenju[158],
7. Bruto plaće zaposlenih na uvođenju rješenja.

Kod upotrebe analize ekonomskog toka sigurnosnog rješenja postavlja se problem **određivanja primitaka** kojima se suprotstavljaju izdaci. Oni se u klasičnom smislu sastoje od ukupnog prihoda tijekom eksploatacije te procijenjenog ostatka vrijednosti na kraju eksploatacije. Takve primitke moguće je definirati nedvojbeno samo u slučaju poduzeća čija je djelatnost orijentirana ka nabavi i pružanju sigurnosnih rješenja drugima i koji zapravo pružaju uslugu drugima a sami poduzimaju investicijsku aktivnost. Svi drugi od investicija u informacijsko sigurnosna rješenja ne deriviraju prihode, no izdacima u analizi ekonomskog toka mogla bi se suprotstaviti potencijalna šteta koju poduzeće može podnijeti ukoliko dođe do ostvarenja određenog sigurnosnog propusta po godinama korištenja nekog sigurnosnog rješenja.

Sa **statičkog stajališta** ovakvog modificiranog ekonomskog toka, inicijalno bi opravdana bila ona investicija u sigurnosno rješenje kod koje su ukupne, kumulativne koristi, odnosno ukupni izbjegnuti trošak nastupa sigurnosnih propusta uvećan za ostatak vrijednosti veći od ukupnih troškova uvođenja sigurnosnog rješenja. Takvu situaciju prikazuje tablica 12.

Tablica 12: Analiza modificiranog ekonomskog toka ulaganja u informacijsku sigurnost

	struktura/razdoblje	1	2	3	...
1.	IZBJEGNUTI TROŠAK	...	...	...	...
2.	OSTATAK VRIJEDNOSTI	-	-	-	...
3.	IZDACI	3.1+3.2+3.3+3.4+3.5+3.6+3.7	...	...	...
3.1	Investicija u sigurnosno rješenje	...	...	...	...
3.2	Trošak održavanja	...	...	...	...
3.3	Materijalni troškovi	...	...	...	...
3.4	Troškovi vanjskih usluga	...	...	...	...
3.5	Troškovi edukacije pri uvođenju	...	...	...	...
3.6	Troškovi edukacije pri korištenju	...			...
3.7	Brutto plaće	...	...	...	...
4.	**NETO EFEKT**	1.+2.-3.			

Izvor: priredio autor

4.4.3.2. Specifičnosti novčanog toka

Kao i kod metode ekonomskog toka, metoda novčanog (**financijskog**) toka može se primijeniti na investicije u rješenja informacijske sigurnosti u nemodificiranom obliku samo u slučaju da poduzeće drži u svom vlasništvu kao imovinu takva sredstva i daje ih u najam drugim korisnicima. Za razliku od metode ekonomskog toka, metoda novčanog toka uzima u obzir i

[157] npr. konzultantske usluge
[158] Svedeno na angažirane ekvivalente.

izvore financiranja u smislu primitaka odnosno obveze prema izvorima financiranja (kamate), s prikazom strukture u tablici 13.

Tablica 13: Modificirana metoda novčanog toka pri ulaganju u informacijsku sigurnost

	struktura/razdoblje	1	2	3	...
1.	IZBJEGNUTI TROŠAK	...	...	...	...
2.	OSTATAK VRIJEDNOSTI	...	...	...	...
3.	UKUPNO PRIMICI	1+2	...	...	...
4.	UKUPNI IZDACI	4.1+4.2+4.3+4.4+4.5+4.6+4.7+	...	...	...
4.1	Investicija u sigurnosno rješenje	...	...	...	...
4.2	Trošak održavanja	...	...	...	...
4.3	Materijalni troškovi	...	...	...	...
4.4	Troškovi vanjskih usluga	...	...	...	...
4.5	Troškovi edukacije pri uvođenju	...	...	...	...
4.6	Troškovi edukacije pri korištenju	...			...
4.7	Brutto plaće	...	...	...	...
4.8	Kamate na kredit (tuđa angažirana fin. sredstva)	...	...	...	...
4.9	Otplatna kvota				
5.	**NETO EFEKT**	3.-4.			

Izvor: priredio autor

Problem koji se postavlja kod ovakvog gledišta je sličan kao kod analize ekonomskog toka, a sastoji se u određivanju izbjegnutog troška. U dinamičkoj analizi mogu se u nastavku koristiti klasične dinamičke metode (Zečević, 2011), a to su:

1. **Metoda razdoblja povrata investicijskih ulaganja** koja predstavlja najjednostavniji kriterij financijskog odlučivanja o realnim investicijama. Njome se izračunava broj godina u kojima će se vratiti uložena sredstva u određeni projekt, a u zadanom kontekstu, u informacijsko sigurnosno sredstvo ili sustav upravljanja informacijskom sigurnošću. U slučaju da se iz izračuna želi eliminirati nedostatak neuzimanja vremenske vrijednosti novca, koristit će se metoda diskontiranog perioda povrata.

- U slučaju različitih identificiranih novčanih tokova u životnom vijeku korištenja informacijsko sigurnosnog rješenja:

$$I = \sum_{t=1}^{t_p} N_t$$

- U slučaju istovjetnih novčanih tokova:

$$t_p = \frac{I}{N_t}$$

$N_1 = N_2 = ... = N_T \equiv N_t$; u obje formule su:

I – ukupni iznos investicije u informacijsku sigurnost,

N_t – konstantni čisti novčani tokovi po godinama 1..t

t_p – razdoblje (period) povrata ulaganja u investiciju u informacijsku sigurnost

- Prag efikasnosti – uvjet prihvaćanja ili odbacivanja investicije: $t_p < t_z$ gdje je:

  t_p - period povrata,
  t_z – zadani, tj. maksimalno prihvatljiv period povrata.

2. Metoda diskontiranog perioda povrata je inačica metode razdoblja povrata u kojoj se nastoji eliminirati nedostatak zanemarivanja utjecaja vremenske vrijednosti novca.

$$I = \sum_{t=1}^{t_p} N_t \frac{1}{(1+k)^t} \text{ ili } I = \sum_{t=1}^{t_p} N_t II_k^t$$

gdje je:

I - ukupni iznos investicije u informacijsku sigurnost, k – diskontna stopa,
N_t – čisti novčani tokovi po godinama 1..t, II_k^t – druge financijske tablice za
t_p – razdoblje (period) povrata ulaganja u investiciju, diskontnu stopu k i za godinu t.

3. **Metoda čiste neto sadašnje vrijednosti** investicijskog ulaganja u informacijsku sigurnost, predstavlja razliku između sume diskontiranih novčanih tokova u cjelokupnom vijeku korištenja informacijsko-sigurnosnog sredstva i iznosa investicije.

- U slučaju različitih identificiranih novčanih tokova u životnom vijeku korištenja informacijsko sigurnosnog rješenja

$$S_o = \sum_{t=1}^{T} \frac{N_t}{(1+k)^t} - I \text{ ili } S_o = \sum_{t=1}^{T} N_t \times II_k^t - I$$

gdje je:

S_O – čista sadašnja vrijednost, T– vijek korištenja projekta,
I - ukupni iznos investicije u inform. sigurnost, k – diskontna stopa,
N_t – čisti novčani tokovi po godinama 1..t, II_k^t – druge financijske tablice za diskontnu stopu k i za godinu t.

- U slučaju identičnih novčanih tokova tijekom životnog vijeka rješenja:

$$S_o = N_t \frac{(1+k)^T - 1}{(1+k)^T k} - I \text{ ili } S_o = N_t IV_k^t - I$$

$$N_1 = N_2 = ... = N_T \equiv N_t$$

gdje je:

S_O – čista sadašnja vrijednost, T– vijek korištenja projekta,
I - investicijski troškovi, k – diskontna stopa,
N_t – čisti novčani tokovi po godinama 1..t, IV_k^t – četvrte financijske tablice za diskontnu stopu k i za godinu t.

- Prag efikasnosti – uvjet prihvaćanja ili odbacivanja: $S_o \geq 0$

4. **Metoda interne stope profitabilnosti ulaganja** u informacijsku sigurnost. Ona predstavlja internu diskontnu stopu koja svodi čiste novčane tokove korištenja informacijsko-sigurnosnog sredstva na vrijednost njegovih investicijskih tokova.

- Različiti čisti novčani tokovi u cjelokupnom vijeku efektuiranja projekta:

$$\sum_{t=1}^{T} \frac{N_t}{(1+R)^t} = I$$

gdje je:

R – interna stopa profitabilnosti, N_t – čisti novčani tokovi po godinama t,

I - investicijski troškovi, T– vijek efektuiranja projekta.

Interpolacija: $y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$;

gdje je:

y – tražena interna (diskontna) stopa profitabilnosti,

y_1 i y_2 – diskontne stope između kojih se vrši interpoliranje,

x – čista sadašnja vrijednost za internu stopu (nulta vrijednost),

x_1 i x_2 – čiste sadašnje vrijednosti za diskontne stope y_1 i y_2 .

- Identični čisti novčani tokovi u cjelokupnom vijeku efektuiranja projekta:

$$IV_R^T = \frac{I}{N_t}$$

gdje je:

R – interna stopa profitabilnosti, T– vijek efektuiranja projekta,

I - investicijski troškovi, IV_k^t – četvrte financijske tablice za

N_t – čisti novčani tokovi po godinama 1..t, diskontnu stopu k i za godinu t.

- Prag efikasnosti – uvjet prihvaćanja ili odbacivanja: $R \geq k$ (k – trošak kapitala)

5. **Indeks profitabilnosti** može se koristiti kao dodatni kriterij investicijskog odlučivanja. On je odnos diskontiranih čistih novčanih tijekova informacijsko sigurnosnog rješenja u cjelokupnom njegovom životnom vijeku i njegovih investicijskih troškova.

- Različiti čisti novčani tokovi u cjelokupnom vijeku efektuiranja projekta: (na sljedećoj stranici)

$$P_I = \frac{\sum_{t=1}^{T} \frac{N_t}{(1+k)^t}}{I} \textbf{ ili } P_I = \frac{\sum_{t=1}^{T} N_t \times II_k^t}{I}$$

gdje je

P_I – indeks profitabilnosti, k – diskontna stopa,

I - investicijski troškovi, II_k^t – druge financijske tablice za diskontnu

N_t – čisti novčani tokovi po godinama 1..t, stopu k i za godinu t.

- Identični čisti novčani tokovi u cjelokupnom vijeku efektuiranja projekta:

$$P_I = \frac{N_t \frac{(1+k)^T - 1}{(1+k)^T k}}{I} \text{ ili } P_I = \frac{N_t * IV_k^t}{I}$$

gdje je

IV_k^t – druge financijske tablice za diskontnu stopu k i za godinu t

- Prag efikasnosti – uvjet prihvaćanja ili odbacivanja: $P_I > 1$

4.4.3.3. Problemi pri korištenju metode interne stope prinosa

Klasično razmatranje korištenja interne stope prinosa zahtijeva da diskontna stopa koja izjednačuje investicijska ulaganja s čistim novčanim tokovima bude veća od definirane **diskontne stope** koja ovisi o rizičnosti i troškovima kapitala. Uobičajeni problem s višestrukim internim stopama povrata u pravilu kod primjene u investicije u informacijsku sigurnost nije prisutan. Budući da je pretpostavka kako su sigurnosni rizici prisutni tijekom cijelog vremena korištenja odgovarajućeg sigurnosnog rješenja ili sistema, te da je raspored novčanih tijekova identičan[159], može se koristiti klasična metode interne stope povrata.

Međutim, kod korištenja metode interne stope prinosa u analizi ulaganja u sustave informacijske sigurnosti treba na umu imati sljedeće činjenice:

1. Ova se metoda **ne može koristiti** pri analizi ili usporedbi investicija u **više različitih sigurnosnih rješenja** nego samo u pojedinačnoj analizi svakog rješenja je dobiveni rezultati nisu usporedivi,
2. Interna stopa prinosa podrazumijeva **reinvestiranje pozitivnog novčanog tijeka** u projekte ili rješenja koja imaju jednaku stopu povrata, neovisno o tome radi li se o reinvestiranju u ista rješenja ili druga usporediva. Iz tog razloga će metoda interne stope povrata precjenjivati

[159] Raspored novačnih tokova je identičan ukoliko nema promjene novčanih tokova i zadnji novačni tijek nije negativan.U praksi je zadnji novčani tijek negativan kada postoje veliki troškovi napuštanja neke investicije (npr. uklanjanje naftne platforme nakon isteka životnog vijeka eksploatacije).

one projekte kod kojih reinvestirani novčani tijek odlazi u projekte s manjom stopom povrata. Ovo je osobito istinito za ona rješenja ili sigurnosne projekte koji imaju visoke stope povrata jer je poduzećima često teško naći usporedive projekte za reinvestiranje po jednako visokim (atraktivnim) stopama,

3. U pravilu, novčani tokovi ne mijenjaju predznak i zadnji novčani tok sigurnosnog rješenja zasigurno nema negativan predznak, stoga se u praksi **ne pretpostavlja da bi mogao postojati problem višestrukih internih stopa prinosa.**

4. Metoda interne stopa povrata dat će samo **relativnu** izmjeru povrata u sredstvo ili sustav informacijske sigurnosti a ne i njegov apsolutni iznos.

Polazne **pretpostavke** izračuna su sljedeće:

1. Izvršeno je početno investicijsko ulaganje u sigurnosno informacijsko rješenje,
2. Ne postoji oportunitetni trošak tog ulaganja,
3. Postoji minimalni ostatak vrijednosti informacijskog rješenja po kraju eksploatacijskog vijeka,
4. Koristi se proporcionalna amortizacijska metoda,
5. Generirani novčani tijek se procjenjuje kao posljedica izbjegavanja nastupa sigurnosnog incidenta i vezanih troškova (direktnih i indirektnih),
6. Porezni kredit ne postoji,
7. Ostale vezane investicije procjenjuju uz uvođenje informacijsko sigurnosnog rješenja procjenjuju se u fiksnom iznosu i ne amortiziraju se tijekom eksploatacijskog vijeka rješenja,
8. Procjenjuje se kako tijekom eksploatacijskog vijeka sigurnosnog sredstva postoji varijabilni trošak koji se izražava relativno u odnosu na prihod,
9. Pretpostavlja se porez na dobit u iznosu od 20 %,
10. Pretpostavlja se kako je obrtni kapitala tijekom životnog vijeka korištenja sredstva nepotreban, odnosno jednak nuli,
11. Diskontna stopa koristi se u obliku direktne diskontne stope. Diskontnu stopu moguće je unutar modela izračunati i na način kako se ona računa u okviru CAPM modela[160] pri čemu se uzimaju u obzir bezrizična stopa, premija na račun tržišnog rizika, trošak posuđivanja kapitala i udio duga u financiranju,
12. Model pretpostavlja kako su koristi od uvođenja informacijsko sigurnosnog rješenja kroz godine korištenja nepromjenjive, odnosno proporcionalno raspodijeljene,

[160] *CAPM* model (kratica od eng. „*Capital Asset Pricing Model*“) je često korišteni model kojim se određuje teoretska poželjna stopa povrata investicije u određenu imovinu, ukoliko se ona dodaje u već diverzificirani portfolio. *CAPM* model je nezavisno razvijen od strane Jacka Traynora (1961.,1962.), Williama Sharpea (1964.), Johna Lintnera (1965.) i Jana Mossina (1966.), kao nastavak istraživanja moderne portfolio teorije.

13. Fiksni troškovi održavanja rješenja tijekom životnog vijeka se ne povećavaju i u biti su održani u inicijalnoj investiciji.

Jednu mogućnost primjene analize novčanog toka prikazuje adaptirana tablica 14.

Tablica 14: Analiza novčanog toka projekta investiranja u informacijsko-sigurnosno rješenje

Analiza projekta investiranja u informacijsko-sigurnosno rjesenje

INICIJALNA INVESTICIJA	
Početna investicija u sigurn. rjesenje	150.000 kn
Oportunitetni tršak	0 kn
Životni vijek sigurn. rjesenja	7 god.
Ostatak vrijednosti sigurn. rješenja	5.000 kn
Amort.metoda	2
Porezni kredit (%)	0%
Iznos ostalih investicija (neamort.)	30000

GENERIRANI NOVČANI TIJEK	
Generirano u prvoj godini	50.000 kn
Varijabilni trošak (% od prihoda)	10%
Fiksni troškovi u prvoj godini	0
Porez na dobit	20%

DISKONTNA STOPA	
Metoda	1
1. Diskontna stopa	8%
2a. Beta	0,9
b. Bezrizična stopa	3,00%
c. Premija trzisnog rizika	5,00%
d. Udio duga u financiranju	0,00%
e. Trosak posudjivanja kapitala	9,00%
Korištena diskontna stopa=	8,00%

OBRTNI KAPITAL	
Inicijalni	0 kn
Obrtni kapital kao % prihoda	0%
Ostatak vrijednosti o.k. na kraju	100%

GODISNJE STOPE RASTA										
Godina	1	2	3	4	5	6	7	8	9	10
Prihodi	n/a	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Fiksni troškovi	n/a	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%

Postotak rasta fiksnih troškova je inicijalno jednak stopi rasta prihoda.

	0	1	2	3	4	5	6	7	8	9	10

INICIJALNA INVESTICIJA	
Investicija	150.000 kn
- Porezni kredit	0 kn
Neto investicija	150.000 kn
+ Obrtni kapital	0 kn
+ Oportun.trošak	0 kn
+ Ostale invest.	30.000 kn
Inicijalna invest.	180.000 kn

OSTATAK VRIJEDNOSTI										
Sigurnosno rješenje	$0	$0	$0	$0	$0	$0	$5.000	$0	$0	$0
Obrtni kapital	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0

OPERATIVNI NOVČANI TIJEKOVI											
Indeks životnog vijeka		1	1	1	1	1	1	1	0	0	0
Prihodi		50.000 kn	50.000 kn	50.000 kn	50.000 kn	50.000 kn	50.000 kn	50.000 kn	0 kn	0 kn	0 kn
-Varijabilni trošak		5.000 kn	5.000 kn	5.000 kn	5.000 kn	5.000 kn	5.000 kn	5.000 kn	0 kn	0 kn	0 kn
- Fiksni trošak		0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn
EBITDA		45.000 kn	45.000 kn	45.000 kn	45.000 kn	45.000 kn	45.000 kn	45.000 kn	0 kn	0 kn	0 kn
- Amortizacija		42.857 kn	30.612 kn	21.866 kn	15.618 kn	11.156 kn	7.969 kn	5.692 kn	0 kn	0 kn	0 kn
EBIT		2.143 kn	14.388 kn	23.134 kn	29.382 kn	33.844 kn	37.031 kn	39.308 kn	0 kn	0 kn	0 kn
-Porez		429 kn	2.878 kn	4.627 kn	5.876 kn	6.769 kn	7.406 kn	7.862 kn	0 kn	0 kn	0 kn
EBIT(1-t)		1.714 kn	11.510 kn	18.507 kn	23.505 kn	27.075 kn	29.625 kn	31.447 kn	0 kn	0 kn	0 kn
+ Amortizacija		42.857 kn	30.612 kn	21.866 kn	15.618 kn	11.156 kn	7.969 kn	5.692 kn	0 kn	0 kn	0 kn
- ∂ Obrtni kapital		0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn	0 kn
Neto novč. tijek	-180.000 kn	44.571 kn	42.122 kn	40.373 kn	39.124 kn	38.231 kn	37.594 kn	37.138 kn	0 kn	0 kn	0 kn
Diskontna stopa	1	1,08	1,1664	1,259712	1,36048896	1,469328077	1,586874323	1,713824269	0	0	0
Diskont. novč. tijek	-180.000 kn	41.270 kn	36.113 kn	32.050 kn	28.757 kn	26.020 kn	23.690 kn	24.587 kn	0 kn	0 kn	0 kn

Investicijski pokazatelji	
NPV =	32.486,95 kn
IRR =	12,82%
ROC =	29,30%

RAČUNOVODSTVENA VRIJEDNOST & AMORTIZACIJA										
Početna rač.vrijedn.	0 kn	150.000 kn	107.143 kn	76.531 kn	54.665 kn	39.046 kn	27.890 kn	19.922 kn	0 kn	0 kn	0 kn
Amortizacija		42.857 kn	30.612 kn	21.866 kn	15.618 kn	11.156 kn	7.969 kn	5.692 kn	0 kn	0 kn	0 kn
Rač. vrij. na kraju	150.000 kn	107.143 kn	76.531 kn	54.665 kn	39.046 kn	27.890 kn	19.922 kn	14.230 kn	0 kn	0 kn	0 kn

Izvor: priredio autor korištenjem aplikacije ***Microsoft Office Excel 2010***.

Izrađeni model pokazuje kako je uz početne pretpostavke modela moguće izračunati neto sadašnju vrijednost, internu stopu povrata i povrat na angažirani kapital kod korištenja ovakvog rješenja. Dalje simulacije pokazuju kako je interna stopa povrata vrlo osjetljiva na tri temeljna **ulazna čimbenika**, prikazana na sljedećoj stranici.

1. **Vrijeme** (dužina trajanja) korištenja informacijsko sigurnosnog rješenja,
2. Percipirana (unaprijed određena) **sposobnost** informacijsko-sigurnosnog sredstva da generira pozitivni novčani tijek za vrijeme svog životnog vijeka,
3. Korištena **diskontna stopa**.

Ovakav model može se u praksi koristiti ukoliko se pravilno procijene svi ulazni parametri. Iskustveno, najveći problem u predviđanju povezuje se uz sposobnost procjene generiranja pozitivnog novčanog tijeka u vidu izbjegavanja troška povezanog uz nastup sigurnosnih incidenata. Ta se procjena može činiti korištenjem **referentnih kataloga** koje vode i obrađuju specijalizirane agencije ili u slučaju kompleksnih poduzeća ili organizacija, korištenjem vlastitih statističkih podataka. Konkretno, upravljanje operativnim rizikom po Basel II. kriterijima predviđa upravo ova dva izvora navedenih podataka.

4.4.3.4. Odlučivanje o zamjeni implementiranog sigurnosnog rješenja

Kod analize zamjene implementiranog sigurnosnog rješenja potrebno je uzeti u obzir sve čimbenike koji utječu na potrebu zamjene, kao i sve vezane, indirektne i skrivene troškove. U realnosti poduzeća takvi su troškovi često skriveni u drugim organizacijskim jedinicama, odnosno prebačeni na druge nosioce troškova. Čest je slučaj da se trošak rada u vidu vremena potrebnog za obrazovanje internih specijalista za uvođenje nekog novog rješenja ili trošak obrazovanja korisnika za korištenje novih rješenja prebacuje na općeniti troškovni centar koji se odnosi na općenite troškove rada ili se tekući troškovi održavanja prebacuju na općenite troškovne centre održavanja. **Specifičnosti zamjene** informacijsko-sigurnosnih rješenja prikazani su u tablici 15.

Tablica 15: Specifičnosti zamjene informacijsko-sigurnosnih rješenja

	Vrsta životnog vijeka	**Opis**	**Specifičnost primijenjena na sustave upravljanja informacijskom sigurnošću**
1.	Korisni životni vijek	Period konkretnog korištenja sredstva	Često duži od amortizacijskog, problemi u određivanju odnosa prema optimalnom. Može se produžiti dodatnim ulaganjem u održavanje.
2.	Ekonomski životni vijek	Vrijeme između trenutka instalacije sredstva i trenutka prestanka korištenja	
3.	Fizički životni vijek	Vrijeme između kupovine rješenja od strane prvog vlasnika i cjelokupnog prestanka korištenja od srane zadnjeg korisnika	U pravilu je jednak ekonomskom i korisnom životnom vijeku. Informacijsko-sigurnosna investicijska rješenja u pravilu su u vlasništvu jednog poduzeća i nisu predmet prodaje i ponovnog korištenja.
4.	Amortizacijski životni vijek	Računovodstveni životni vijek u kojemu se pretpostavlja da će sredstvo biti amortizirano	U RH računalni hardver, mrežna oprema i računalni softver amortiziraju se po stopi od najviše 50 % godišnje
5.	Garancijski životni vijek	Životni vijek sredstva za koji garantira proizvođač	Vrlo ograničena garancija na informacijsko-sigurnosna rješenja, u slučaju uređaja odnosi se na električnu ispravnost a ne temeljnu

			funkcionalnost. Često ovisi o razini godišnjeg ugovorenog održavanja.
6.	Optimalni životni vijek	Optimalni životni vijek je točka u kojoj je suma godišnjih troškova održavanja i upravljanja sigurnosnim rješenjem minimalna	

Izvor: prilagodio autor prema Malik, Krishan A., „**Petroleum Project Evaluation & Investment Decision Making**“, Institute for Petroleum Development, Austin, Texas, 2011., p. 107.

Vrlo je razumno u portfelju sigurnosnih rješenja svako od implementiranih promatrati u kontekstu „*rješenja koje se brani*“ nasuprot novog rješenja koje je „*rješenje izazivač*“. U takvoj analizi postojeća rješenja u pravilu imaju niske investicijske troškove a visoke operativne troškove i troškove održavanja dok „*rješenje izazivač*“ ima visoke investicijske troškove ali može imati niže operativne troškove i troškove održavanja.

Postoji nekoliko razloga zbog kojih poduzeća izbjegavaju promjene rješenja informacijske sigurnosti:

1. Pitanje **raspoloživosti** investicijskih sredstava,
2. Implementacijska **inercija**: poduzeće je zadovoljno postojećim rješenjem i njegovom funkcionalnošću te načinom na koji uklanja sigurnosne propuste,
3. Postoji **nesigurnost** o ukupnim troškovima novog sigurnosnog rješenja dok su troškovi postojećeg rješenja poznati,
4. Postoji **neizvjesnost** o ostalim resursima kod uvođenja novog rješenja vezano uz dodatni trošak rada i edukacije,
5. Uvođenjem novog rješenja preuzima se **obaveza** koja seže daleko u budućnost u odnosu na postojeće, funkcionalno rješenje,
6. **Nevoljkost** implementacije novih tehnologija s jedne strane i **rizik** da stara tehnologija neće pružiti dovoljnu razinu zaštite.

4.4.3.5. Ostale mogućnosti korištenja financijskih metoda pri odlučivanju o ulaganju u sustave upravljanja informacijskom sigurnošću

U okviru ove teme, razmotriti će se mogućnosti primjene **moderne portfolio metode** pri odlučivanju o ulaganju u sustave upravljanja informacijskom sigurnošću.

Moderna portfolio teorija ima gotovo šezdeset godina i doživjela je tijekom vremena brojne modifikacije usmjerene ka tome da njene temeljne pretpostavke budu realističnije. Tako su nastale varijacije poput post-moderne portfolio teorije koja pokušava adresirati problem asimetričnosti mjere rizika (Elton, et al., 2009, p. 74), kao i primjene portfolio teorije izvan

područja upravljanja portfeljem investicija[161]. Takve su primjene npr. u istraživanju varijacija u kvaliteti i strukturi radne snage koje se provode od 70-tih godina, u psihologiji na području istraživanja osobnosti koja se promatra kao portfelj karakteristika osobnosti ili kao jedna od metoda kod pretraživanja podataka kojom se pokušava poboljšati uspješnost postupka.

Temeljna pretpostavka teorije je da se investicija u pojedino rješenje, a u ovom kontekstu u rješenje informacijske sigurnosti ne bira individualno, sukladno ciljevima koje rješenje samostalno postiže već je potrebno promatrati **utjecaj pojedinog rješenja** na ostala rješenja u portfelju i cjelokupnu razinu postignute informacijske sigurnosti koristeći rješenja iz portfelja. Prema tome, sama metoda opisuje kako odabrati portfelj investicija na način da za zadanu razinu rizika povrat bude maksimalan pri čemu vrijedi i obrat, kako odabrati portfelj koji ima najniži rizik za zadanu razinu povrata.

Budući da alati za informacijsku sigurnost doista imaju karakter investicija a sa sobom nose karakteristiku rizika koji je moguće kvantificirati, portfolio teorija bila bi primjenjiva i na portfelj rješenja unutar sustava upravljanja informacijskom sigurnošću. No, prije toga potrebno je vidjeti koje su temeljne pretpostavke portfolio teorije kako bi se ustanovila je li model praktično primjenjiv, budući da temeljne pretpostavke modela često predstavljaju i njegova ograničenja.

Neke temeljne **pretpostavke** moderne portfolio teorije koje bi se mogle pokazati problematičnima kod primjene na sustave upravljanja informacijskom sigurnošću su sljedeće:

1. Funkcija upravljanja informacijskom sigurnošću je često **podvojena** na tehničku disciplinu kojom se bave rukovoditelji i timovi i na funkcije koje odlučuju o investicijama u informacijsku sigurnost. Između dvaju funkcija trebala bi postojati povezanost, no često dolazi do temeljnog sukoba jer zbog financijskih razloga ili averzije prema investicijama u razmjerno „*nepoznate*“ projekte oni koji odlučuju o investicijama odbijaju investirati u sustave upravljanja informacijskom sigurnošću. Time se preuzima rizik, svjesno ili nesvjesno. Budući da je temeljna pretpostavka moderne portfolio teorije činjenica kako postoji nesklonost riziku, iz psiholoških razloga, to bi mogla biti kontraindikacija ili poteškoća kod korištenja ove metode,
2. Procjena rizika na kojoj se temelji tehnički dio upravljanja sustava informacijske sigurnosti je **subjektivna**. Oni koji procjenu rizika izvode ne mogu biti upoznati sa svim mogućim rizicima ili tehnički dio procjene rizika može biti izveden na način da je

[161] Portfelj investicija u ovom kontekstu odnosi se na realne ili financijske investicije. Naime, jedna od početnih pretpostavki moderne portfolio teorije (*MPT*) je da rizik slijedi Gaussovu ili normalnu distribuciju.

sposobnost informacijsko sigurnosnog rješenja da ukloni sigurnosni rizik umanjena ili uvećana,

3. Akcije pri odabiru sigurnosnih rješenja **ne bi trebale utjecati na sposobnost rješenja** da umanji ili (neželjeno) uveća vjerojatnost nastupa sigurnosnog incidenta. U praksi to nije tako jer između sigurnosnih rješenja postoji jaka korelacija i samim time moguće je da uvođenje jednog sigurnosnog rješenja značajno umanji rizik nekog naizgled nevezanog sigurnosnog incidenta te samim time promijeni vjerojatnost nastupa takvog događaja i promijeni vjerojatnosnu karakteristiku nekog drugog sigurnosnog rješenja u portfelju,
4. Rizici pojedinih komponenti informacijskog sustava koji se pokušavaju umanjiti sigurnosnim rješenjima **ne prate normalnu (*Gaussovu*) distribuciju**, što je temeljni zahtjev moderne portfolio teorije.

5. PRIKAZ I ANALIZA REZULTATA ANKETNOG ISTRAŽIVANJA

Prikaz i analiza rezultata preliminarnog istraživanja predstavlja ključni dio doktorske disertacije u kojemu se analizira zatečena razina zrelosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj prema novo razvijenom modelu. Značaj ove glave zahtijeva njeno izlaganje u više povezanih poglavlja: **1) Analiza i ocjena dostignute razine uporabe internih sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, 2) Kriteriji vrednovanja modela upravljanja sustavom informacijske sigurnosti u malim i srednjim poduzećima i 3) Prikaz i interpretacija rezultata istraživanja – poznavanje zakonske regulative, korištenje sustava certifikacije i ekonomski učinci uporabe sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj.**

5.1. ANALIZA I OCJENA DOSTIGNUTE RAZINE UPORABE INTERNIH SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA U REPUBLICI HRVATSKOJ

U ovom poglavlju analiziraju se na znanstveni način rezultati provedenog istraživanja dostignute razine **zrelosti** sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj. Posebna pažnja posvećena je razini poznavanja **zakonskih propisa** od strane rukovoditelja poduzeća, ekonomskoj analizi investicija u informacijsku sigurnost i troška njihovog korištenja te korištenja sustava profesionalne certifikacije kao alata u provođenju mjera upravljanja sustavom informacijske sigurnosti u malim i srednjim poduzećima. Predstavljaju se i oni rezultati istraživanja koji se odnose na ekonomske učinke uporabe sustava upravljanja informacijskom sigurnošću, trošak edukacije zaposlenika i rukovoditelja iz područja informacijske sigurnosti te nastupe sigurnosnih incidenata. Istraživanje je obavljeno u obliku **ankete** tijekom čijeg provođenja su se sistematski prikupili, analizirali i interpretirali stavovi slučajno odabrane grupe iz ciljne populacije svih malih i srednjih poduzeća u Republici Hrvatskoj. Korištena je znanstvena metodologija kreiranja reprezentativnog statističkog uzorka, procesa ispitivanja i analize odgovora i interpretacije dobivenih rezultata, te ekonometrijsko-statistička metoda regresijske analize čime su identificirane one nezavisne varijable čija vrijednost je izmjerena tijekom provođenja istraživanja, za koje se pretpostavljalo i potvrdilo kako adekvatno opisuju identificirane nezavisne varijable, a to su dostignuta ukupna razina upravljanja informacijskom sigurnošću u

malim i srednjim poduzećima i funkcija informacijske sigurnosti kao strateška poslovna funkcija. Po dobivanju numeričkih pokazatelja, isti su analizirani i interpretirani u okviru postojećih znanstvenih i praktičnih spoznaja vezanih uz upravljanje informacijskom sigurnošću. Cjeline ovog poglavlja su: **1) Svrha i ciljevi anketnog istraživanja, 2) Metodologija anketnog istraživanja, 3) Odabir anketne metode, 4) Formuliranje statističkog uzorka (uzorkovanje) i 5) Struktura anketnog upitnika.**

5.1.1. Svrha i ciljevi anketnog istraživanja

Tijekom provođenja ankete sistematski su prikupljeni, analizirani i interpretirani stavovi slučajno odabrane grupe iz ciljne populacije svih malih i srednjih poduzeća u Republici Hrvatskoj.

Svrha istraživanja je provođenje znanstveno utemeljene statističke analize ankete postojećeg (zatečenog) stanja upravljanja funkcijom informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj u drugom kvartalu 2013. godine. Ovo istraživanje primarno se odnosi na kvantitativne pokazatelje ulaganja u informacijsku sigurnost, te načine i metode kojima taj izolirani segment ukupne populacije hrvatskih poduzeća osigurava minimum sukladnosti sa zakonskim zahtjevima te pokazatelja primjene najbolje prakse.

Cilj istraživanja je istražiti koliki je utjecaj nastupa informacijsko sigurnosnih incidenata na poslovni rezultat poduzeća, a koji nastaju kao posljedica neadekvatnog ustroja sustava upravljanja informacijskom sigurnošću. Cilj je postignut postavljanjem pitanja pomno identificiranoj ciljnoj publici ankete na način da je ona prvo odgovorila na postavljena pitanja, a zatim se statističkom analizom razjasnilo je li dostignuta razina upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, a koja je izmjerena putem inicijalno postavljenog instrumentarija na dovoljnoj razini kako poslovanje poduzeća ne bi bilo ugroženo čestim nastupima sigurnosnih incidenata, kako bi se osigurala sukladnost sa postavljenim zakonskim zahtjevima, i kako bi rukovoditelji imali jasan pregled vezanih investicijskih i tekućih (operativnih) troškova posjedovanja i korištenja takvog sustava.

5.1.2. Metodologija anketnog istraživanja

Anketnu populaciju čine mala i srednja poduzeća u Republici Hrvatskoj na koja je orijentirana izrada doktorske disertacije. Stoga je inicijalno potrebno strogo definirati koji se podskup poduzeća iz skupa svih poduzeća u Republici Hrvatskoj može smatrati malim i srednjim poduzećima, budući da, kako će se pokazati, ne postoji jedinstvena definicija takvih poduzeća, iako razne definicije ne odstupaju osobito jedna od druge u rasponu i kvaliteti postavljenih

kriterija, odnosno parametra uvrštenja. Stoga je ključno pitanje početne faze anketnog istraživanja - *„Koje kriterije mora zadovoljiti poduzeće u Republici Hrvatskoj, kako bi bilo klasificirano kao malo ili srednje poduzeće?"* Naime, u pripremama za istraživanje pokazalo se kako postoji više kriterija za ovu klasifikaciju, te se stoga trebalo metodološki odlučiti za jednu od raspoloživih mogućnosti. U ovoj cjelini objašnjavaju se: **1) Definicija malog i srednjeg poduzeća prema Zakonu o računovodstvu i 2) Definicija malog i srednjeg poduzeća korištena u Europskoj uniji.**

5.1.2.1. Definicija malog i srednjeg poduzeća prema Zakonu o računovodstvu

Zakon o računovodstvu (Narodne novine 144., 2012) u članku 3[162] pruža okvir za klasifikaciju poduzeća u Republici Hrvatskoj s obzirom na veličinu. Poduzetnici se razvrstavaju na male, srednje i velike ovisno o pokazateljima utvrđenim na zadnji dan poslovne godine koja prethodi poslovnoj godini za koju se sastavljaju financijski izvještaji, prema uvjetima koji su prikazani u tablici 16. Pritom poduzetnici ne smiju prijeći dva od navedenih uvjeta dok su veliki poduzetnici oni koji prelaze **dva uvjeta** za klasifikaciju srednjeg poduzeća (poduzetnika).

Sukladno Zakonu o računovodstvu, poduzetnici su:

1. **Trgovačko društvo** i **trgovac pojedinac** određeni propisima koji uređuju trgovačka društva,
2. **Poslovna jedinica poduzetnika** iz točke 1. sa sjedištem u stranoj državi ako prema propisima te države ne postoji obveza vođenja poslovnih knjiga i sastavljanja financijskih izvještaja te poslovna jedinica poduzetnika iz strane države koji su obveznici poreza na dobit sukladno propisima koji uređuju poreze.

Odredbe Zakona o računovodstvu dužna je primjenjivati i svaka pravna i fizička osoba, koja je obveznik poreza na dobit određena propisima koji uređuju poreze, osim točno određenih, taksativno navedenih odredbi. Odredbe navedenog Zakona ne primjenjuju se na državni proračun i proračunske korisnike državnog proračuna, proračune jedinica lokalne i područne (regionalne) samouprave te njihove proračunske korisnike, vjerske zajednice, političke stranke, sindikate i ostale neprofitne organizacije. Klasifikaciju poduzetnika prema kriterijima ovog zakona prikazuje tablica 16. na sljedećoj stranici.

[162] Naziv navedenog članka je „*Razvrstavanje poduzetnika*".

Tablica 16: Klasifikacija malih i srednjih poduzetnika prema kriterijima prosječnog broja zaposlenika, iznosa godišnjeg prihoda i ukupnog iznosa aktive prema Zakonu o računovodstvu

Pokazatelj	Mali poduzetnici	Srednji poduzetnici
Prosječan broj zaposlenika tijekom poslovne godine	< 50 zaposlenika	< 250 zaposlenika
Iznos godišnjeg prihoda	≤ 65.000.000,00 kuna (8.666.667 EUR)*	≤ 260.000.000,00 kuna (34.666.667 EUR)
Ukupan iznos aktive	≤ 32.500.000,00 kuna (4.333.333 EUR)	≤ 130.000.000,00 kuna (17.333.333 EUR)

(* - temeljeno na tečajnom odnosu 1 EUR=7,5 Kn)

Izvor: prilagodio autor prema **Zakonu o računovodstvu** (NN 109/07, NN 144/12)

U smislu ovog zakona velikim se poduzećima po automatizmu i definiciji, a neovisno o kriterijima navedenim u tablici 16. smatraju banke, štedne banke, stambene štedionice, institucije za elektronički novac, društva za osiguranje, leasing društva, društva za upravljanje investicijskim fondovima i zasebna imovina bez pravne osobnosti kojom oni upravljaju, društva za upravljanje investicijskim fondovima i imovina investicijskih fondova s pravnom osobnosti, društva za upravljanje obveznim odnosno dobrovoljnim mirovinskim fondovima i zasebna imovina kojom oni upravljaju te mirovinska osiguravajuća društva.

5.1.2.2. Definicija malog i srednjeg poduzeća korištena u Europskoj uniji

Kratica „*MSP*“ označava mala i srednja poduzeća kako su definirana u zakonodavstvu EU-a **prema preporuci EU-a 2003/36** (Official Journal of the European Union 156., 2003). Glavni čimbenici koji prema toj preporuci određuju je li neko poduzeće dijelom kategorije malih i srednjih poduzeća su:

1. Broj zaposlenika, i
2. Promet ili ukupan iznos bilance.

Izmjenama i dopunama Zakona o poticanju razvoja malog gospodarstva (Narodne novine 53., 2012) **definicija mikro, malih i srednjih poduzeća usklađena je s istovjetnom definicijom Europske komisije (EK), Europske investicijske banke (EIB) i Europskog investicijskog fonda (EIF)**, čime je omogućen dostup izvorima financiranja i mehanizmima potpora namijenjenih srednjem i malom poduzetništvu kroz programe Europske unije.

Prema kriteriju broja zaposlenih i financijskim pokazateljima, subjekti malog gospodarstva su fizičke i pravne osobe koje prosječno godišnje imaju zaposleno manje od 250 radnika **i** ostvaruju ukupni godišnji prihod u iznosu protuvrijednosti kuna do 50.000.000,00 EUR, **ili**

imaju ukupnu aktivu ako su obveznici poreza na dobit, odnosno imaju dugotrajnu imovinu ako su obveznici poreza na dohodak, u iznosu protuvrijednosti kuna do 43.000.000,00 EUR. Ovu klasifikaciju prikazuje tablica 17.

Tablica 17: Klasifikacija mikro, malih i srednjih poduzetnika prema kriterijima broja zaposlenika, iznosa godišnjeg prihoda i ukupnog iznosa bilance prema izmjenama i dopunama Zakona o poticanju razvoja malog gospodarstva

Pokazatelj	Mikro poduzeće	Malo poduzeće	Srednje poduzeće
Broj zaposlenika	1-9 zaposlenika	10-49 zaposlenika	50-249 zaposlenika
Godišnji promet (prihod)	≤ 2 mil. EUR	≤ 10 mil. EUR	≤ 50 mil. EUR
Ukupan iznos bilance	≤ 2 mil. EUR	≤ 10 mil. EUR	≤ 43 mil. EUR

Izvor: **Program poticanja poduzetništva i obrta "Poduzetnički impuls 2013."**, Ministarstvo gospodarstva RH, siječanj 2013., Zagreb

Malo gospodarstvo prema zakonodavstvu čine subjekti registrirani kao trgovačka društva (mikro, mali i srednji), obrti i zadruge. Prema broju, malo gospodarstvu u 2012. godini čini ukupno 170.356 subjekta (podaci financijskih izvještaja i Obrtnog registra). U ukupnom broju je 71.243 mikro subjekata (udio od 41,8%), 11.533 malih subjekata (udio od 6,8%), 1.299 srednje velikih subjekata (udio od 0,8%), 1.046 zadruga (udio od 0,6%), 4.128 obrta koji posluju kao trgovci pojedinci (udio od 2,4%). Ovom prigodom treba istaknuti kako predmet istraživanja nije cijelo malo gospodarstvo, jer bi takav pristup metodološki uključivao i obrte, zadruge i trgovce pojedince, već su predmet istraživanja mala i srednja poduzeća, odnosno trgovačka društva.

Budući da je anketa provedena u prvom i drugom kvartalu 2013. godine, dok je 01.07.2013. godine Republika Hrvatska postala punopravnom članicom Europske unije, u metodologiji interpretacije rezultata ocijenjeno je kako je primjereno adaptirati klasifikaciju koju koriste Europska komisija, Europska investicijska banka i Europski investicijski fond. Potvrdu za ovu činjenicu može se naći i u činjenici kako je istovjetnu klasifikaciju adaptiralo Ministarstvo gospodarstva Republike Hrvatske, i to kako je već objašnjeno, izmjenama i dopunama Zakona o poticanju razvoja malog gospodarstva (Narodne novine 56., 2013).

5.1.3. Odabir anketne metode

Razmatrane su **metoda panel-studije**, koje bi mogle dati dinamički presjek ponašanja malih i srednjih poduzeća pri odlučivanju o ulaganje i upravljanje poslovnom funkcijom informacijske sigurnosti i metoda fokusnih grupa. Metoda panel-studije kao longitudinalna metoda koja promatra ciljnu populaciju s identičnom vremenskom ishodišnom točkom je odbačena kao neprikladna iz više razloga, među kojima je najvažnija činjenica kako se ova vrsta studije

oslanja na vremensku dimenziju koja nije pogodna s obzirom na vremenski period u kojemu je očekivan razvoj doktorske disertacije. Očekuje se kako će rezultati pokazati da je upravljanje informacijskom sigurnošću u malim i srednjim poduzećima stohastičko i da ne postoji sustavno vođenje niti upravljanje investicijama u informacijsko-sigurnosnu tehnologiju, te bi ovakva metoda imala značaj u slučaju da se panel grupa analizira prije i poslije uvođenja znanstveno utemeljenog sustava upravljanja, te se zatim izmjere konkretni učinci.

Metoda fokusne grupe je odbačena upravo zbog kvalitativnih karakteristika navedene metode, ali i samostalnosti izrade doktorske disertacije. Naime, cilj anketnog ispitivanja je dobiti kvantitativne pokazatelje kojima se pokušava potkrijepiti, te posljedično dokazati postavljena znanstvena hipoteza. Metoda fokusne grupe je po svojoj prirodi kvalitativna metoda u kojoj grupa ljudi na strukturiran način odgovara na fokusirana pitanja o percepcijama, mišljenjima i stavovima u odnosu na određeni predmet ili problem istraživanja, no specifičnost te metode je u činjenici da su sudionici slobodni raspravljati o svojim stavovima sa drugim članovima grupe. U konkretnom slučaju, ta grupa bi trebala biti sastavljena od ljudi koji su konkretno uključeni u odlučivanje ili operativno provođenje odluka vezanih uz investiranje u informacijsku sigurnost te koji posljedično imaju saznanja ili spoznaje relevantne za tu tematiku. Pretpostavka je kako u malim i srednjim poduzećima ne postoji svijest o važnosti sustavnog upravljanja sigurnošću informacijskih sustava, te se usprkos činjenici da bi ova metoda vjerojatno producirala zaključke koji podupiru hipotezu, ona ne smatra relevantnom za anketiranje dionika, jer bi u sebi fokusna grupa već imala ugrađenu pristranost. Dodatni problemi zbog kojih se smatra da metoda fokusne grupe ne bi bila adekvatna za ovo istraživanje je činjenica kako ona ne garantira anonimnost, te je samim time pitanje koliko bi odgovori na postavljena pitanja bili iskreni, a osobito ako su vezani uz osjetljive podatke poduzeća kao što je razina ulaganja u informacijsku sigurnost, broj sigurnosnih incidenata ili zatečeno stanje informacijske sigurnosti. (Wilson, 2012) Standardna problematika korištenja fokusnih grupa vezana je uz pojavu grupnog ili konformističkog mišljenja, ali i iskustvena slaba primjenjivost metode fokusnih grupa pri istraživanju vezanih uz informatičke tehnologije. Naposljetku, kao i kod metode panel-studija, ova metoda može producirati isključivo kvalitativne rezultate, a budući da je cilj istraživanja dobiti točne kvantitativne pokazatelje koje je moguće statistički obraditi, ova se metoda odbacuje kao nepodesna.

Tijekom odabira resursa potrebnih za izvođenje ankete identificirano je kako su važna četiri skupa resursa potrebnih za izvođenje ankete:

1. **Potrebno znanje iz područja statistike** je vrlo opsežno, a osobito se odnosi na instrumentarij deskriptivne statistike i ekonometriju u dijelu koji se tiče regresijske analize,

2. **Vrijeme** je identificirano kao važan resurs, kako zbog aktualnosti korištenih podataka, tako i zbog dinamike uklapanja provođenja ankete u aktivnosti cjelokupnog istraživanja. Anketni upitnik i metodologija definirani su tijekom veljače 2013. godine, anketa je distribuirana tijekom ožujka 2013. godine a obrada i prikaz rezultata tijekom travnja 2013. godine. Rezultati ankete postali su dijelom formalnog procesa prijave i obrane prethodnih rezultata istraživanja s prijavom u svibnju 2013. godine i prezentacijom tijekom rujna 2013. godine,
3. **Tim identificiranih eksperata** je bitan resurs jer su anketni upitnik i metodologija prije distribuiranja ankete povjereni mentoru i nekolicini predmetnih eksperata na provjeru i očitovanje. Na predloženi upitnik i metodologiju nisu zaprimljene značajnije primjedbe. Upitnik je revidiran prema zapažanjima predmetnih eksperata i formuliran je konačni upitnik,
4. **Platforma za distribuciju ankete** je posljednji bitan identificirani resurs, a kako je već rečeno, koristila se metoda popunjavanja ankete putem anketnih obrazaca koji su distribuirani u papirnatom obliku, te metoda Internet anketne platforme usmjerene ka ciljnoj skupini. Po analizi više sustava Internet anketiranja prema kriterijima jednostavnosti korištenja i dovoljnim mogućnostima unosa potrebnih tipova anketnih pitanja, u konačnom izboru između sustava *LimeSurvey*[163] i *Google Docs / Google Forms*[164] odluka pala na *Google Docs* sustav zbog jednostavnosti, činjenice kako je besplatan, te mogućnosti utjecaja na to da ispitanik ispravno popuni sva traženja pitanja, odnosno jednostavnog, automatiziranog i već ugrađenog smanjivanja mogućnosti pogrešaka pri ispunjavanju.

5.1.4. Formuliranje statističkog uzorka (uzorkovanje)

Kod formuliranja statističkog uzorka posebna pažnja posvećena **je izbjegavanju čestih pogrešaka** kod određivanja statističkog uzorka poput pristranosti istraživača, isključivanja dijela populacije iz istraživanja, uključivanja u uzorak populacije koja ne bi trebala biti obuhvaćena istraživanjem, te uključivanje u statistički uzorak previše velikog ili previše malog broja članova. Način na koji je to postignuto prikazan je u nastavku; naime, tijekom planiranja istraživanja u prvom kvartalu 2013. godine pokazalo se problematičnim identificirati točan broj poduzeća koja bi pripadala podskupu malih i srednjih poduzeća. Takvi se podaci mogu dobiti od više institucija, poput FINE[165] ili Hrvatske gospodarske komore[166], no obje institucije su imale

[163] Za detalje, cf. *LimeSurvey*, **https://www.limesurvey.org/** (20.08.2013.)
[164] Za detalje, cf. *Google Docs*, **https:// docs.google.com/** (20.08.2013.)
[165] *FINA* je kratica od „*Financijska agencija*“, koja je vodeća hrvatska tvrtka na području financijskog posredovanja. Za detalje cf. *FINA*, **http://www.fina.hr/Default.aspx?sec=896** (11.08.2013.)
[166] *HGK* je kratica od „*Hrvatska gospodarska komora*“. Za detalje cf. *HGK*, **http://www.hgk.hr/o-hgk** (11.08.2013.).

podatke samo za 2011. godinu koji su nedovoljni za provođenje istraživanja. Tijekom pokušaja traženja točnog broja malih i srednjih poduzeća, ustanovilo se kako treća institucija, a to je Ministarstvo gospodarstva Republike Hrvatske, u okviru provođenja programa poticanja poduzetništva i obrta jedino početkom 2013. godine već posjeduje točne podatke o broju poduzetnika i poduzeća razvrstanih prema potrebnoj metodologiji. Ove podatke za trenutak izrade anketnog upitnika i početak provođenja anketnog istraživanja prikazuje tablica 18.

Tablica 18: Broj i postotak poduzetnika u ukupnoj populaciji prema vrstama (mikro, mali, srednji, zadruge, obrtnici-trgovci pojedinci, ostali obrtnici)

Tip subjekta	Broj	Postotak u populaciji
Mikro subjekti	71.243	41,8 %
Mali subjekti	11.533	6,8 %
Srednje veliki subjekti	1.299	0,8 %
Zadruge	1.046	0,6 %
Obrtnici-trgovci pojedinci	4.128	2,4 %
Ostali obrtnici	81.107	47,6 %
UKUPNO	170.356	

84.075 subjekata

Izvor: priredio autor prema „**Programu poticanja poduzetništva i obrta "Poduzetnički impuls 2013."**, Ministarstvo gospodarstva RH, siječanj 2013., Zagreb

Budući da su predmet istraživanja mala i srednja poduzeća u Republici Hrvatskoj, ukupna populacija sastoji se **84.075 identificirana subjekta**, od čega 71.243 ili 41,8 % od ukupne populacije poduzetnika čine mikro subjekti, 11.533 ili 6,8 % čine mali subjekti dok 1.299 ili 0,8 % čine srednje veliki subjekti. Međutim, ukoliko se u omjer uzimaju pojedine sastavnice poduzeća u odnosu na ukupni broj mikro, malih i srednjih poduzeća, tada mikro poduzeća čine 84,7 %, mala poduzeća čine 13,7 % dok srednja poduzeća čine 1,5 %.

Uz razinu pouzdanosti od 95 % te interval pouzdanosti od 5 %, za zadanu populaciju bi traženi uzorak bio 382 ispitanika dok je uz razinu pouzdanosti od 90 % te interval pouzdanosti od 5 % za zadanu populaciju traženi uzorak 270 ispitanika.

Tijekom provođenja anketiranja, prikupljeno je 347 anketnih odgovora metodom slučajnog uzorkovanja. **Distribuiranje upitnika** je obavljeno na sljedeće načine:

1. Putem socijalne mreže *LinkedIn* (LinkedIn, 2013), a osobito prema korisnicima grupe *„ICT Management and Security – Croatia"*[167],
2. Elektroničkom poštom, korištenjem vlastitog adresara doktoranda,

[167] Socijalna mreža *LinkedIn* omogućuje kreiranje interesnih grupa u kojima se okupljaju ljudi koje zanimaju zajedničke teme. Anketa je, između ostalog, distribuiranja korištenjem takve jedne grupe, *ICT Management and Security – Croatia,* čiji je osnivač i vlasnik (moderator) autor, a koja okuplja više od 600 ljudi koji su profesionalci informatičke struke, rukovoditelji i direktori sektora informatike, te osobe odgovorne za informacijsku sigurnost.

3. Elektroničkom poštom, putem kontakt adresa Ekonomskog fakulteta u Rijeci,
4. Elektroničkom poštom, putem kontakt adresa Hrvatske gospodarske komore.

Doseg distribucije ankete putem Interneta je tradicionalno teško procijeniti zbog prirode distribucijskog medija, no temeljem broja poslanih e-mail poruka s pozivom na popunjavanje ankete, te broja korisnika izloženih LinkedIn grupi *„ICT Management and Security – Croatia“,* može se kvalificirano procijeniti kako je pozivu za popunjavanje ankete izloženo oko 35.520 potencijalnih respondenata[168]. U potpunosti je i ispravno elektroničkim putem ispunjena 341 anketa, što znači da je procjena odaziva oko 0,96 %.

Distribuirano je svega 90 anketnih listića u **papirnatom obliku** od čega je u potpunosti i ispravno popunjeno 6 anketnih listića, što čini odaziv od 6,7 %. Sustav je verificiran nakon 30 ispunjenih anketa i procijenjen ispravnim te je anketni postupak nastavljen.

Ciljna populacija uzorka, odnosno sudionici ankete su ključne osobe u slučajnom uzorku malih i srednjih poduzeća koje imaju potrebne informacije i to dovoljne kvalitete, kako bi mogli odgovoriti na postavljena pitanja. Budući da se tražene informacije odnose na organizaciju poslovne funkcije informacijske sigurnosti, ali i financijske pokazatelje (npr. kvantitativni iznosi godišnjih ulaganja u informacijsku sigurnost ili podaci o procjeni štete uzrokovane nastupom sigurnosnog incidenta), na takva će pitanja moći odgovoriti populacija rukovoditelja informatičkog odjela, rukovoditelja informacijskom sigurnošću, direktora, te članova uprava poduzeća, a osobito onih koji su zaduženi za rukovođenje informatičkom poslovnom funkcijom. Iz tog razloga anketa je dostavljana isključivo osobama na navedenim razinama rukovođenja u svakom od poduzeća, te je u uputama navedeno da na anketu ne odgovaraju oni koji nemaju raspoložive točne podatke za svoje poduzeće.

Podaci dobiveni provođenjem anketnog postupa **pohranjeni** su na sljedeće načine:

1. Oni podaci koji su dobiveni korištenjem anketnog Internet sustava bili su odmah po završetku ankete uklonjeni s Interneta i pohranjeni u formatu koji omogućuje dalju obradu i čuvanje,
2. Anketni upitnici u papirnatom obliku bili su skenirani, digitalizirani i pretvoreni u format koji omogućuje dalju obradu i čuvanje.

[168] Procjena izloženosti anketi utemeljena je na zbroju poslanih poruka elektroničke pošte sa zamolbom za popunjavanjem ankete, procijenjenom sudionika u aktivnostima socijalne mreže *LinkedIn* te broju distribuiranih anketnih listića.

5.1.5. Struktura anketnog upitnika

Pri formuliranju **anketnog upitnika** valjalo je koristiti metodu sinteze i analize u parovima, odnosno trebalo je sukladno postavljenoj hipotezi pokušati pretpostaviti koji su čimbenici koji su od odlučujućeg utjecaja na ukupnu razinu funkcionalnosti upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, osmisliti instrumentarij za izmjeru čimbenika koji utječu na funkcionalnost i izmjeriti ih, korištenjem metode regresijske analize ustanoviti utjecaj izmjerenih zavisnih varijabli na nezavisnu, a onda instrument mjerenja pretočiti u konkretna anketna pitanja. Osobiti **izazov** u istraživanju, a osobito pri kreiranju anketnog upitnika predstavlja priroda malih i srednjih poduzeća, naime, oskudnost kapitalne osnove i raspoloživih financijskih sredstava, nedovoljna razina obrazovanja rukovoditelja i zaposlenih te pretpostavljena nerazvijenost informacijske sigurnosti u tom poslovnom segmentu izazivaju poteškoće pri mjerenju kvantitativnih obilježja.

U kreiranju anketnog upitnika korišten je **dizajn presjeka**[169], što znači da je prikupljano više skupina podataka odnosno serija koje su promatrane u istom vremenu a ne različitim vremenskim periodima.

Pri konstrukciji anketnih pitanja korištene su četiri **mjerne skale**:

1. **Nominalna skala**, uključivo binarna obilježja, što znači da su korištene dihotomne varijable,
2. **Ordinarna skala** s obilježjima poput Likertovih, preuzeta iz psihometrije, s cjelobrojnim oznakama od „1“ do „5“ i uobičajeno percipiranim značenjem od *„ne slažem se”* do *„slažem se potpuno”*,
3. **Intervalna skala**,
4. **Omjerna skala**.

Anketni upitnik strukturiran je u ukupno pet odjeljaka (poglavlja) s brojem anketnih pitanja, kako je objašnjeno u nastavku:

1. **Upute** – Radi se o uvodnom dijelu anketnog upitnika u kojemu se ispitanicima objašnjava svrha provođenja anketnog istraživanja, anticipiraju se oblici pitanja koja će biti postavljena te se objašnjava kako istraživanje nema komercijalni već znanstveni karakter i da je anonimno,
2. **Opći podaci** - U ovom dijelu anketnog upitnika postavljeno je ukupno sedam pitanja. Dijelom su ta pitanja klasifikacijska, odnosno temeljem njih moguće je raspodijeliti anketirana poduzeća prema kriteriju iznosa bilance, prihoda i broja zaposlenih te se

[169] Prijevod eng. „*cross sectional survey design*“.

odnose na kontakt adresu elektroničke pošte onih anketiranih ispitanika koji žele primiti rezultate istraživanja. U oba oblika distribucije anketnih upitnika predviđeno je kako je anketu moguće ispuniti anonimno. Ujedno je pitanje o adresi elektroničke pošte jedino pitanje na koje je moguće ne odgovoriti a da anketni upitnik ne bude proglašen nevažećim, dok je kod popunjavanja anketnog upitnika korištenjem Internet sustava *Google Drive / Google Survey* to jedino pitanje na koje je tehnički moguće ne odgovoriti a da se anketa popuni do kraja,

3. **Diskriminacijska, neobavezna pitanja,**
4. **Opća pitanja o upravljanju informacijskom sigurnošću** – U ovom dijelu upitnika postavljeno je ukupno 35 pitanja,
5. **Pitanja vezana uz formalne domene upravljanja informacijskom sigurnošću** – Ukupno je postavljeno sedam pitanja vezanih uz formalne domene upravljanja informacijskom sigurnošću,
6. **Pitanja vezana uz operativne mjere is i sigurnosne incidente -** Uz ovu domenu postavljeno je ukupno pet pitanja.

Prema tome, postavljena su ukupno 54 anketna pitanja. Međutim, pet od navedenih pitanja su s Likertovim obilježjima i imaju, redom, 7, 3, 6, 6 i 5 potpitanja. Ukoliko bi se promatrao apsolutan broj postavljenih pitanja, njih je 76. Broj pitanja je optimiziran na minimalno potreban za dokazivanje hipoteza no on je i značajno impliciran kompleksnošću predmeta istraživanja.

U strukturiranju anketnih instrumenata korištena su dva tipa obilježja:

1. **Kvantitativna obilježja**[170]: npr. trošak za obrazovanje u području informacijske sigurnosti, investicije, trošak održavanja sustava, broj incidenata informacijske sigurnosti, prosječan broj zaposlenih,
2. **Kvalitativna obilježja**[171]: npr. klasifikacija poslovne djelatnosti, stanje uvedenosti sustava upravljanja informacijskom sigurnošću, način odlučivanja o investiranju u navedene sustave. Uključivanje ovih obilježja omogućuje detaljniju analizu zatečenog stupnja kulture i svijesti unutar poduzeća o potrebi i važnosti investiranja u sustave informacijske sigurnosti.

Kako bi se izmjerila **kulturalna dimenzija**, tamo gdje je bilo moguće nije korištena obična binarna[172] varijabla, već je dopuštena i mogućnost da poduzeće određenu mjeru nema implementiranu, ali je planira u skorom vremenskom razdoblju implementirati. Na taj način

[170] Kvantitativna su obilježja predstavljena npr. stupanjem ili omjerom.
[171] Primjeri kvalitativnih obilježja su npr. vrsta ili kategorija.
[172] Ili dihotomna varijabla.

moguće je izmjeriti činjenicu kako poduzeće nema implementiranu odgovarajuću kontrolu na nekoj od razina funkcionalnosti, ali posjeduje svijest o tome kako bi je trebalo implementirati. No, i dalje sve odgovore na pitanja u tom smislu treba promatrati u okviru činjenice da takva poduzeća zapravo nemaju implementiranu odgovarajuću kontrolu ili mjeru, odnosno valja ih pribrojiti onima koji su negativno odgovorili na to pitanje.

5.2. KRITERIJI VREDNOVANJA MODELA UPRAVLJANJA SUSTAVOM INFORMACIJSKE SIGURNOSTI U MALIM I SREDNJIM PODUZEĆIMA

Pri kreiranju modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima polazi se od glavne i pomoćnih hipoteza istraživanja. Na odgovarajućim razinama funkcionalnosti modela koje su identificirane, bilo je potrebno iz pomoćnih hipoteza derivirati impliciranje sastavnica modela upravljanja. **Pet polaznih sastavnica** pri kreiranju modela su sljedeće:

1. Upravljanje sustavom informacijske sigurnosti u malim i srednjim poduzećima temelji se na primjeni tehničkih, organizacijskih i zakonskih obrazaca zaštite,
2. Upravljanje sustavom informacijske sigurnosti je podložno normiranim sustavima[173]
3. Sustav upravljanja informacijskom sigurnošću je inherentno kompleksan i menadžment nema informacije o ukupnom trošku takvog sustava, stoga te troškove treba analizirati i sistematizirati,
4. Uvriježeni pristup upravljanja informacijskom sigurnošću je onaj je autonomno-tehnički i ne sadrži u sebi procjenu troškovnog efekta,
5. Ulazi modela upravljanja informacijskom sigurnošću su statički[174] i dinamički[175].

5.2.1. Razine funkcionalnosti informacijske sigurnosti

Budući kako su pojedini elementi modela **inherentno složeni**, potrebno je njihovo sustavno grupiranje u više razina (faza) funkcionalnosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima. Iz navedenog razloga predlaže se sljedećih **pet razina** (faza) takve funkcionalnosti:

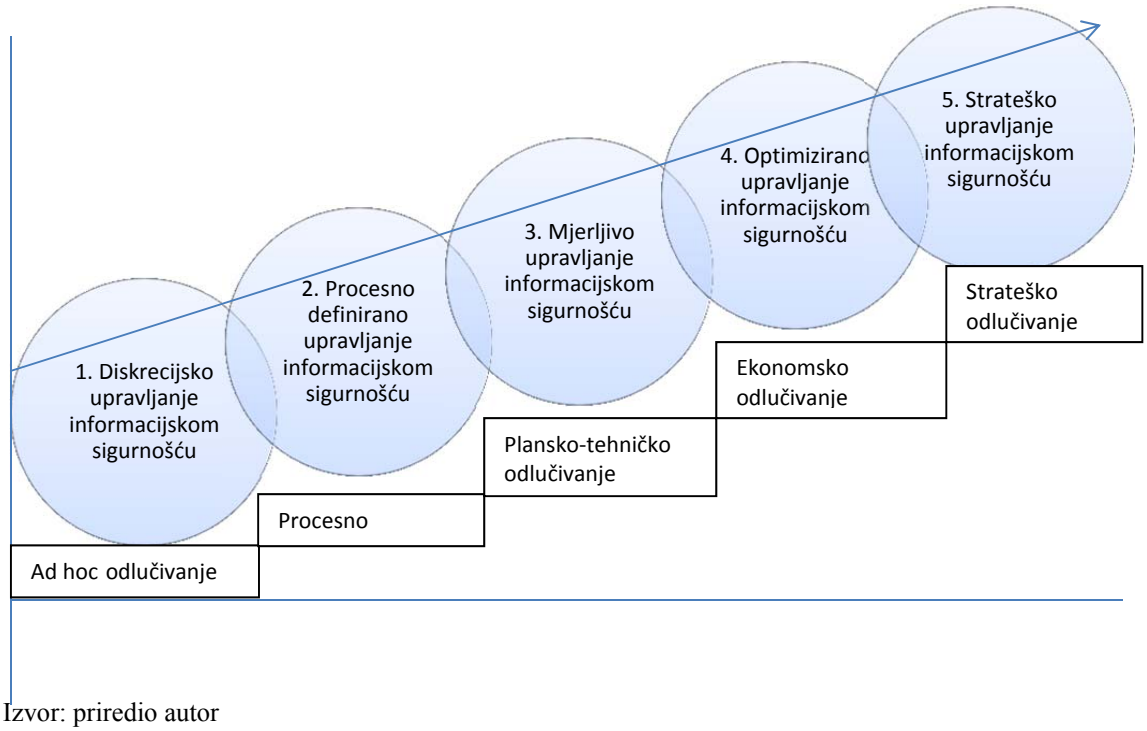
1. Razina: Razina diskrecijske odluke (*ad hoc*, intuitivnog) upravljanja ISMSom
2. Razina: Razina upravljanja informacijskom sigurnošću s definiranim procesima

[173] Normiranim sustavima u okviru ovog rada smatraju se zakonski propisi, strukovni standardi i certifikacijski sustavi koji se odnose na područje informacijske sigurnosti.
[174] Relativno statički zahtjevi zakonski zahtjevi, jer nisu podložnim čestim promjenama.
[175] U okviru postavljenog modela, dinamički zahtjevi proistječu iz tehničkih i organizacijskih osobitosti malih i srednjih poduzeća odnose se na certifikacijske zahtjeve i zahtjeve najbolje prakse, odnosno strukovne standarde.

3. Razina: Razina upravljane i mjerljive informacijske sigurnosti
4. Razina: Razina optimizirane informacijske sigurnosti
5. Razina: Razina strateške informacijske sigurnosti

Prikaz razina funkcionalnosti i zrelosti upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj vidljiv je na shemi 13.

Shema 13: Prikaz razina funkcionalnosti i zrelosti upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj



Izvor: priredio autor

Kako bi se kreirao **novi model** upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, inicijalno je potrebno odrediti temeljne elemente modela koji obuhvaćaju sve njegove aspekte, prema odgovarajućim razinama koje odgovaraju kompleksnosti implementiranih mjera. Neovisno o različitostima malih i srednjih poduzeća koja su bila uključena u istraživanje, a koje su detaljno obrazložene, moguće je determinirati elemente koji izražavaju posredan ili neposredan utjecaj na dostignutu razinu funkcionalnosti upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj. Ti će elementi biti grupirani na takav način da čine ukupno pet različitih razina funkcionalnosti modela po čijem će određivanju zatim biti istražena razina dostignute funkcionalnosti upravljanja informacijskom sigurnošću u svakom od pojedinih anketiranih malih i srednjih poduzeća.

Korištenjem modela najbolje prakse COBIT, kontrola sustava upravljanja kvalitetom sustava informacijske sigurnosti ISO 27001:2005 te praktičnih spoznaja, određeni su **temeljni elementi**

modela funkcionalnosti (zrelosti) upravljanja informacijskom sigurnošću u malim i srednjim poduzećima[176]:

1. Identificiranost i klasificiranost elemenata informacijske imovine, uključujući rizike i ranjivosti vezane uz njih,
2. Imenovana osoba u poduzeću zadužena za provođenje informacijske sigurnosti,
3. Implementiran plan upravljanja kontinuitetom poslovanja,
4. Implementiran sustav logičke kontrole pristupa resursima,
5. Implementiran sustav upravljanja u kojemu je informacijska sigurnost ključna poslovna funkcija u postizanju poslovnih ciljeva poduzeća,
6. Korištenje metoda reaktivnog rješavanja posljedica informacijsko sigurnosnih incidenata,
7. Korištenje osobne inicijative zaposlenika za upravljanje informacijskom sigurnošću,
8. Korištenje planiranja mjera informacijske sigurnosti na godišnjoj razini,
9. Organiziran odjel za informatičku podršku,
10. Organiziran odjel za upravljanje informacijskom sigurnošću,
11. Organiziran sustav učenja i poboljšanja sustava nakon nastupa sigurnosnih incidenata,
12. Provođenje mjera informacijske sigurnosti putem direktnog upravljanja od strane rukovoditelja,
13. Razvijen sustav procedura vezanih uz operativno provođenje informacijske sigurnosti,
14. Uspostavljen certificirani sustav upravljanja informacijskom sigurnošću sukladno normama i najboljoj praksi,
15. Uspostavljen sustav mjerenja stanja upravljanja informacijskom sigurnošću,
16. Uspostavljen sustav obrazovanja zaposlenika po pitanju informacijske sigurnosti,
17. Uspostavljen sustav obrazovanja rukovoditelja o zahtjevima informacijske sigurnosti,
18. Uspostavljen sustav upravljanja informacijskom sigurnošću,
19. Usvojena politika informacijske sigurnosti,
20. Uveden plan oporavka u slučaju katastrofe,
21. Uveden sustav izdvojenog praćenja ulaganja u informacijsku sigurnost,
22. Uveden sustav kapitalnog budžetiranja pri nabavi novih informacijsko sigurnosnih rješenja,
23. Uveden sustav operativnih mjera informacijske sigurnosti,
24. Uveden sustav praćenja promjena i nadzora nad komunikacijskim poslovnim sustavima,
25. Uveden sustav praćenja zakonskih zahtjeva po pitanju informacijske sigurnosti i sukladnosti poduzeća,

[176] Temeljni elementi modela funkcionalnosti upravljanja informacijskom sigurnošću ovom prigodom navedeni su abecednim redom.

26. Uveden sustav upravljanja fizičkom sigurnošću ljudi i imovine,
27. Uveden sustav upravljanja informacijsko sigurnosnim incidentima,
28. Uveden sustav upravljanja informacijskom sigurnošću u odnosu na procese nabave, održavanja i razvoja informacijskih sustava,
29. Uveden sustav zasebnog praćenja investicija i troškova održavanja sustava za upravljanje informacijskom sigurnošću od ostalih troškova poslovanja,
30. Uvedeno godišnje planiranje investicija u sustav upravljanja informacijskom sigurnošću.

U tablici 19. prikazani su elementi modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj po pojedinim razinama funkcionalnosti.

Tablica 19: Elementi modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj po pojedinim razinama funkcionalnosti

Razina	Elementi modela
5.	• Sustav obrazovanja rukovoditelja o zahtjevima informacijske sigurnosti (S,F,R) • Sustav kapitalnog budžetiranja pri nabavi novih informacijsko sigurnosnih rješenja (F,R) • Sustav učenja i poboljšanja sustava nakon nastupa sigurnosnih incidenata (S,R) • Sustav upravljanja u kojemu je informacijska sigurnost ključna poslovna funkcija u postizanju poslovnih ciljeva poduzeća (S,F,R) • Certificirani sustav upravljanja informacijskom sigurnošću sukladno normama i najboljoj praksi (S,R)
4.	• Odjel za upravljanje informacijskom sigurnošću (S,F,R) • Korištenje osobne inicijative zaposlenika za upravljanje informacijskom sigurnošću (S) • Sustav zasebnog praćenja investicija i troškova održavanja sustava za upravljanje informacijskom sigurnošću od ostalih troškova poslovanja (F,R) • Sustav upravljanja informacijskom sigurnošću u odnosu na procese nabave, održavanja i razvoja informacijskih sustava (S) • Sustav izdvojenog praćenja ulaganja u informacijsku sigurnost (F,R) • Godišnje planiranje investicija u sustav upravljanja informacijskom sigurnošću (F,R)
3.	• Sustav upravljanja informacijskom sigurnošću (S,R) • Sustav mjerenja stanja upravljanja informacijskom sigurnošću (S) • Planiranje mjera informacijske sigurnosti na godišnjoj razini (S) • Sustav obrazovanja zaposlenika po pitanju informacijske sigurnosti (S,R) • Identificiranost i klasificiranost elemenata informacijske imovine, uključujući rizike i ranjivosti vezane uz njih (S) • Sustav upravljanja fizičkom sigurnošću ljudi i imovine (S) • Sustav praćenja promjena i nadzora nad komunikacijskim poslovnim sustavima (S) • Plan oporavka u slučaju katastrofe (S,Z) • Plan upravljanja kontinuitetom poslovanja (S,Z) • Sustav praćenja zakonskih zahtjeva po pitan ju informacijske sigurnosti i sukladnosti poduzeća (S,Z) • Sustav operativnih mjera informacijske sigurnosti (S,Z) • Sustav upravljanja informacijsko sigurnosnim incidentima (S)
2.	• Osoba u poduzeću zadužena za provođenje informacijske sigurnosti (S,R) • Politika informacijske sigurnosti (S) • Sustav procedura vezanih uz operativno provođenje informacijske sigurnosti (S,R) • Sustav logičke kontrole pristupa resursima (S)
1.	• Provođenje mjera informacijske sigurnosti putem direktnog upravljanja od strane rukovoditelja (R)

	• Organiziran odjel za informatičku podršku (R) • Korištenje metoda reaktivnog rješavanja posljedica informacijsko sigurnosnih incidenata (R)

Izvor: priredio autor

U tablici 19. je uz svaki element pridodana i oznaka slovima *„Z“, „S“, „F“* i *„R“* sa sljedećim mogućim značenjem, koja predstavlja povezanost pojedinih elemenata modela s pridodanim kriterijima vrednovanja

1. *„Z“:* Zakonski zahtjevi,
2. *„S“:* Stručni kriteriji najbolje prakse,
3. *„F“*: Financijski kriteriji,
4. *„R“*: Razvojni kriteriji.

5.2.1.1. Kriteriji vrednovanja modela upravljanja sustavom informacijske sigurnosti na prvoj razini - razina diskrecijske odluke (ad hoc, intuitivnog upravljanja)

Na prvoj razini zrelosti funkcije upravljanja informacijskom sigurnošću, mala i srednja poduzeća upravljaju informacijskom sigurnošću bez separiranja odgovornosti za upravljanje poslovnom funkcijom informatike i informacijskom sigurnošću te se oslanjaju na primjenu strukovnih mjera od strane osoba ili odjela zaduženih za upravljanje informatikom. Upravljanje informacijskom sigurnošću provodi se isključivo kroz prizmu nastupa incidenata informacijske sigurnosti i reaktivnog rješavanja posljedica nastupa incidenata informacijske sigurnosti.

Elementi modela na osnovnoj, prvoj razini funkcionalnosti određuju se kako slijedi[177]:

1. Provođenje mjera informacijske sigurnosti putem direktnog upravljanja od strane rukovoditelja,
2. Organiziran odjel za informatičku podršku,
3. Korištenje metoda reaktivnog rješavanja posljedica informacijsko sigurnosnih incidenata.

5.2.1.2. Kriteriji vrednovanja modela upravljanja sustavom informacijske sigurnosti na drugoj razini - razina s definiranim procesima

Na drugoj razini funkcionalnosti i zrelosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima, aktivnosti i dostignuća nadograđuju se na prvi fazu (razinu) na način da se unutar poduzeća definira točno određena osoba koja je zadužena od strane rukovoditelja ili vlasnika za provođenje mjera informacijske sigurnosti. Ta osoba koordinira kreiranje dokumenta najviše razine koji definira sve ostale aktivnosti u provođenju mjera

[177] Redoslijed elemenata modela na prvoj razini funkcionalnosti je slučajan.

informacijske sigurnosti, a to je politika informacijske sigurnosti. Temeljem usvojene politike, unutar poduzeća razvija se sustav procedura vezanih uz operativno provođenje informacijske sigurnosti. Takve procedure su u samom početku razvoja sustava upravljanja informacijskom sigurnošću obično usmene ili običajno uvriježene, dok se kasnije formaliziraju u obliku dokumenta koji odobravaju rukovoditelji poduzeća ili poslovnih jedinica. Naposljetku, identificirani su informacijski resursi i imovina te je implementiran sustav logičkih kontrola pri pristupu tim resursima.

Elementi modela na drugoj razini, razini upravljanja informacijskom sigurnošću s definiranim procesima, određuju se kako slijedi[178]:

1. Imenovana osoba u poduzeću zadužena za provođenje informacijske sigurnosti,
2. Usvojena politika informacijske sigurnosti,
3. Razvijen sustav procedura vezanih uz operativno provođenje informacijske sigurnosti,
4. Implementiran sustav logičke kontrole pristupa resursima.

5.2.1.3. Kriteriji vrednovanja modela upravljanja sustavom informacijske sigurnosti na trećoj razini - razina upravljane i mjerljive informacijske sigurnosti

Na trećoj razini funkcionalnosti i zrelosti sustava upravljanja informacijskom sigurnošću, značajno su kompleksnije aktivnosti koje poduzeće mora provoditi u kontinuitetu kako bi osiguralo sigurnost svojih informacijskih sustava. Dodatni naglasak na ovoj razini funkcionalnosti stavljen je na uspostavljen sustav upravljanja informacijskom sigurnošću uključivo mjerenje stanja i planiranje mjera informacijske sigurnosti na godišnjoj razini, osiguranje sukladnosti po pitanju zakonskih zahtjeva, upravljanje informacijsko sigurnosnim incidentima i fizičku sigurnost ljudi i imovine uz temeljne mjere i izrađenost plana oporavka od katastrofe.

Elementi modela na trećoj razini funkcionalnosti zrelosti modela, razini upravljane i mjerljive informacijske sigurnosti određuju se kako slijedi[179]:

1. Uspostavljen sustav upravljanja informacijskom sigurnošću,
2. Uspostavljen sustav mjerenja stanja upravljanja informacijskom sigurnošću,
3. Korištenje planiranja mjera informacijske sigurnosti na godišnjoj razini,
4. Uspostavljen sustav obrazovanja zaposlenika po pitanju informacijske sigurnosti,
5. Identificiranost i klasificiranost elemenata informacijske imovine, uključujući rizike i ranjivosti vezane uz njih,
6. Uveden sustav upravljanja fizičkom sigurnošću ljudi i imovine,

[178] Redoslijed elemenata modela na drugoj razini funkcionalnosti je slučajan.
[179] Redoslijed elemenata modela na trećoj razini funkcionalnosti je slučajan.

7. Uveden sustav praćenja promjena i nadzora nad komunikacijskim poslovnim sustavima,
8. Uveden plan oporavka u slučaju katastrofe,
9. Implementiran plan upravljanja kontinuitetom poslovanja,
10. Uveden sustav praćenja zakonskih zahtjeva po pitanju informacijske sigurnosti i sukladnosti poduzeća,
11. Uveden sustav operativnih mjera informacijske sigurnosti,
12. Uveden sustav upravljanja informacijsko sigurnosnim incidentima.

5.2.1.4. Kriteriji vrednovanja modela upravljanja sustavom informacijske sigurnosti na četvrtoj razini - razina optimizirane informacijske sigurnosti

Na četvrtoj razini funkcionalnosti i zrelosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima, poduzeća posjeduju organiziran odjel za upravljanje informacijskom sigurnošću, odnosno navedenu su aktivnost koncentrirali u jednoj točki. Zaposlenici nisu samo kontrolirani objekti u procesu provođenja informacijske sigurnosti već postaju aktivni subjekti. Informacijska se sigurnost razmatra tijekom cijelog životnog vijeka korištenja informatičkih tehnologija a posebna je pažnja posvećena izdvojenom, periodičkom praćenju investicija i troškova sustava upravljanja informacijskom sigurnošću.

Elementi modela na četvrtoj razini funkcionalnosti, razini optimizirane informacijske sigurnosti, određuju se kako slijedi[180]:

1. Organiziran odjel za upravljanje informacijskom sigurnošću,
2. Korištenje osobne inicijative zaposlenika za upravljanje informacijskom sigurnošću,
3. Uveden sustav zasebnog praćenja investicija i troškova održavanja sustava za upravljanje informacijskom sigurnošću od ostalih troškova poslovanja,
4. Uveden sustav upravljanja informacijskom sigurnošću u odnosu na procese nabave, održavanja i razvoja informacijskih sustava,
5. Uveden sustav izdvojenog praćenja ulaganja u informacijsku sigurnost,
6. Uvedeno godišnje planiranje investicija u sustav upravljanja informacijskom sigurnošću.

5.2.1.5. Kriteriji vrednovanja modela upravljanja sustavom informacijske sigurnosti na petoj razini - razina strateške informacijske sigurnosti

Na petoj razini funkcionalnosti i zrelosti sustava upravljanja informacijskom sigurnošću, informacijska je sigurnost ključna i strateška poslovna funkcija u postizanju poslovnih ciljeva poduzeća, rukovoditelji i vlasnici se neprestano educiraju o specifičnostima razvoja poslovne

[180] Redoslijed elemenata modela na četvrtoj razini funkcionalnosti je slučajan.

funkcije informacijske sigurnosti, koriste se kvantitativne metode pri odlučivanju o investiranju u informacijsko-sigurnosna rješenja, a sustav upravljanja informacijskom sigurnošću i formalno je certificiran sukladno normama i najboljoj praksi.

Elementi modela na petoj razini funkcionalnosti, razini strateške informacijske sigurnosti, određuju se kako slijedi[181]:

1. Uspostavljen sustav obrazovanja rukovoditelja o zahtjevima informacijske sigurnosti,
2. Uveden sustav kapitalnog budžetiranja pri nabavi novih informacijsko sigurnosnih rješenja,
3. Organiziran sustav učenja i poboljšanja sustava nakon nastupa sigurnosnih incidenata,
4. Implementiran sustav upravljanja u kojemu je informacijska sigurnost ključna poslovna funkcija u postizanju poslovnih ciljeva poduzeća,
5. Uspostavljen certificirani sustav upravljanja informacijskom sigurnošću sukladno normama i najboljoj praksi.
6. Temeljem postavljenog modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima i vrednovanja elemenata prema kompleksnosti i razinama funkcionalnosti predstavljenim u prethodnom poddijelu, analizirani su svi podaci koji su dobiveni tijekom anketnog istraživanja, na način da su stavljeni u usporedbu sa teoretskim malim ili srednjim poduzećem koje bi posjedovalo sve elemente modela na svim razinama funkcionalnosti implementacije.

5.2.2. Određivanje vrijednosti kriterija

Elementi modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima raščlanjeni su s ciljem analize anketiranih malih i srednjih poduzeća u Republici Hrvatskoj te je određeno odgovarajućih **pet razina funkcionalnosti**, koje korespondiraju s **pet različitih razina kompleksnosti** tako determiniranog sustava. Cilj kreiranja ovakvog modela je anticipiranje mogućnosti implementacije viših razina modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima, a u tu svrhu potrebno je vrednovati postavljeni model elektroničkog poslovanja sukladno kompleksnosti određenih razina funkcionalnosti.

Korištenjem uvriježene metodologije modeliranja prema kojoj je svaka sljedeća razina funkcionalnosti modela upravljanja informacijskom sigurnošću provedbeno i sadržajno kompleksnija od prethodne, predlaže se sljedeći sustav **vrednovanja elemenata modela** prema razinama funkcionalnosti, odnosno prema njihovoj kompleksnosti:

[181] Redoslijed elemenata modela na petoj razini funkcionalnosti je slučajan.

1. Prva razina funkcionalnosti modela/razina kompleksnosti - razina diskrecijske odluke (*ad hoc*, intuitivnog) upravljanja sustavom informacijske sigurnosti: **čimbenik 1**,
2. Druga razina funkcionalnosti modela/razina kompleksnosti - razina upravljanja informacijskom sigurnošću s definiranim procesima: **čimbenik 2**,
3. Treća razina funkcionalnosti modela/razina kompleksnosti - razina upravljane i mjerljive informacijske sigurnosti: **čimbenik 3**,
4. Četvrta razina funkcionalnosti modela/razina kompleksnosti - razina optimizirane informacijske sigurnosti: **čimbenik 4**,
5. Peta razina funkcionalnosti modela/razina kompleksnosti - razina strateške informacijske sigurnosti: **čimbenik 5**.

U tablici 20. prikazani su **elementi modela** upravljanja informacijskom sigurnošću u malim i srednjim poduzećima sa pripadajućim razinama (čimbenicima) funkcionalnosti koji korespondiraju s razinama kompleksnosti, kao i oni teorijski rezultati funkcionalnosti upravljanja informacijskom sigurnošću u malim i srednjim poduzećima koji mogu biti dostignuti korištenjem ovako postavljenog modela.

Tablica 20: Elementi modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima sa razinama funkcionalnosti

Elementi modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima sa razinama funkcionalnosti	**Razina/čimbenik**	**Vrijednost**
Tri elementa prve razine funkcionalnosti	1	3
Četiri elementa druge razine funkcionalnosti	2	8
Dvanaest elemenata treće razine funkcionalnosti	3	36
Šest elemenata četvrte razine funkcionalnosti	4	24
Pet elemenata pete razine funkcionalnosti	5	25
UKUPNO trideset elemenata modela		**96**

Izvor: priredio autor

Zbroj vrijednosti svih elemenata modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima sa pripadajućim razinama kompleksnosti **iznosi 96**. To znači kako bi **poduzeće s idealno upravljanim sustavom informacijske sigurnosti** i s **implementiranim svim identificiranim elementima upravljanja informacijskom sigurnošću na svim opisanim razinama funkcionalnosti imalo tu ocjenu dostignute funkcionalnosti**. Kao što se vidi, ovaj je model ciljano asimetričan jer se veću težinsku vrijednost ukupne ocjene funkcionalnosti nose više, a samim time metodološki i kompleksnije razine funkcionalnosti, odnosno treća, četvrta i peta. Pojedinačno, najvišu ocjenu funkcionalnosti nosi treća, centralna razina funkcionalnosti dok jednostavnije, metodološki manje kompleksne prva i druga razina funkcionalnosti posjeduju najnižu ukupnu vrijednost. Ovakva metodologija izabrana je između ostalog i iz razloga što se na trećoj, centralnoj razini funkcionalnosti nalaze one mjere

informacijske sigurnosti koje su u provođenju najopsežnije po pitanju zahtjeva postavljenih pred mala i srednja poduzeća, te je stoga i njoj smještaj unutar modela obavljen na opisani način.

Korištenjem ovako izloženog vrednovanja pet razina modela iz navedenog se može zaključiti kako u modelu postoje tri elementa sa čimbenikom kompleksnosti „*1*“, četiri elementa sa čimbenikom kompleksnosti „*2*“, dvanaest elemenata s čimbenikom kompleksnosti „*3*“, šest elemenata s čimbenikom kompleksnosti „*4*“ i pet elemenata s čimbenikom kompleksnosti „*5*“.

5.3. PRIKAZ I INTERPRETACIJA REZULTATA ISTRAŽIVANJA – POZNAVANJE ZAKONSKE REGULATIVE, KORIŠTENJE SUSTAVA CERTIFIKACIJE I EKONOMSKI UČINCI UPORABE SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U MALIM I SREDNJIM PODUZEĆIMA U REPUBLICI HRVATSKOJ

U ovom poglavlju obrađene su sljedeće cjeline: **1) Obrada anketnih rezultata - opća pitanja, 2) Obrada anketnih rezultata po razinama funkcionalnosti, 3) Obrada anketnih rezultata – upravljanje sustavima kvalitete, 4) Obrada anketnih rezultata – utrošak u obrazovanje iz područja informacijske sigurnosti, 5) Obrada anketnih rezultata – upravljanje informacijskom sigurnošću, 6) Obrada anketnih rezultata – kapitalna ulaganja i tekući trošak, 7) Obrada anketnih rezultata – planiranje upravljanja informacijskom sigurnošću, 8) Obrada anketnih rezultata – incidenti informacijske sigurnosti, 9) Obrada anketnih rezultata – korištenje operativnih mjera informacijske sigurnosti, 10) Obrada anketnih rezultata – incidenti informacijske sigurnosti, 11) Obrada anketnih rezultata – korporativna kultura informacijske sigurnosti.**

5.3.1. Obrada anketnih rezultata – opća pitanja

Klasifikacija poduzeća ponuđena tijekom istraživanja izvedena je iz Nacionalne klasifikacije djelatnosti[182] (Narodne novine 28., 2007) iz 2007. godine, koja je prikazana u tablici 21. Prethodne Nacionalne klasifikacije djelatnosti bile su iz godina 1995. (Narodne novine 6., 1995), 1997. (Narodne novine 3., 1997) i 2003. (Narodne novine 13., 2003) Prema NKD sve se poslovne djelatnosti u Republici Hrvatskoj mogu podijeliti na ukupno 21 temeljno područje djelatnosti označeno velikim slovima od „*A*“ do „*U*“. Područja poslovnih djelatnosti se dalje

[182] „*NKD*“ je kratica za „*Nacionalna klasifikacija djelatnosti*“.

dijele na odjeljke, odjeljci na skupine, a skupine u razrede. Za potrebe istraživanja dovoljna je vršna podjela na poslovna područja prikazana u tablici 21.

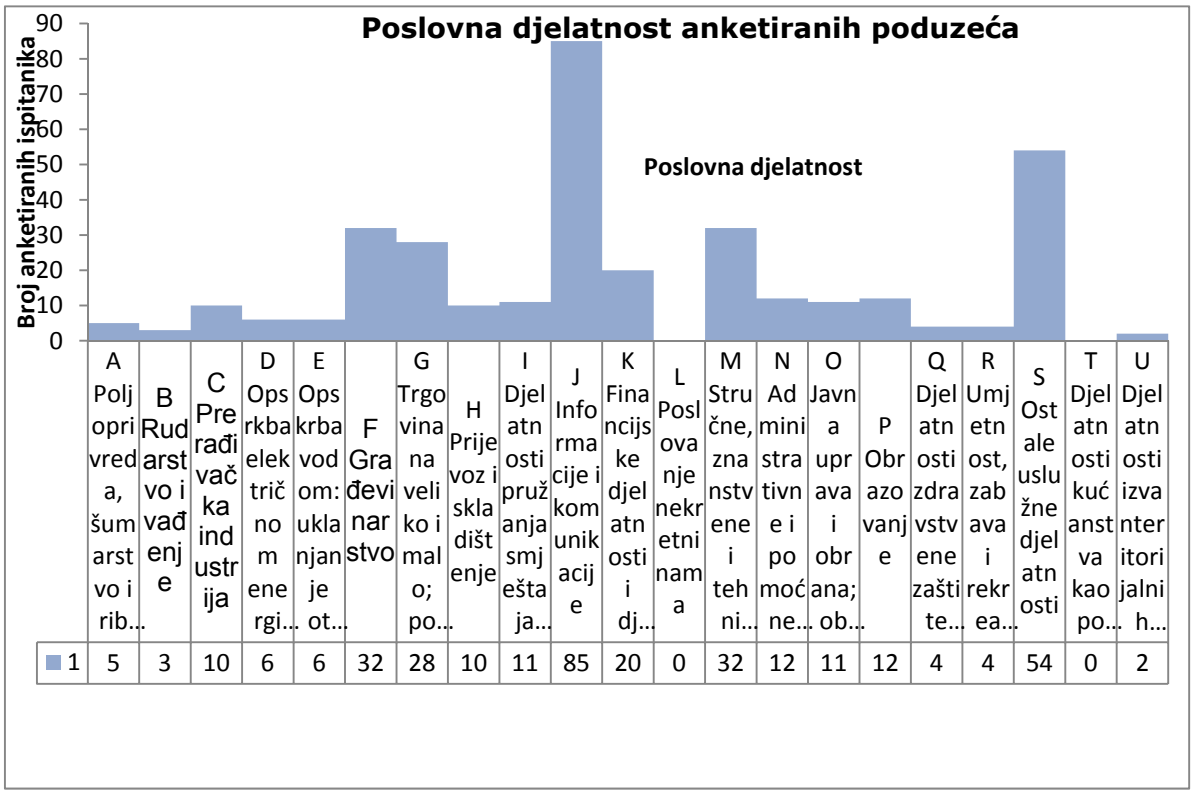
Tablica 21: Nacionalna klasifikacija djelatnosti iz 2007. godine

PODRUČJE	DJELATNOST
A	Poljoprivreda, šumarstvo i ribarstvo
B	Rudarstvo i vađenje
C	Prerađivačka industrija
D	Opskrba električnom energijom, plinom, parom i klimatizacija
E	Opskrba vodom: uklanjanje otpadnih voda, gospodarenje otpadom te djelatnosti sanacije okoliša
F	Građevinarstvo
G	Trgovina na veliko i malo; popravak motornih vozila i motocikala
H	Prijevoz i skladištenje
I	Djelatnosti pružanja smještaja te pripreme i usluživanja hrane
J	Informacije i komunikacije
K	Financijske djelatnosti i djelatnosti osiguranja
L	Poslovanje nekretninama
M	Stručne, znanstvene i tehničke djelatnosti
N	Administrativne i pomoćne uslužne djelatnosti
O	Javna uprava i obrana; obvezno socijalno osiguranje
P	Obrazovanje
Q	Djelatnosti zdravstvene zaštite i socijalne skrbi
R	Umjetnost, zabava i rekreacija
S	Ostale uslužne djelatnosti
T	Djelatnosti kućanstva kao poslodavca; djelatnosti kućanstava koja proizvode različitu robi i obavljaju različite usluge za vlastite potrebe
U	Djelatnosti izvanteritorijalnih organizacija i tijela

Izvor: „**Nacionalna klasifikacija djelatnosti“**, Narodne novine 28/2007.

Statistički uzorak nije posebno stratificiran prema pojedinim djelatnostima prisutnim u NKD budući da je temeljna premisa kako je statistički uzorak reprezentativan u odnosu na cjelokupnu populaciju po svim obilježjima, pa tako i strukturi anketiranih. Struktura poslovnih djelatnosti anketiranih poduzeća prikazana je na grafikonu 3. Na *Y* osi prikazana je stupčastim grafikonom mjerna skala **frekvencija pojave** pojedinog područja poslovne djelatnosti u statističkom uzorku dok su na osi *X* prikazana pojedina **područja**, a dodatno je ispod osi prikazana apsolutna pojavnost frekvencije pojedinog područja poslovne djelatnosti. Najviše anketiranih poduzeća (24,5 %) pripada području J – „*Informacije i telekomunikacije*“, a to područje slijede s 15,6 % S – „*Ostale uslužne djelatnosti*“, s 9,2 % M – „*Stručne, znanstvene i tehničke djelatnosti*“ i F – „*Građevinarstvo*“ te s 8,1 % G – „*Trgovina na veliko i malo; popravak motornih vozila i motocikla*.“ Valja uočiti kako u anketi nisu zastupljena poslovna područja T – „*Djelatnosti kućanstva kao poslodavca; djelatnosti kućanstava koja proizvode različitu robu i obavljaju različite usluge za vlastite potrebe*“ i L – „*Poslovanje nekretninama*“, jer niti jedan respondent iz poduzeća koja obavljaju djelatnost u navedenim područjima nije odgovorio na anketni poziv.

Grafikon 3: Prikaz strukture poslovne djelatnosti anketiranih poduzeća prema Nacionalnoj klasifikaciji djelatnosti (NKD)



Izvor: priredio autor

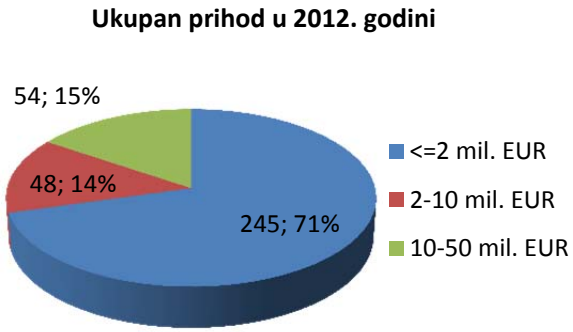
Budući da je istraživanje orijentirano na mala i srednja poduzeća, od interesa je analizirati strukturu broja zaposlenih u anketiranim poduzećima. U ovom i svim dijagramima trodimenzionalnog strukturnog kruga prvi broj označava frekvenciju pojave određenog obilježja u statističkom uzorku dok drugi broj, odnosno postotak, odvojen točka-zarezom, predstavlja postotak odnosno relativni odnos pojave obilježja i ukupnog broja anketiranih poduzeća. Kao što se vidi na grafikonu 4. na sljedećoj stranici, 162 anketirana poduzeća ili 47 % su mikro-poduzeća s 0-9 zaposlenih, njih 102 ili 29 % anketiranih poduzeća su mala poduzeća koja imaju 10 do 49 zaposlenih dok 83 poduzeća ili 24 % pripada u skupinu srednjih poduzeća s 50-249 zaposlenih.

Grafikon 4: Prosječan broj zaposlenih u anketiranim poduzećima u 2012. godini

Izvor: priredio autor

Drugo važno obilježje koje jednoznačno identificira anketirana poduzeća je ukupan prihod. 71 % anketiranih poduzeća ili njih 245 ima prihod manji ili jednak od 2 milijuna EUR u 2012. godini. 14 %, odnosno 48 poduzeća ostvaruje prihod od 2 do 10 milijuna EUR, dok 15 % ili 54 poduzeća realizira prihod od 10 do 50 milijuna EUR. Ukoliko se u usporedbu stave kriteriji broja zaposlenih i ukupnog prihoda anketiranih poduzeća, može se zaključiti kako značajan udio poduzeća koja po klasifikaciji prosječnog broja zaposlenih pripadaju segmentu srednjih poduzeća ostvaruje ukupan prihod koji se klasifikacijski atribuira malim poduzećima, dok sličan zaključak vrijedi i za srednja poduzeća prema istom kriteriju. Iz navedenog se može izvesti i zaključak o razmjerno manjoj produktivnosti čimbenika rada od one koja bi bila očekivana sukladno klasifikaciji malih i srednjih poduzeća. Naime, očekivano stanje bilo bi da ne postoje značajnija odstupanja kriterija prosječnog broja zaposlenika u odnosu na ukupan prihod u klasifikacijskoj populaciji. Ovi podaci prikazani su na grafikonu 5.

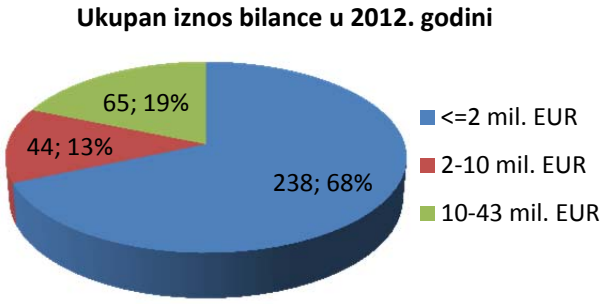
Grafikon 5: Ukupan prihod anketiranih poduzeća u 2012. godini



Izvor: priredio autor

Naposljetku, posljednji klasifikacijski kriterij, odnosno ukupan iznos bilance anketiranih poduzeća u 2012. godini pokazuje slične rezultate kao kod kriterija ukupnog prihoda. 238 anketiranih poduzeća ili 68 % ukupne populacije ima ukupan iznos bilance manji ili jednak od 2 milijuna EUR. 44 anketirana poduzeća odnosno njih 13 % ima ukupan iznos bilance u rasponu od 2 do 10 milijuna EUR dok 65 anketiranih poduzeća, ili 19 ima iznos bilance u rasponu od 10 do 34 milijuna EUR. Strukturni krug za ovaj klasifikacijski kriterij je prikazan na grafikonu 6.

Grafikon 6: Ukupan iznos bilance anketiranih poduzeća u 2012. godini



Izvor: priredio autor

Zadržavanje rasponskog mjerila, odnosno intervalne skale, kako je to i u zakonskom propisu koji definira klasifikaciju mikro, malih i srednjih poduzeća, omogućilo je i diskriminaciju svih onih potencijalno anketiranih koji ne pripadaju u anketnu populaciju, bilo da se radi o velikim poduzećima[183], ili o drugim subjektima, npr. onima koji obavljaju neprofitnu djelatnost. Ovo je osobito izraženo kod izrađenog računalnog sustava Internet anketiranja, čime je automatski ugrađen samoregulirajući mehanizam koji osigurava konzistentnost podataka sukladno definiranom objektu istraživanja a iz istog isključuje sve koji ne pripadaju istraživanoj populaciji odnosno ne zadovoljavaju definicijske kriterije.

5.3.2. Obrada anketnih rezultata po razinama funkcionalnosti

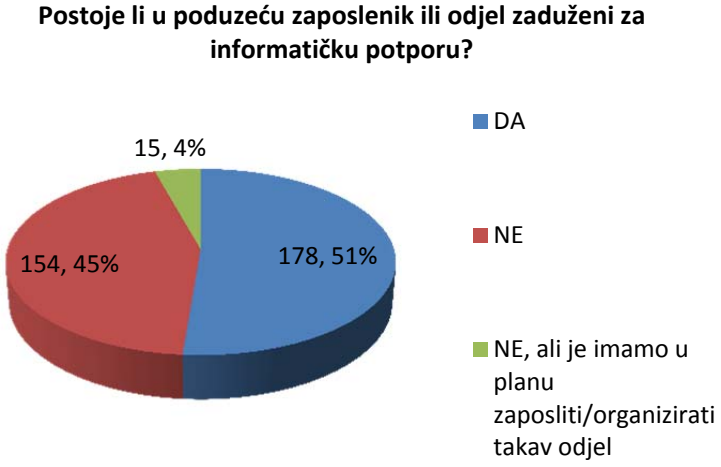
U ovoj cjelini obrazlažu se sljedeće cjeline: **1) Obrada anketnih rezultata – I. razina funkcionalnosti, 2) Obrada anketnih rezultata – II. razina funkcionalnosti, 3) Obrada anketnih rezultata – III. razina funkcionalnosti, 4) Obrada anketnih rezultata – IV. razina funkcionalnosti, 5) Obrada anketnih rezultata – V. razina funkcionalnosti. 6) Obrada anketnih rezultata – ukupna funkcionalnost**

[183] Anketa je konstruirana na način da anketirani iz velikog poduzeća po kriteriju prosječnog broja zaposlenih, ostvarenom prihodu ili iznosu bilance ne može odgovoriti na postavljena pitanja, budući da nema odgovarajućeg odgovora, čime su oni diskvalificirani iz daljeg postupka.

5.3.2.1. Obrada anketnih rezultata – I. razina funkcionalnosti

Od 347 anketiranih poduzeća, preko polovice, odnosno 178 poduzeća ili 51 % ima u poduzeću instancu, bilo da je to jedan zaposlenik ili više njih koji čine organizirani odjel, a koji je zadužen za informatičku potporu. 154 anketirana poduzeća ili 45 % nema organiziranu internu informatičku potporu, što znači da se ista pruža ili od slučaja do slučaja, od strane zaposlenika koji imaju dostignutu neku razinu informatičkog znanja koja može biti od pomoći u rješavanju problema na *ad hoc* način, dok 15 anketiranih poduzeća ili njih 4 % nema zaposlenu takvu osobu ili organiziran odjel informatičke podrške ali je namjeravaju zaposliti ili organizirati takav odjel. Dobiveni rezultati su znakoviti, budući da bi se očekivalo kako će čak i najmanjim poduzećima biti određena makar jedna osoba za informatičku potporu. Iznenađuje i činjenica kako samo 4 % anketiranih poduzeća uopće namjerava zaposliti takvu osobu ili organizirati odjel informatičke podrške. Ovo je obilježje vrlo bitno za provođenje mjera informacijske sigurnosti u svakom poduzeću budući da je isto nužno vezano uz organiziran i sustavan način upravljanja poslovnom funkcijom informatike te se bez poboljšanja odnosa poduzeća prema njoj ne može očekivati niti značajan napredak dostignute razine funkcionalnosti upravljanja informacijskom sigurnošću. Ovi podaci grafički su prikazani na grafikonu 7.

Grafikon 7: Prikaz postotnog udjela anketiranih poduzeća koja imaju zaposlenika ili odjel zadužene za informatičku potporu (anketno pitanje br. 8)



Izvor: priredio autor

Na prvom razini funkcionalnosti sljedeći bitan identificiran upit je onaj koji je povezan uz provođenje mjera informacijske sigurnosti direktnim upravljanjem, odnosno donošenjem mjera, akcija i odluka od strane rukovoditelja. U malim i srednjim poduzećima često se provođenje

mjera informacijske sigurnosti ne eskalira do razine rukovoditelja[184], već se oslanja na slučajno rukovođenje. Temeljna pretpostavka modela upravljanja informacijskom sigurnošću na prvoj razini funkcionalnosti je da su rukovoditelji upoznati s problemima i mjerama vezanim uz informacijsku sigurnost u poduzeću, odnosno da aktivno participiraju u njihovom provođenju. Ova je mjera funkcionalnosti direktno preuzeta iz temeljnih odrednica ISO 27001:2005 standarda po kojemu je uključenost rukovodstva poduzeća temeljna postavka funkcioniranja sustava. Na ovaj upit postoji gotovo ravnomjerna raspoređenost prema ponuđenim odgovorima, odnosno 165 anketiranih poduzeća ili 48 % odgovorilo je kako provode takve mjere na način da uključuju diskreciono upravljanje rukovoditelja, dok 182 anketirana poduzeća ili 52 % mjere ne provodi na taj način. Ovaj odnos prikazan je na grafikonu 8.

Grafikon 8: Prikaz postotnog udjela anketiranih poduzeća koja provode mjere informacijske sigurnosti isključivo direktnim upravljanjem od strane rukovoditelja (anketno pitanje br. 16)

Izvor: priredio autor

Na kraju, kao temeljna mjera funkcionalnosti sustava upravljanja informacijskom sigurnošću na prvoj razini identificirano je tijekom pripreme ocjene modela dostignute funkcionalnosti provođenje mjera informacijske sigurnosti isključivo reaktivnim rješavanjem posljedica informacijsko sigurnosnih incidenata. 126 anketiranih poduzeća ili 36 % ukupno anketiranih odgovorilo je kako isključivo rješavaju posljedice sigurnosnih incidenata kada oni već nastanu. S metodološkog i upravljačkog stajališta, ova je činjenica osobito zabrinjavajuća budući kako je jasno da u takvim poduzećima vjerojatno ne postoji uspostavljeno upravljanje sustavom informacijske sigurnosti i nije implementirano sustavno i proaktivno planiranje, već samo reakcija na nastupe sigurnosnih incidenata. 221 anketirano poduzeće ili njih 64 % odgovara

[184] Odnosno, u slučaju mikro poduzeća, vlasnika.

kako ne provode mjere informacijske sigurnosti isključivo reaktivnim rješavanjem posljedica nastalih informacijsko sigurnosnih incidenata. Grafikon 9. prikazuje ove podatke.

Grafikon 9: Prikaz postotnog udjela anketiranih poduzeća koja provode mjere informacijske sigurnosti isključivo reaktivnim rješavanjem posljedica informacijsko sigurnosnih incidenata (anketno pitanje br. 17)

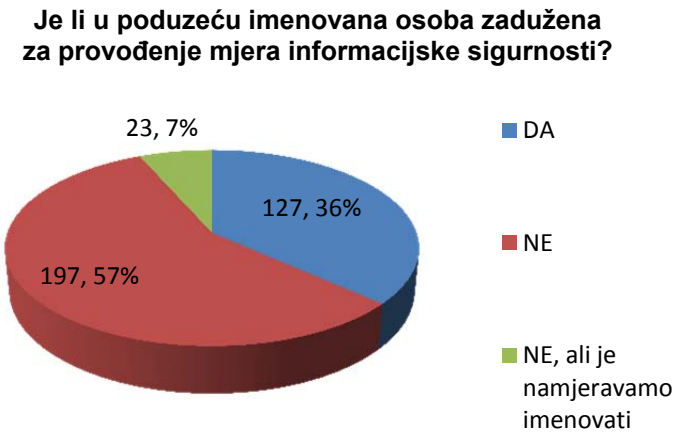
Izvor: priredio autor

Već na prvoj razini funkcionalnosti razvidno je kako gotovo polovica anketiranih poduzeća nema osobu ili odjel zadužene za informatičku potporu, preko polovica anketiranih ne uključuje rukovoditelje u proces upravljanja informacijskom sigurnošću dok više od trećine rješava probleme informacijsko sigurnosnih incidenata tek po njihovom nastanku, odnosno reaktivno. Iz ovih pokazatelja može se zaključiti kako prema postavljenom modelu već na prvoj razini funkcionalnosti značajan broj poduzeća neće imati funkcionalno implementirano upravljanje informacijskom sigurnošću, odnosno ono je utemeljeno na slučajnom upravljanju i rješavanju posljedice incidenata bez proaktivnosti.

5.3.2.2. Obrada anketnih rezultata – II. razina funkcionalnosti

36 % anketiranih poduzeća (njih 127) odgovara kako je u poduzeću imenovana (identificirana) osoba zadužena za provođenje mjera informacijske sigurnosti. 57 % ili 197 anketiranih poduzeća odgovara kako u poduzeću nije imenovana osoba zadužena za provođenje mjera informacijske sigurnosti dok 7 % anketiranih (23 poduzeća) odgovara kako takva osoba još nije imenovana, ali postoji namjera imenovati je. Na drugoj razini točno identificiranje takve osobe bio bi temeljni preduvjet potpune funkcionalnosti. Ove podatke prikazuje strukturni krug na grafikonu 10. na sljedećoj stranici.

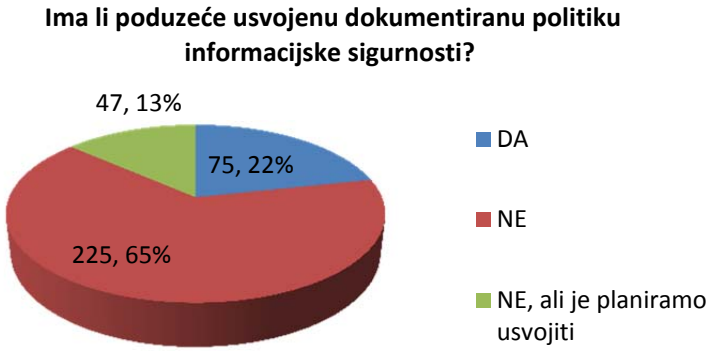
Grafikon 10: Prikaz postotnog udjela anketiranih poduzeća koja imaju imenovanu osobu poduzeća zaduženu za provođenje mjera informacijske sigurnosti (anketno pitanje br. 13)



Izvor: priredio autor

Na pitanje posjeduje li poduzeće usvojenu i dokumentiranu politiku informacijske sigurnosti kao dokument vrhovne razine koji definira upravljanje informacijskom sigurnošću i na koji se moraju oslanjati i referirati svi ostali dokumenti vezani uz to upravljanje, nešto više od petine anketiranih poduzeća (75 poduzeća ili 22 %) odgovara kako imaju takav dokument. Gotovo dvije trećine (225 anketiranih poduzeća ili 65 % u odnosu na anketirani uzorak) odgovara kako nemaju usvojen takav dokument, dok 47 anketiranih ili 13 % odgovara kako nemaju usvojen takav dokument ali ga planiraju donijeti. U svim poduzećima u kojima takav dokument nije formaliziran, ne može se smatrati kako je uspostavljen sustav upravljanja informacijskom sigurnošću koji bi bio sukladan najboljoj praksi i standardima koji danas reguliraju tu problematiku. Ovi podaci prikazani su na grafikonu 11.

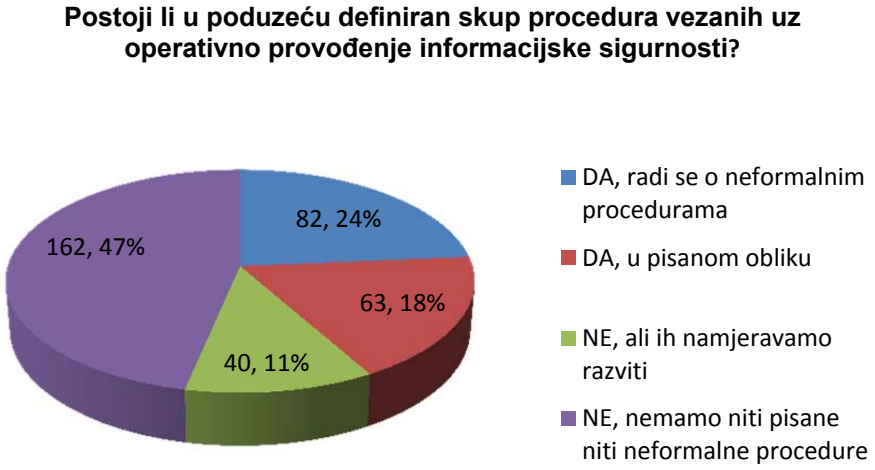
Grafikon 11: Prikaz postotnog udjela anketiranih poduzeća koja imaju usvojenu dokumentiranu politiku informacijske sigurnosti (anketno pitanje br. 19)



Izvor: priredio autor

U okviru mjernog instrumenta, anketiranim je poduzećima postavljeno pitanje kojim se pokušava izmjeriti dostignuta razina zrelosti formaliziranja postupaka i procedura vezanih uz operativno provođenje informacijske sigurnosti a koje se tipično izdaju i komuniciraju interno unutar poduzeća u obliku kriterija, standarda, procedura ili radnih uputa. Gotovo polovica anketiranih poduzeća, njih 162 ili 47 % nema niti pisane niti neformalne procedure, i ova činjenica ukazuje na to kako se na ovoj razini funkcionalnosti ne koriste sustavni i unaprijed anticipirani postupci u upravljanju informacijskom sigurnošću. 82 anketirana poduzeća ili 24 % ukupne anketne populacije koristi neformalne procedure, što znači da procedure nisu donesene i odobrene od strane rukovodstva ili vlasnika u formaliziranom, pisanom obliku, već su dogovorene usmeno ili „*uvriježene*“ unutar poslovnog procesa, 63 anketirana poduzeća ili nešto manje od jedne petine (18 %) ima takve procedure donesene u pisanom obliku. Osobito je zanimljivo kako 40 anketiranih poduzeća ili malo više od jedne desetine (11 %) nema takve procedure, ali ih namjerava razviti. Svi podaci vezani uz ovo pitanje prikazani su strukturnim krugom na grafikonu 12.

Grafikon 12: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju razvijenosti skupa procedura vezanih uz operativno provođenje informacijske sigurnosti (anketno pitanje br. 22)

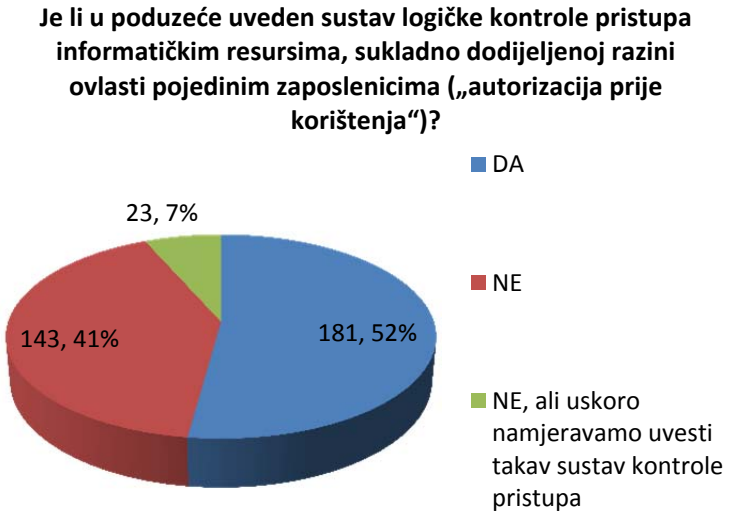


Izvor: priredio autor

Sljedeće postavljeno anketno pitanje odnosi se na kriterij uvedenosti sustava logičke kontrole pristupa informatičkim resursima sukladno dodijeljenoj razini ovlasti pojedinim zaposlenicima. Naime, temeljna je sastavnica sustava upravljanja inforopera:speeddialmacijskom sigurnošću uspostavljen sustav u kojemu više razine upravljanja odlučuju o pristupima informacijskim i podatkovnim resursima, a sukladno dodijeljenim ovlastima. Ova funkcija se operativno provodi

kroz dodjele lozinki potrebnih za pristup pojedinim dijelovima poslovnog informacijskog sustava[185]. 181 anketirano poduzeće ili 52 % odgovara kako imaju uveden sustav logičke autorizacije prije pristupa informatičkim resursima. Čak 143 poduzeća ili 41 % odgovara kako ne kontroliraju pristup informacijama i informatičkim resursima unutar poduzeća a 23 poduzeća ili 7 % nema implementiran takav sustav kontrole pristupa, ali posjeduje svijest o neispravnosti takvog pristupa, i planiraju ga uvesti. Ovi su podaci prikazani na grafikonu 13.

Grafikon 13: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju uvedenosti sustava logičke kontrole pristupa informatičkih resursa sukladno dodijeljenoj razini ovlasti pojedinim zaposlenicima (anketno pitanje br. 26)



Izvor: priredio autor

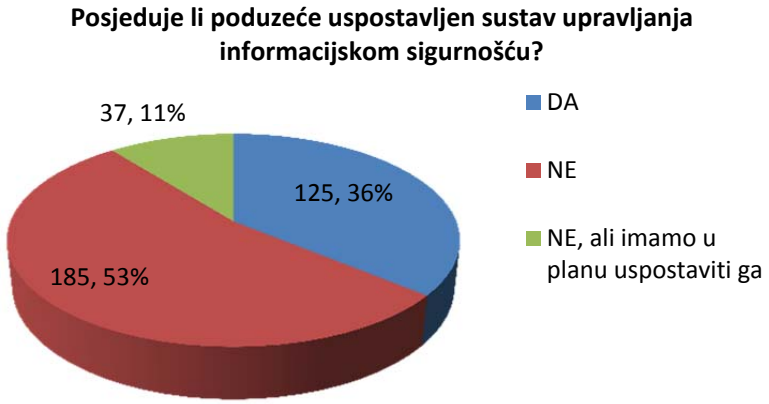
Prema iznesenome, na drugoj razini funkcionalnosti tek nešto malo više od jedne trećine anketiranih poduzeća ima osobu imenovanu za upravljanje informacijskom sigurnošću u poduzećima, gotovo četiri petine nema usvojenu politiku informacijske sigurnosti kao vršni dokument provođenja te poslovne funkcije, manje od jedne petine poduzeća ima pisane procedure vezane uz informacijsku sigurnost, uz napomenu kako 42 % poduzeća ima pisane ili neformalne procedure, a ostala poduzeća ih uopće ne posjeduju, dok gotovo polovica anketiranih poduzeća na ovoj razini funkcionalnosti ne koristi autorizaciju korisnika prije korištenja kao sredstvo logičke kontrole pristupa. Već iz ovih pokazatelja jasno je kako velik broj poduzeća ne zadovoljava uvjete druge razine funkcionalnosti upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj.

[185] Pritom se misli na ERP, CRM, PIS, IBIS, b2b, b2c, b2g, e-mail i slične sustave.

5.3.2.3. Obrada anketnih rezultata – III. razina funkcionalnosti

Na trećoj razini funkcionalnosti prvo pitanje mjernog instrumenta povezano je uz uspostavljenost sustava upravljanja informacijskom sigurnošću. Naime, preko polovice (185 anketiranih poduzeća ili 53 % od ukupnog broja) odgovara kako ne posjeduju uspostavljen sustav upravljanja informacijskom sigurnošću. Nešto više od trećine (125 anketiranih poduzeća ili 36 %) odgovara kako posjeduju takav sustav, dok 37 anketiranih poduzeća ili 11 % odgovara kako ne posjeduje takav sustav ali ga namjerava uspostaviti. Ovo je anketno pitanje s namjerom postavljeno s nešto širim obuhvatom, na način da se ne definira, a samim time ne favorizira neki od formalnih sustava najbolje prakse. Ovi rezultati su prikazani na grafikonu 14.

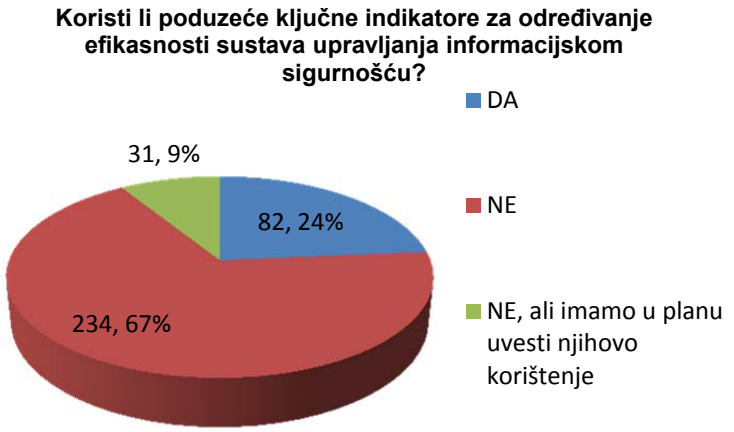
Grafikon 14: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju uspostavljenosti sustava upravljanja informacijskom sigurnošću (anketno pitanje br. 9)



Izvor: priredio autor

Drugo anketno pitanje na trećoj razini funkcionalnosti odnosi se na korištenje ključnih indikatora za određivanje efikasnosti sustava upravljanja informacijskom sigurnošću. Ukoliko poduzeće ne mjeri, odnosno ne postavlja, ne mjeri i ne uspoređuje ključne pokazatelje u odnosu prema postavljenim ciljevima, ne može se smatrati kako sustavno upravlja poslovnom funkcijom informacijske sigurnosti. Grafikon 15. na sljedećoj stranici prikazuje analizu dostavljenih odgovora na ovo pitanje. 234 anketirana poduzeća ili 67 % odgovara kako ne koriste ključne indikatore za određivanje efikasnosti sustava upravljanja informacijskom sigurnošću, 82 anketirana poduzeća ili 24 % odgovara kako ih koriste dok 31 anketirano poduzeće ili 9 % još ne koristi ključne pokazatelje, ali ima u planu uvesti njihovo korištenje.

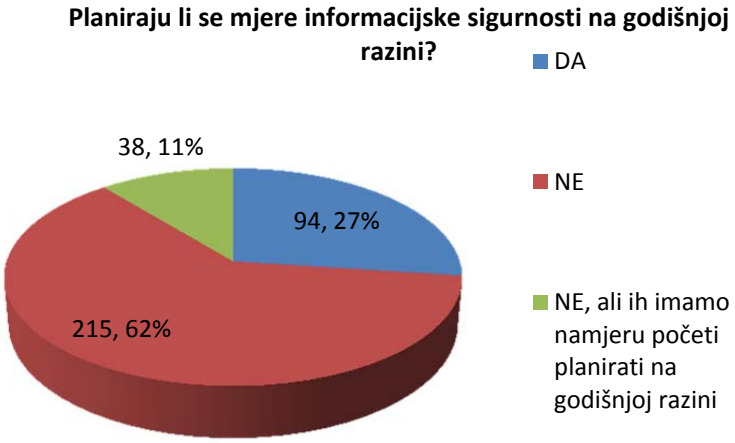
Grafikon 15: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju korištenja ključnih indikatora za određivanje efikasnosti sustava upravljanja informacijskom sigurnošću (anketno pitanje br. 10)



Izvor: priredio autor

Malo više od jedne četvrtine anketiranih poduzeća (94 poduzeća ili 27 % ukupno anketiranih) odgovara kako planiraju mjere informacijske sigurnosti na godišnjoj razini. 38 poduzeća koja čine 11 % ukupno anketiranih poduzeća ne planiraju takve mjere na godišnjoj razini ali ih imaju namjeru početi planirati. Naposljetku, nešto manje od dvije trećine (215 anketiranih poduzeća ili 62 %) ne planira mjere informacijske sigurnosti na godišnjoj razini. Ovi su podaci prikazani strukturnim krugom na grafikonu 16 na sljedećoj stranici . Naime, planiranje informacijske sigurnosti na godišnjoj razini predstavlja temeljni postupak u upravljanju informacijskom sigurnošću na održiv način, jer se anticipirane potrebne mjere informacijske sigurnosti pretvaraju u plan investicijskih i operativnih troškova, temeljem kojih ekonomsko rukovodstvo poduzeća može upravljati troškovima sustava upravljanja informacijskom sigurnošću u odnosu na rizike i raspoloživu tehnologiju.

Grafikon 16: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju planiranja mjera informacijske sigurnosti na godišnjoj razini (anketno pitanje br. 18)

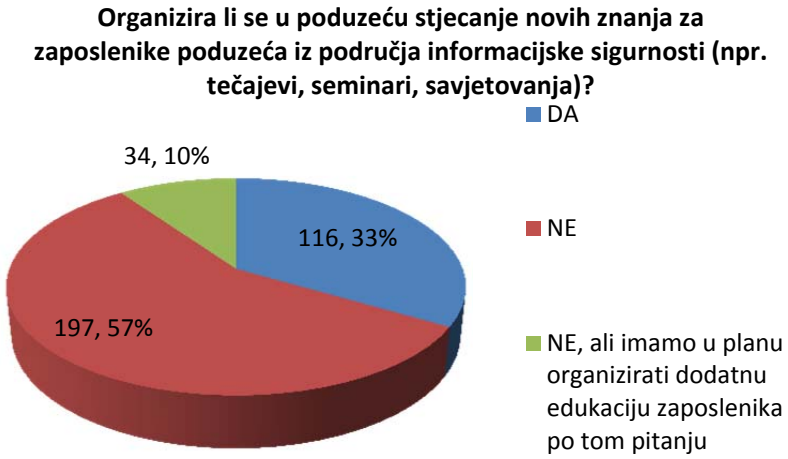


Izvor: priredio autor

Sljedeće anketno pitanje razlaže problematiku ulaganja u ljudski kapital, odnosno u kompetencije vezane uz područje informatičke sigurnosti[186]. Proces konstantnog učenja i usavršavanja je jedna od temeljnih postavki funkcionalnosti sustava upravljanja informacijskom sigurnošću na trećoj razini. Rezultati obrade ovog anketnog pitanja prikazani su na grafikonu 17. na sljedećoj stranici. Točno jedna trećina anketiranih poduzeća ili njih 116 odgovara kako ulažu u postizanje viših razina znanja iz područja informacijske sigurnosti. 197 anketiranih poduzeća ili 57 % odgovara kako ne organiziraju u poduzeću stjecanje novih znanja za zaposlenike iz područja informacijske sigurnosti. 34 anketirana poduzeća ili njih 10 % odgovaraju kako trenutačno to ne čine, ali imaju namjeru organizirati dodatnu edukaciju.

[186] npr. tečajevi, seminari, savjetovanja i sl.)

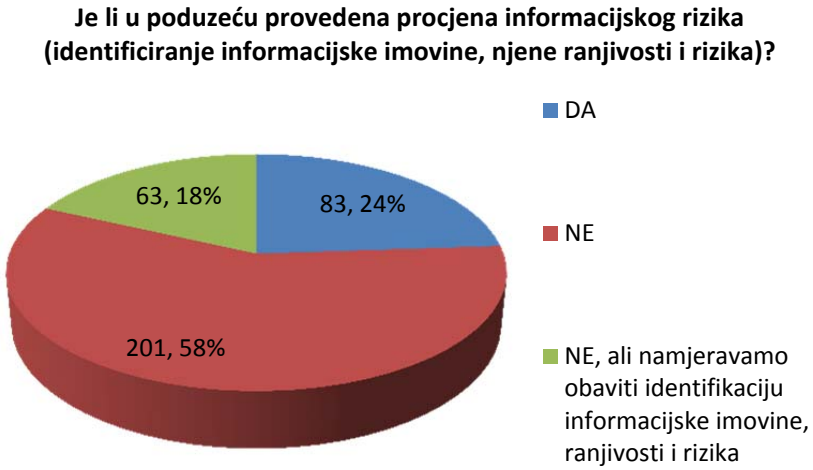
Grafikon 17: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju organizacije stjecanja novih znanja za zaposlenike poduzeća iz područja informacijske sigurnosti (tečajevi, seminari, savjetovanja – anketno pitanje br. 12)



Izvor: priredio autor

Točno identificiranje informacijske imovine, njenih inherentnih svojstava koje su opisane ranjivostima koje mogu iskoristiti određene ugroze i zatim rezultirati nastupom sigurnosnih incidenata predstavlja *de facto* standardni postupak u upravljanju informacijskom sigurnošću, kako u korporativnim okruženjima, tako i u ostalim kompleksnim organizacijama. Bez procjene informacijskog rizika nije moguće govoriti o sustavnom upravljanju informacijskom sigurnošću. Rezultati ispitivanja po ovoj činjenici grafički su prikazani grafikonom 18 na sljedećoj stranici na kojemu je vidljivo kako oko jedne četvrtine ispitanih poduzeća (83 poduzeća ili 24 %) obavlja procjenu informacijskog rizika, 201 poduzeće ili 58 % nije provelo procjenu informacijskog rizika, dok 63 poduzeća ili njih 18 % nije obavilo tu identifikaciju ali je namjeravaju obaviti.

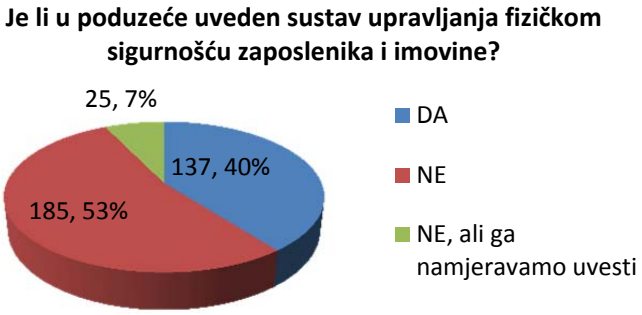
Grafikon 18: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju provedenosti procjene informacijskog rizika (identificiranje informacijske imovine, njene ranjivosti i rizika – anketno pitanje br. 23)



Izvor: priredio autor

Rezultati odgovora na sljedeće pitanje koje je vezano uz posjedovanje sustava upravljanja fizičkom sigurnošću zaposlenika i imovine prikazani su na grafikonu 19 na sljedećoj stranici. Općenito govoreći, sustav upravljanja fizičkom sigurnošću odvaja imovinu i zaposlenike poduzeća od okoline i onemogućuje otuđivanje ili neautoriziran pristup, a samim time ima i direktan utjecaj na sigurnost informacija sadržanim u informacijskim sustavima poduzeća budući da je pristup njima najčešće povezan uz korištenje fizičke informacijske imovine poduzeća. Iznenađujuće je da na ovoj razini dostignute funkcionalnosti samo 40 % anketiranih poduzeća ili njih 137 posjeduje takav sustav. 53 % anketiranih poduzeća (njih 185) ne posjeduje takav sustav, dok samo 7 % poduzeća ili njih 25 posjeduje svijest o potrebi organiziranja takvog sustava, te ga trenutačno ne posjeduju ali ga namjeravaju uvesti.

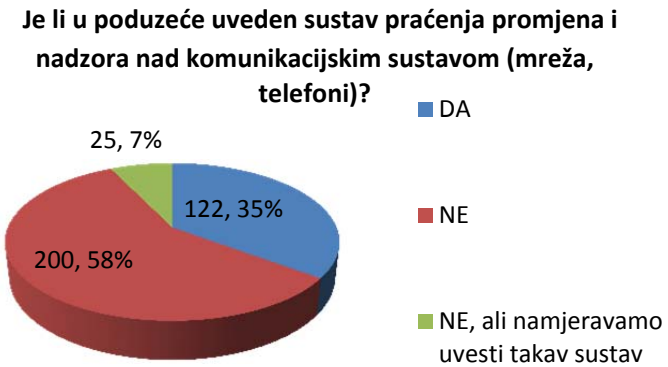
Grafikon 19: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju uvedenosti sustava upravljanja fizičkom sigurnošću zaposlenika i imovine – anketno pitanje br. 24



Izvor: priredio autor

Logičko praćenje promjena i nadzor nad komunikacijskim sustavom temeljna je mjera kojom se osiguravaju povjerljivost, integritet i raspoloživost informacija sadržanih u poslovnim informacijskim sustavima poduzeća. Odgovori na ovo pitanje vrlo su slični kao i na prethodno pitanje, povezano uz kontrolu upravljanja fizičkom sigurnošću zaposlenika i imovine. Nešto manje anketiranih poduzeća, njih 122 ili 35 % nadzire i prati promjene nad komunikacijskim sustavom. Nešto više njih, 200 poduzeća ili 58 % ne obavlja tu vrstu nadzora dok isti broj poduzeća, njih 25 ili 7 % ne koristi takav sustav nadzora ali ga namjerava uvesti. Ovi su podaci prikazani na grafikonu 20 u nastavku.

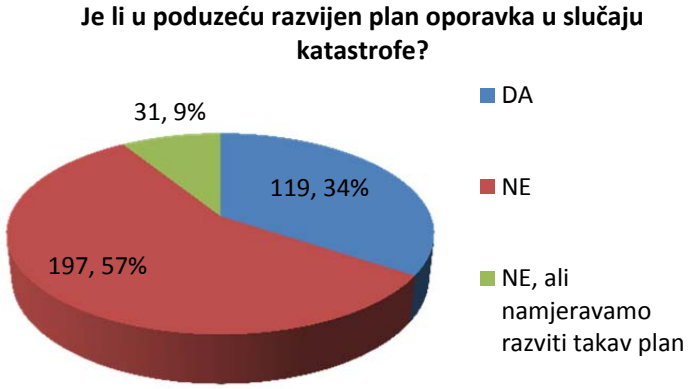
Grafikon 20: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju uvedenosti sustava praćenja promjena i nadzora nad komunikacijskim sustavom mreža, telefoni - anketno pitanje br. 25)



Izvor: priredio autor

Stav poduzeća prema kriteriju razvedenosti plana oporavka u slučaju nastupa katastrofe prikazuje strukturni krug na grafikonu br. 21. Jedna trećina anketiranih poduzeća ima razvijen plan oporavka u slučaju katastrofe, a radi se o 119 anketiranih poduzeća. 197 anketiranih poduzeća koja čine 57 % ukupnog broja anketiranih poduzeća nemaju takav plan dok 31 anketirano poduzeće ili njih 9 % nema takav plan ali ima svijest o potrebi njegovog razvoja. Planiranje oporavka u slučaju katastrofe[187] je značajna poslovna funkcija čija ispravna implementacija omogućuje veću vjerojatnost nastavka poslovanja u slučaju nastupa katastrofalnog neželjenog događaja. Za mala i srednja poduzeća ovakvo planiranje osobito je važno budući da već nastanak jednog incidenta ove vrste može značiti kraj poslovanja poduzeća na tržištu odnosno prestanak poslovne aktivnosti.

Grafikon 21: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju razvijenosti plana oporavka u slučaju nastupa katastrofe (anketno pitanje br. 30)

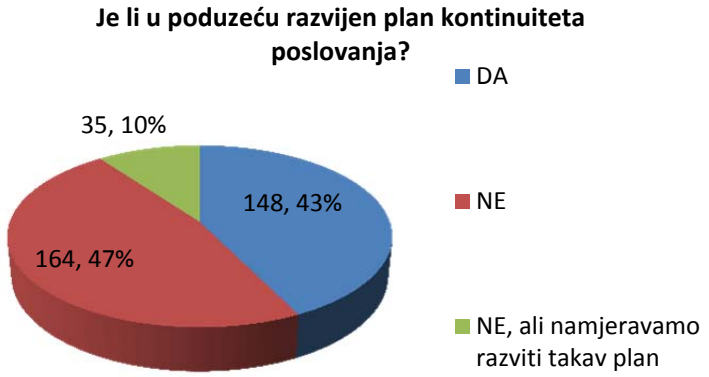


Izvor: priredio autor

Vezano uz prethodno pitanje, anketiranim poduzećima postavljeno je i sljedeće pitanje povezano uz aktivnost oporavka od katastrofe, a ono se tiče razvijenosti plana kontinuiteta poslovanja. Planiranje kontinuiteta poslovanja[188] je aktivnost koja je više hijerarhijske razine od plana oporavka od katastrofe. 43 % poduzeća ili njih 148 odgovara kako je u poduzeću razvijen plan kontinuiteta poslovanja, 47 % poduzeća ili njih 164 odgovara kako takav plan ne postoji dok točno jedna desetina poduzeća – 35 poduzeća nema razvijen takav plan ali ga namjerava razviti. Odgovori ove vrste su očekivani budući da svako poduzeće koje ima razvijen plan kontinuiteta poslovanja kao sastavni dio mora nužno imati i razvijen plan oporavka od katastrofe, dok obrat te teze ne vrijedi nužno. Opisani su podaci prikazani na grafikonu 22. na sljedećoj stranici.

[187] Prijevod od eng. „*Disaster Recovery Planning*“, kratica „*DRP*“.
[188] Prijevod od *eng. „Business ContinuityPplanning“* ,kratica *„BCP“*.

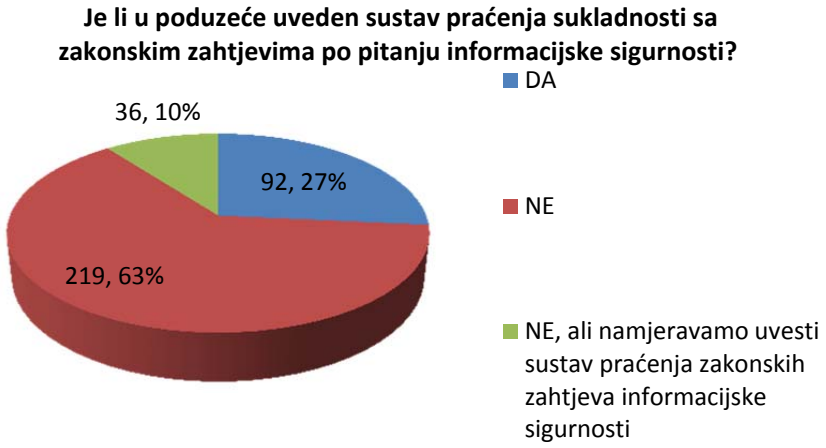
Grafikon 22: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju razvijenosti plana kontinuiteta poslovanja (anketno pitanje br. 31)



Izvor: priredio autor

Na ovoj razini funkcionalnosti izrazito je bitno i da poduzeća imaju razvijen sustav praćenja sukladnosti sa zakonskim zahtjevima po pitanju informacijske sigurnosti. Naime, usklađenost poduzeća sa zakonskim zahtjevima ne bi nikako trebala biti voluntaristička kategorija, već obaveza. Samo 92 poduzeća ili njih 27 % na ovo anketno pitanje odgovara kako prate zakonske zahtjeve po pitanju informacijske sigurnosti, što znači da ne zadovoljavaju niti temeljne zahtjeve postavljene po pitanju informacijske sigurnosti – zakonske zahtjeve. Iako je zakonska regulativa po pitanju malih i srednjih poduzeća vrlo nezahtjevna, mala i srednja poduzeća u Republici Hrvatskoj ne uspijevaju osigurati niti tu elementarnu sukladnost. 219 poduzeća ili njih 63 % izjavljuje kako ne prate zakonske zahtjeve po pitanju informacijske sigurnosti dok jedna desetina anketiranih ili 36 poduzeća nema takav sustav ali ga namjeravaju uvesti. Navedeni podaci prikazani su na grafikonu 23. na sljedećoj stranici.

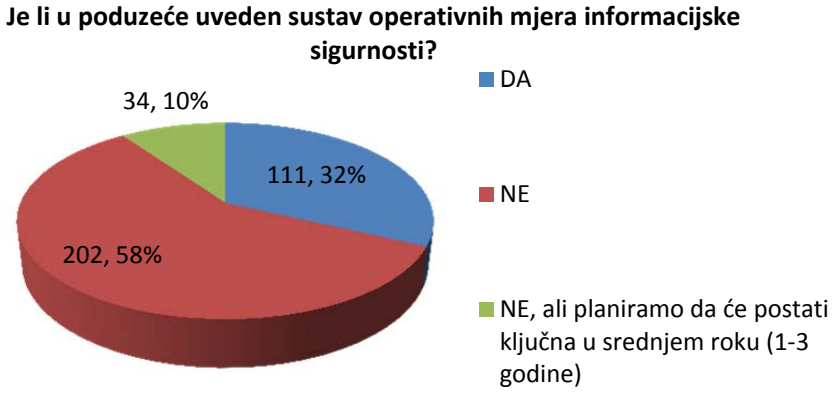
Grafikon 23: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju uvedenosti sustava praćenja sukladnosti sa zakonskim zahtjevima po pitanju informacijske sigurnosti (anketno pitanje br. 32)



Izvor: priredio autor

Sljedeće pitanje grafički je obrađeno i prikazano na grafikonu 24. 111 anketiranih poduzeća ili 32 % od ukupnog broja ima uveden sustav operativnih mjera informacijske sigurnosti. 202 poduzeća ili 58 % ne posjeduje uveden sustav operativnih mjera informacijske sigurnosti dok 10 % ili 34 poduzeća takav sustav ne posjeduje, ali planira kako će takav sustav postati ključan u srednjem roku od 1-3 godine. Sustav operativnih mjera predstavlja temeljne instrumente kojima na operativnoj razini poduzeće dnevno upravlja informacijskom sigurnošću.

Grafikon 24: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju uvedenosti sustava operativnih mjera informacijske sigurnosti (anketno pitanje br. 34)

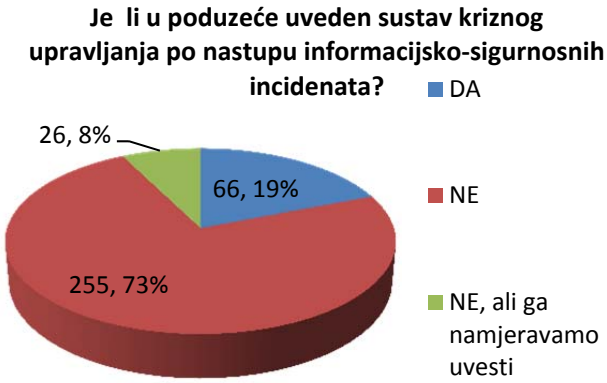


Izvor: priredio autor

Posljednje pitanje koje je vezano uz treću razinu funkcionalnosti tiče se kriterija uvedenosti sustava kriznog upravljanja po nastupu informacijsko-sigurnosnih incidenata. Krizno

upravljanje nužno uključuje rukovodstvo poduzeća i povećava šanse za potpuni oporavak poslovne aktivnosti poduzeća uz najmanje moguće kvantificirane posljedica. Rezultati obrade rezultate odgovora na ovo pitanje prikazani su na grafikonu 25. 73 % poduzeća ili 255 anketiranih ne posjeduje sustav kriznog upravljanja u slučaju nastupa informacijsko-sigurnosnog incidenta. Samo 19 % poduzeća ili njih 66 posjeduje takav sustav dok 8 % ili njih 26 nema takav sustav ali ga namjeravaju uvesti.

Grafikon 25: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju uvedenosti sustava kriznog upravljanja po nastupu informacijsko-sigurnosnih incidenata (anketno pitanje br. 29)



Izvor: priredio autor

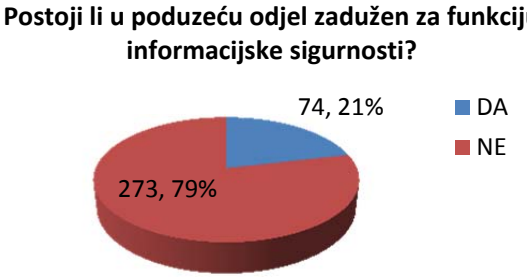
Promatrajući sumarno rezultate dobivene mjerenjem dostignute razine funkcionalnosti sustava upravljanja informacijskom sigurnošću na trećoj razini funkcionalnosti sustava može se zaključiti kako 36 % poduzeća ima uspostavljen sustav upravljanja informacijskom sigurnošću, 24 % poduzeća koristi ključne indikatore za određivanje efikasnosti sustava upravljanja informacijskom sigurnošću, 27 % poduzeća planira mjere informacijske sigurnosti na godišnjoj razini, dok samo 33 % poduzeća organizira edukaciju iz područja informacijske sigurnosti za zaposlenike. Samo u četvrtini anketiranih poduzeća provedena je procjena informacijskog rizika u obliku identificiranja informacijske imovine, njene ranjivosti i rizika koji joj prijete, 40 % poduzeća posjeduje uveden sustav upravljanja fizičkom sigurnošću zaposlenika i imovine, 35 % anketiranih poduzeća prati promjene i nadzire komunikacijski sustav. Područje oporavka od katastrofe i kontinuiteta poslovanja je regulirano na način da 34 % poduzeća ima razvijen plan oporavka a 43 % poduzeća ima razvijen plan kontinuiteta poslovanja. Naposljetku, samo 27 % anketiranih poduzeća prati zakonske zahtjeve po pitanju informacijske sigurnosti, 32 % ima uveden sustav operativnih mjera informacijske sigurnosti dok 19 % poduzeća ima uveden sustav kriznog upravljanja po nastupu informacijsko-sigurnosnih incidenata. Ovi rezultati pokazuju kako je model neadekvatno funkcionalan na trećoj razini funkcionalnosti.

5.3.2.4. Obrada anketnih rezultata – IV. razina funkcionalnosti

Za poduzeća, a osobito ona koja posjeduju dovoljnu financijsku snagu, organizaciju te znanje vezano uz upravljanje informacijskom sigurnošću, ključno je koncentriranje svih napora vezanih uz to upravljanje u jednoj točki, a to je odjel zadužen za funkciju informacijske sigurnosti. Organiziranje takvog odjela predstavlja jedan od čimbenika na četvrtoj razini funkcionalnosti modela upravljanja informacijskom sigurnošću. Od anketiranih poduzeća, 74 ili 21 % odgovara kako postoji odjel zadužen za funkciju informacijske sigurnosti dok 273 ili 79 % odgovara kako takav odjel ne postoji.

Navedene podatke prikazuje grafikon 26. Pritom treba napomenuti kako ovo pitanje nije orijentirano ka tome da se pokuša ustanoviti je li organiziran posebni odjel koji se bavi samo i isključivo informacijskom sigurnošću, već postoji li jedan zaseban odjel od postojećih koji bi bio zadužen za tu poslovnu funkciju. Naime, veličina malih i srednjih poduzeća te broj zaposlenih impliciraju malu vjerojatnost da će u njima biti organiziran zaseban odjel koji bi se bavio samo tom poslovnom djelatnošću, osim u slučajevima uslužnih poduzeća koja se bave visokom tehnologijom.

Grafikon 26: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju organiziranosti odjela zaduženog za upravljanje informacijskom sigurnošću (anketno pitanje br. 15)



Izvor: priredio autor

Drugo postavljeno mjerno pitanje na četvrtoj razini funkcionalnosti modela odnosi se na provođenje mjera informacijske sigurnosti isključivo od jedne osobe, imenovane za njihovo provođenje, ili i ostalih zaposlenika, odnosno čitavog poduzeća. Metodološki je značajno da su u provođenje mjera informacijske sigurnosti uključeni svi djelatnici poduzeća jer se samo na taj način mogu postići postavljeni ciljevi informacijske sigurnosti. Od anketiranih poduzeća 74 ili 58 % odgovara kako mjere informacijske sigurnosti provodi isključivo osoba imenovana za njihovo provođenje dok 53 ili 42 % odgovara kako te mjere ne provodi isključivo ta osoba. Na ovo pitanje odgovaraju samo one osobe koje su odgovorile potvrdno na anketno pitanje br.

13.[189], odnosno ono je primjenjivo na poduzeća koja su imenovala osobu zaduženu za provođenje mjera informacijske sigurnosti. Grafički prikaz obrađenih rezultata izrađen je na grafikonu 27.

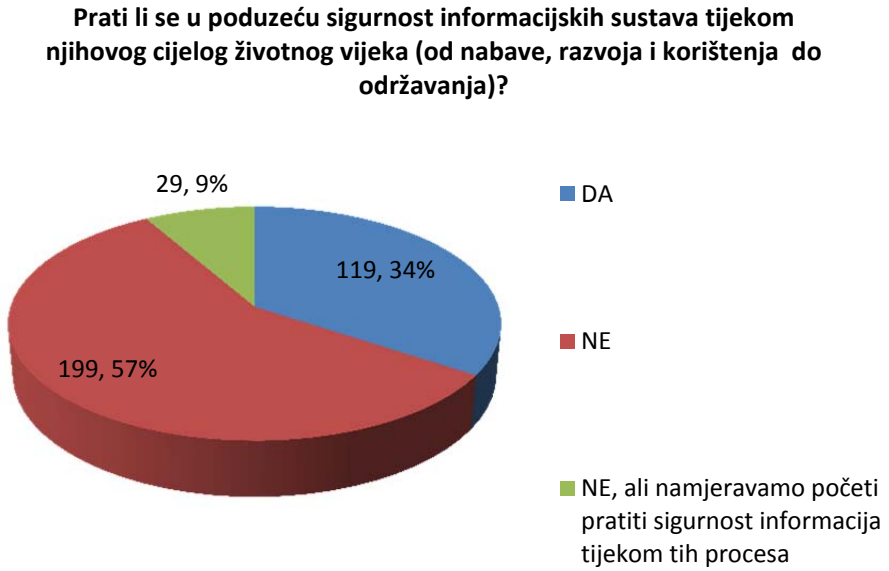
Grafikon 27: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju provođenja mjera informacijske sigurnosti isključivo od strane osobe imenovane za njihovo provođenje (anketno pitanje br. 14)

Izvor: priredio autor

Sljedeće se pitanje odnosi na praćenje sigurnosti informacijskog sustava tijekom njegovog cijelog životnog vijeka, od nabave, razvoja i korištenja do održavanja. Obrađene rezultate odgovora na ovo pitanje prikazuje grafikon 28 na sljedećoj stranici. 119 anketiranih poduzeća (34 %) prati informacijske sustave tijekom cijelog njihovog životnog vijeka. 199 anketiranih poduzeća (57 %) ne prati sigurnost informacijskih poduzeća tijekom cijelog životnog vijeka dok 29 (9%) shvaća važnost tog procesa i namjerava početi s takvim praćenjem.

[189] Anketno pitanje br. 13. odnosi se na drugu razinu funkcionalnosti modela upravljanja informacijskom sigurnošću.

Grafikon 28: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju praćenja sigurnosti informacijskog sustava tijekom cijelog životnog vijeka informacijskog sustava, od nabave, razvoja i korištenja do održavanja (anketno pitanje br. 27)



Izvor: priredio autor

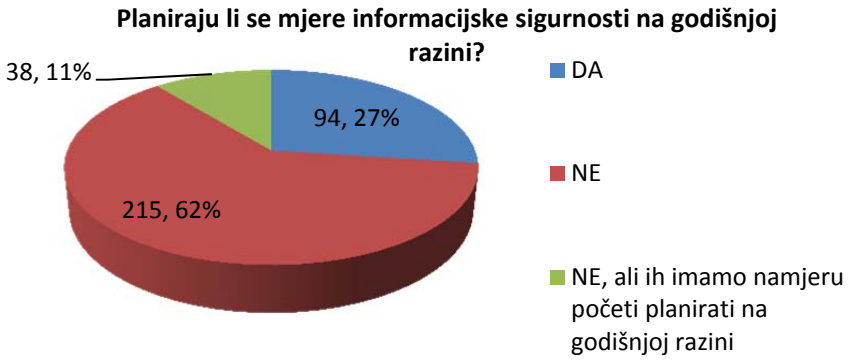
Sljedeći grafikon, grafikon 29, prikazuje aktivnosti anketiranih poduzeća s obzirom na kriterij planiranja investicija u sustav upravljanja informacijskom sigurnošću i trošak upravljanja takvim sustavom na godišnjoj razini. Uvrštenjem ovog pitanja u anketu pokušava se steći slika o tome koliko sustavno i planski mala i srednja poduzeća u Republici Hrvatskoj planiraju svoje investicije i troškove održavanja sustava upravljanja informacijskom sigurnošću. Analiza odgovora na ovo pitanje pokazuje kako manje od jedne četvrtine anketiranih, odnosno 79 poduzeća ili 23 % ima evidenciju o investicijama i trošku sustava upravljanja informacijskom sigurnošću na godišnjoj razini. 229 poduzeća ili točno dvije trećine anketiranih uopće ne planira godišnje investicije i ne poznaje iznos ukupnog troška sustava upravljanja informacijskom sigurnošću na godišnjoj razini. 39 poduzeća ili 11 % od anketiranih poduzeća shvaća važnost takve vrste financijskog planiranja te iskazuju da usprkos tome što trenutačno ne vode tu vrstu evidencije, namjeravaju uskoro s njom započeti.

Grafikon 29: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju planiranja investicija i troška sustava upravljanja informacijskom sigurnošću na godišnjoj razini (anketno pitanje br. 20)

Izvor: priredio autor

Planiranje investicijskih troškova i troška održavanje pojedinih elemenata sustava upravljanja informacijskom sigurnošću je usko vezano uz planiranje mjera informacijske sigurnosti na godišnjoj razini. Naime, samo detaljno i sustavno planiranje mjera informacijske sigurnosti može biti pretočeno u konkretna potrebna rješenja, a zatim i u financijska sredstva potrebna za njihovo provođenje. Rezultate ovog dijela istraživanja prikazuje grafikon 30. 27 % anketiranih poduzeća ili njih 94 iskazuje kako mjere informacijske sigurnosti planiraju na godišnjoj razini. 62 % anketiranih poduzeća ili njih 215 iskazuje kako mjere informacijske sigurnosti ne planiraju na godišnjoj razini. 11 % anketiranih poduzeća ili njih 38 iskazuje kako ne planiraju mjere informacijske sigurnosti na godišnjoj razini, ali to planiraju početi činiti.

Grafikon 30: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju planiranja mjera informacijske sigurnosti na godišnjoj razini (anketno pitanje br. 18)

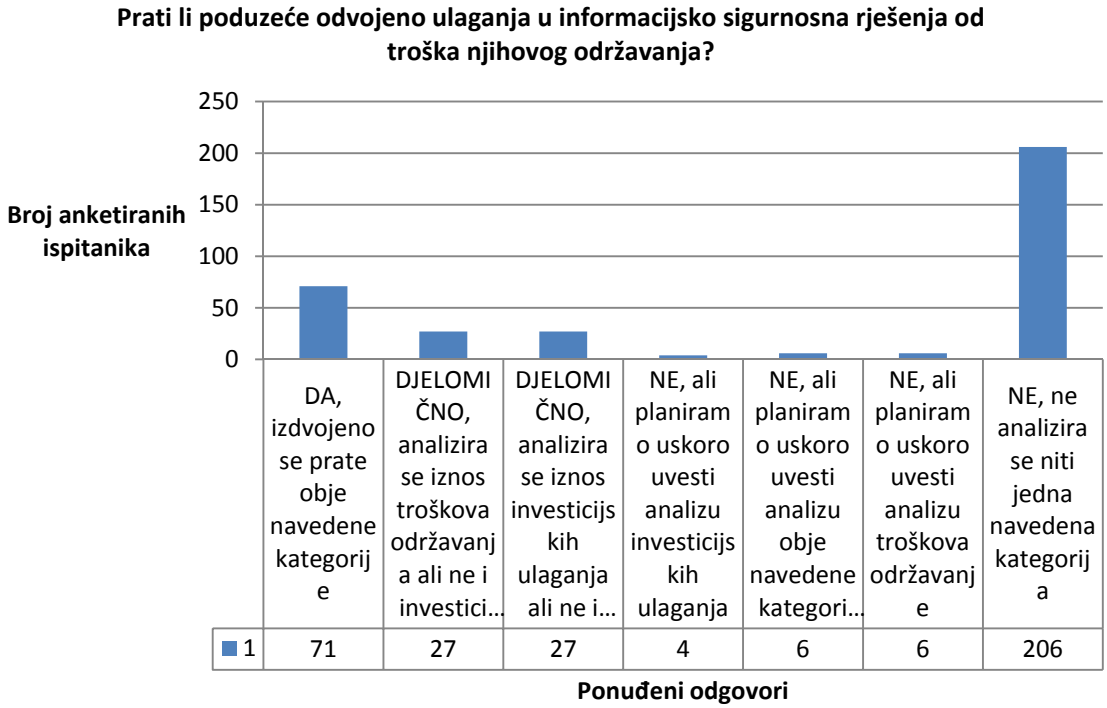


Izvor: priredio autor

Osim planiranja ukupnog utroška za poslovnu funkciju upravljanja informacijskom sigurnošću, izrazito je važno da poduzeća odvojeno prate ulaganja u informacijsko sigurnosna rješenja od troška njihovog održavanja. Naime, poduzeće može upravljati svojom investicijskom

aktivnošću ovisno o fazi rasta i razvoja u kojoj se nalazi, te raspoloživim sredstvima, odnosno investirajući u potpunosti u novu investiciju vlastitim sredstvima, korištenjem kredita u jednom dijelu investicije ili u potpunosti, odnosno najmom ili *leasingom* nekog rješenja informacijske sigurnosti. Na grafikonu 31. prikazani su rezultati odgovora na pitanje analiziraju li poduzeća investicije u informacijsko sigurnosna rješenja odvojeno u odnosu na trošak njihovog održavanja te na koji način.

Grafikon 31: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju odvojenog praćenja ulaganja u informacijsko sigurnosna rješenja od troška njihovog održavanja (anketno pitanje br. 46)



Izvor: priredio autor

Ponuđeno je više različitih odgovora, odnosno kombinacija odgovora. 206 od 347 anketiranih poduzeća odgovara kako ne analiziraju niti jednu od navedenih kategorija, dok dodatnih 16 poduzeća planira uskoro uvesti analizu investicija, troška ili obje kategorije. 54 poduzeća djelomično analiziraju iznos investicijskih ulaganja ali ne i troškova održavanja rješenja i obrnuto, i to s jednakom raspodjelom između te dvije navedene kategorije[190]. Naposljetku, 71 od 347 anketiranih poduzeća izdvojeno prati obje kategorije. Na grafikonu 31 na *Y* osi stupcima

[190] U jednakom omjeru, po 27 poduzeća nalazi se u svakoj od navedene dvije kategorije.

je prikazana pojavnost[191] pojedinog obilježja, dok su obilježja prikazana na osi *X*. Ispod pojedinih obilježja dodatno je označen broj poduzeća u svakoj od navedenih kategorija.

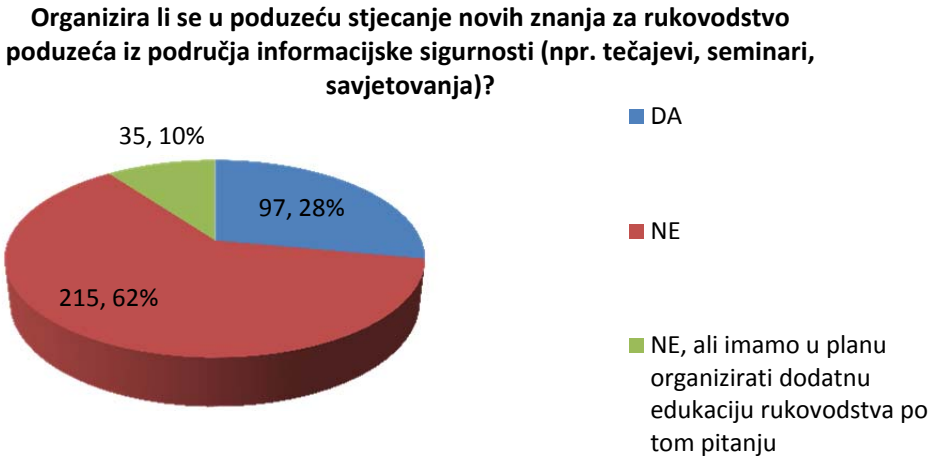
Promatrajući rezultate dobivene primjenom mjernog instrumenta na pitanja usmjerena ka izmjeri dostignute razine funkcionalnosti upravljanja informacijskom sigurnošću na četvrtoj razini funkcionalnosti,može se uočiti kako u 79 % anketiranih poduzeća nije organiziran odjel zadužen za funkciju informacijske sigurnosti, u 58 % poduzeća mjere informacijske sigurnosti provodi isključivo osoba koja je imenovana za njihovo provođenje i one se ne dijele kroz čitavu organizaciju, samo 34 % poduzeća prati sigurnost informacijskih sustava tijekom njihovog cijelog životnog vijeka, od nabave, razvoja i korištenja do održavanja. U trenutku anketiranja 77 % poduzeća nije planiralo investicije i trošak sustava upravljanja informacijskom sigurnošću na godišnjoj razini, 63 % poduzeća ne planira mjere informacijske sigurnosti na godišnjoj razini kao podlogu za procjenu investicijskog i tekućeg troška održavanja informacijsko-sigurnosnih rješenja. Na kraju analize funkcionalnosti na ovoj razini, čimbenik odvojenog praćenja investicijskog ulaganja od troška održavanja informacijsko sigurnosnih rješenja zadovoljava u potpunosti 71 od 347 anketiranih poduzeća a djelomično njih 54, dok svi ostali trenutačno ne analiziraju jednu, drugu ili obje navedene kategorije.

5.3.2.5. Obrada anketnih rezultata – V. razina funkcionalnosti

Na petoj, najvišoj razini funkcionalnosti ispitan je čimbenik edukacije rukovodstva poduzeća iz područja informacijske sigurnosti. Radi se o tečajevima, seminarima i savjetovanjima za rukovodstvo, u okviru procesa konstantnog stjecanja obrazovanja iz područja informacijske sigurnosti za koje nije nužno da ih rukovodstvo inicijalno posjeduje, štoviše, s obzirom na činjenicu da se radi o razmjerno novoj poslovnoj funkciji visoke kompleksnosti, izvjesno je kako rukovoditelji neće imati potrebna znanja i kompetencije. Samo 97 anketiranih poduzeća ili 28 % odgovara kako se u poduzeću organizira stjecanje novih znanja za rukovoditelje poduzeća iz područja informacijske sigurnosti. 215 anketiranih poduzeća ili 62 % odgovara kako se takvo stjecanje novog znanja ne provodi dok 35 anketiranih poduzeća ili 10 % odgovara kako se ono trenutačno ne provodi ali postoji plan organiziranja dodatne edukacije. Ovi su pokazatelji prikazani strukturnim krugom na grafikonu 32. na sljedećoj stranici.

[191] Pojavnost je predstavljena frekvencijom obilježja.

Grafikon 32: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju organizacije stjecanja novih znanja za rukovodstvo poduzeća iz područja informacijske sigurnosti (tečajevi, seminari, savjetovanja – anketno pitanje br. 11)

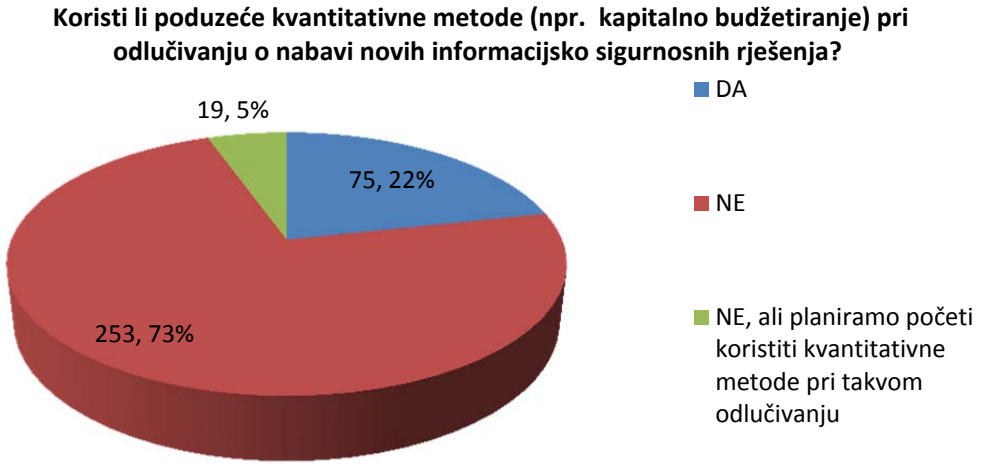


Izvor: priredio autor

Drugi čimbenik pete razine funkcionalnosti modela je kriterij korištenja kvantitativnih metoda pri odlučivanju o nabavi novih informacijsko sigurnosnih rješenja. Na postavljeno pitanje u tom smislu samo 22 % poduzeća odgovara potvrdno, odnosno da koriste kvantitativne metode[192] pri odlučivanju o nabavi novih informacijsko sigurnosnih rješenja, a radi se o 75 anketiranih poduzeća. Od preostalih poduzeća, 73 % ili 253 poduzeća ne koriste takve metode kao osnovu pri odlučivanju o investiranju u pojedine mjere ili rješenja informacijske sigurnosti dok 5 % ili 19 anketiranih poduzeća u činjenici da ne koriste kvantitativne metode vide problem ili prepreku osiguranju viših razina funkcionalnosti modela i planiraju započeti s korištenjem kvantitativnih metoda u tu svrhu. Rezultate ispitivanja ovog čimbenika prikazuje grafikon 33. na sljedećoj stranici.

[192] Primjerice, kapitalno budžetiranje, metoda neto sadašnje vrijednosti, interne stope povrata ili diskontiranih novčanih tijekova.

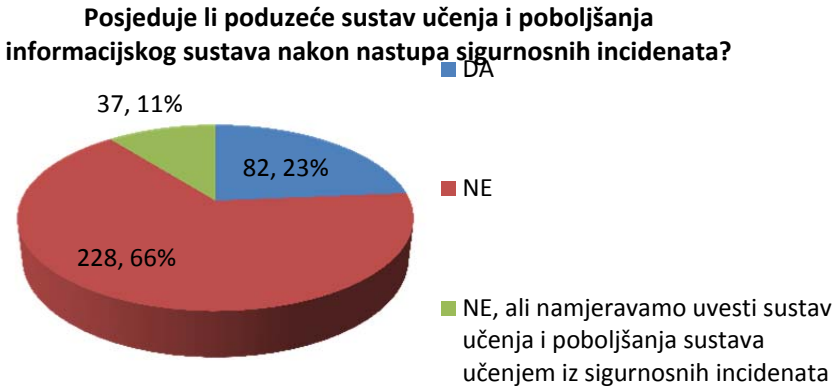
Grafikon 33: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju korištenja kvantitativnih metoda pri odlučivanju o nabavi novih informacijsko-sigurnosnih rješenja (anketno pitanje br. 21)



Izvor: priredio autor

Na grafikonu 34 na sljedećoj stranici prikazan je čimbenik posjedovanja sustava učenja i poboljšanja informacijskog sustava po nastupu sigurnosnih incidenata. Prema sustavu upravljanja kvalitetom informacijske sigurnosti koji ISO 27001:2005 koji definira temeljne značajke sustava upravljanja informacijskom sigurnošću, učenje iz nastupa sigurnosnih incidenata je jedna od značajnih kontrola koja omogućuje organizaciji proaktivnu orijentaciju utemeljenu na prošlim iskustvima relevantnim za poduzeće. 82 anketirana poduzeća odgovaraju potvrdno na pitanje posjeduju li uspostavljen sustav učenja i poboljšanja informacijskog sustava po nastupu sigurnosnog incidenta, a pritom se radi se o samo 23 % ukupno anketiranih poduzeća. Čak 228 anketiranih poduzeća, ili točno dvije trećine od ukupnog broja, odgovara kako ne posjeduju sustav učenja i poboljšanja po nastupu sigurnosnih incidenata. Daljih 37 anketiranih poduzeća ili 11 % također ne posjeduju takav sustav ali smatraju kako ga je potrebno uvesti i to namjeravaju učiniti.

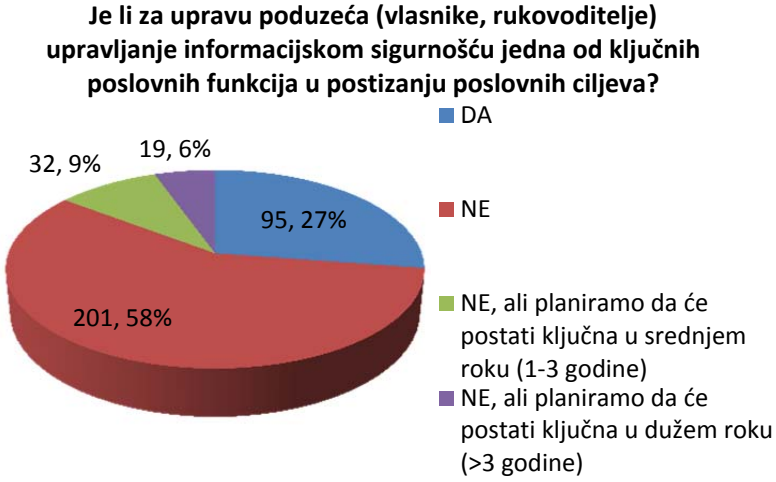
Grafikon 34: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju posjedovanja sustava učenja i poboljšanja informacijskog sustava nakon nastupa sigurnosnih incidenata (anketno pitanje br. 28)



Izvor: priredio autor

Postavljeno je pitanje je li informacijska sigurnost ključna u postizanju poslovnih ciljeva za vlasnike i rukovoditelje poduzeća, a dobiveni su rezultati prikazani grafički na grafikonu 35.

Grafikon 35: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju ključnosti poslovnih funkcija upravljanja informacijskom sigurnošću u postizanju poslovnih ciljeva postavljenih od strane uprave poduzeća (vlasnika, rukovoditelja – anketno pitanje br. 33)



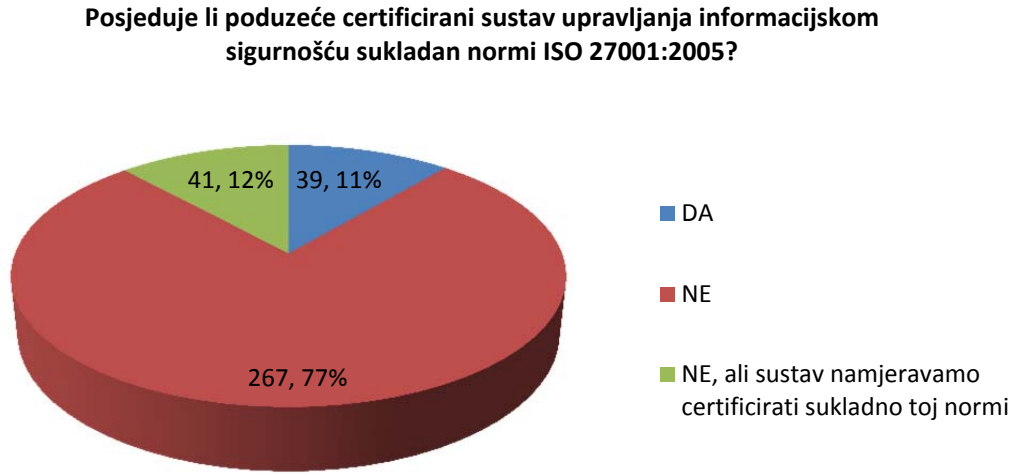
Izvor: priredio autor

Vezano uz rezultate prikazane na grafikonu 35, potrebno je istaknuti da ukoliko je upravljanje informacijskom sigurnošću dio vrhovnih ciljeva postavljenih od strane rukovodstva ili vlasnika, odnosno, ukoliko se poslovna funkcija informacijske sigurnosti nameće kao ključna poslovna funkcija u postizanju poslovnih ciljeva, veća je vjerojatnost da će razina implementacije

informacijske sigurnosti i funkcionalnosti modela biti viša. Ova vrsta orijentacije dijelom je strateškog horizonta poduzeća i ne može se smatrati kako je moguće provesti je u kratkom vremenskom roku, već je adekvatan srednji rok.

Jedan od ključnih alata pri uspostavljanju sustava upravljanja informacijskom sigurnošću je i korištenje standarda najbolje prakse upravljanja kvalitetom informacijske sigurnosti kroz sustav ISO 27001:2005 te je stoga ovaj čimbenik uvršten kao važan kriterij na petoj razini funkcionalnosti modela. 39 anketiranih poduzeća ili 11 % ukupne anketirane populacije posjeduje takav sustav a 267 anketiranih poduzeća, odnosno 77 % ga ne posjeduje. Ohrabrujuće je kako čak 41 anketirano poduzeće ili 12 % namjerava sustav upravljanja informacijskom sigurnošću certificirati sukladno navedenoj normi, za što se razlozi mogu tražiti u prednostima koje pruža takva certifikacija kao prepoznata na tržištu ali i vjerojatno iz razloga što je često tražena u postupcima sudjelovanja u javnoj nabavi. Ovi su pokazatelji prikazani na grafikonu 36.

Grafikon 36: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju posjedovanja certificiranog sustava upravljanja informacijskom sigurnošću sukladno normi ISO 27001:2005 (anketno pitanje br. 38)



Izvor: priredio autor

5.3.2.6. Ukupno vrednovanje modela prema odabranim kriterijima

U tablici 22. prikazane su zasebne karakteristike srednjih vrijednosti dostignutih razina zrelosti funkcije upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj. U prvom retku tablice, naslovljenom „*Ukupni mogući zbroj vrijednosti na razini*“, prikazano je vrednovanje funkcionalnosti teoretskog poduzeća s punom implementacijom

modela na svim razinama. Takvo bi poduzeće, kao što je već objašnjeno, dostiglo ukupnu vrijednost čimbenika na prvoj razini od 3, na drugoj razini od 8, na trećoj razini od 36, na četvrtoj razini od 24 i na petoj razini od 25, odnosno ukupan mogući zbroj vrijednosti svih implementiranih razina funkcionalnosti bio bi 96.

Srednja vrijednost **na prvoj razini** implementacije modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima iznosi 1,35 mjereno aritmetičkom sredinom odnosno 1 mjereno medijanom; to znači kako je u prosjeku u malim i srednjim poduzećima u Republici Hrvatskoj dostignuto 45 % (1,35 / 3) funkcionalnosti predviđenih čimbenika na prvoj razini funkcionalnosti modela mjereno aritmetičkom sredinom, odnosno 33,33 % (1 / 3) istih funkcionalnosti mjereno medijanom. Standardna devijacija izmjere iznosi 0,85.

Srednja vrijednost **na drugoj razini** implementacije modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima iznosi 2,21 mjereno aritmetičkom srednjom odnosno 2 mjereno medijanom; prema tome, u prosjeku je u malim i srednjim poduzećima u Republici Hrvatskoj dostignuto 27,63 % (2,21 / 8) funkcionalnosti predviđenih čimbenika na drugoj razini funkcionalnosti modela mjereno aritmetičkom sredinom, odnosno 25 % (2 / 8) funkcionalnosti mjereno medijanom. Standardna devijacije ove izmjere iznosi 1,89.

Na trećoj razini implementacije funkcionalnosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima istraživanjem je utvrđeno kako srednja vrijednost implementacije funkcionalnosti predviđenih čimbenika na toj razini iznosi 19,89 % (7,16 / 36) mjereno aritmetičkom sredinom ili 25 % (9 / 36) mjereno medijanom. Na trećoj razini implementacije modela upravljanja informacijskom sigurnošću standardna devijacija iznosi 7,87.

U slučaju **četvrte razine** funkcionalnosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj obradom rezultata anketnog istraživanja je utvrđeno kako je srednja vrijednost implementacije funkcionalnosti determiniranih čimbenika 21,33 % mjereno aritmetičkom sredinom (5,12 / 24), odnosno 16,67 % (4 / 24) ukoliko je mjera sredine niza medijan. Standardna devijacija u ovom slučaju iznosi 5,02.

Na posljednjoj, **petoj razini** funkcionalnosti modela, srednja vrijednost implementacije determiniranih čimbenika ove razine funkcionalnosti iznosi 22,36 % mjereno aritmetičkom sredinom (5,59 / 25), dok u slučaju uzimanja medijana kao mjere sredine niza ta vrijednost iznosi 20 % (5 / 25). Standardna devijacija na petoj razini funkcionalnosti modela iznosi 6,10.

Promatrano **sintetički**, uz jednake dodijeljene vrijednosti svih razinama funkcionalnosti, na razini cjelokupne funkcionalnosti modela upravljanja informacijskom sigurnošću u malim i

srednjim poduzećima u Republici Hrvatskoj, obradom navedenih rezultata dolazi se do zaključka kako je **srednja vrijednost cjelokupne implementacije** ovako postavljenog modela 23,32 % (21,43 / 96) od teoretski moguće vrijednosti mjereno aritmetičkom sredinom odnosno 19,79 mjereno medijanom (19 / 96). Ukupna standardna devijacija izmjere iznosi 16,98.

Tablica 22: Zasebne karakteristike srednjih vrijednosti dostignutih razina zrelosti funkcije upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj

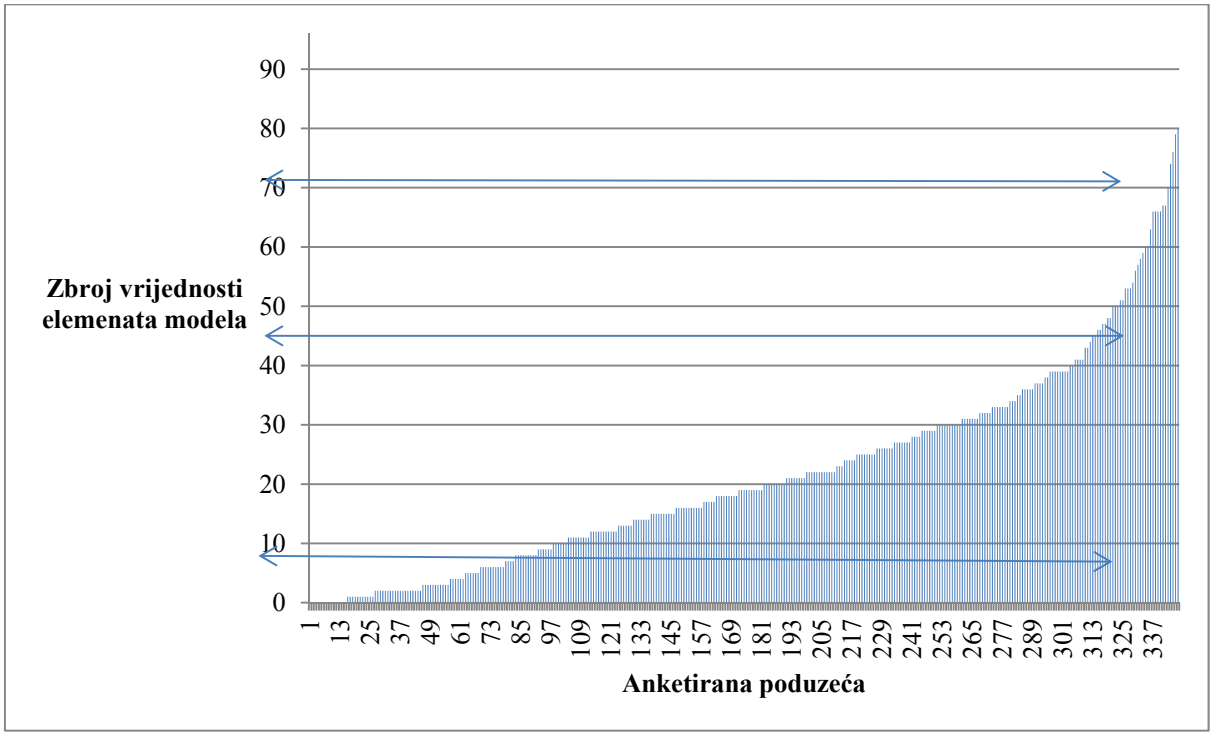
Pokazatelj	UKUPNO	Prva razina	Druga razina	Treća razina	Četvrta razina	Peta razina
Ukupni mogući zbroj vrijednosti na razini	96	3	8	36	24	25
Medijan	19	1	2	9	4	5
Aritmetička sredina	21,43	1,35	2,21	7,16	5,12	5,59
Standardna devijacija	16,98	0,85	1,89	7,87	5,02	6,10
Koeficijent varijacija	0,79	0,63	0,86	1,10	0,98	1,09
Standardna greška	0,91	0,05	0,10	0,42	0,27	0,33

Izvor: priredio autor

Rezultati iz tablice 22. su na drugi način prikazani slikovito histogramom frekvencija na grafikonu 37. na sljedećoj stranici. Za svako od 347 anketiranih malih i srednjih poduzeća prikazana je stupčasto dostignuta ukupna razina funkcionalnosti upravljanja informacijskom sigurnošću, na način da su zbrojene pojedine razine funkcionalnosti po čimbenicima i pet definiranih razina funkcionalnosti. Ukupan zbroj vrijednosti elemenata modela može poprimiti vrijednosti od 0 do 96[193]. Vodoravnim linijama sa strelicama označene su pojedine razine funkcionalnosti od prve do pete koja poprimaju stalne vrijednosti u iznosima od 3, 8, 36, 24 i 25, kao što je prikazano u tablici x. Kada bi sva poduzeća imala implementirane sve čimbenike na svim razinama funkcionalnosti, histogrami frekvencija bi popunili u potpunosti površinu grafa do vrijednosti 96 na ordinati; budući da nije tako, ukupna površina pokrivena funkcionalnostima modela upravljanja iznosi, kao što je objašnjeno, tek 22,32 %, mjereno aritmetičkom sredinom kao centralnom mjerom.

[193] Kao što je već objašnjeno, teoretsko poduzeće s implementiranim svim čimbenicima funkcionalnosti na svim razinama, imalo bi ukupan zbroj vrijednosti funkcionalnosti modela od 96.

Grafikon 37: Zbrojeni rezultati analize zrelosti funkcije upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj



Izvor: priredio autor

Analiziraju li se dobiveni podaci prema pet razina funkcionalnosti modela, valja izložiti i neke značajne zaključke koji se mogu dobiti tom vrstom analize. U tablici 22-1. prikazana je analiza onih poduzeća koja prema ukupnoj, ili nekoj od razina funkcionalnosti nemaju implementiran niti jedan čimbenik funkcionalnosti.

Tablica 22-1: Broj poduzeća koja u ukupnosti, ili na nekoj od razina funkcionalnosti modela upravljanja informacijskom sigurnošću imaju rezultat funkcionalnosti jednak nuli

		Razine funkcionalnosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj				
	Ukupna funkcionalnost	I.	II.	III.	IV.	V.
Broj anketiranih poduzeća s rezultatom nula	15	58	107	161	120	140
Postotak od ukupne populacije anketnog uzorka	4,3 %	16,71 %	30,84 %	46,4 %	34,58 %	40,35 %

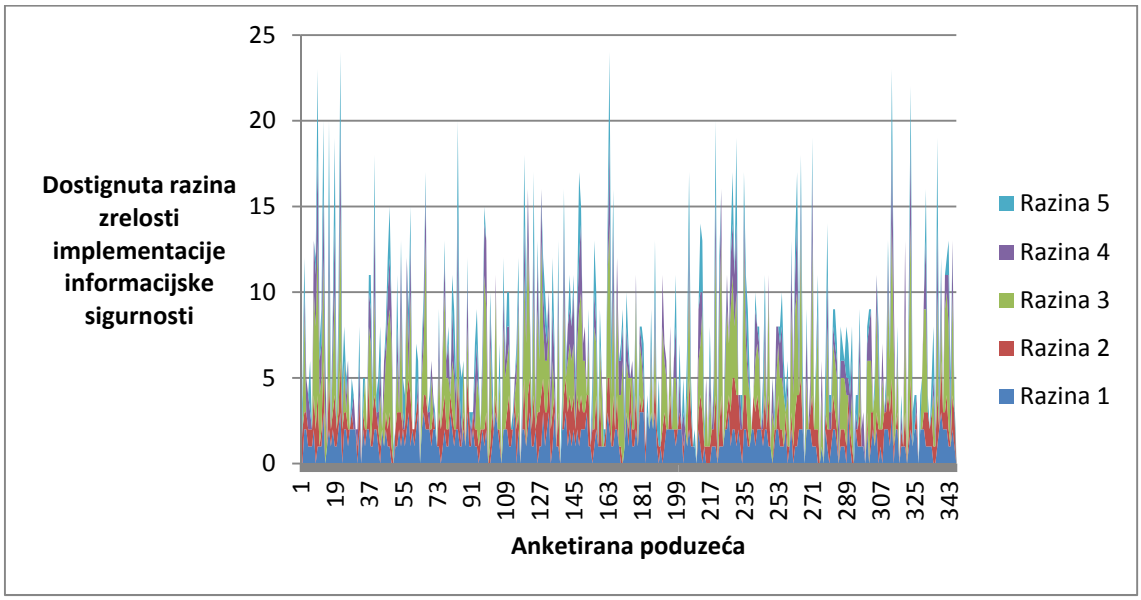
Izvor: priredio autor

Iz prikazanih rezultata može se zaključiti kako čak 15 anketiranih poduzeća ili 4,3 % nema implementiran niti jedan čimbenik niti na jednoj razini funkcionalnosti modela upravljanja informacijskom sigurnošću. Situacija je još više zabrinjavajuća kada se analiziraju poduzeća s

funkcionalnosti jednakoj nuli po razinama funkcionalnosti[194]. Tako na prvoj, najnižoj razini funkcionalnosti, koja nosi ukupnu vrijednost čimbenika od 3, 15 anketiranih poduzeća ili 4,3 % nema implementiran niti jedan čimbenik. Na drugoj razini funkcionalnosti koja nosi ukupnu vrijednost čimbenika 8, 107 anketiranih poduzeća ili 30,84 % nema implementiran niti jedan čimbenik. Na trećoj razini funkcionalnosti koja nosi ukupnu vrijednost čimbenika 36, 161 anketirano poduzeće ili čak 46,4 % nema implementiran niti jedan čimbenik. Na četvrtoj razini funkcionalnosti koja nosi ukupnu vrijednost čimbenika 24, 34,58 % svih anketiranih poduzeća nema implementiran niti jedan čimbenik. Naposljetku, na petoj razini funkcionalnosti s ukupnom vrijednošću čimbenika 25, 40,35 % poduzeća nema niti jedan implementirani čimbenik.

Ovi su podaci dodatno prikazani histogramom frekvencija po razinama. Svih 347 anketiranih poduzeća prikazano je na apscisi, dok je na ordinati dostignuta razina zrelosti implementacije informacijske sigurno prema pet identificiranih razina. Pojedine su razine funkcionalnosti prikazane različitim bojama na način prikazan u legendi grafikona 38.

Grafikon 38: Zbrojeni rezultati analize zrelosti funkcije upravljanja informacijskom sigurnošću (dostignute razine zrelosti implementacije informacijske sigurnosti) u malim i srednjim poduzećima u Republici Hrvatskoj prema razinama funkcionalnosti



Izvor: priredio autor

Kao što je vidljivo iz do sada izloženog, rezultati provedenog istraživanja upravljanja sustavom informacijske sigurnosti pokazuju kako je stupanj dostignute sustavne kontrole i ekonomske

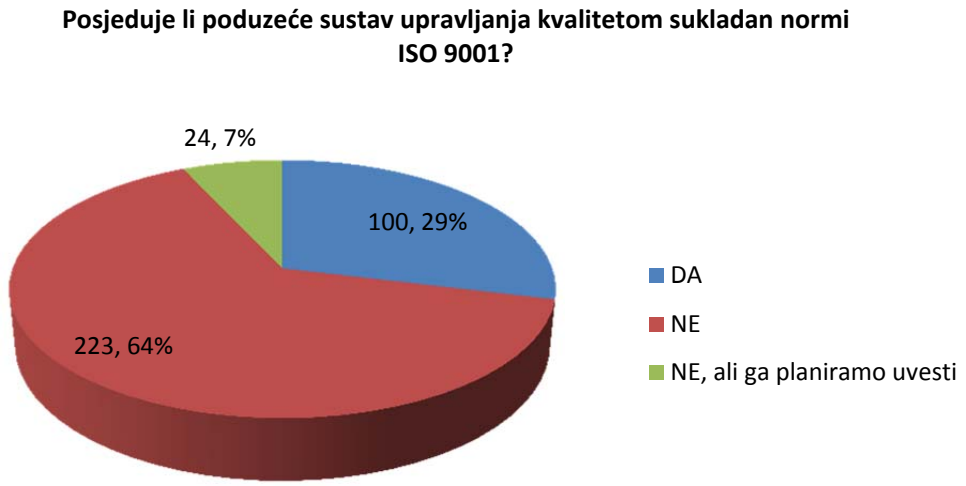
[194] Poduzeće s razinom funkcionalnosti nula nema niti jedan implementiran čimbenik funkcionalnosti modela upravljanja informacijskom sigurnošću niti na jednoj od pet definiranih razina modela.

održivosti uvjetovane korištenjem ekonomskih kriterija, financijske analize i kvantitativnih metoda vrlo nizak, odnosno ograničen. Mala i srednja poduzeća, što je potvrđeno istraživanjem, posjeduju nizak stupanj poštivanja zakonskih zahtjeva, uključenosti rukovodstva poduzeća u provođenje informacijske sigurnosti kao strateške poslovne funkcije, lošu razinu implementiranosti temeljnih operativnih mjera informacijske sigurnosti i nedostaju im potrebna financijska sredstva i akumulirano potrebno znanje za upravljanje novom i kompleksnom poslovnom funkcijom.

5.3.3. Obrada anketnih rezultata – upravljanje sustavima kvalitete

Poduzeća koja imaju implementiran sustav upravljanja kvalitetom mogu u opseg certifikacije uvrstiti i upravljanje informacijskom sigurnošću, ili mogu tretirati upravljanje informacijskom sigurnošću kao jednu od potpornih poslovnih funkcija u ostvarivanju onih ciljeva koji su postavljeni na godišnjoj razini te se prate kroz ključne pokazatelje sustava. Osim toga, ova certifikacija omogućuje i formalizaciju sustava kreiranjem politika, standarda, kriterija i radnih uputa vezanih uz upravljanje informacijskom sigurnošću u okviru standarda ISO 9001. Na taj način, certificiranost po normi ISO 9001, ukoliko se pravilno usmjeri, može biti iskorištena kao alat u postizanju ciljeva upravljanja informacijskom sigurnošću. Od anketiranih poduzeća, 64 % ili 223 anketirana poduzeća ne posjeduju sustav certificiran sukladno normi ISO 9001, a 7 % ili 24 anketirana poduzeća ga ne posjeduju ali ga imaju namjeru uvesti. 29 % anketiranih poduzeća, odnosno 100 od 347 ispitanih posjeduje sustav upravljanja kvalitetom sukladan navedenoj normi. Izložene su činjenice grafički prikazane na grafikonu 39.

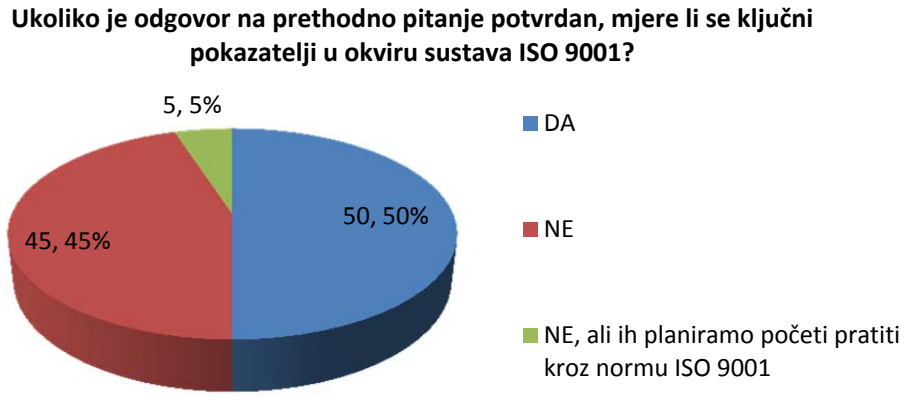
Grafikon 39: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju posjedovanja sustava upravljanja kvalitetom sukladno normi ISO 9001



Izvor: priredio autor

Nastavno na prethodno anketno pitanje, moguće je zaključiti kako pola anketiranih poduzeća koja su certificirana sukladno normi ISO 9001 mjeri ključne pokazatelje informacijske sigurnosti kroz taj sustav dok ih druga polovica ne mjeri, odnosno ne koristi sustav ISO 9001 na navedeni način. 5 anketiranih poduzeća ili 5 % od svih koja posjeduju poduzeće certificirano po normi ISO 9001 ne mjere ključne pokazatelje u okviru sustava ISO 9001 ali to namjeravaju početi činiti. Navedeni su kvantitativni pokazatelji grafički prikazani na grafikonu 40.

Grafikon 40: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju mjerenja ključnih pokazatelja u okviru sustava ISO 9001

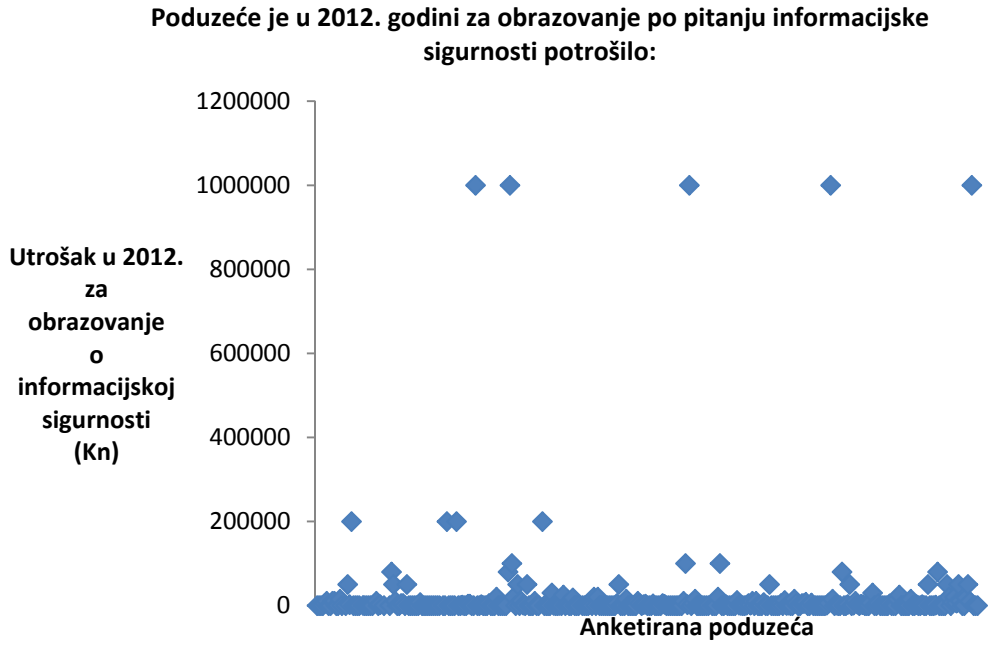


Izvor: priredio autor

5.3.4. Obrada anketnih rezultata – utrošak u obrazovanje iz područja informacijske sigurnosti

Vrlo zanimljive rezultate daje odgovor na anketno pitanje vezano uz utrošak u obrazovanje iz područja informacijske sigurnosti. Ispitanici iz anketiranih poduzeća upitani su koliki je bio iznos utroška u obrazovanje iz područja informacijske sigurnosti u njihovim poduzećima, a odgovori na to pitanje su vrlo raznoliki. Velik broj ispitanika odgovorio je kako uopće ne ulažu u obrazovanje iz područja informacijske sigurnosti. Nekoliko ispitanika odgovorilo je kako se ulaganja kreću oko 1,000.000 Kn godišnje a dodatna nekolicina kako se ona kreću oko 200.000 Kn. Većina anketiranih poduzeća odgovorila je kako se ta ulaganja kreću u rasponu od 0 do 50.000 Kn. Grafički prikaz ovog pitanja na skali s linearnim mjerilom prikazan je na grafikonu 41. na sljedećoj stranici, putem histograma frekvencija gdje se na ordinati nalazi iznos utroška za obrazovanje o informacijskoj sigurnosti u 2012. godini.

Grafikon 41: Prikaz utroška u obrazovanje iz područja informacijske sigurnosti u anketiranim poduzećima (linearno mjerilo)

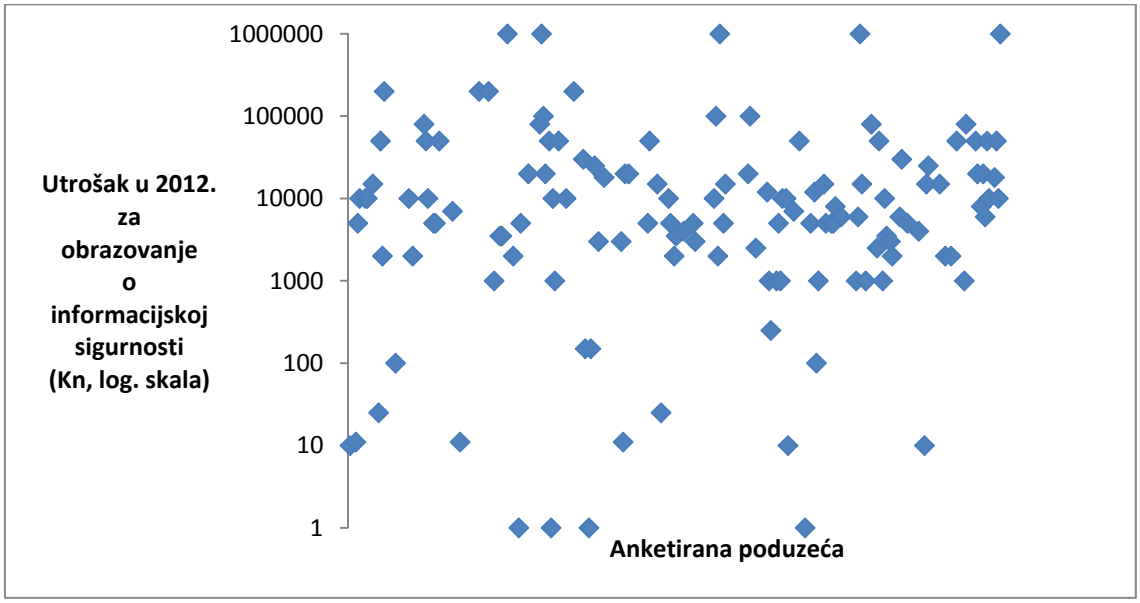


Izvor: priredio autor

U slučaju velikog raspršenja frekvencija i pojave nepodobnih članova grupe[195], metodološki bi bilo ispravno transformirati podatke radi lakšeg razumijevanja nekom od raspoloživih metoda[196], ili u obzir za analizu uzeti samo one vrijednosti koje se nalaze unutar nekog raspona, npr. unutar dvije standardne devijacije. U cijelom istraživanju nisu korištene metode koje bi rezultirale gubitkom podataka, iako se kod nekih obilježja, a osobito kod izmjere utroška u obrazovanje iz područja informacijske sigurnosti i broja sigurnosnih incidenata u 2012. godini, pojavljuju ovakvi ekstremi. Stoga će ovi podaci biti obrađeni u integralnom obliku te se prvo prikazuju korištenjem logaritamskog mjerila na bazi broja 10. Ovako obrađeni podaci prikazani su na grafikonu 42. na sljedećoj stranici.

[195] „*Nepodobni član grupe*" prijevod je od eng. „*outlier*". U statistici se taj pojam koristi za opažanje koje je numerički udaljeno od ostatka podataka.
[196] Uobičajene metode transformiranja podataka u statistici su logaritmiranje prirodnom bazom ili bazom 10, ili korjenovanje.

Grafikon 42: Prikaz utroška u obrazovanje iz područja informacijske sigurnosti u anketiranim poduzećima (logaritamsko mjerilo baze 10)



Izvor: priredio autor

Iz ovog grafikona jasnije je nego iz prethodnog grafikona kako se većina ispitanih poduzeća grupira u točnije određenom rasponu od 1.000 do 100.000 Kn godišnje. Neke druge karakteristike iznosa ulaganja u obrazovanje po pitanju ove poslovne funkcije prikazuje tablica 23.

Tablica 23: Svojstva čimbenika utroška u obrazovanje po pitanju informacijske sigurnosti

Pokazatelj	**Vrijednost**
Medijan	-
Aritmetička sredina	22.732,60
Standardna devijacija	121.434,06
Koeficijent varijacija	5,34
Standardna greška	6.518,82

Izvor: priredio autor

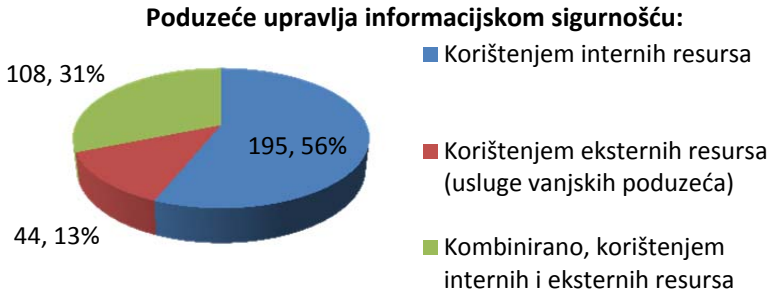
Kao što se vidi iz tablice 23, aritmetička sredina utroška vezanog uz obrazovanje po pitanju informacijske sigurnosti iznosi 22.732,60 Kn ali uz vrlo visoku standardnu devijaciju, a ova je činjenica već prethodno objašnjena velikim rasponom deklariranih vrijednosti. Iznos ovog čimbenika nema neku apsolutnu ili preporučenu vrijednost, ali je za očekivati da poduzeća s višom razinom ulaganja u obrazovanje po pitanju informacijske sigurnosti dostižu i više razine funkcionalnosti modela informacijske sigurnosti. Ova hipoteza, iako zanimljiva, nije dijelom ovog istraživanja te se neće detaljnije razmatrati, ali veliki raspon i različitost iznosa utroška u obrazovanje iz područja informacijske sigurnosti uz činjenicu da mnoga poduzeća uopće ne

iskazuju takav utrošak ukazuje na to da mala i srednja poduzeća ne upravljaju sustavno ovom vrstom troška već se on iskazuje slučajnim kretanjem.

5.3.5. Obrada anketnih rezultata – upravljanje informacijskom sigurnošću

Upravljanje informacijskom sigurnošću kao i općenita poslovna funkcija informatike unutar poduzeća može biti postignuto na dva načina ili kombinacijom dvaju mogućnosti, a to je korištenjem internih resursa, korištenjem eksternih resursa odnosno usluga vanjskih poduzeća ili kombinirano, korištenjem internih i eksternih resursa u odgovarajućim kombinacijama. 195 anketiranih poduzeća ili 56 % upravlja informacijskom sigurnošću isključivo korištenjem internih resursa. 44 anketirana poduzeća ili 13 % upravlja samo korištenjem eksternih resursa odnosno vanjskih poduzeća dok 108 anketiranih poduzeća ili 31 % koristi odgovarajuću kombinaciju internih i vanjskih resursa. Ova je činjenica prikazana na grafikonu 43., a od važnosti je osobito u uvjetima pojačanog korištenja usluga *„u oblaku"* koje predstavljaju eksternalizaciju informacijskih usluga i infrastrukture, a u tom kontekstu i onih koje se tiču pojedinih rješenja informacijske sigurnosti, pri čemu se takve poslovne funkcije promatraju isključivo kao operativni trošak a nisu imovina poduzeća. Osim toga, rješenja *„u oblaku"* sa sobom ne nose korisniku probleme vezane uz skalabilnost rješenja pri proširenju poslovne djelatnosti ili potreba za dodatnim kapacitetima. Za pretpostaviti je kako će već budućnost u srednjem roku donijeti pomak od korištenja internih resursa za upravljanje informacijskom sigurnošću u smjeru korištenja eksternih resursa i hibridnih[197] modela.

Grafikon 43: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju načina upravljanja informacijskom sigurnošću (korištenjem internih resursa, eksternih resursa ili kombinirano)



Izvor: priredio autor

[197] Kombinirani ili hibridni modeli upravljanja informacijskom sigurnošću uključuju eksternalizaciju poslovne funkcije informacijske sigurnosti. Uslijed specifičnih problema povezanih uz očuvanje privatnosti podataka i efikasnosti ovakvog modela upravljanja informacijkom sigurnošću, poduzeća oklijevaju u provođenju jače eksternalizacije ove poslovne funkcije. Osim toga, u područjima poput financijskog sektora koja su čvršće regulirana propisima, regulator obično propisuje potrebu za internim provođenjem informacijske sigrunosti.

Drugu temeljnu odrednicu upravljanja informacijskom sigurnošću u malim i srednjim poduzećima, a osobito u uvjetima u kojima poduzeća imaju na raspolaganju ograničena sredstva, predstavlja planiranje investicija i troška održavanja sustava upravljanja informacijskom sigurnošću na godišnjoj razini, jer samo ovakvo upravljanje može osigurati sukladnost postavljenim poslovnim ciljevima, strategiji, ali i raspoloživim financijskim sredstvima. Točno dvije trećina anketiranih poduzeća (ili 229 poduzeća) uopće ne planira investicije i trošak sustava upravljanja informacijskom sigurnošću na godišnjoj razini. Samo 23 % poduzeća (ili 79 poduzeća) investicije i trošak planira godišnje dok 11 % (odnosno 39 poduzeća) planira investicije i trošak upravljanja informacijskom sigurnošću na godišnjoj razini. Ovi su pokazatelji grafički prikazani na grafikonu 44.

Grafikon 44: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju planiranja investicija i troška sustava upravljanja informacijskom sigurnošću na godišnjoj razini

Izvor: priredio autor

Detaljnija razrada ponašanja poduzeća s obzirom na to planiraju li odvojeno investicije od troška ili ne, razvijena je upravo od ovog anketnog pitanja (čimbenika) i već je prethodno prikazana na odgovarajućim razinama funkcionalnosti modela[198].

5.3.6. Obrada anketnih rezultata – kapitalna ulaganja i tekući trošak

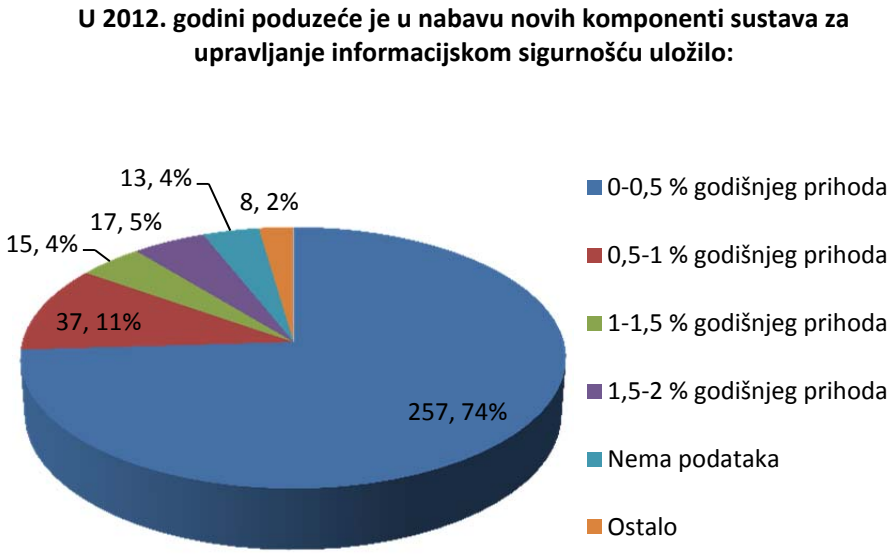
Tijekom istraživanja postavljena su i dva pitanja usmjerena ka izmjeri utroška nabave novih komponenti sustava za upravljanje informacijskom sigurnošću. Budući da apsolutan iznos investicije u informacijsku sigurnost sam po sebi nije značajan pokazatelj, te da iznos apsolutnih investicija ovisi o više čimbenika među kojima su najznačajniji dostignuti stupanj kompleksnosti informacijskog sustava i sustava upravljanja informacijskom sigurnošću, raspoloživa financijska sredstva na raspolaganju poduzeću i vrsta poslovne djelatnosti kojom se poduzeće bavi, ocijenjeno je kako je od značaja ponderirati apsolutni iznos ulaganja ili troška prihodom poduzeća i zatim obavljati usporedbe i agregiranja temeljem tako dobivenog

[198] Konkretno, na četvrtoj razini funkcionalnosti modela u poglavlju 5.2.5.

sintetskog pokazatelja. Anketiranim poduzećima postavljeno je pitanje koliki postotak godišnjeg prihoda troše na nove komponente sustava upravljanja informacijskom sigurnošću s njihovi su odgovori grafički prikazani na grafikonu 45.

Gotovo tri četvrtine anketiranih poduzeća, odnosno 257 poduzeća ili 74 % za investicije u nove komponente sustava za upravljanje informacijskom sigurnošću utrošilo je između 0 i 0,5 % godišnjeg prihoda. 37 poduzeća ili 11 % utrošilo je u tu svrhu između 0,5 i 1 % godišnjeg prihoda, 15 poduzeća ili 4 % između 1 i 1,5 % godišnjeg prihoda, 17 poduzeća ili 5 % anketiranih između 1,5 i 2 % prihoda. Budući da odgovor na ovo pitanje zahtijeva poznavanje dva pokazatelja, a to je pored iznosa investicije i prihod poduzeća, ostavljene su i dodatne dvije mogućnosti odgovora, a to su „*nema podataka*“, čime se očitovalo 13 anketiranih poduzeća ili 4 % anketiranih, dok s „*ostalo*“, a to su svi utrošci veći od 2 % godišnjeg prihoda odgovara 8 poduzeća ili 2 % od ukupno anketiranih. Navedene omjere prikazuje grafikon 45.

Grafikon 45: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju troška nabave novih komponenti sustava za upravljanje informacijskom sigurnošću u odnosu prema godišnjem prihodu poduzeća u 2012. godini

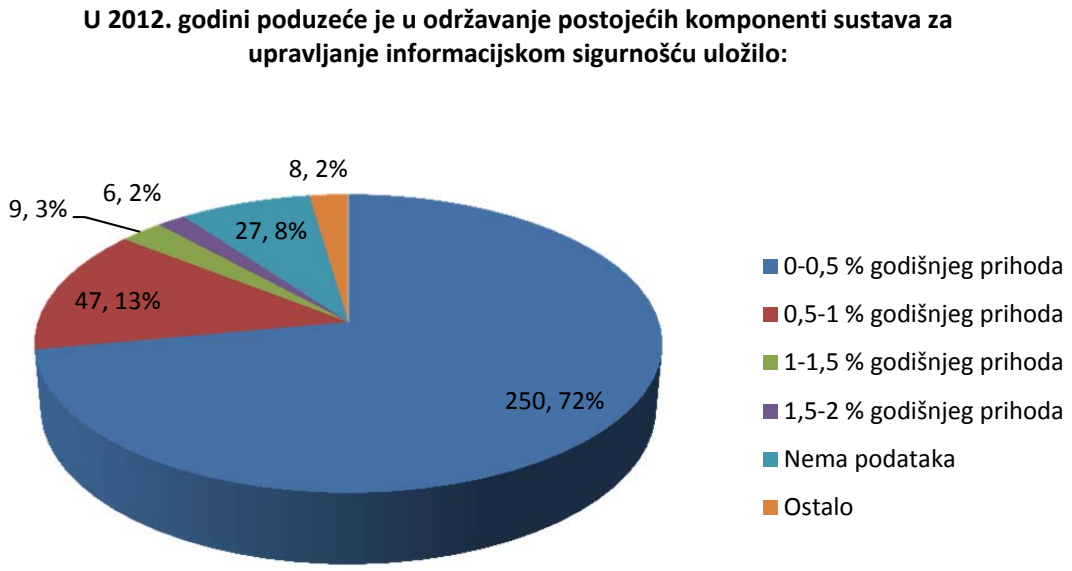


Izvor: priredio autor

Slično pitanje postavljeno je i za trošak održavanja postojećih komponenti sustava za upravljanje informacijskom sigurnošću u odnosu prema godišnjem prihodu poduzeća u 2012. godini i očekivano, dobiveni su vrlo slični odgovori. 250 poduzeća ili 72 % anketiranih odgovara kako za održavanje postojećih komponenti sustava za upravljanje informacijskom

sigurnošću troše 0-0,5 % godišnjeg prihoda. 47 anketiranih poduzeća ili 13 % troši 0,5-1 % godišnjeg prihoda, 9 anketiranih poduzeća ili 3 % troši 1-1,5 % godišnjeg prihoda, 6 anketiranih poduzeća ili 2 % troši 1,5-2 % godišnjeg prihoda. Naposljetku, 27 poduzeća ili 8 % anketiranih ne posjeduje tražene podatke ili ih ne bilježi dok 8 poduzeća ili 2 % anketiranih odgovara na ovo pitanje s „*ostalo*“ što znači da troše više od 2 % prihoda u navedene svrhe. Ovi su podaci prikazani na grafikonu 46.

Grafikon 46: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju troška održavanja postojećih komponenti sustava za upravljanje informacijskom sigurnošću u odnosu prema godišnjem prihodu poduzeća u 2012. godini



Izvor: priredio autor

Analiza odnosa utroška u nove investicije komponenti sustava upravljanja informacijskom sigurnošću te troška održavanja postojećeg sustava pokazuje kako otprilike tri četvrtine malih i srednjih poduzeća u Republici Hrvatskoj ulaže između 0 i 0,5 % godišnjeg prihoda u 2012. godini, dok se ista količina financijskih sredstava troši i na održavanje postojećih komponenti sustava informacijske sigurnosti. U oba slučaja svega 2 % poduzeća koristi više od 2 % godišnjeg prihoda za nabavu novih komponenti sustava informacijske sigurnosti a isti postotak poduzeća troši više od 2 % godišnjeg prihoda za održavanje postojećeg sustava.

5.3.7. Obrada anketnih rezultata – planiranje upravljanja informacijskom sigurnošću

Područje planiranja upravljanja informacijskom sigurnošću obuhvaćeno je u istraživanju sa četiri anketna pitanja. Prvo, temeljno pitanje, problematizira temeljnu aktivnost sustavnog planiranja informacijske sigurnosti poduzeća a to je godišnje planiranje investicija i troška sustava upravljanja informacijskom sigurnošću i prikazano je korištenjem strukturnog kruga na grafikonu 47. Kroz godišnje anticipiranje troškova i aktivnosti, poduzeće može usmjeriti svoje aktivnosti vezane uz informacijsku sigurnost na način da su one sukladne poslovnoj politici poduzeća i temeljnoj poslovnoj aktivnosti te usklađene s raspoloživošću financijskih sredstava. Točno dvije trećine poduzeća ili 229 anketiranih (66 %) ne planira takve investicije na navedeni način, što je metodološki nespojivo s razvijenim stupnjem funkcionalnosti modela upravljanja informacijskom sigurnošću. Dodatnih 39 anketiranih poduzeća ili 11 % te troškove ne planira na godišnjoj razini ali ih planira početi pratiti. Samo 79 anketiranih poduzeća ili 23 % na godišnjoj razini planira investicije i troškove sustava upravljanja informacijskom sigurnošću.

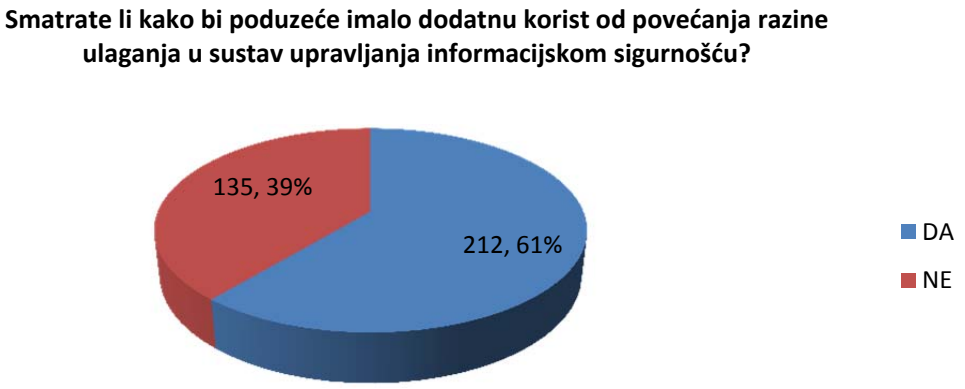
Grafikon 47: Prikaz postotnog udjela poduzeća prema kriteriju planiranja investicija i troška sustava upravljanja informacijskom sigurnošću na godišnjoj razini

Izvor: priredio autor

Na grafikonu 48. na sljedećoj stranici prikazan je postotni udio anketiranih poduzeća prema anticipiranim dodatnim koristima od povećanja razine ulaganja u sustav upravljanja informacijskom sigurnošću. Naime, postavljeno je pitanje smatraju li anketirani kako bi poduzeće imalo dodatnih koristi od povećanja razine ulaganja u sustav upravljanja informacijskom sigurnošću. Iako je dostignuta razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima vrlo niska, čak 135 anketiranih poduzeća ili 39 % smatra kako ne bi bilo dodatnih koristi od povećanja razine ulaganja u sustav upravljanja informacijskom

sigurnošću. Preostalih 212 poduzeća ili 61 % smatra kako bi od dodatnih ulaganja u sustav upravljanja informacijskom sigurnošću postojale dodatne koristi.

Grafikon 48: Prikaz postotnog udjela anketiranih poduzeća prema anticipiranim dodatnim koristima od povećanja razine ulaganja u sustav upravljanja informacijskom sigurnošću anketiranih poduzeća

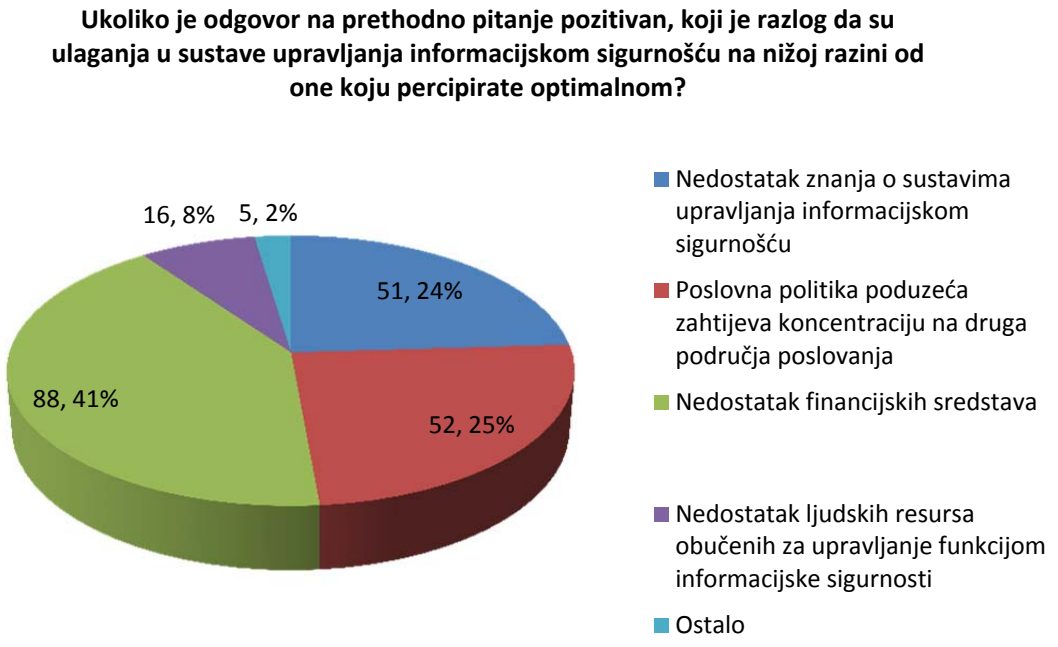


Izvor: priredio autor

Razlozi nedovoljne razine ulaganja u sustave upravljanja informacijskom sigurnošću u odnosu na onu koju bi se percipiralo optimalnom prikazani su na sljedećem grafikonu, grafikonu 49. Na ovo pitanje su odgovarala samo anketirana poduzeća koja su prethodno odgovorila kako smatraju da bi postojale dodatne koristi od povećanja razine ulaganja u sustav upravljanja informacijskom sigurnošću u odnosu na dostignutu razinu a cilj postavljanja ovog pitanja je pokušaj određivanja čimbenika koji utječu na podinvestiranje u poslovnu funkciju informacijske sigurnosti, koji mogu biti mnogobrojni a obično se smatra kako su povezani uz nedostatak financijskih sredstava. Ponuđeno je nekoliko odgovora i dobiveni su vrlo zanimljivi rezultati. Naime, ponuđeni odgovori obuhvaćaju iskustava gotovo svih anketiranih poduzeća jer je samo 5 anketiranih poduzeća ili 2 % odgovorilo kako su ostali, nenavedeni razlozi odgovorni za podinvestiranje u ovu poslovnu funkciju. Najviše poduzeća, njih 88 ili 41 % odgovara kako je razlog za ovu činjenicu nedostatak financijskih sredstava. Sljedeći postotno najveći broj respondenata, njih 52 ili 25 % smatra kako postoji natjecanje između investicija unutar poduzeća, tako da poslovna politika poduzeća zahtijeva koncentraciju na druga područja poslovanja. 51 anketirano poduzeće ili 24 % svih poduzeća smatra kako je ograničavajući čimbenik nedostatka znanja o sustavima upravljanja informacijskom sigurnošću. Činjenica kako gotovo četvrtina anketiranih smatra da ih u povećanju ulaganja u sustave upravljanja informacijskom sigurnošću sprječava nedostatak znanja opravdava uključivanje više pitanja vezanih uz sustav obrazovanja zaposlenika, a osobito rukovoditelja koji odlučuju o

investicijama u mjerni instrument istraživanja, te dodatno pojačava stav kako je edukacija, odnosno obrazovanje o informacijskoj sigurnosti jedan od ključnih čimbenika provođenja iste. Naposljetku, 16 anketiranih poduzeća ili 8 % identificira kako je problem u tome što nedostaju ljudski resursi obučeni za upravljanje funkcijom informacijske sigurnosti.

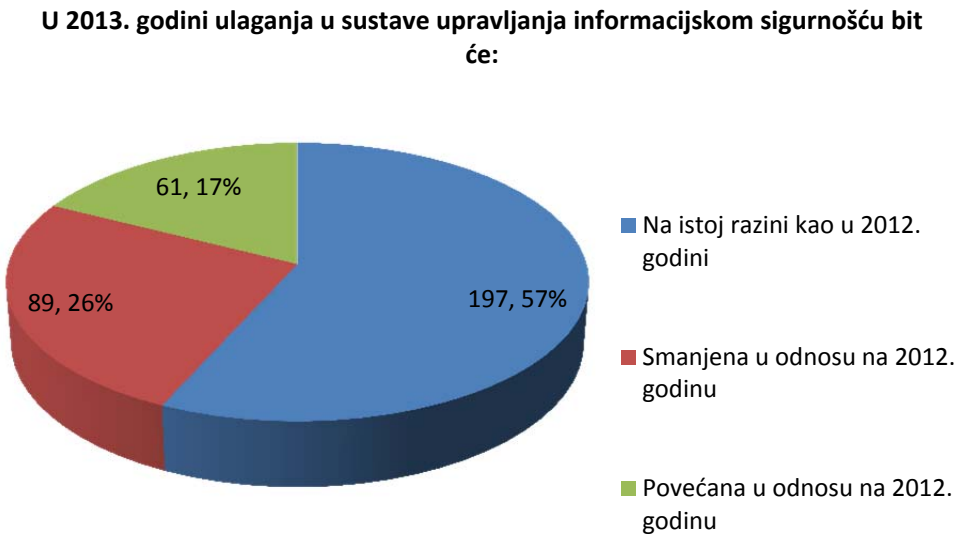
Grafikon 49: Prikaz postotnog udjela anketiranih poduzeća prema razlozima percipirane nedovoljne razine ulaganja u sustave upravljanja informacijskom sigurnošću u odnosu na optimalnu



Izvor: priredio autor

Budući da je istraživanje provedeno u prvom i drugom kvartalu 2013. godine te je u tom trenutku bilo moguće postaviti pitanja vezana uz prihode iz 2012. godine, anketiranim poduzećima postavljeno je pitanje vezano uz planiranu razinu ulaganja u sustave upravljanja informacijskom sigurnošću u 2013. godini. Čak 197 poduzeća ili 57 % svih anketiranih u 2013. godini namjerava zadržati ulaganja na istoj razini kao u 2012. godini. Zabrinjava činjenica kako 89 poduzeća ili 26 % poduzeća namjerava smanjiti ulaganja u odnosu na 2012. godinu a 61 anketirano poduzeće ili 17 % svih poduzeća namjerava povećati ulaganja u sustave upravljanja informacijskom sigurnošću. Navedeni su podaci prikazani na grafikonu 50. na sljedećoj stranici.

Grafikon 50: Prikaz postotnog udjela anketiranih poduzeća prema planiranoj razini ulaganja u sustave upravljanja informacijskom sigurnošću u 2013. godini



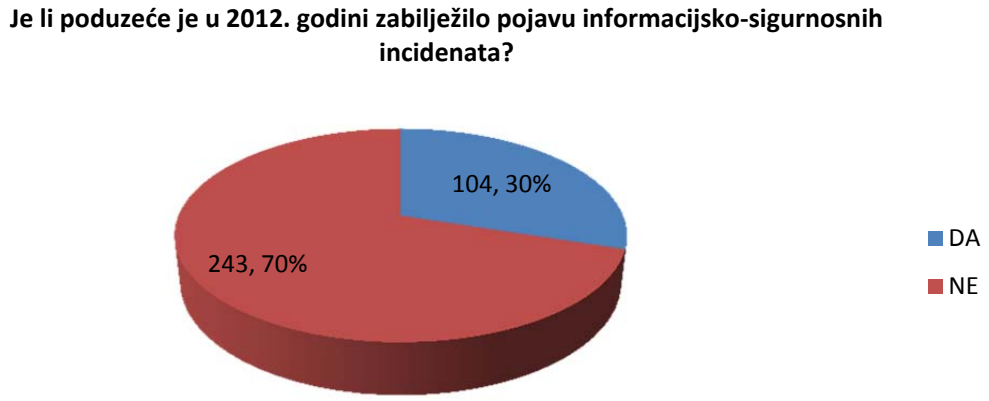
Izvor: priredio autor

Prema izrečenome, analiza planiranja upravljanja informacijskom sigurnošću pokazuje kako trenutačno 77 % poduzeća ne planira investicije i trošak sustava upravljanja informacijskom sigurnošću na godišnjoj razini pri čemu 11 % anketiranih planira uvesti godišnje planiranje. 39 % poduzeća smatra kako ne bi imalo dodatnu korist od povećanja ulaganja u sustav upravljanja informacijskom sigurnošću. Od poduzeća koja smatraju kako bi dodatne koristi postojale, najviše njih smatra kako je razlog za podinvestiranje financijske naravi (41 %), a taj razlog slijede nedostatak znanja o sustavima upravljanja informacijskom sigurnošću s 24 % i koncentracija poslovne politike poduzeća na druga područja s 25 %. Više od četvrtine anketiranih poduzeća namjerava smanjiti ulaganja u sustave upravljanja informacijskom sigurnošću u 2013. godini u odnosu na 2012. godinu. Ovi svi pokazatelji ukazuju na činjenicu kako je planiranje ulaganja u informacijsku sigurnost u malim i srednjim poduzećima u Republici Hrvatskoj stihijsko, na nedovoljnoj razini, a izrazito je pomanjkanje znanja unutar samih poduzeća, pored nedostatka financijskih sredstava, kao ograničavajući čimbenik za dostizanje viših razina funkcionalnosti zadanog modela.

5.3.8. Obrada anketnih rezultata – incidenti informacijske sigurnosti

Na grafikonu 51, prikazani su obrađeni rezultati anketnog pitanja vezanog uz informacijsko-sigurnosne incidente u 2012. godini. 243 poduzeća ili točno 70 % svih anketiranih odgovara kako u 2012. godini nisu zabilježili pojavu sigurnosnih incidenata dok 104 poduzeća ili 30 % anketiranih odgovara kako su takve incidente zabilježili.

Grafikon 51: Prikaz postotnog udjela anketiranih poduzeća prema zabilježenim informacijsko-sigurnosnim incidentima u 2012. godini

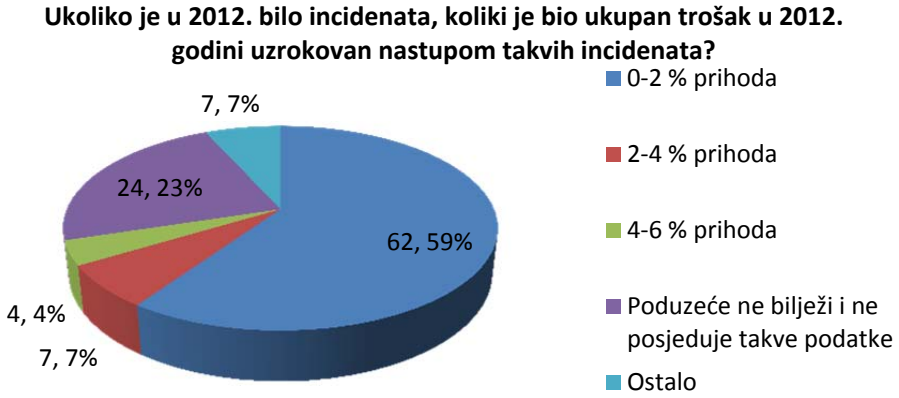


Izvor: priredio autor

Za dalju analizu utjecaja incidenata informacijske sigurnosti po poslovanje malih i srednjih poduzeća koristi se slična metodologija kakva je bila korištena i kod konstruiranja pitanja vezanog uz omjer investicija i troškova u sustave upravljanja informacijskom sigurnošću prema ukupnom prihodu poduzeća u 2012. godini. Tako se u ovom slučaju koristi pitanje na koje su odgovorila samo ona anketirana poduzeća koja su u 2012. godini zabilježila pojavu informacijsko-sigurnosnih incidenata, a pritom su trebali procijeniti koliki je ukupan trošak nastupa takvih incidenata prema postignutom prihodu. Ovi su rezultati prikazani na grafikonu 52. na sljedećoj stranici. 62 anketirana poduzeća ili 59 % od svih poduzeća koja su zabilježila pojavu nastupa sigurnosnih incidenata iz područja informacijske sigurnosti imala su nanesenu štetu u iznosu od 0 do 2 % ukupnog prihoda poduzeća. Po 7 poduzeća ili 7 % poduzeća pogođenih informacijskim incidentima zabilježilo je štetu u rasponu od 2 do 4 % ukupnog prihoda i veću od 6 % prihoda, što je osobito dojmljiv rezultat. 4 anketirana poduzeća ili 4 % bilježi štetu u iznosu od 4 do 6 % ukupnog prihoda dok gotovo četvrtina poduzeća (24 anketirana poduzeća ili 23 %) iako je imalo zabilježenu štetu uslijed nastupa jednog ili više sigurnosnih incidenata ne bilježi i ne posjeduje takve podatke. Ova činjenica može biti značajna prepreka poboljšanju razine upravljanja informacijskom sigurnošću a osobito korištenju

kvantitativnih metoda ili uspoređivanja iznosa apsolutnog rizika u odnosu na trošak informacijsko-sigurnosnog rješenja kojim se taj rizik pokušava umanjiti.

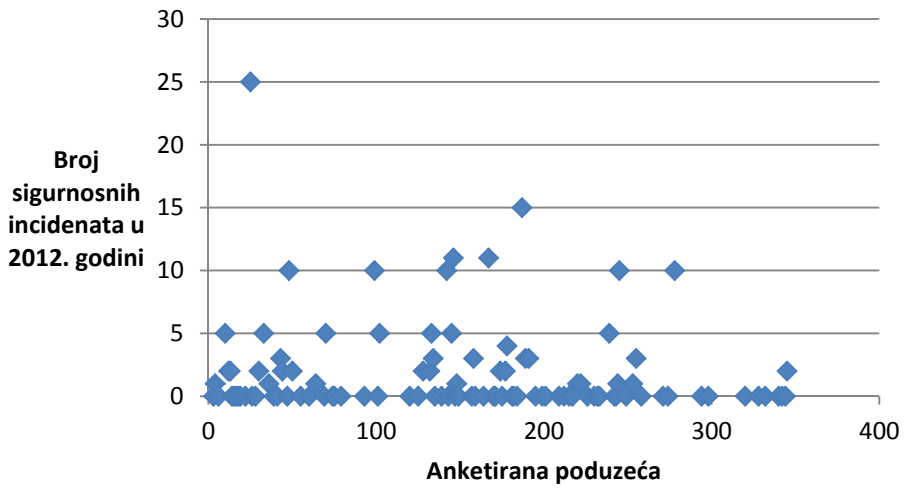
Grafikon 52: Prikaz postotnog udjela anketiranih poduzeća prema ukupnom trošku nastupa informacijsko-sigurnosnih incidenata u 2012. godini



Izvor: priredio autor

Nadalje, slično kao i kod anketnog pitanja povezanog uz utrošak u obrazovanje po pitanju informacijske sigurnosti, ali u nešto manjem opsegu, kod ispitivanja broja sigurnosnih incidenata u anketiranim poduzećima u 2012. godini nailazi se na problem nepodobnih članova grupe, odnosno nekih vrijednosti koje se nalaze značajno izvan raspona dvije standardne devijacije. Na grafikonu 53. prikazan je histogram frekvencija broja sigurnosnih incidenata na kojemu se vizualno može uočiti kako je većina poduzeća koja su imala identificirane incidente informacijske sigurnosti imala od jednog do tri takva incidenta godišnje.

Grafikon 53: Broj sigurnosnih incidenata u anketiranim poduzećima u 2012. godini



Izvor: priredio autor

Dalja analiza navedenih podataka prikazana je u tablici 24.

Tablica 24: Deskriptivna svojstva čimbenika broja sigurnosnih incidenata u anketiranim poduzećima u 2012. godini

Mjera	Vrijednost
Medijan	3
Aritmetička sredina	4,80
Standardna devijacija	4,84
Koeficijent varijacija	1,01
Standardna greška	0,26

Izvor: priredio autor

Iz podataka u ovoj tablici se vidi kako je medijan broja incidenata informacijske sigurnosti 3 dok je aritmetička sredina 4,80. No, standardna je devijacija visoka i iznosi čak 4,84.

5.3.9. Obrada anketnih rezultata – korištenje operativnih mjera informacijske sigurnosti

Korištenjem operativnih mjera informacijske sigurnosti[199] poduzeća se pokušavaju nositi s narastajućim ugrozama koje prijete informacijskim sustavima poduzeća. Analiza operativnih mjera informacijske sigurnosti izložena je u tablici 25.

Tablica 25: Operativne mjere informacijske sigurnosti korištene od strane anketiranih malih i srednjih poduzeća u Republici Hrvatskoj u 2012. godini

Operativna mjera informacijske sigurnosti	Broj poduzeća	Postotak od ukupnog broja poduzeća
Odvojena korisnička imena i lozinke za sve korisnike	245	70.61%
Antivirusnu zaštitu na svim računalima	266	76.66%
Vatrozid *(firewall)* koji odvaja unutrašnju mrežu poduzeća od Interneta	238	68.59%
Najnovije sigurnosne zakrpe za računalnu opremu i programe	62	17.87%
Praćenje i analiza mrežnog komunikacijskog prometa u poduzeću	83	23.92%
Filtriranje (selektivni pristup) Internet sadržajima	24	6.92%
Odvajanje pristupa podacima po grupama ovlaštenih korisnika (npr. odjeli, organizacijske jedinice)	107	30.84%

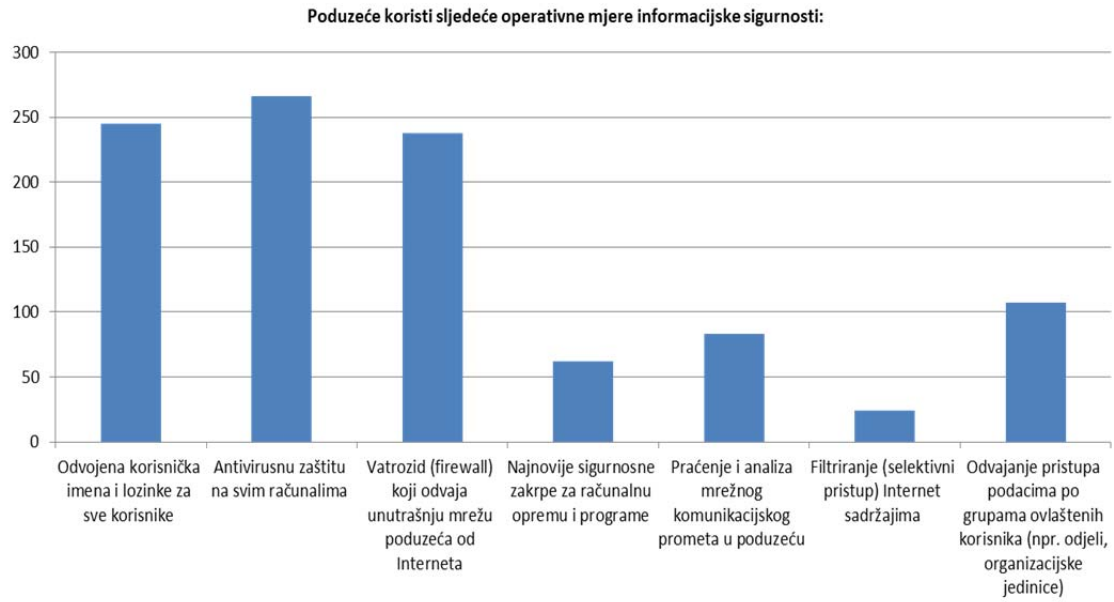
Izvor: priredio autor

Kao što je vidljivo iz tablice 25., najviše poduzeća, njih 76,7 %, koristi antivirusnu zaštitu na svim računalima, a tu mjeru slijede odvojena korisnička imena i lozinka za sve korisnike s

[199] U terminima ISO 27001:2005 standarda, ovakve se operativne mjere nazivaju kontrolama, a radi se o određenim postupcima ili rješenjima kojima poduzeća pokušavaju umanjiti, transferirati ili ukloniti rizik informacijske sigurnosti kojemu je izložena odgovarajuća informacijska imovina poduzeća.

pojavnošću od 70,6 % u anketnoj populaciji te vatrozid kojim se odvaja unutrašnja mreža poduzeća od Interneta sa 68,6 % . Svi ovi podaci prikazani su radi lakšeg razumijevanja u apsolutnom iznosu izmjerenih frekvencija na stupčastom grafikonu 54.

Grafikon 54: Prikaz postotnog udjela anketiranih poduzeća prema kriteriju korištenja odgovarajućih vrsta operativnih mjera informacijske sigurnosti u 2012. godini



Izvor: priredio autor

Osobito je zanimljivo kako su najmanje korištene mjere filtriranja odnosno selektivnog pristupa Internet sadržajima koje koristi 6,9 % anketiranih poduzeća, a zatim instalacija najnovijih sigurnosnih zakrpa za računalnu opremu i programe, korištena od strane 17,9 % malih i srednjih poduzeća te praćenje i analiza mrežnog komunikacijskog prometa u poduzeću (23,9 % poduzeća) i odvajanje logičkog pristupa po grupama ovlaštenih korisnika[200], što je mjera koju koristi samo 30,8 % anketiranih poduzeća. Izrazito je zanimljiva dodatna analiza navedenih podataka, budući da npr. korištenje najnovijih sigurnosnih zakrpa za računalnu opremu i programe što je vrlo slabo korištena operativna mjera informacijske sigurnosti zasigurno nije povezana uz velike financijske izdatke, a isto se odnosi i na logičko odvajanje pristupa podacima po grupama ovlaštenih korisnika. Razlog za ovakvu zatečenu situaciju zasigurno treba tražiti u nedovoljnom inzistiranju rukovodstva ili vlasnika poduzeća na mjerama informacijske sigurnosti, odnosno na nedovoljnoj razini znanja vezanog uz provođenje mjera informacijske sigurnosti. No, također treba dodati kako čak i u slučaju mjera koje se relativno najviše provode poput odvajanja korisničkih imena i lozinki za sve korisnike, treba napomenuti kako 29,4 %

[200] npr. Odjeli, radne grupe, projektne grupe, sektori ili organizacijske jedinice, koji koriste isti skup informacija i informacijskih sustava tijekom odvijanja poslovne aktivnosti.

poduzeća ne provodi tako jednostavnu mjeru koja spada u strukovne osnove informacijske sigurnosti dok preko 23 % poduzeća ne koristi antivirusnu zaštitu na svim računalima, iako su antivirusni programi prije više godina postali temeljnim dijelom operativnih sustava na korisničkim računalima koji se ne plaćaju zasebno. Ovo je još jedan prilog tezi kako gospodarska situacija, nedovoljna financijska sredstva ili orijentacija na druge poslovne aktivnosti ne mogu biti uzrok niskoj razini dostignute funkcionalnosti modela informacijske sigurnosti u malim i srednjim poduzećima, već je ona dobrim dijelom rezultat nedovoljnog inzistiranja vertikale odlučivanja u poduzeću na mjerama informacijske sigurnosti i stihijskog provođenja te poslovne funkcije.

5.3.10. Obrada anketnih rezultata – incidenti informacijske sigurnosti

U tablici 26. su zajednički prikazane sve mogućnosti, odnosno ishodi negativnog utjecaja pojave informacijsko-sigurnosnih incidenata u poduzeću koji su analizirani u odgovarajućim pitanjima tijekom istraživanja, zajedno s njihovim srednjim vrijednostima, standardnim devijacijama, koeficijentom varijacija i standardnim greškama.

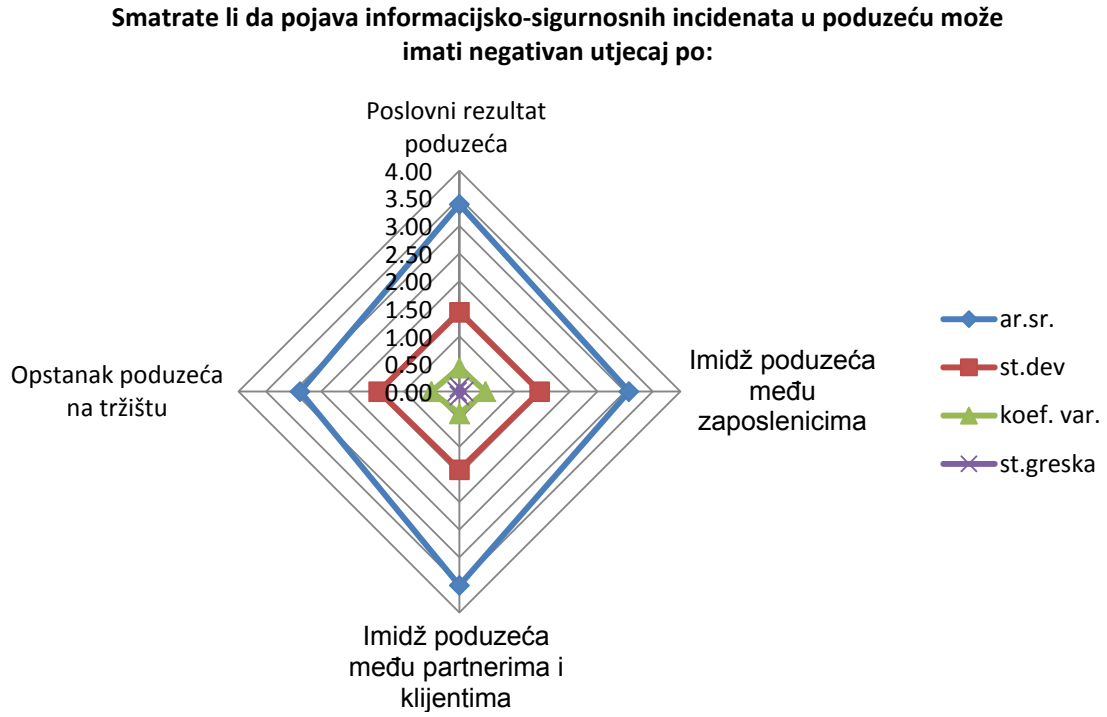
Tablica 26: Rezultati obrade obilježja vezanih uz negativni utjecaj učinaka pojave informacijsko-sigurnosnih incidenata u anketiranim poduzećima

Čimbenik	ar.sr.	st.dev	koef. var.	st.greška
Poslovni rezultat poduzeća	3.39	1.44	0.42	0.08
Imidž poduzeća među zaposlenicima	3.07	1.45	0.47	0.08
Imidž poduzeća među partnerima i klijentima	3.51	1.41	0.40	0.08
Opstanak poduzeća na tržištu	2.88	1.46	0.51	0.04
Ostalo (navedite):	-	-	-	-

Izvor: priredio autor

Radi lakšeg razumijevanja i analize, podaci iz tablice 26. grafički su prikazani na grafikonu 55. na sljedećoj stranici.

Grafikon 55: Zajednički prikaz negativnog utjecaja učinaka pojave informacijsko - sigurnosnih incidenata u anketiranih poduzećima



Izvor: priredio autor

Iz ovog grafikona je razvidno kako anketirana poduzeća smatraju čimbenik „*Imidž poduzeća među partnerima i klijentima*“ čimbenikom s najvećom važnošću (s ocjenom 3,51) dok čimbenik „*Opstanak poduzeća na tržištu*“ s ocjenom 2,88 smatraju čimbenikom s najmanjom važnošću. Standardne devijacije su vrlo ujednačene za sva četiri čimbenika i kreću se u rasponu od 1,41 do 1,46.

5.3.11. Obrada anketnih rezultata – korporativna kultura informacijske sigurnosti

Tijekom istraživanja postavljena su tri anketna pitanja kojima je izmjerena korporativna kultura informacijske sigurnosti. Radi se o pitanjima koja se tiču odnosa rukovoditelja i zaposlenih prema provođenju sigurnosnih politika, zakonskim zahtjevima po pitanju informacijske sigurnosti i poštivanju donesenih mjera informacijske sigurnosti, načinu odlučivanja o investiranju u komponente sustava upravljanja informacijskom sigurnošću i stavu rukovoditelja anketiranih poduzeća po pitanju informacijske sigurnosti.

Prvo od tih pitanja se tiče odnosa rukovoditelja i zaposlenih prema provođenju sigurnosnih politika, zakonskim zahtjevima i poštivanju donesenih mjera informacijske sigurnosti. Obrada

dobivenih rezultata pokazuje kako je srednja vrijednost izmjerenih obilježja razmjerno niska, a dobiveni rezultati su prikazani u tablici 27.

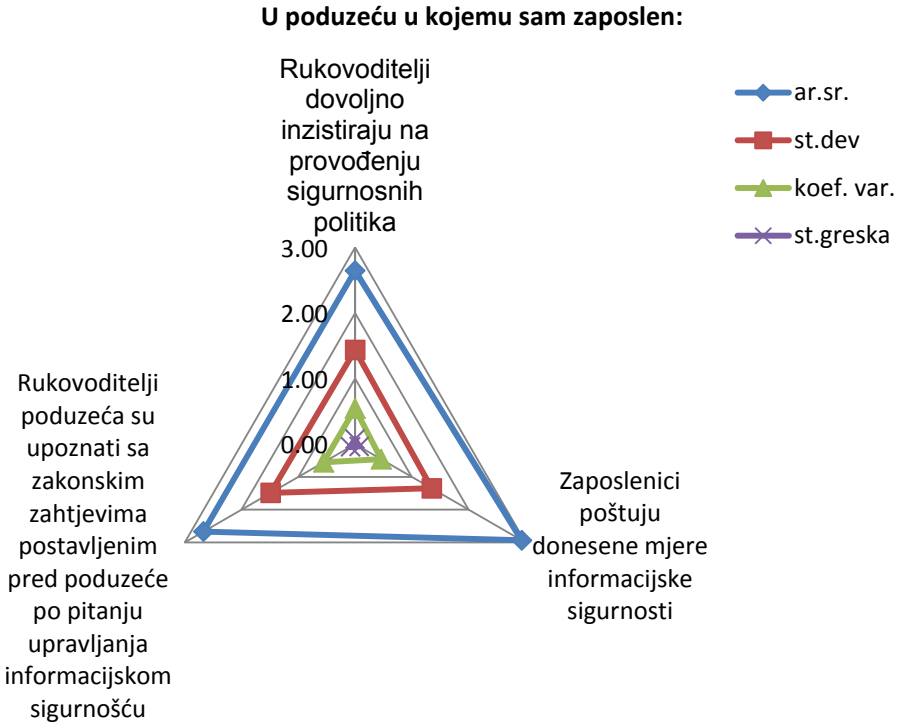
Tablica 27: Rezultati obrade obilježja vezanih uz odnos rukovoditelja i zaposlenih prema provođenju sigurnosnih politika, zakonskim zahtjevima i poštivanju donesenih mjera informacijske sigurnosti

Čimbenik	ar.sr.	st.dev	koef. var.	st.greška
Rukovoditelji dovoljno inzistiraju na provođenju sigurnosnih politika	2.65	1.44	0.54	0.08
Zaposlenici poštuju donesene mjere informacijske sigurnosti	2.94	1.35	0.46	0.07
Rukovoditelji poduzeća su upoznati sa zakonskim zahtjevima postavljenim pred poduzeće po pitanju upravljanja informacijskom sigurnošću	2.67	1.49	0.56	0.08

Izvor: priredio autor

Rezultati ove obrade prikazani su zajednički radi lakšeg razumijevanja na grafikonu 56.

Grafikon 56: Zajednički prikaz odnosa rukovoditelja i zaposlenih prema provođenju sigurnosnih politika, zakonskim zahtjevima po pitanju informacijske sigurnosti i poštivanju donesenih mjera informacijske sigurnosti u anketiranim poduzećima



Izvor: priredio autor

Najvišom prosječnom ocjenom, 2,94, ocijenjen je čimbenik *„Zaposlenici poštuju donesene mjere informacijske sigurnosti"*, a najnižom ocjenom, 2,65, čimbenik „*Rukovoditelji dovoljno inzistiraju na provođenju sigurnosnih politika*". Standardna devijacija je kao i kod prethodnog pitanja u vrlo uskom rasponu od 1,35 do 1,44.

Sljedeće pitanje odnosi se na način odlučivanja o investiranju u komponente sustava upravljanja informacijskom sigurnošću a rezultati dobiveni odgovaranjem anketiranih poduzeća na ovo pitanje prikazani su u tablici 28.

Tablica 28: Rezultati obrade obilježja vezanih uz način odlučivanja o investiranju u komponente sustava upravljanja informacijskom sigurnošću

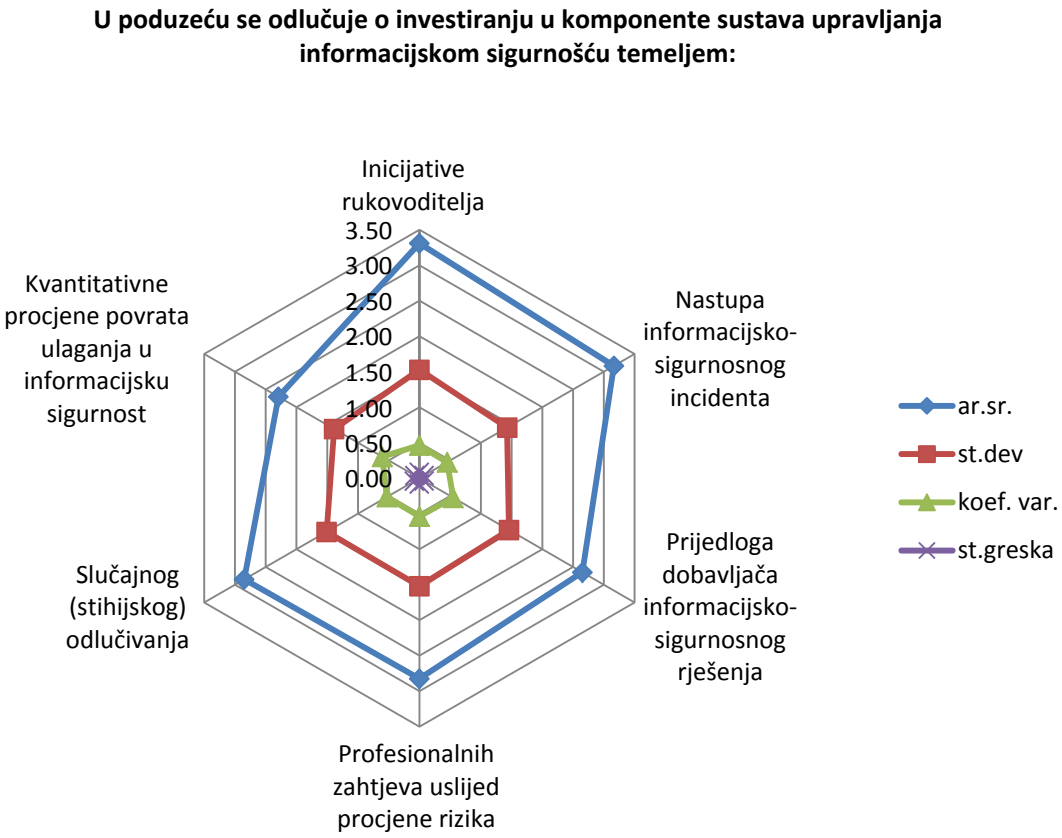
Čimbenik	**ar.sr.**	**st.dev**	**koef. var.**	**st.greška**
Inicijative rukovoditelja	3.31	1.53	0.46	0.08
Nastupa informacijsko-sigurnosnog incidenta	3.16	1.43	0.45	0.08
Prijedloga dobavljača informacijsko-sigurnosnog rješenja	2.65	1.46	0.55	0.08
Profesionalnih zahtjeva uslijed procjene rizika	2.82	1.52	0.54	0.08
Slučajnog (stihijskog) odlučivanja	2.85	1.51	0.53	0.08
Kvantitativne procjene povrata ulaganja u informacijsku sigurnost	2.29	1.39	0.60	0.07

Izvor: priredio autor

Prema dobivenim rezultatima, najvišom ocjenom, 3,31, ocijenjeno je obilježje „*Temeljem inicijative rukovoditelja*" a najnižom ocjenom, samo 2,29, ocijenjeno je obilježje „*Temeljem kvantitativne procjene povrata ulaganja u informacijsku sigurnost*". Ovakvi rezultati nisu neočekivani i podupiru postavljenu hipotezu kako je odlučivanje o investiranju u sustav informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj stihijsko i neutemeljeno, kako po pitanju strukovnih i operativnih mjera, tako i po pitanju ekonomski održivih ulaganja u informacijsku sigurnost. Standardna devijacija odgovora na ova pitanja najniža je za čimbenik „*Temeljem kvantitativne procjene povrata ulaganja u informacijsku sigurnost*" i iznosi 1,39, dok je najviša za čimbenik „*Temeljem inicijative rukovoditelja*" i iznosi 1,53.

Navedeni su dobiveni rezultati skupno prikazani na grafikonu 57. na sljedećoj stranici Zanimljiva je činjenica kako anketirana poduzeća smatraju, uz srednju ocjenu 2,85, kako njihovo odlučivanje o investicijama u komponente sustava upravljanja informacijskom sigurnošću nije stihijsko, dok većina ostalih čimbenika ukazuje kako je provođenje te poslovne aktivnosti s visokim stupnjem značajnosti nesustavno.

Grafikon 57: Zajednički prikaz načina odlučivanja o investiranju u komponente sustava upravljanja informacijskom sigurnošću u anketiranim poduzećima



Izvor: priredio autor

Posljednje obilježje koje je istraženo u okviru razmatranja dostignute razine korporativne kulture upravljanja informacijskom sigurnošću je ono vezano uz način odlučivanja o investiranju u komponente sustava upravljanja informacijskom sigurnošću. Korištenjem iste metodologije izmjereno je šest čimbenika. Rezultati dobiveni anketnim istraživanjem prikazani su u tablici 29.

Tablica 29: Rezultati obrade obilježja vezanih uz način odlučivanja o investiranju u komponente sustava upravljanja informacijskom sigurnošću

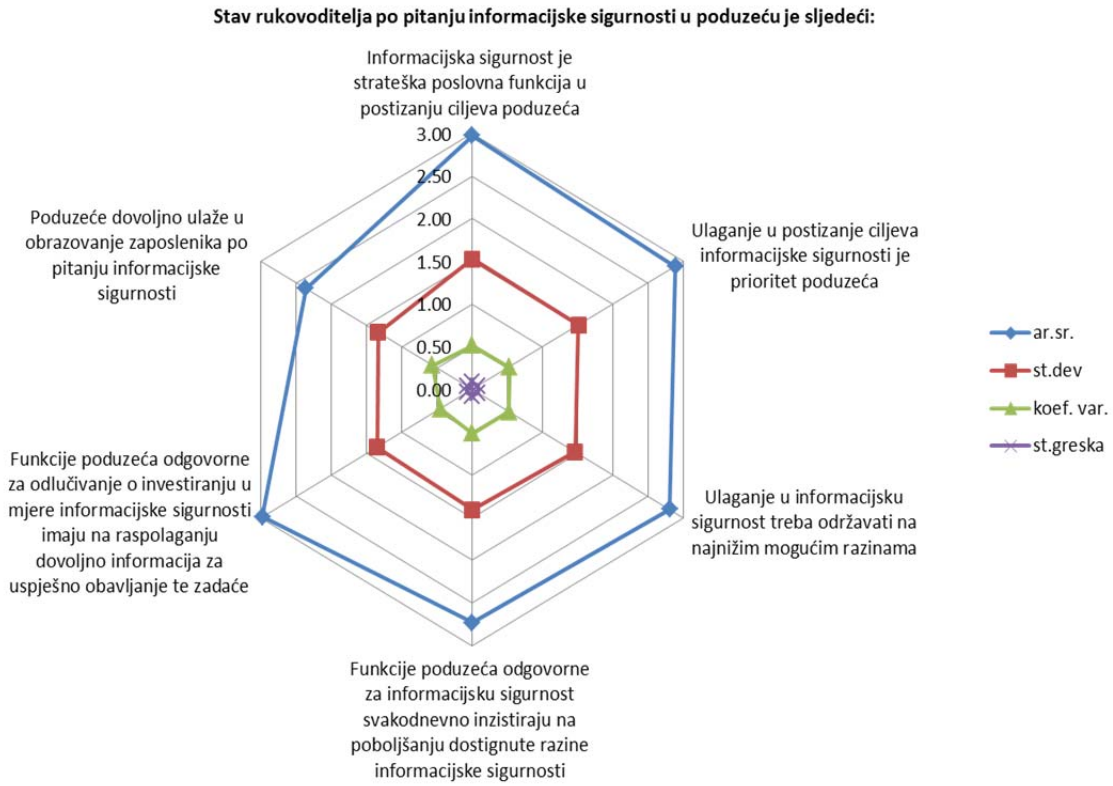
Čimbenik	**ar.sr.**	**st.dev**	**koef. var.**	**st.greška**
Informacijska sigurnost je strateška poslovna funkcija u postizanju ciljeva poduzeća	2.97	1.53	0.51	0.08
Ulaganje u postizanje ciljeva informacijske sigurnosti je prioritet poduzeća	2.88	1.51	0.52	0.08
Ulaganje u informacijsku sigurnost treba održavati na najnižim mogućim razinama	2.80	1.46	0.52	0.08
Funkcije poduzeća odgovorne za informacijsku sigurnost svakodnevno inzistiraju na poboljšanju dostignute razine informacijske sigurnosti	2.73	1.41	0.52	0.08

Funkcije poduzeća odgovorne za odlučivanje o investiranju u mjere informacijske sigurnosti imaju na raspolaganju dovoljno informacija za uspješno obavljanje te zadaće	2.98	1.35	0.45	0.07
Poduzeće dovoljno ulaže u obrazovanje zaposlenika po pitanju informacijske sigurnosti	2.36	1.34	0.57	0.07

Izvor: priredio autor

Radi lakšeg razumijevanja, rezultati iz tablice 58. prikazani su zajednički na grafikonu 58. Čimbenik „*Poduzeće dovoljno ulaže u obrazovanje zaposlenika po pitanju informacijske sigurnosti*“ anketirana mala i srednja poduzeća smatraju čimbenikom koje je najslabije ocijenjeno, prosječnom ocjenom 2,36. Najbolje su ocijenjeni čimbenici *„Informacijska sigurnost je strateška poslovna funkcija u postizanju ciljeva poduzeća*“ i *„Funkcije poduzeća odgovorne za odlučivanje o investiranju u mjere informacijske sigurnosti imaju na raspolaganju dovoljno informacija za uspješno obavljanje te zadaće*“, i to ocjenama 2,97, odnosno 2,98.

Grafikon 58: Zajednički prikaz čimbenika stava rukovoditelja anketiranih poduzeća po pitanju informacijske sigurnosti



Izvor: priredio autor

Najnižu standardnu devijaciju ima čimbenik **„***Poduzeće dovoljno ulaže u obrazovanje zaposlenika po pitanju informacijske sigurnosti*“, dok najvišu standardnu devijaciju ima čimbenik *„Informacijska sigurnost je strateška poslovna funkcija u postizanju ciljeva poduzeća*“, a one se kreću u rasponu od 1,34 do 1,53.

6. KVANTIFICIRANJE MODELA UPRAVLJANJA SUSTAVOM INFORMACIJSKE SIGURNOSTI U MALIM I SREDNJIM PODUZEĆIMA

6.1. Metodologija i korišteni postupci

Istraživanje je usmjereno ka određivanju **modela funkcionalnosti upravljanja**[201] poslovnom funkcijom informacijske sigurnosti u malim i srednjim poduzećima, te je stoga u nastavku istraživanja trebalo od svih izmjerenih varijabli identificirati one koje su od utjecaja na ukupnu funkcionalnost modela i izmjeriti kolika je snaga tog utjecaja. Ocijenjeno je kako je u tu svrhu pogodna statističko-ekonometrijska metoda regresijske analize kojom će se procijeniti odnos između varijabli. Fokus istraživanja će biti na procjeni utjecaja različitih varijabli izmjerenih tijekom provedenog istraživanja na dvije zavisne varijable, a to su u kontekstu ovog rada:

1. Y_1: **Dostignuta ukupna razina funkcionalnosti modela** upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, za koju se u pripremama za istraživanje pretpostavilo kako ovisi o pet zavisnih varijabli:
    - X_1: Mjera zrelosti funkcije operativnog upravljanja IS[202],
    - X_2: Mjera dostignute razine poštivanja zakonskih propisa, politika i najboljih standarda IS,
    - X_3: Mjera uključenosti i posvećenosti rukovodstva poduzeća postizanju strateških ciljeva informacijske sigurnosti,
    - X_4: Mjera percepcije posljedica nastupa informacijsko-sigurnosnih incidenata u poduzeću po imidž i poslovni rezultat poduzeća, i
    - X_5: Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja IS.

    Dakle, postavljena je hipoteza: $H0$: $Y_1 = f(X_1, X_2 \dots X_5)$.
2. Y_2: **Dostignuta razina strateškog upravljanja informacijskom sigurnošću** za koju se inicijalno pretpostavilo kako ovisi o sljedećim izmjerenim zavisnim varijablama[203]:
    - X_1: Uveden sustav praćenja zakonskih zahtjeva,
    - X_2: Uspostavljen sustav upravljanja IS,
    - X_3: Uveden sustav operativnih mjera IS,
    - X_4: Korištenje kvantitativnih metoda pri odlučivanju,
    - X_5: Uveden skup operativnih procedura pri provođenju IS, i

[201] Viša razina izmjerene funkcionalnosti ovako postavljenog modela direktno ukazuje na višu razinu zrelosti poslovne funkcije upravljanja informacijskom sigurnošću u malim i srednjim poduzećima.
[202] IS je kratica od *„informacijska sigurnost“* ili eng. *„information security“*.
[203] U konkretnom slučaju, sve navedene varijable su dihotomne ili binarne varijable , odnosno prediktori.

- X_6: Posjedovanje ISO 9001 certifikata.

Prema tome, postavljena je **hipoteza:** $H0$: $Y_2 = f(X_1, X_2 \dots X_6)$

6.2. Regresijska analiza zavisne varijable Y:„Dostignuta ukupna razina funkcionalnosti (zrelosti) modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj“

Ovo poglavlje izlaže se u pet međusobno povezanih cjelina**: 1) Nezavisne varijable, 2) Svojstva nezavisnih varijabli, 3) Korelacijska analiza, 4) Analiza varijance** i **5) Svojstva regresijske jednadžbe za zavisnu varijablu Y1: „Dostignuta ukupna razina funkcionalnosti (zrelosti) modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj“.**

6.2.1. Nezavisne varijable

Tijekom provođenja ove regresijske analize, inicijalno su konstruirane zavisne varijable $X_1, X_2 \dots X_5$. Zavisne varijable konstruirane su kao jednostavna aritmetička sredina sljedećih izmjerenih varijabli s obilježjima na ljestvici poput Likertove[204]:

- X_1: **Mjera zrelosti funkcije operativnog upravljanja informacijskom sigurnošću**, konstruirana kao aritmetička sredina obilježja: „*Reaktivnim rješavanjem posljedica informacijsko sigurnosnih incidenata“, „Osobnom inicijativom zaposlenika“, „Direktnim mjerama upravljanja od strane rukovoditelja-vlasnika“, „Aktivnostima odjela informatičke podrške“, „Putem osobe imenovane za upravljanje informacijskom sigurnošću“, „Aktivnostima odjela za informacijsku sigurnost“ i „Planiranjem mjera informacijske sigurnosti na godišnjoj razini“,*
- X_2: **Mjera dostignute razine poštivanja zakonskih propisa, politika i najboljih standarda informacijske sigurnosti**, konstruirana kao aritmetička sredina obilježja: *„Rukovoditelji dovoljno inzistiraju na provođenju sigurnosnih politika“, „Zaposlenici poštuju donesene mjere informacijske sigurnosti“ i „Rukovoditelji poduzeća su upoznati sa zakonskim zahtjevima postavljenim pred poduzeće po pitanju upravljanja informacijskom sigurnošću“,*
- X_3: **Mjera uključenosti i posvećenosti rukovodstva poduzeća postizanju strateških ciljeva informacijske sigurnosti**, konstruirana kao aritmetička sredina

[204] *Rensis Likert* (1903.-1981.) bio je američki organizacijski psiholog koji se bavio istraživanjem stilova upravljanja te jeautor Likertove ljestvice, izvorno psihometrijske ljestvice koja se često koristi u anketnim istraživanjima.

obilježja: *„(temeljem) Inicijative rukovoditelja“ ,“(temeljem) Nastupa informacijsko-sigurnosnog incidenta“, „(temeljem) Prijedloga dobavljača informacijsko-sigurnosnog rješenja“, „(temeljem) Profesionalnih zahtjeva uslijed procjene rizika“, „(temeljem) slučajnog (stihijskog), odlučivanja“, „(temeljem) Kvantitativne procjene povrata ulaganja u informacijsku sigurnost“,*

- X_4: **Mjera percepcije posljedica nastupa informacijsko-sigurnosnih incidenata u poduzeću na imidž i poslovni rezultat poduzeća** konstruirana kao aritmetička sredina obilježja: *„(negativni utjecaj na) Poslovni rezultat poduzeća“, „(negativni utjecaj na) Imidž poduzeća među zaposlenicima“, „(negativni utjecaj na) Imidž poduzeća među partnerima i klijentima“, „(negativni utjecaj na) Opstanak poduzeća na tržištu“,*
- X_5: **Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja informacijskom sigurnošću** konstruirana kao aritmetička sredina ocjene obilježja: *„Informacijska sigurnost je strateška poslovna funkcija u postizanju ciljeva poduzeća“, „Ulaganje u postizanje ciljeva informacijske sigurnosti je prioritet poduzeća“, „Ulaganje u informacijsku sigurnost treba održavati na najnižim mogućim razinama“, „Funkcije poduzeća odgovorne za informacijsku sigurnost svakodnevno inzistiraju na poboljšanju dostignute razine informacijske sigurnosti“, „Funkcije poduzeća odgovorne za odlučivanje o investiranju u mjere informacijske sigurnosti imaju na raspolaganju dovoljno informacija za uspješno obavljanje te zadaće“ i „Poduzeće dovoljno ulaže u obrazovanje zaposlenika po pitanju informacijske sigurnosti.“.*

6.2.2. Svojstva nezavisnih varijabli

Metodološki je radi ispravnog određivanja korištenih statističkih metoda potrebno inicijalno odrediti kakva su svojstva izdvojenih varijabli, a osobito radi li se o varijablama koje su normalno distribuirane ili ne. Temeljni razlog ovome je činjenica kako je u slučaju da su varijable distribuirane na drugi način osim normalne distribucije, potrebno koristiti neparametrijske metode i testove čija temeljna postavka nije određena distribucija podataka. Izračunata svojstva zavisnih izdvojenih varijabli $X_1, X_2 \dots X_5$ s obzirom na normalnost distribucije prikazuje tablica 30.

Tablica 30: Ispitivanje normalnosti distribucije nezavisnih varijabli $X_1, X_2 \dots X_5$

Varijabla	Kurtoza	Pomak	Signifikantnost Kolmogorov-Smirnov testa	Signifikantnost Shapiro-Wilk testa
Mjera zrelosti funkcije operativnog upravljanja informacijskom sigurnošću (X_1)	0.233	0.572	0	0.001

Mjera dostignute razine poštivanja zakonskih propisa, politika i najboljih standarda informacijske sigurnosti (X_2)	-0.436	0.261	0	0
Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja informacijskom sigurnošću (X_3)	0.71	0.198	0	0
Mjera uključenosti i posvećenosti rukovodstva poduzeća postizanju strateških ciljeva informacijske sigurnosti (X_4)	-0.29	0.226	0.001	0.001
Mjera percepcije posljedica nastupa informacijsko-sigurnosnih incidenata u poduzeću na imidž i poslovni rezultat poduzeća (X_5)	-0.495	-0.299	0	0
Trošak obrazovanja za IS u 2012.	59.069	7.645	0	0
Broj incidenata IS u 2012.	12.004	3.066	0	0
Ukupna razina funkcionalnosti upravljanja informacijskom sigurnošću **(Y)**	0.839	1	0	0

Izvor: priredio autor

Pri analizi normalnosti distribucije valja ocijeniti dva parametra, a to su kurtoza i pomak. "*Savršena"* normalna distribucija imala bi vrijednosti kurtoze i pomaka jednake nuli. Varijabla koja je pozitivno pomaknuta, ima nepripadajuće članove grupe s desne strane mjere sredine, odnosno distribucija je pomaknuta udesno. S druge strane, kurtoza ispituje horizontalni pomak od savršene, zvonolike normalne distribucije. Varijabla koja iskazuje pozitivnu kurtozu[205] ima povišeno zvono distribucije u odnosu na normalnu, dok je varijabla koja iskazuje negativnu kurtozu[206] je previše "*niska*" u odnosu na zvono normalne distribucije.

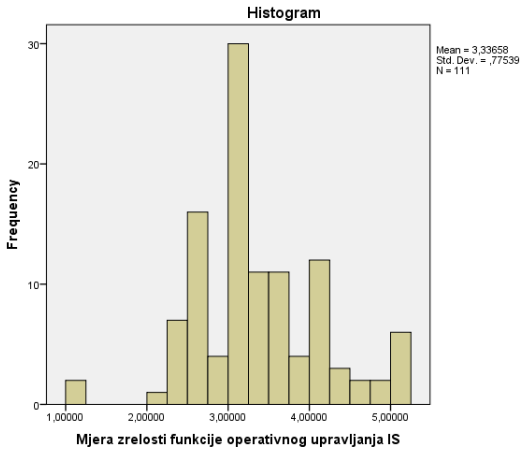
Postoji više načina na koje je moguće procijeniti uz odgovarajući interval pouzdanosti je li distribucija neke varijable normalna ili nije. Prva bi bila zbrajanje i oduzimanje izračunatih vrijednosti kurtoze i pomaka sa izračunatim standardnim greškama, te ukoliko se vrijednost nula nalazi unutar oba intervala, na toj razini pouzdanosti može se ustvrditi kako je distribucija varijable normalna. Druga mogućnost je korištenje specijaliziranih testova, za što se najčešće koriste dva testa, Kolmogorov-Smirnov test[207] i Shapiro-Wilk test, za koji postoji preporuka da se koristi kada je broj opažanja manji od 50. Izračunate vrijednosti signifikantnosti Kolmogorov-Smirnov i Shapiro-Wilkes testa u svim slučajevima su manje od 0,05 te se stoga s 95 % pouzdanosti može ustanoviti kako niti jedna od varijabli prikazanih u tablici 30. nije normalno distribuirana.

Kao što je već i prije istaknuto, osobiti otklon od normalne distribucije pokazuju varijable "*Trošak obrazovanja za informacijsku sigurnost u 2012*." i "*Broj incidenata informacijske sigurnosti u 2012*.".

[205] Ili leptokurtozna varijabla
[206] Ili platikurtozna varijabla
[207] Kolmogorov-Smirnov test kraći je naziv za *„Kolmogorov-Smirnov-Lilliefors test normalnosti"*.

Ovaj se zaključak može provjeriti i vizualnim prikazom histograma frekvencija determiniranih varijabli, što se čini u nastavku. Na grafikonu 59. se vidi kako distribucija varijable X_1: "*Mjera zrelosti funkcije operativnog upravljanja informacijskom sigurnošću*" ne korespondira s normalnom i prisutan je značajan pomak distribucije u desno (pozitivan pomak) te iskazuje leptokurtozu u odnosu na normalnu distribuciju.

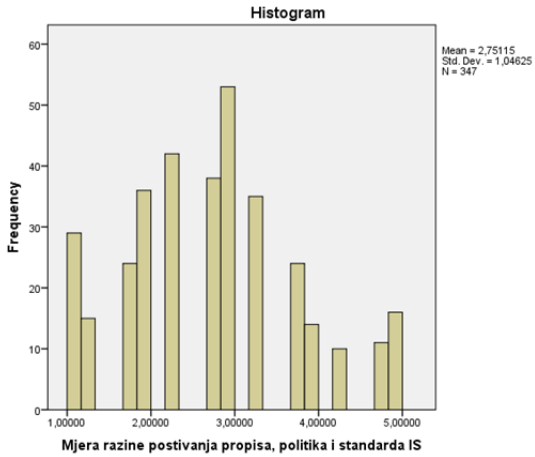
Grafikon 59: Histogram frekvencija varijable X_1: "Mjera zrelosti funkcije operativnog upravljanja informacijskom sigurnošću"



Izvor: priredio autor

Na grafikonu 60. prikazuje se distribucija varijable X_2: "*Mjera dostignute razine poštivanja zakonskih propisa, politika i najboljih standarda informacijske sigurnosti*". Ova distribucija također pokazuje pozitivan pomak, ali je platikurtozna.

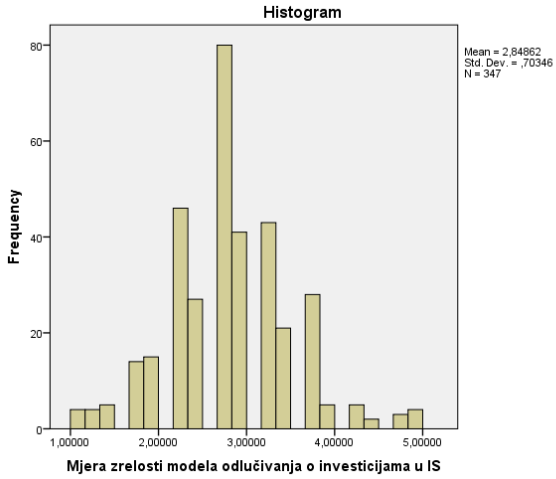
Grafikon 60: Histogram frekvencija varijable X_2: "Mjera dostignute razine poštivanja zakonskih propisa, politika i najboljih standarda informacijske sigurnosti"



Izvor: priredio autor

Na grafikonu 61. prikazana je distribucija frekvencija varijable X_3: "*Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja informacijskom sigurnošću*". Ova varijabla je leptokurtozna i pokazuje pozitivan pomak.

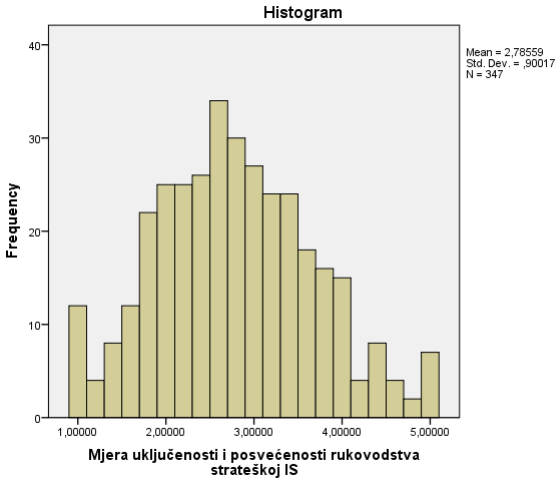
Grafikon 61: Histogram frekvencija varijable X_3: "Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja informacijskom sigurnošću"



Izvor: priredio autor

Distribucija frekvencija varijable X_4: "*Mjera uključenosti i posvećenosti rukovodstva poduzeća postizanju strateških ciljeva informacijske sigurnosti*" prikazana je na grafikonu 62. Ova distribucija pokazuje karakteristike platikurtoze i pozitivnog pomaka.

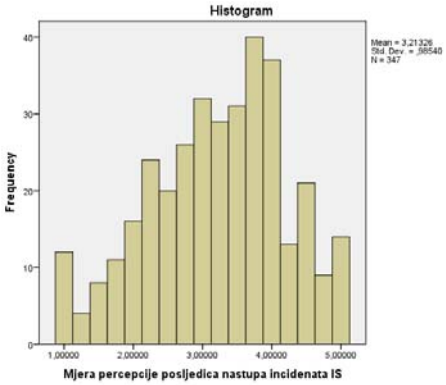
Grafikon 62: Histogram frekvencija varijable X_4: "Mjera uključenosti i posvećenosti rukovodstva poduzeća postizanju strateških ciljeva informacijske sigurnosti"



Izvor: priredio autor

Distribucija frekvencija varijable X_5: "*Mjera percepcije posljedica nastupa informacijsko-sigurnosnih incidenata u poduzeću na imidž i poslovni rezultat poduzeća*" prikazana je na grafikonu 63. Iz ove distribucije vizualno je razvidno kako pokazuje karakteristike platikurtoze i negativnog pomaka.

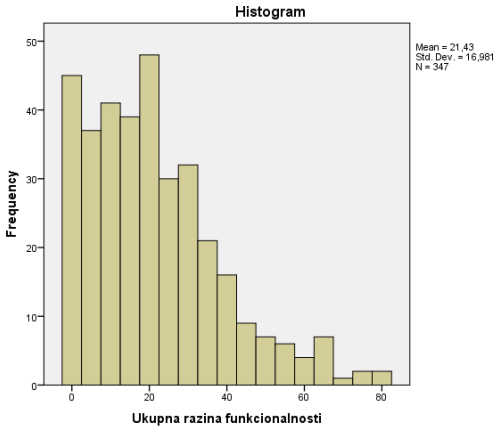
Grafikon 63: Histogram frekvencija varijable X_5: "Mjera percepcije posljedica nastupa informacijsko-sigurnosnih incidenata u poduzeću na imidž i poslovni rezultat poduzeća"



Izvor: priredio autor

Distribucija zavisne varijable *Y*: "*Ukupna razina funkcionalnosti upravljanja informacijskom sigurnošću*" pokazuje karakteristike jake leptokurtoze i pomaka u desnu stranu. Ova činjenica može se provjeriti vizualnim pregledom histograma frekvencija prikazanih na grafikonu 64.

Grafikon 64: Histogram frekvencija varijable Y: "Ukupna razina funkcionalnosti upravljanja informacijskom sigurnošću"

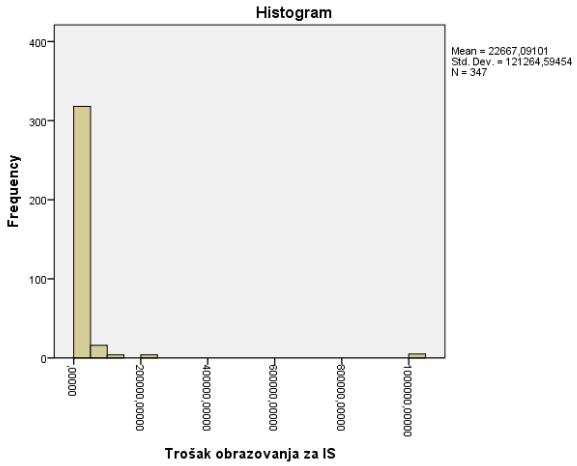


Izvor: priredio autor

Izrazita leptokurtoza i pozitivan pomak vide se kod distribucije varijable "*Trošak obrazovanja za informacijsku sigurnost u 2012. godini*" koja zasigurno nije normalno distribuirana i ima

izražene nepripadajuće članove grupe. Ova je činjenica prikazana histogramom frekvencija na grafikonu 65.

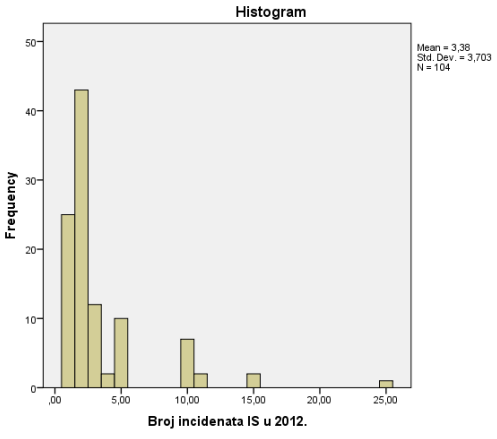
Grafikon 65: Histogram frekvencija varijable Y: "Ukupna razina funkcionalnosti upravljanja informacijskom sigurnošću"



Izvor: priredio autor

Analiza svojstava normalnosti varijabli od interesa za istraživanje završava grafikonom 66. na kojemu su prikazana slična svojstva varijable "*Broj incidenata informacijske sigurnosti u 2012. godini*" kao i kod prethodne varijable, te je stoga jasno kako niti ta varijabla nema normalnu distribuciju.

Grafikon 66: Histogram frekvencija varijable "Broj incidenata informacijske sigurnosti u 2012. godini"



Izvor: priredio autor

Ovime je u potpunosti pokazano korištenjem odgovarajućih izračuna pomaka, kurtoze i testova te vizualnom provjerom kako sve navedene varijable iz tablice 30. nisu normalno distribuirane, te je time opravdano dalje korištenje neparametrijskih metoda u statističkoj analizi.

6.2.3. Korelacijska analiza

Po određivanju nezavisnih varijabli $X_1, X_2 \dots X_5$ za koje se pretpostavlja kako će adekvatno sudjelovati u određivanju vrijednosti zavisne varijable *Y: „Ukupna razina funkcionalnosti upravljanja informacijskom sigurnošću"*, pristupilo se korelacijskoj analizi kako bi se utvrdilo postoji li korelacija između pojedinih navedenih nezavisnih varijabli. Važno je istaknuti kako će se korelacije računati kao mjera sukladnosti variranja parova varijabli čime će se provjeriti postoji li sustavan odnos među promatranim varijablama, ali se neće na osnovi korelacije direktno zaključivati o uzročno-posljedičnom odnosu među varijablama. (Rodgers & Nicewander, 1988, p. 62)

Ovako dobivene rezultate prikazuje tablica 31.

Tablica 31: Korelacijska analiza (neparametrijska, Spearman ρ) varijabli $X_1, X_2 \dots X_5$ i dvije dodatne odabrane varijable[208]

Correlations

			Mjera zrelosti funkcije operativnog upravljanja IS	Mjera razine postivanja propisa, politika i standarda IS	Mjera zrelosti modela odlučivanja o investicijama u IS	Mjera uključenosti i posvećenosti rukovodstva strateškoj IS	Mjera percepcije posljedica nastupa incidenata IS	Trošak obrazovanja za IS	Broj incidenata IS u 2012.
Spearman's rho	Mjera zrelosti funkcije operativnog upravljanja IS	Correlation Coefficient	1,000	,388**	,276**	,394**	,079	,353**	-,314*
		Sig. (2-tailed)	.	,000	,003	,000	,410	,000	,045
		N	111	111	111	111	111	111	41
	Mjera razine postivanja propisa, politika i standarda IS	Correlation Coefficient	,388**	1,000	,222**	,372**	,158**	,232**	-,196*
		Sig. (2-tailed)	,000	.	,000	,000	,003	,000	,046
		N	111	347	347	347	347	347	104
	Mjera zrelosti modela odlučivanja o investicijama u IS	Correlation Coefficient	,276**	,222**	1,000	,262**	,121*	,137*	,047
		Sig. (2-tailed)	,003	,000	.	,000	,025	,011	,633
		N	111	347	347	347	347	347	104
	Mjera uključenosti i posvećenosti rukovodstva strateškoj IS	Correlation Coefficient	,394**	,372**	,262**	1,000	,212**	,246**	,031
		Sig. (2-tailed)	,000	,000	,000	.	,000	,000	,755
		N	111	347	347	347	347	347	104
	Mjera percepcije posljedica nastupa incidenata IS	Correlation Coefficient	,079	,158**	,121*	,212**	1,000	,116*	,188
		Sig. (2-tailed)	,410	,003	,025	,000	.	,031	,056
		N	111	347	347	347	347	347	104
	Trošak obrazovanja za IS	Correlation Coefficient	,353**	,232**	,137*	,246**	,116*	1,000	-,027
		Sig. (2-tailed)	,000	,000	,011	,000	,031	.	,786
		N	111	347	347	347	347	347	104
	Broj incidenata IS u 2012.	Correlation Coefficient	-,314*	-,196*	,047	,031	,188	-,027	1,000
		Sig. (2-tailed)	,045	,046	,633	,755	,056	,786	.
		N	41	104	104	104	104	104	104

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Izvor: priredio autor

U tablici 31. prikazane su ukrižene korelacijske vrijednosti koje su izračunate korištenjem neparametrijske korelacijske metode, odnosno računanjem koeficijenata Spearmanove

[208] Koeficijenti korelacija kraj kojih se nalazi jedna zvjezdica značajni su na razini 95 %, dok su oni kraj kojih se nalaze dvije zvjezdice značajni na razini 99 %.

korelacije ρ[209]. Korelacije se računaju korištenjem razdiobe s dva kraja[210]. Crvenom bojom označene su oni koeficijenti korelacija koji su značajni bilo na razini 95 % ili na razini 99 %.

Pri interpretiranju dobivenih rezultata valja uzeti u razmatranje činjenicu kako je ovakav izračun koeficijenata korelacija ukrižen te zrcalan, odnosno podaci iznad zamišljene dijagonale su zrcalna slika onih podataka ispod nje, te je stoga dovoljno interpretirati podatke koji se nalaze ispod zamišljene dijagonale tablice. Pri interpretaciji rezultata bit će korištena skala prema Petzu (Petz, 2002, p. 211) koja je osobito prilagođena korištenju kod društvenih znanosti. Obilježja ove skale prikazana su u tablici 32.

Tablica 32: Skala objašnjenja koeficijenata korelacije prema Petzu

Koeficijent korelacije		**Značenje**
od	**do**	
0,00	±0,20	**nikakva ili neznatna povezanost**
±0,20	0,40	**laka povezanost**
±0,40	±0,70	**značajna povezanost**
±0,70	±1,00	**visoka ili vrlo visoka povezanost**

Izvor: priredio autor

Postavlja se hipoteza H_0: r=0, odnosno da ne postoje korelacije među parovima varijabli. Korelacijskom analizom ustanovilo se kako su za istaknute kombinacije varijabli $X_1, X_2 \dots X_5$ one postojeće, odnosno hipoteza H_0 se odbacuje i za sve parove nezavisnih varijabli uzima se alternativna hipoteza H_1: r<>0 , odnosno da među parovima naznačenih varijabli postoji korelacijska povezanost i to, neznatna do laka. Savršena kolinearnost ne postoji među prediktorskim varijablama.

Zanimljivo je da kod varijabli za koje se smatra da su od interesa za istraživanje ali neće biti dijelom regresijskog modela, (a to su „*Trošak obrazovanja za informacijsku sigurnost u 2012. godini* " i „*Broj incidenata informacijske sigurnosti u 2012.*"), za varijablu „*Trošak obrazovanja za informacijsku sigurnost u 2012. godini*" valja prihvatiti hipotezu H_0, i to za korelacije parova koje čini ta varijabla te varijable $X_3, X_4 \dots X_5$ i „*Trošak obrazovanja za informacijsku sigurnost u 2012. godini*", odnosno između njih ne postoji korelacijska veza.

Izračunati su i faktori inflacije varijance[211] za sve kombinacije i varijable, te su oni za sve slučajeve manji od 2,225 što znači da između varijabli nije prisutan problem multikolinearnosti.

[209] Radi se o neparametrijskoj korelacijskoj metodi koja je bolje prilagođena korištenju kod distribucija koje ne podrazumijevaju normalnost, a što je slučaj kod nizova podataka dobivenim istraživanjem. Osim toga, Spearmanovi koeficijenti korelacije mogu se računati kod ordinalne mjerne ljestvice, malih uzoraka i ne podrazumijevaju linearnost.
[210] Često se koristi i izraz „*dva repa*".
[211] Faktor inflacije varijance (od eng. *VIF* – „*Variance Inflation Factor*") je pokazatelj koji kvantificira ozbiljnost problema multikolinearnosti u regresijskoj analizi.

Korelacijska analiza pokazuje kako se metodološki niz varijabli $X_1, X_2 \ldots X_5$ može koristiti u regresijskom modelu.

6.2.4. Analiza varijance (X_1, X_2, X_3)

Prije nastavka regresijske analize, čime će se pokušati ustanoviti povezanost između nezavisnih varijabli i zavisne varijable, valja provjeriti je li stratifikacija uzorka ispravna, odnosno je li ispravno metodološki ispitati skupinu mikro, malih i srednjih poduzeća kao jedan homogeni uzorak, ili je trebalo obaviti dodatnu stratifikaciju uzorka na način da se on podijeli na tri poduzorka koji bi se zatim razmatrali odvojeno. To će se učiniti na način da se analizom varijance utvrdi koliko se varijance u zavisnoj varijabli *Y* može objasniti pripadnošću odgovarajućoj grupi. Identificiraju se tri varijable za koje treba obaviti analizu varijance, sukladno klasifikaciji poduzeća. To su:

- X_1*: broj zaposlenih u 2012. godini,*
- X_2*: godišnji prihod u 2012. godini,*
- X_3*: iznos godišnje bilance u 2012. godini.*

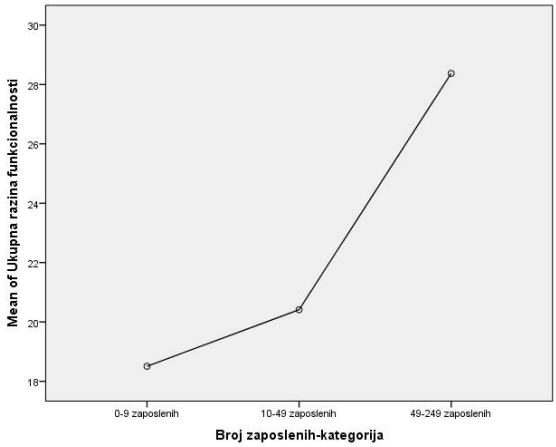
Analiza varijance obavlja se u nastavku kroz sljedeće cjeline: **1) Analiza varijance za X_1, 2) Analiza varijance za X_2 i 3) Analiza varijance za X_3.**

6.2.4.1. Analiza varijance za X_1

Kao što je prikazano, odgovor na pitanje koliko pojedino poduzeće ima zaposlenih može biti u jednoj od tri kategorije: "*0-9 zaposlenih*", "*10-49 zaposlenih*" i "*50-250 zaposlenih*". Ova vrsta odgovora ponuđena je zato jer točan broj zaposlenih nije od interesa za istraživanje, kategoriziranje na ovaj način također omogućuje adekvatnu analizu a izbjegnuta je mogućnost da ispitanici ne znaju točan broj zaposlenih u nekom trenutku pa nagađaju ili daju netočan odgovor. Postavlja se hipoteza H_0: μ1=μ2=μ3, odnosno nema razlike između varijanci ukupne razine funkcionalnosti informacijske sigurnosti u Republici Hrvatskoj po navedenim kategorijama broja zaposlenih.

Na grafikonu 67. na sljedećoj stranici na ordinati su prikazane aritmetičke sredine dostignute razine ukupne funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj, dok su na apscisi nominalne grupe broja zaposlenih.

Grafikon 67: Prikaz aritmetičkih sredina zavisne varijable Y: Ukupna razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj u odnosu na kategorijalnu varijablu X_1: broj zaposlenih



Izvor: priredio autor

Za testiranje homogenosti varijance koristi se Leveneov test. Rezultate Leveneovog testa prikazuje tablica 33. Leveneov test testira jednakost varijanci u uzorcima. Ako je izračunata p vrijednost manja od kritične, nul hipoteza se odbacuje i zaključuje da postoje razlike između varijanci u populacijama. Kao što se vidi iz rezultata prikazanih u tablici 33, varijance su homogene (p<0,001).

Tablica 33: Rezultati Leveneovog testa homogenosti varijance (kategorijalna varijabla X_1: broj zaposlenih)

Test of Homogeneity of Variances

Ukupna razina funkcionalnosti

Levene Statistic	df1	df2	Sig.
7,104	2	344	,00095

Izvor: priredio autor

Za testiranje jednakosti mjera centralne vrijednosti[212] koriste se Welch i Brown-Forsythe testovi robusnosti jednakosti. Welchov test koristi aritmetičke sredine i radi se o adaptiranom Studentovom testu dok Brown-Forsytheov test koristi medijane. Rezultate ovih testova prikazuje tablica 34. na sljedećoj stranici. Kao što je razvidno iz te tablice, oba su signifikantni na razini 99,9 % (p<0,001) te stoga valja odbaciti hipotezu H_0 i prihvatiti alternativnu hipotezu

[212] Pod mjerama centralne vrijednosti misli se na aritmetičku sredinu i medijan.

H_1: postoji razlika između aritmetičkih sredina funkcionalnosti sustava informacijske sigurnosti među nominalnim grupama.

Tablica 34: Robusni testovi jednakosti središnjih mjera varijable X_1: broj zaposlenih

Robust Tests of Equality of Means

Ukupna razina funkcionalnosti

	Statistic[a]	df1	df2	Sig.
Welch	7,480	2	178,608	,00076
Brown-Forsythe	9,005	2	225,190	,00017

a. Asymptotically F distributed.

Izvor: priredio autor

Međutim, kako bi se izmjerilo koliko od ukupnog iznosa varijance u pojavi se može objasniti pripadnošću nominalnoj grupi, pristupa se univarijatnoj analizi varijance.[213] Dobivene rezultate prikazuje tablica 35.

Tablica 35: Univarijatna analiza varijance (Anova) - kategorijalna varijabla X_1: broj zaposlenih

ANOVA

Ukupna razina funkcionalnosti

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5492,255	2	2746,127	10,021	,00006
Within Groups	94272,621	344	274,048		
Total	99764,876	346			

Izvor: priredio autor

Kako bi se procijenilo koliko varijance u ukupnoj razini funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj može objasniti pripadnošću nominalnoj grupi broja zaposlenih, računa se parcijalni Eta^2 koji iznosi 5,5 %. Ovaj izračun prikazuje tablica 36. na sljedećoj stranici.

[213] Metoda univarijatne analize varijance ili ANOVA je metoda koja razlaže zapaženu varijancu pojave na komponente koje se mogu dodijeliti pojedinim izvorima varijance. Za detalje cf. Roberts, M, Russo R..: „**A Student's Guide to Analysis of Variance“,** Routledge, London, Velika Britanija, 1999., p.234.

Tablica 36: Izračun parcijalnog Eta^2 za pripadnost nominalnoj grupi broja zaposlenih

Tests of Between-Subjects Effects

Dependent Variable: Ukupna razina funkcionalnosti

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	5492,255[a]	2	2746,127	10,021	,000	,055
Intercept	161575,173	1	161575,173	589,586	,000	,632
Brojzap	5492,255	2	2746,127	10,021	,000	,055
Error	94272,621	344	274,048			
Total	259071,000	347				
Corrected Total	99764,876	346				

a. R Squared = .055 (Adjusted R Squared = .050)

Izvor: priredio autor

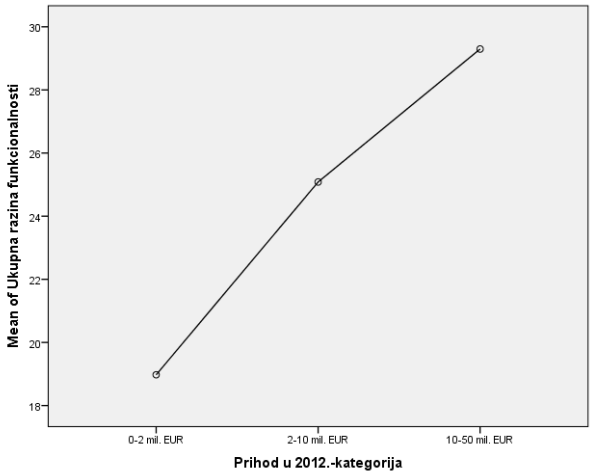
Prema tome, samo 5.5 % varijance u ukupnoj razini funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj može se objasniti pripadnošću nominalnoj grupi X_1: *broj zaposlenih*.

6.2.4.2. Analiza varijance za X_2

Slična analiza provodi se za X_2: godišnji prihod. Nominalna grupa (kategorija) prihoda može poprimiti vrijednosti „*0-2 milijuna EUR*“, „*2-10 milijuna EUR*“ i „*10-50 milijuna EUR*“. Postavlja se hipoteza H_0: μ1=μ2=μ3, odnosno da nema razlike između varijanci ukupne razine funkcionalnosti informacijske sigurnosti u Republici Hrvatskoj po navedenim prihodovnim kategorijama malih i srednjih poduzeća.

Na grafikonu 68. na sljedećoj stranici prikazane su aritmetičke sredine dostignute razine ukupne funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj (ordinata), dok su na apscisi nominalne prihodovne grupe poduzeća.

Grafikon 68: Prikaz aritmetičkih sredina zavisne varijable Y: Ukupna razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj u odnosu na kategorijalnu varijablu X_2: prihod poduzeća u 2012.



Izvor: priredio autor

Za testiranje homogenosti varijance koristi se Leveneov test.[214] Rezultate Leveneovog testa prikazuje tablica 37. Leveneov test u ovom slučaju ukazivao bi kako je prisutna homoskedastičnost varijance, odnosno da su varijance populacije nominalne grupe prihoda poduzeća u 2012. godini jednake.

Tablica 37: Rezultati Leveneovog testa homogenosti varijance (kategorijalna varijabla X_2: prihod poduzeća u 2012.)

Test of Homogeneity of Variances

Ukupna razina funkcionalnosti

Levene Statistic	df1	df2	Sig.
2,908	2	344	,05593

Izvor: priredio autor

Nadalje, budući da se Mann Whitney U-test ne može koristiti zbog tri nominalne prihodovne grupe, koristi se Kruskal-Wallis test koji je neparametrijski test koji ne podrazumijeva normalnost podataka. Izračunati Asymp.Sig. koeficijent, prikazan u tablici 38., iznosi p=0,00056 te je manji od 0,001 te stoga odbacujemo hipotezu H_0 i prihvaća se alternativna hipotezu H_1: postoji razlika između varijanci funkcionalnosti sustava informacijske sigurnosti

[214] Leveneov test testira jednakost varijanci u uzorcima. Ako je izračunata p vrijednost manja od kritične, nul hipoteza se odbacuje i zaključuje da postoje razlike između varijanci u populaciji.

unutar nominalne grupe prihoda poduzeća u 2012. godini. Izračunate vrijednosti prikazane su u tablici 38.

Tablica 38: Kruskal-Wallis test jednakosti varijance unutar nominalne grupe X_2: prihod poduzeća u 2012.

Test Statistics[a,b]

	Ukupna razina funkcionalnosti
Chi-Square	14,966
df	2
Asymp. Sig.	,00056

a. Kruskal Wallis Test

b. Grouping Variable: Prihod u 2012.-kategorija

Izvor: priredio autor

Za mjeru efekta u ukupnoj razini funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj prema pripadnosti nominalnim grupama unutar X_2: prihod poduzeća u 2012., računa se $\frac{\chi^2}{n-1}$ koji iznosi 4,3 %, što znači da se 4,3 % varijabilnosti varijance u ukupnoj razini funkcionalnosti može objasniti pripadnošću izloženim nominalnim kategorijama unutar X_2: prihod poduzeća u 2012. Zanimljivo je da se koristila univarijatna analiza a ne neparametrijski testovi, Eta^2 bio bi 5,5 % kao i kod X_1: broj zaposlenih, što prikazuje izračun prikazan u tablici 39.

Tablica 39: Primjer univarijatne analize jednakosti varijance unutar nominalne grupe X_2: prihod poduzeća u 2012.

Tests of Between-Subjects Effects

Dependent Variable: Ukupna razina funkcionalnosti

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	5458,097[a]	2	2729,049	9,955	,000	,055
Intercept	123890,049	1	123890,049	451,910	,000	,568
Prihod	5458,097	2	2729,049	9,955	,000	,055
Error	94306,779	344	274,148			
Total	259071,000	347				
Corrected Total	99764,876	346				

b. R Squared = .055 (Adjusted R Squared = .049)

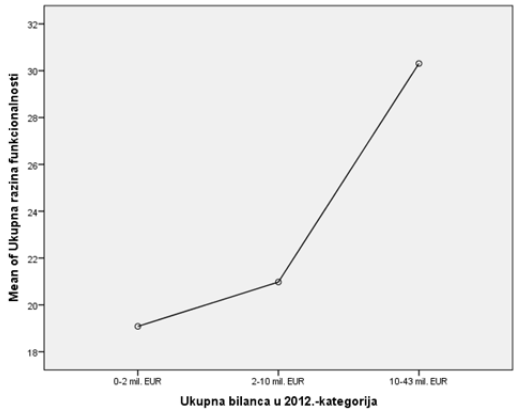
Izvor: priredio autor

6.2.4.3. Analiza varijance za X_3

Naposljetku, provodi se istovjetna analiza i za preostalu kategorijalnu varijablu, X_3*:* „*iznos godišnje bilance u 2012. godini*“. Analiza se obavlja na isti način kao i za varijablu X_2*: „prihod poduzeća u 2012“*. Postavlja se početna hipoteza H_0: μ1=μ2=μ3, odnosno nema razlike između varijanci ukupne razine funkcionalnosti informacijske sigurnosti u Republici Hrvatskoj po navedenim kategorijama iznosa godišnje bilance[215] malih i srednjih poduzeća.

Na grafikonu 69. na ordinati su prikazane aritmetičke sredine dostignute razine ukupne funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj, dok su na apscisu smještene nominalne grupe malih i srednjih poduzeća sukladno iznosu godišnje bilance. Kao i u zakonskoj klasifikaciji malih i srednjih poduzeća, koriste se rasponi godišnjeg iznosa bilance od „*0-2 milijuna EUR*“, „*2-10 milijuna EUR*“ i „*10-43 milijuna EUR*“.

Grafikon 69: Prikaz aritmetičkih sredina zavisne varijable Y: Ukupna razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj u odnosu na kategorijalnu varijablu X_3: iznos godišnje bilance u 2012. godini



Izvor: priredio autor

I u ovom slučaj za testiranje homogenosti varijance koristi se Leveneov test. Rezultate Leveneovog testa prikazuje tablica 40. na sljedećoj stranici. Leveneov test u ovom slučaju također bi ukazivao bi kako je prisutna homoskedastičnost varijance, odnosno da su varijance populacije nominalnih grupa iznosa bilanci poduzeća u 2012. godini jednake.

[215] Aktive, odnosno pasive bilance.

Tablica 40: Rezultati Leveneovog testa homogenosti varijance (kategorijalna varijabla X_3: iznos godišnje bilance u 2012. godini)

Test of Homogeneity of Variances

Ukupna razina funkcionalnosti

Levene Statistic	df1	df2	Sig.
2,327	2	344	,09917

Izvor: priredio autor

Nastavlja se s analizom Kruskal-Wallis testom koji ne podrazumijeva normalnost podataka. Izračunati pokazatelj označen s "*Asymp.Sig.*" u tablici 41 manji je od 0,001 (p<0,001) te se stoga odbacuje inicijalna hipoteza H_0 a prihvaća se alternativna hipoteza H_1: postoji razlika između varijanci funkcionalnosti sustava informacijske sigurnosti među nominalnim grupama godišnje bilance u 2012. godini.

Tablica 41: Kruskal-Wallis test jednakosti varijance unutar nominalne grupe X_3: iznos godišnje bilance u 2012. godini

Test Statistics[a,b]

	Ukupna razina funkcionalnosti
Chi-Square	19,382
df	2
Asymp. Sig.	,000

a. Kruskal Wallis Test

b. Grouping Variable: Ukupna bilanca u 2012.-kategorija

Izvor: priredio autor

Potrebno je izračunati i mjeru ovog efekta koja se računa kao $\frac{\chi^2}{n-1}$=5,6 % varijabilnosti koja se može objasniti pripadnošću prihodovnim kategorijama. Da se koristila obična univarijatna analiza a ne neparametrijski Kruskal-Wallis test, Eta^2 bio bi 6,5 %, što prikazuje tablica 42. na sljedećoj stranici. Prema tome, razlika između korištenja univarijatne analize i neparametrijskog testa vrlo je mala, no bolje je i ispravnije u zadanim okolnostima koristiti neparametrijski test koji nema pretpostavku normalnosti po pitanju inicijalne distribucije podataka.

Tablica 42: Primjer univarijatne analize jednakosti varijance unutar nominalne grupe X_3: iznos godišnje bilance u 2012. godini

Tests of Between-Subjects Effects

Dependent Variable: Ukupna razina funkcionalnosti

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	6441,733[a]	2	3220,867	11,872	,000	,065
Intercept	117026,195	1	117026,195	431,372	,000	,556
Bilanca	6441,733	2	3220,867	11,872	,000	,065
Error	93323,143	344	271,288			
Total	259071,000	347				
Corrected Total	99764,876	346				

a. R Squared = .065 (Adjusted R Squared = .059)

Izvor: priredio autor

Iz navedene kompleksne analize varijance nominalnih kategorija unutar varijabli $\{X_1, X_2, X_3\}$ može se zaključiti kako je statistički dokazano da se svega 5,5 % – 6,5 % varijance može pripisati pripadnošću nominalnim kategorijama unutar navedenih varijabli te je **promatranje statističkog uzorka malih i srednjih poduzeća kao homogenog, bez korištenja dodatne stratifikacije uzorka opravdano**. Naime, kao što je već rečeno, u samom početku izrade dizajna istraživanja, pojavio se problem kompleksnosti stratifikacije uzroka te je kalkulirani rizik istraživanja bilo adaptiranje metode kod koje se uzorak promatra homogenim, a iskustveni razlog za takvo iniciranje anketnog istraživanja bilo je prijašnje iskustvo autora, prema kojemu je subjektivna dostignuta razina zrelosti modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj podjednaka. Kada bi veća količina varijance bila objašnjena pripadnošću nominalnim grupama, tada bi trebalo izraditi stratifikaciju statističkog uzorka na drugi način. Budući da osobno iskustvo predstavlja nižu razinu dokazivanja, na ovaj je način i korištenjem statističkih i kvantitativnih metoda opravdan početni dizajn istraživanja.

6.2.5. Svojstva regresijske jednadžbe za zavisnu varijablu Y1: „Dostignuta ukupna razina funkcionalnosti (zrelosti) modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj“

U izradi regresijskog modela korištena je opcija "*Enter*" statističkog paketa *SPSS*[216]. To znači da se sve nezavisne varijable uključuju u regresijsku jednadžbu prvom koraku analize. Iako se to ne očekuje budući da ne postoji problem multikolinearnosti te da su korelacije među nezavisnim varijablama neznatne do niske, izrađuje se nekoliko preliminarnih jednostavnih linearnih regresijskih modela gdje se u model unosi samo po jedna od identificiranih nezavisnih varijabli. Rezultati dobiveni ovom analizom prikazani su u tablici 43. Kao što se vidi prema izračunatim koeficijentima determinacije (R^2), niti jedna od nezavisnih varijabli sama za sebe ne objašnjava dovoljno dobro odnos prema zavisnoj varijabli jer bi tako postavljeni model s determiniranim varijablama objasnio od 4,9 % do 32,4 % ukupne varijance.

Tablica 43: Regresijska analiza odabranih nezavisnih varijabli u odnosu na zavisnu varijablu (ukupna razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj)

Nezavisna varijabla	R^2 (koeficijent determinacije)	Koeficijent B	Sig.
Mjera zrelosti funkcije operativnog upravljanja informacijskom sigurnošću	0.324	14.626	0
Mjera razine poštivanja propisa, politika i standarda informacijske sigurnosti	0.182	6.931	0
Mjera zrelosti modela odlučivanja o investicijama u informacijsku sigurnost	0.115	7.403	0
Mjera uključenosti i posvećenosti rukovodstva strateškoj informacijskoj sigurnosti	0.2	8.439	0
Mjera percepcije posljedica nastupa incidenata informacijske sigurnosti	0.049	3.821	0

Izvor: priredio autor

Iz navedenog je jasno kako je ovisnost između zavisne i nezavisnih varijabli kompleksna i da se ne radi o funkciji kod koje bi samo jedna nezavisna varijabla mogla objasniti zavisnu varijablu. Pri izgradnji modela razmatrana su četiri oblika mogućih regresijskih funkcija.[217] Korištenjem paketa *SPSS* je ustanovljeno kako je najbolji model koji objašnjava odnos nezavisnih i zavisne varijable linearna funkcija. Ova je činjenica dodatno pojačana uvriježenim pravilom regresijske

[216] SPSS Statistics je računalni program proizvođača IBM koji se koristi za statističku analizu. Zadnja važeća inačica je 22.0. Za detalje cf. IBM Sofware>SPSS Software, **http://www-01.ibm.com/software/analytics/spss/** (23.08.2013.)

[217] Konkretno, razmatrane su mogućnosti korištenja linearne, kvadratne, kubne i eksponencijalne funkcije.

analize prema kojemu je u slučaju da više različitih oblika regresijske funkcije može objasniti neku zavisnu varijablu, preporučljivo koristiti onu jednostavniju[218]. Pregled postavljenog modela prikazuje tablica 44. Koeficijent varijacije modela R=0,918[219] dok je koeficijent determinacije R^2=0,843, što znači da je 84,3 % ukupne varijacije u zavisnoj varijabli objašnjeno nezavisnim varijablama modela.

Tablica 44: Pokazatelji reprezentativnosti postavljenog regresijskog modela (Zavisna varijabla Y: Ukupna razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj; nezavisne varijable $X_1, X_2 \ldots X_4$)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.918[a]	.843	.839	14.909

a. Model Summary

Izvor: priredio autor

U tablici 45. prikazani su koeficijenti dobiveni regresijskom analizom.

Tablica 45: Koeficijenti korelacijske analize (Zavisna varijabla Y: Ukupna razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj; nezavisne varijable $X_1, X_2 \ldots X_4$)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	-38.494	7.922		-4.859	.000					
	Mjera zrelosti funkcije operativnog upravljanja IS	9.023	2.259	.351	3.994	.000	.570	.362	.285	.659	1.518
	Mjera razine postivanja propisa, politika i standarda IS	4.567	1.680	.241	2.718	.008	.518	.255	.194	.650	1.537

[218] Odnosno, nižeg reda.
[219] Koeficijent varijacije modela je normalizirana mjera disperzije distribucije vjerojatnosti.

Mjera uključenosti i posvećenosti rukovodstva strateškoj IS	3.754	2.161	.155	1.737	.085	.496	.166	.124	.642	1.558
Mjera percepcije posljedica nastupa incidenata IS	4.184	1.531	.201	2.733	.007	.289	.257	.195	.939	1.064

a. Dependent Variable: Ukupna razina funkcionalnosti

Izvor: priredio autor

Iz tablice 45. izvodi se regresijska funkcija:

$$\boldsymbol{Y = 9,023 * X_1 + 4,567 * X_2 + 3,754 * X_3 + 4,184 * X_4 - 38,494}$$

(P_1<0,001; P_2<<0,001; P_3<<0,01; 4<<0,01); odbacuje se H_0 i prihvaća se modificirana hipoteza $H_1,\ Y = f(X_1, X_2 \dots X_4)$

Naime, ukoliko bi se u regresijski model uključila i varijabla X_5, odnosno „*Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja informacijskom sigurnošću*“, tada bi pala predikcijska moć modela bila značajno lošija (R=0,679; R^2=0,462), kao što je prikazano u tablici 46.

Tablica 46: Pokazatelji reprezentativnosti postavljenog regresijskog modela (Zavisna varijabla Y: Ukupna razina funkcionalnosti informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj; nezavisne varijable $X_1, X_2 \dots X_5$)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.679[a]	.462	.436	14.95507

a. Predictors: (Constant), Mjera zrelosti modela odluèivanja o investicijama u IS, Mjera percepcije posljedica nastupa incidenata IS, Mjera razine postivanja propisa, politika i standarda IS, Mjera uključenosti i posvećenosti rukovodstva strateškoj IS, Mjera zrelosti funkcije operativnog upravljanja IS

Izvor: priredio autor

Činjenicu kako uključenje varijable X_5, odnosno „*Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja informacijskom sigurnošću*“ pogoršava predikcijsku moć modela može se objasniti činjenicom kako je kretanje te varijable slučajno, nesustavno, neplanirano, a dostignuta razina funkcionalnosti i utjecaja na ukupnu razinu funkcionalnosti na trenutačnoj razini upravljanja informacijskom sigurnošću mala. Pretpostavlja se da bi implementacija modela koji će biti predložen podigla razinu na kojoj se koriste kvantitativne metode, a samim time i utjecala pozitivno na ukupnu funkcionalnost modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima.

6.3. Regresijska analiza zavisne varijable Y2: „Strateško upravljanje informacijskom sigurnošću“

Druga obavljena regresijska analiza odgovara na pitanje koje su sastavnice zavisne funkcije *Y: „Strateško upravljanje informacijskom sigurnošću“*. Istraživanjem je izmjereno šest dihotomnih varijabli[220] za koje se smatra kako su važne odrednice regresijskog modela, te se sukladno tome postavlja hipoteza:

- X_1: Uveden sustav praćenja zakonskih zahtjeva,
- X_2: Uspostavljen sustav upravljanja informacijskom sigurnošću,
- X_3: Uveden sustav operativnih mjera informacijske sigurnosti,
- X_4: Korištenje kvantitativnih metoda pri odlučivanju,
- X_5: Uveden skup operativnih procedura pri provođenju informacijske sigurnosti,
- X_6: Posjedovanje ISO 9001 certifikata.

Cilj predikcijskog modela je:

$$H_0\colon Y = f(X_1, X_2 \dots X_6);$$
$$izgled = e^{logit};$$
$$\text{logit} = y(x_{1..6}) = \beta + \sum_{i=1}^{n} \alpha_i x_i;$$

6.3.1. Korelacijska analiza

Kao preliminarni test, koristi se korelacijski model dihotomnih varijabli, odnosno neparametrijska *Spearman ρ* metoda izračuna korelacija odabranih dihotomnih varijabli, koja je osobito podesna za korištenje u tu svrhu. Ovako izračunati ukriženi koeficijenti korelacija prikazani su u tablici 47. na sljedećoj stranici. Crvenom bojom označene su oni koeficijenti korelacija koji su značajni bilo na razini 95 % ili na razini 99 % pouzdanosti.

[220] Dihotomne ili binarne varijable mogu poprimiti vrijednosti *„DA“* ili *„NE*“, odnosno imaju binarna obilježja.

Tablica 47: Korelacijska analiza dihotomnih varijabli $X_1, X_2 \dots X_6$

Correlations

			SustavIS (DA-NE)	Kvantitativne metode (DA-NE)	Operativne procedure (DA-NE)	Pracenje zakona (DA-NE)	Operativne mjere (DA-NE)	ISO 9001 (DA-NE)
Spearman's rho	SustavIS (DA-NE)	Correlation Coefficient	1.000	.189**	.143**	.243**	.193**	.305**
		Sig. (2-tailed)	.	.000	.008	.000	.000	.000
		N	347	347	347	347	347	347
	Kvantitativne metode (DA-NE)	Correlation Coefficient	.189**	1.000	.251**	.176**	.210**	.176**
		Sig. (2-tailed)	.000	.	.000	.001	.000	.001
		N	347	347	347	347	347	347
	Operativne procedure (DA-NE)	Correlation Coefficient	.143**	.251**	1.000	.153**	.095	.041
		Sig. (2-tailed)	.008	.000	.	.004	.076	.441
		N	347	347	347	347	347	347
	Pracenje zakona (DA-NE)	Correlation Coefficient	.243**	.176**	.153**	1.000	.274**	.252**
		Sig. (2-tailed)	.000	.001	.004	.	.000	.000
		N	347	347	347	347	347	347
	Operativne mjere (DA-NE)	Correlation Coefficient	.193**	.210**	.095	.274**	1.000	.137*
		Sig. (2-tailed)	.000	.000	.076	.000	.	.011
		N	347	347	347	347	347	347
	ISO 9001 (DA-NE)	Correlation Coefficient	.305**	.176**	.041	.252**	.137*	1.000
		Sig. (2-tailed)	.000	.001	.441	.000	.011	.
		N	347	347	347	347	347	347

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Izvor: priredio autor

Postavlja se hipoteza H_0: r=0, odnosno da ne postoje korelacije među parovima varijabli. Korelacijskom analizom ustanovilo se kako su za istaknute kombinacije varijabli $X_1, X_2 \dots X_6$ one postojeće, odnosno hipoteza H_0 se odbacuje i za sve parove nezavisnih varijabli uzima se alternativna hipoteza H_1: r<>0 , odnosno da među parovima naznačenih varijabli postoji korelacijska povezanost i to, neznatna do laka. Savršena kolinearnost ne postoji među prediktorskim varijablama.

Izračunati su i faktori inflacije varijance (VIF) za sve kombinacije i varijable, te su oni za sve slučajeve manji od 1,171 što znači da između varijabli nije prisutan problem multikolinearnosti.

Korelacijska analiza pokazuje kako se metodološki niz varijabli $X_1, X_2 \dots X_5$ može koristiti u regresijskom modelu.

6.3.2. Svojstva regresijske jednadžbe za zavisnu varijablu Y2: „Strateško upravljanje informacijskom sigurnošću“

U nastavku izrade multinomnog logističkog regresijskog modela dihotomnih varijabli, poseže se za *Hosmer-Lemeshow* testom.[221] U konkretnom slučaju, p<0,005, pri čemu viši p ukazuje na stanovitu razinu neinterpretacije modela. Ovi su podaci prikazani u tablici 48.

Tablica 48: Hosmer-Lemeshow test

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	20.089	7	.005

Izvor: priredio autor

[221] Hosmer-Lemeshow test je baziran na decilima. Taj test je u pravilu značajan na više od 400 opažanja. (u konkretnom slučaju, n=347).

Nadalje, računaju se *Cox-Snell* i *Nagelkerke pseudo-*R^2, koji su prikazani u tablici 49. Prema ovim pokazateljima, modelom bi bilo objašnjeno svega 16 % varijance.

Tablica 49: Izračun Cox-Snell R^2 i Nagelkerke R^2 pseudo-R^2 pokazatelja

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	366.821[a]	.110	.160

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Izvor: priredio autor

Korištenjem ugrađenog instrumentarija statističkog programa za društvene znanosti *IBM SPSS*, iz modela se izbacuju varijable X_5 i X_6 jer ga ne poboljšavaju. U modelu ostaju varijable X_1, $X_2 ... X_4$. Zanimljivo je kako ovako korigiran prognostički model **ispravno predviđa 77,5 % pojava u odnosu na nul-model**. Takva vrsta poboljšanja može se smatrati vrlo dobrim pa i prognostički model vrlo dobrim modelom. Izračunate koeficijente i parametre modela prikazuje tablica 50.

Tablica 50: Koeficijenti i parametri regresijskog logističkog modela

Variables in the Equation

		B	Sig.	Exp(B)	95% C.I.for EXP(B)	
					Lower	Upper
Step 1[a]	pracenjezak_bin	.790	.006	2.204	1.251	3.883
	sustavIS_bin	.609	.027	1.839	1.070	3.160
	operatproc_bin	.543	.041	1.721	1.023	2.893
	kvantmet_bin	.525	.084	1.691	.931	3.072
	Constant	-1.963	.000	.140		

a. Variable(s) entered on step 1: pracenjezak_bin, operatmjere_bin, sustavIS_bin, operatproc_bin, ISO9001_bin, kvantmet_bin.

Izvor: priredio autor

Prema do sada pokazanome, i izračunatim parametrima i koeficijentima modela, prognostički model upravljanja informacijskom sigurnošću kao strateškom sigurnosti u odnosu na navedene varijable se može postaviti na sljedeći način:

$$\text{logit} = \ln\left(\frac{p}{1-p}\right) = -1{,}963 + 0{,}79 * \text{X1} + 0{,}609 * \text{X2} + 0{,}543 * \text{X3} + 0{,}525 * \text{X4}$$

$$\text{izgled} = \frac{\text{p}}{1-\text{p}} = e^{logit} = e^{-1{,}963+0{,}79*\text{X1}+0{,}609*\text{X2}+0{,}543*\text{X3}+0{,}525*\text{X4}}$$

7. PRIJEDLOG EKONOMSKI ODRŽIVOG MODELA UPRAVLJANJA SUSTAVOM INFORMACIJSKE SIGURNOSTI U MALIM I SREDNJIM PODUZEĆIMA

U sedmom poglavlju doktorske disertacije, prijedlog novog ekonomski održivog modela upravljanja sustavom informacijske sigurnosti u malim i srednjim poduzećima izlaže se u dvije međusobno povezane cjeline: **1) Prijedlog aktivnosti za implementaciju novog modela upravljanja informacijskom sigurnošću malih i srednjih poduzeća** i **2) Učinci primjene ekonomski održivog modela upravljanja informacijskom sigurnošću malih i srednjih poduzeća.**

7.1. PRIJEDLOG AKTIVNOSTI ZA IMPLEMENTACIJU NOVOGA MODELA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU MALIH I SREDNJIH PODUZEĆA

Prijedlog aktivnosti za implementaciju novoga modela upravljanja informacijskom sigurnošću malih i srednjih poduzeća sastoji se od dva poglavlja: **1) Pripremne aktivnosti** i **2) Provedbene aktivnosti i aktivnosti praćenja implementiranog modela**.

7.1.1. Pripremne aktivnosti

Izlaganje pripremnih aktivnosti implementacije novog modela upravljanja informacijskom sigurnošću malih i srednjih poduzeća zahtijeva obradu sljedećih cjelina**: 1) Modeliranje poslovnih procesa primjenom ARIS BPM metodologije, 2) Objekti modela poslovnih procesa prema ARIS BPM metodologiji, 3) Elementi procesa reinženjeringa poslovne funkcije informacijske sigurnosti, 4) Tretman rizika, 5) Katalog temeljnih mjera informacijske sigurnosti, 6) Komparacija procesa informacijske sigurnosti u velikim u odnosu na mala i srednja poduzeća, 7) Analiza pristupa provođenju informacijske sigurnosti od dna prema vrhu, 8) Ekonomsko razmatranje interakcije internog perimetra i okoline malih i srednjih poduzeća u aktivnostima provođenja informacijske sigurnosti, 9) Definiranje odrednica modela ekonomski održivog upravljanja informacijskom sigurnošću u malim i srednjim poduzećima.**

7.1.1.1. Modeliranje poslovnih procesa primjenom ARIS BPM metodologije

Za prikaz aktivnosti provedbe uvođenja modela upravljanja informacijskom sigurnošću u mala i srednja poduzeća u Republici Hrvatskoj korištena je metodologija ARIS BPM[222]. To je jedna od uvriježenih metodologija modeliranja poslovnih procesa, njemačkog proizvođača Aris AG, koji je ujedno i proizvođač niza softverskih paketa koji se mogu koristiti u svrhu analize poslovnih procesa, izgradnje platforma korporativne arhitekture te platforme za korporativno upravljanje te upravljanje rizikom i sukladnošću. U navedene svrhe mogu se koristiti paketi prikazani na shemi 14.

Shema 14: Programski paketi sustava ARIS

Analiza poslovnih procesa

- ARIS Architect & Designer
- ARIS Connect
- ARIS for SAP
- ARIS Publisher
- ARIS Business Strategy
- ARIS Simulation
- ARIS Process Governance
- ARIS Process Performance Manager
- ARIS MashZone
- BPE LifeCycle

Platforma korporativne arhitekture

- ARIS Enterprise Architecture
- ARIS IT Inventory
- CentraSite
- ARIS Architect & Designer
- ARIS Connect
- ARIS MashZone
- ARIS Publisher
- ARIS Business Strategy
- ARIS Process Governance

Platforma za korporativno upravljanje, te upravljanje rizikom i sukladnošću

- ARIS Risk&Compliance Manager
- ARIS MashZone
- ARIS Architect&Designer
- ARIS Connect
- ARIS Publisher

Izvor: priredio autor

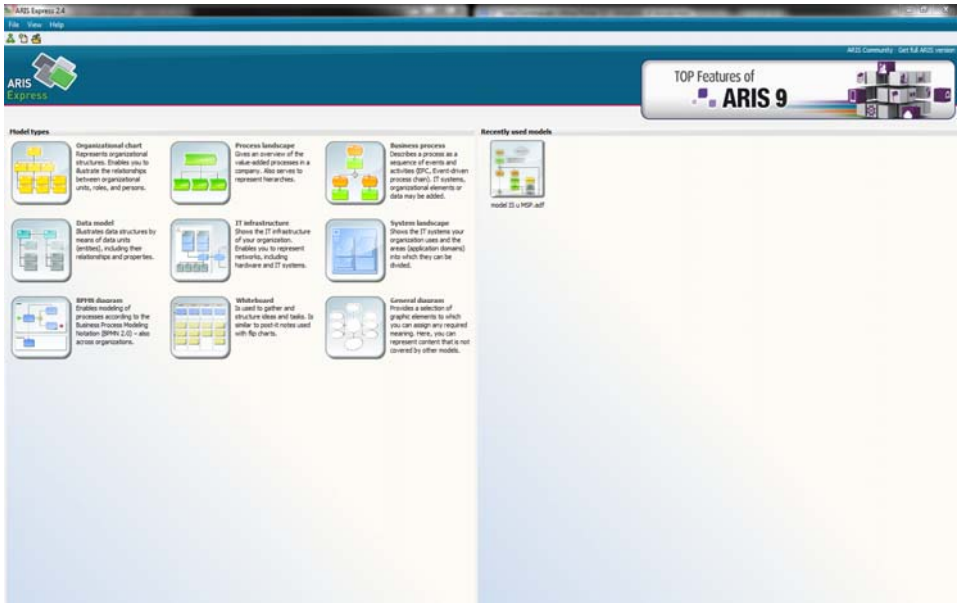
ARIS pristup modeliranju poslovnih procesa pruža metode za analizu procesa i kreiranja holističkog pristupa dizajnu procesa i hodograma akcija. ARIS je metodologija prof. Augusta Wilhelma Scheera iz 1992. godine (Scheer, 1992, p. 18) koja predstavlja osnove intelektualnog vlasništva na kojemu je izgradio svoje poduzeće *„IDS Scheer"*[223]. Za izradu prikaza aktivnosti provedbe uvođenja modela upravljanja informacijskom sigurnošću u mala i srednja poduzeća u Republici Hrvatskoj korišten je alat ARIS Express u inačici 2.4 koji je besplatan za korištenje

[222] *ARIS BPM* je kratica od eng. *„Architecture of Integrated Information Systems Business Process Modeling"*.

[223] Poduzeće *„IDS Scheer"* razvija, implementira i podržava računalne programe za modeliranje i upravljanje poslovnim procesima te se smatra osnivačem industrije upravljanje poslovnim procesima. Osnovano je 1984. godine sa sjedištem u Saarbrueckenu u Saveznoj Republici Njemačkoj.

nakon što se korisnik s vlastitim podacima registrira na Internet sjedištu (IDS Scheer AG, 2013) i prvi put pokrene instaliranu aplikaciju koja je utemeljena na paketu Oracle Java[224]. ARIS Express u inačici 1.0 izdan je u rujnu 2009. godine, a njegova radna površina prikazana je na ilustraciji 2.

Ilustracija 2: Radna površina programa ARIS Express



Izvor: priredio autor – ekranska slika programa „**ARIS Express**“

Aplikacija Aris Express omogućava izgradnju devet vrsta modela:

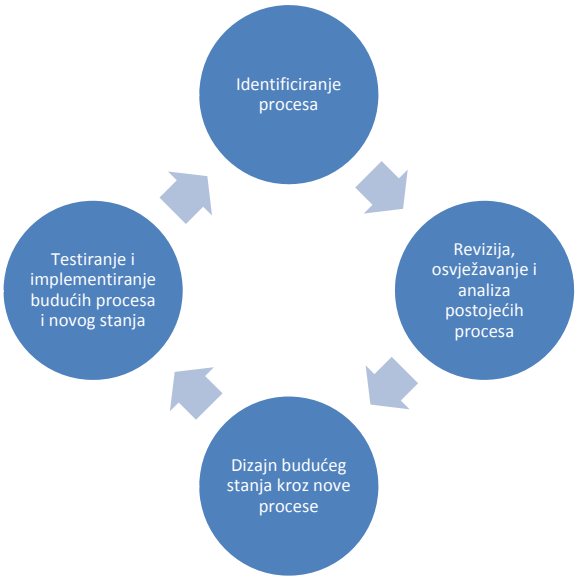
1. Organizacijske sheme[225],
2. Model procesnih krajobraza[226],
3. Model poslovnih procesa[227],
4. Podatkovni model[228],
5. Model informatičke infrastrukture[229],
6. Model sustavnih krajobraza[230],
7. BPMN dijagram,
8. Brainstorming model[231],
9. Opći model[232].

[224] Za više detalja cf. Oracle Java – Make the Future Java, **http://www.oracle.com/us/technologies/java/overview/index.html** (22.08.2013.)
[225] eng. *„Organizational chart“*
[226] eng. *„Process landscape“*
[227] eng. *„Business process“*
[228] eng. *„Data model“*
[229] eng. *„IT infrastructure“*
[230] eng. *„System landscape“*
[231] eng. *„Whiteboard“*

U izgradnji modela korišteni su modeli informatičke infrastrukture te je ocijenjeno, budući da se svi koraci modela procesa nalaze unutar jedne organizacije a nisu dijeljeni između više organizacija, kako je optimalno koristiti jednostavniji, model poslovnih procesa. U protivnom, kada bi se određene linije poslovnih procesa izvodile kod drugih entiteta[233], bilo bi potrebno koristiti BPMN dijagram. Naime, BPMN 2.0[234],grafička reprezentacija specifikacije poslovnih procesa u modelu poslovnih procesa omogućuje prikaz više poslovnih linija[235] u okviru kojih se obavlja neki poslovni proces[236], te stoga ima vrlo razgranate i raznolike objekte, odnosno elemente koji se mogu koristiti pri izgradnji modela. Povodeći se za principom jednostavnosti, budući da je ARIS-ov model poslovnih procesa dovoljan za prikaz procesa informacijske sigurnosti, on je adaptiran umjesto kompleksnijeg BPMN 2.0 modela.

Pri izgradnji modela, koristio se proces reinženjeringa poslovnih procesa[237], čiji je cilj poboljšanje efikasnosti postojećih procesa unutar organizacija na način da se oni proučavaju temeljito, od samih početnih postavki, kako bi se odredio najbolji način za njihovu rekonstrukciju. (Čičin-Šain, et al., 2004, p. 83) Navedeni procesi prikazani su na shemi 15.

Shema 15: Ciklus reinženjeringa poslovnih procesa



Izvor: priredio autor

Proces reinženjeringa poslovnih procesa sastoji se od četiri faze:

1. Identificiranje procesa,

---

[232] eng. *„General diagram"*
[233] npr. Poduzeća, organizacije, dobavljači.
[234] Trenutačna verzija *BPMN 2.0 (Business Process Model and Notation*) modela je od ožujka 2011. godine.
[235] npr. Sektora, jedinica, projekata, odjela, jedinica ili poduzeća.
[236] U terminologiji modeliranja poslovnih procesa, ovakva se poslovna linija naziva eng. „*swim lane*".
[237] „*BPR*" je kratica od eng. *„Business process reengineering"*

2. Revizija, osvježavanje i analiza postojećih procesa,
3. Dizajn budućeg stanja kroz nove procese,
4. Testiranje i implementiranje budućih procesa i novog stanja.

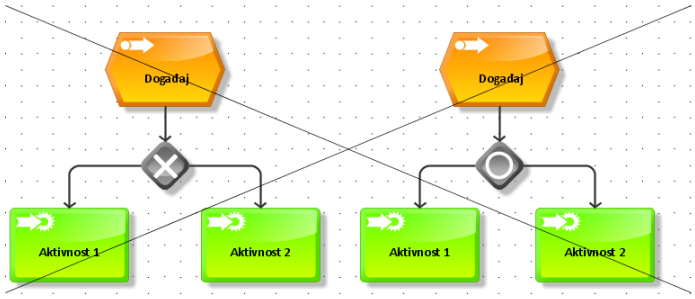
7.1.1.2. Objekti modela poslovnih procesa prema ARIS BPM metodologiji

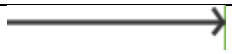
ARIS koristi jezik za modeliranje koji pripada široj skupini procesnih metodologija poznatih i pod nazivom „procesni lanci pokretani događajima“[238], a koji predstavljaju značajan aspekt *ARIS* modela. Ova metoda je razvijena od strane Scheera, Kellera i Nuettgensa sa Saarskog univerziteta ranih 90-tih godina prošlog stoljeća a koristi jednostavnu notaciju kako bi se prikazali kompleksni poslovni procesi i hodogrami. *EPC* metodologija je sposobna prikazati kompleksne poslovne informacijske sustave, ali ujedno inkorporirati i ostale važne informacije koje ih opisuju, poput funkcija, podataka, organizacijske strukture i informacijskih resursa. U ovim modelima koristi se nekoliko temeljnih elemenata koje vjerno replicira i *EPC* reprezentacija *ARIS Expressa*. Ove elemente, kao i njihovo značenje, prikazuje tablica 51.

Tablica 51: Objekti ARIS BPM metodologije

Redni broj	Grafički element objekta	Naziv i objašnjenje značenja objekta
1.		Aktivnost ili funkcija (*eng. „Activity“*) uz događaj drugi je najvažniji element EPC modela a reprezentiran je grafičkim simbolom pravokutnika. Aktivnosti opisuju transformaciju iz početnog stanja u rezultirajuće stanje. Neke funkcije mogu biti dodatno rafinirane (razgranate) u druge EPC lance i takve se funkcije nazivaju hijerarhijskim funkcijama. Primjeri: *„Osigurati financijska sredstva za analizu informacijskih sustava“, „Provođenje analize rizika“, „Provjeriti sukladnost sa zakonskim propisima“, „Analizirati povrat na investiciju u sredstvo informacijske sigurnosti“*
2.		Organizacijska jedinica (eng. *„Organizational unit“*). Organizacijska jedinica je element preuzet iz ARIS Express modela organizacijske strukture a omogućuje da se uz odgovarajuće događaje, odnosno funkcije, dodijele organizacijske jedinice odgovorne za njihovo provođenje Primjeri: *„Uprava poduzeća“, „Odjel za informatičku podršku“, „Odjel nabave“.*
3.		Osoba (*eng. „Person“*). Osoba je također element preuzet iz ARIS Express modela organizacijske strukture, a omogućuje da se uz odgovarajuće događaje, odnosno funkcije, dodijele osobe odgovorne za njihovo provođenje. Primjeri: *„CISO“, „Direktor sektora informatike“, „Predsjednik Uprave“.*
4.		Entitet (*eng. „Entity“).* Entitet je element iz ARIS Express podatkovnog modela, a omogućuje da se uz odgovarajuće događaje, odnosno funkcije, naznači entitet o kojemu se vode podaci u bazi podataka. Entitet je moguće jednoznačno identificirati po primarnom ključu. Primjeri: *„Informacijski sustav“, „Pružatelj usluge“, „Zaposlenici“.*

[238] *EPC* je kratica od eng. *„Event-driven Process Chains“*. Radi se o jednom od oblika dijagrama toka koji se koriste za modeliranje poslovnih procesa pri planiranju korporativnih resursa te poboljšanju poslovnih procesa. *EPC* metodologija također je razvijena od strane prof. Wilhelm-August Scheera na Institutu za poslovnu informatiku Sarskog univerziteta ranih 1990.-tih godina.

5.		Dokument (*eng. „Document“)* je element koji prikazuje koji dokument (fizički ili logički) je rezultat nekog događaja ili aktivnosti dijagrama poslovnih procesa. Primjeri: *„Izvješće o rizicima informacijske sigurnosti“, „Račun za usluge informacijsko-sigurnosnog savjetovanja“, „Obrazac o procjeni rizika informacijskog sustava“.*
6.		Proizvod (*eng. „Product“*) je element ARIS modela poslovnih procesa koji prikazuje točku u kojoj je isporučen krajnji proizvod koji je rezultat provođenja modela. Primjeri: *„Procjena rizika“, „Sustav upravljanja informacijskom sigurnošću“, „Firewall“.*
7.		Procesna poveznica (*eng. „Process interface“*) je element modela koji prikazuje funkciju (aktivnost) koja se dalje može granati u sljedeći EPC model, ali se ne prikazuje u postojećem modelu. Primjeri: *„Financiranje sustava upravljanja informacijskom sigurnošću“, „Proces vanjskog savjetnika za informacijsku sigurnost“, „Programiranje sustava za analizu dnevnika pristupa“*
8.		Događaj (eng. *„Event“)* je uz aktivnost (funkciju), glavni element EPC lanca a reprezentiran je šesterokutnim simbolom. Događaj opisuje pod kojim okolnostima se odvija određena funkcija ili aktivnost, odnosno stanje kojim rezultira odgovarajući proces. Primjeri: *„Implementirane temeljne mjere informacijske sigurnosti“, „Identificiran rizik informacijske sigurnosti“, „Financijska sredstva nisu raspoloživa“.*
9.		Baza podataka (*eng. „Database“*) je element koji prikazuje koja baza podataka se koristi vezano uz odvijanje nekog događaja ili aktivnosti dijagrama poslovnih procesa. Primjeri: *„Baza rizika informacijske sigurnosti“, „Poslovni informacijski sustav“, „b2b sustav poslovanja“.*
10.		Informacijski sustav (*eng. „IT system“*) je element preuzet iz ARIS modela informatičke infrastrukture, a njime se prikazuju informatički sustavi koji moraju biti izgrađeni ili su povezani uz odgovarajući događaj ili aktivnost. Primjeri: *„Poslovni transakcijski sustav“, „CRM sustav“, „b2g sustav“, „Sustav nadzora i analize dnevnika pristupa“.*
11.		Logička spojnica „ekskluzivno ili“ *(eng. „logical connector XOR“)* je prvi od tri logička elementa (operatora) koji kontroliraju tijek procesa. U slučaju korištenja operatora XOR pri razdvajanju procesnih putova, odabire se samo jedan od rezultirajućih procesnih puteva. U slučaju spajanja procesnih puteva kroz operator XOR, samo jedan od prethodnih procesnih puteva će aktivirati rezultirajući proces. Važno pravilo EPC modeliranja poslovnih procesa je da nije dozvoljeno slijediti događaj s logičkim operatorima XOR ili OR, jer u tom slučaju nije izvjesno koji od više procesnih puteva će uslijediti po ispunjenju odgovarajućeg događaja. Ovo pravilo prikazano je u ilustraciji nedozvoljenog procesnog spajanja operatorima XOR ili OR  Izvor: Priredio autor

12.		Logička spojnica „ili“ *(eng. „logical connector OR“)* je drugi od tri logička elementa (operatora) koji kontroliraju tijek procesa. U slučaju korištenja operatora OR pri razdvajanju procesnih putova, odabire se barem jedan od rezultirajućih procesnih puteva, može više njih a mogu i svi. U slučaju spajanja procesnih puteva kroz operator OR, barem jedan od prethodnih procesnih puteva će aktivirati rezultirajući proces, može više njih, a mogu i svi.
13.		Logička spojnica „i“ *(eng. „logical connector AND“)* je posljednji logički element (operator) koji kontrolira tijek procesa. U slučaju korištenja operatora AND pri razdvajanju procesnih putova, odabiru se odjednom svi rezultirajući procesni putevi. U slučaju spajanja procesnih puteva kroz operator AND, svi procesni putevi moraju biti dovršeni prije nego je iniciran sljedeći proces.
14.		Spojnica ili poveznica *(eng. „connector“)*. Spojnice koje spajaju događaje i aktivnosti obavezno su reprezentirane strelicama koje pokazuju smjer procesne aktivnosti. Svaki događaj i svaka aktivnost posjeduju najviše jednu spojnicu kola inicira događaj ili aktivnost i najviše jednu spojnicu koja rezultira iz događaja ili aktivnosti. U slučaju potrebe za više ulazaka ili izlazaka procesnih puteva, nužno je koristiti odgovarajuće logičke operatore.

Izvor: priredio autor

7.1.1.3. Tretman rizika

Za razliku od autonomno-tehničkog pristupa kod kojega se u analizi uglavnom u obzir uzima informacijska imovine poduzeća, njena inherentna svojstva predstavljena ranjivostima, a koja mogu iskoristiti prijetnje na način da ugroze informacijsku imovinu, što rezultira pojavom sigurnosnih incidenata koji nanose mjerljivu štetu malim i srednjim poduzećima, predlaže se u proces upravljanja informacijskom sigurnošću uvesti i ekonomsku analizu[239] čiji je cilj usporediti utjecaj rizika s troškom uvođenja protumjera, te na taj način pružiti dionicima-donosiocima odluka instrumentarij procjene isplativosti uvođenja mjera informacijske sigurnosti, a samim time i kreirati ekonomski utemeljen i održiv sustav informacijske sigurnosti u malim i srednjim poduzećima.

Uvriježeni pristup organizaciji procesa informacijske sigurnosti koji se koristi u velikim poduzećima utemeljen je na kvantitativnoj procjeni razine rizika kojima je poduzeće izloženo. Razina rizika pokušava se zatim kvantificirati i radi se o subjektivnoj procjeni objektivne pojavnosti u okolini poduzeća. Na kraju procesa identifikacije rukovoditelji su upoznati s ostatkom rizika[240] koji mora biti prihvaćen od njihove strane. Za mala i srednja poduzeća predlaže se adaptacija sljedeće kategorizacije rizika s obzirom na njegove pojavne oblike:

1. **Tretirani rizik** – U ovaj oblik rizika pripadaju oni oblici i razine rizika koji su identificirani, povezani uz informacijsku imovinu poduzeća, njene ranjivosti i prijetnje kojima

[239] Odnosno, financijsku analizu.

[240] U terminologiji upravljanja rizicima ostatak rizika obično se naziva rezidualnim rizikom, a razvrstava se prema njegovim karakteristikama s obzirom na pojavne oblike (tehnički, organizacijski, rizik vezan uz ljudske resurse itd.).

je izložena, i koji su uklonjeni, odnosno neutralizirani korištenjem tehničkih, organizacijskih i drugih mjera,

2. **Transferirani rizik** – Ovaj pojavni oblik rizika čine oni rizici koji su identificirani i uklonjeni na način da su prebačeni na treću stranu. Pritom se obično novim nosiocem rizika uzimaju osiguravajuća društva ili poduzeća kojima je određena usluga eksternalizirana. U slučaju osiguranja od nastupa pojedinog rizika, ova vrsta transfera zahtijeva razvijenu paletu ponude osiguranja, kao i sposobnost osiguravajućih društava da procijene mogućnost nastupa pojedinih osiguranih događaja a samim time i novčani iznos police osiguranja. Kod poduzeća koja pružaju eksternalizirane informatičke usluge, rizik je i dalje prisutan, implicitno je prebačen na treću stranu kroz ugovore o razinama usluge[241], a u slučaju nastupa rizika, ugovaraju se penali ili kazne za kašnjenje u isporuci,

3. **Transferirani rizik računalstva u oblaku** – Ovaj oblik rizika predstavlja novi oblik transferiranog rizika koji valja priznati uslijed razvoja informatičke tehnologije. Kod transferiranog rizika računalstva u oblaku rizici korištenja pojedine usluga, spremišta podataka, računalne mreže, aplikativnog sustava ili infrastrukturne platforme prebačeni su na pružatelja virtualnih usluga, u slučaju da se radi o trećoj strani, no u slučaju tzv. „*privatnog oblaka*“[242], oni i dalje ostaju unutar poduzeća i valja ih tretirati po pojedinim segmentima informacijske imovine.[243] Specifičnosti rizika računalstva u oblaku ogledaju se u financijskom tretmanu takvog rizika odnosno utjecaju na poduzeće o čemu će biti više govora u nastavku,

4. **Neidentificirani rizik** – Radi se o riziku koji postoji unutar poduzeća ali nije prepoznat. Cilj svake procjene rizika je da neidentificirani rizik bude jednak nuli. Razlozi za postojanje neidentificiranog rizika su razni, a moguće je identificirati sljedeće:

- Razvoj tehnologije od zadnje provedene procjene rizika do trenutka nastupa sigurnosno-informacijskog incidenta,
- Promjena informacijske imovine i vezanih resursa od zadnje provedene procjene rizika do trenutka nastupa sigurnosno-informacijskog incidenta,
- Neadekvatna metodologija izrade procjene rizika,
- Nedovoljna vještina i znanje osoba zaduženih za izradu procjene rizika.

U malim i srednjim poduzećima u kojima nije proveden proces procjene rizika, valja uzeti kako je razina neidentificiranog rizika jednaka maksimalnom mogućem riziku informacijskog sustava. Isto vrijedi i za ona poduzeća za koja je utvrđeno tijekom analize ukupne

[241] *SLA*, kratica od eng. „*Service Level Agreements*“. Radi se o ugovorima između pružatelja usluga i korisnika kojima se definira tražena razina usluge. Za detalje cf. Webopedia, **http://www.webopedia.com/TERM/S/Service_Level_Agreement.html** (11.08.2013.)

[242] Virtualni privatni oblak (*VPC*, eng. *Virtual Private Cloud*) je skup dijeljenih računalnih resursa koji je alociran unutar javnog oblaka, no koji omogućuje određenu razinu izolacije od ostalih korisnika. Privatni oblak odnosi se na istu paradigmu, no u slučaju kada se resursi nalaze u potpunoj kontroli same organizacije koja ih i koristi.

[243] npr. Hardver, softver, mreža, ljudski resursi.

funkcionalnosti sustava upravljanja informacijskom sigurnošću kako nemaju implementiranu niti jednu od identificiranih razina funkcionalnosti.

5. **Prihvaćeni rizik.** Razina prihvaćenog rizika metodološki bi trebala biti čim manja a idealno bi trebala biti jednaka nuli, kao i kod neidentificiranog rizika. Radi se o onim razinama rizika koje su rukovoditelji, odnosno vlasnici malih ili srednjih poduzeća odlučili prihvatiti. Razlozi za prihvaćanje mogu biti razni, a najčešće se radi o sljedećim razlozima:

- Rukovoditelji i vlasnici ne pridaju dovoljno pažnje aktivnostima i procesima informacijske sigurnosti,
- Poduzeća ne raspolažu dovoljnim financijskim sredstvima za investiranje u komponente sustava upravljanja informacijskom sigurnošću ili njihovo održavanje,
- Poduzeća raspolažu dovoljnim financijskim sredstvima za investiranje u komponente sustava upravljanja informacijskom sigurnošću ili njihovo održavanje, ali rukovoditelji i vlasnici smatraju kako je oportunije uložiti ih u druge svrhe, npr. proširenje proizvodnih ili prodajnih kapaciteta ili obrtni kapital, umjesto u mjere informacijske sigurnosti čak i onda kada su dobrobiti od takvih dodatnih investicija u temeljnu djelatnost poduzeća u nerazmjeru s gubicima koji mogu nastati u slučaju nastanka incidenta informacijske sigurnosti
- Razine rizika koje su izračunate, a koje se prihvaćaju, razumne su u odnosu na kvantificirani iznos moguće štete koju poduzeće može trpiti u slučaju nastupa incidenta informacijske sigurnosti.

7.1.1.4. Katalog temeljnih mjera informacijske sigurnosti

Rizike koji nisu prihvaćeni, a koji su klasificirani na izloženi način potrebno je pokušati otkloniti mjerama informacijske sigurnosti. Te je mjere moguće podijeliti u dvije skupine:

1. **Obavezne (obligatorne) mjere informacijske sigurnosti**. Radi se o mjerama informacijske sigurnosti koje može provesti i sam vlasnik u najmanjem mikro-poduzeću, a sukladno katalogu takvih mjera. Obavezne ili obligatorne mjere potrebno je poduzimati sukladno katalogu obaveznih mjera informacijske sigurnosti. To su one mjere za čije provođenje nisu potrebna značajnija financijska ili materijalna sredstva, a čak i varijabilni trošak potrebnog rada je vrlo nizak. Ovo su uglavnom operativne mjere koje ovise o dostignutoj razini tehničke kompleksnosti informacijskog sustava i djelatnosti poduzeća, no radi se o temeljnim operativnim mjerama koje se često propuštaju provesti, a osobito u poduzećima koja su vrlo mala ili se ne bave djelatnostima iz područja informatike i visokih tehnologija. Nekoliko

obligatornih mjera koje je moguće identificirati sukladno navedenoj definiciji, a koje su lako provedive su sljedeće[244]:

1. Kreiranje odluke kojom se rukovoditelji prve linije ili vlasnici **obvezuju** za provođenje mjera informacijske sigurnosti, te ukoliko se radi o poduzeću s više zaposlenih, od kojih je nekoga moguće imenovati kao osobu odgovornu za provođenje mjera informacijske sigurnosti, odluka o imenovanju te osobe. Ovakav dokument kasnije može poslužiti i kao osnova za izradu politike informacijske sigurnosti. [245]

2. Uvedena redovita **provjera** klauzula o povjerljivosti suradnje u ugovorima koja poduzeće sklapa. Ovakve klauzule trebaju biti standardni dio sljedećih ugovora:

- Ugovori o zapošljavanju
- Ugovori o suradnji s klijentima
- Ugovori o nabavi roba i usluga
- Ugovori o telekomunikacijskim uslugama
- Ugovori o servisnim uslugama koje pružaju treće strane

Ova vrsta aktivnosti odnosi se ne samo na uključivanje klauzula o povjerljivosti u ugovore koje inicira poduzeće, već i na pažljivu analizu klauzula o povjerljivosti koje su poduzeću predočene ukoliko se radi o tipskim ugovorima dobavljača ili klijenata.[246]

3. Kreiranje i održavanje spiska jasno identificirane informacijske **imovine** poduzeća. Ovo se u samom početku uvođenja procesa informacijske sigurnosti u malim i srednjim poduzećima primarno odnosi na materijalnu imovinu kao što su računala, mrežna oprema, mobilni telefoni i prijenosne memorije, a kasnije je moguće ovu aktivnost proširiti i na drugu, nematerijalnu informacijsku imovinu poduzeća, kao što su računalni sustavi, računalni softver (aplikacije), i podaci poduzeća. Uz kreiranje i održavanje spiska informacijske imovine poduzeća nužno je održavati i listu osoba koje su za nju zadužene[247]. Upravljanje informacijskom imovinom uključuje i odgovornosti pri prestanku ugovornih odnosa, povrat zadužene informacijske imovine, uklanjanje pristupa zaposlenicima, dobavljačima i klijentima po završetku ugovornog odnosa.[248]

4. Osnovna **provjera** zaposlenika, dobavljača i trećih strana[249] prije zapošljavanja i ulazaka u ugovorne odnose, uz korištenje etičkih metoda pristupa javnim informacijama. Ovu vrstu provjere u današnjim uvjetima moguće je obaviti kroz osobne kontakte, korištenjem

[244] Izvedeno iz primjenjivih mjera standarda ISO 27002.
[245] Sukladno mjerama iz poglavlja A6 – *"Organization of information security*" standarda ISO 27002.
[246] Sukladno mjerama iz poglavlja A6. standarda ISO 27002
[247] Radi se o listi (popisu) vlasništva nad informacijskom imovinom poduzeća.
[248] Sukladno mjerama iz poglavlja A7 i A8 standarda ISO 27002.
[249] npr. suradnika, klijenata, privremenih zaposlenika i sl.

usluga detektivskih agencija i korištenjem Interneta (npr. putem socijalnih mreža, vijesti na Internet portalima, ili vijesti objavljenih na Internet stranicama dnevnih novina ili magazina).[250]

5. Inzistiranje **vlasnika** ili **rukovoditelja** poduzeća na pravilima informacijske sigurnosti, obrazovanja ili treninga. Ova aktivnost sastoji se u malim i srednjim poduzećima od jasnog komuniciranja prema svim zaposlenicima, dobavljačima, klijentima i suradnicima o tome kako poduzeće polaže pažnju na mjere informacijske sigurnosti. Radi se o aktivnosti koje se ne provode jednom, već stalno, kontinuirano, u redovnim vremenskim razmacima koji ovise o vrsti aktivnosti koju poduzeće obavlja a najmanje jednom godišnje.[251]

6. Provođenje temeljnih **mjera** fizičke sigurnosti i sigurnosti radne okoline. Ovo se odnosi na strukturirane i primjerene mjere fizičke sigurnosti radnih prostora a osobito onih koje se odnose na lokacije na kojima je pohranjena informacijska imovina. Mjere fizičke sigurnosti i sigurnosti radne okoline osobito se odnose na sigurnost prostorija, fizičku zaštitu od vatre, poplave i prirodnih katastrofa te sigurnost fizičkog pristupa računalima i računalnim sustavima.[252]

7. Temeljna razmatranja **rizika** korištenja informacijske imovine izvan prostorija poduzeća i utjecaja takvog korištenja na informacijsku sigurnost informacijskih sustava poduzeća. To se osobito odnosi na pametne telefone, tablete, prijenosna računala, te na transfer podataka putem računalnih mreža, prijenosnih medija, odnosno na podatke sadržane na memorijama računala koja su poslana na servis.[253]

8. **Dokumentiranje promjena** na računalnoj imovini poduzeća. Ova se obligatorna mjera odnosi na održavanje dnevnika promjena na računalnoj imovini, a to se u okruženju malih i srednjih poduzeća osobito odnosi na dnevnik instaliranja aplikativnog softvera, instalaciju novih mrežnih komponenti ili naprava, te promjene na konfiguraciji računalnog, serverskog ili mrežnog hardvera.[254]

9. Kreiranje rezervnih **kopija podataka** je obavezna mjera implementacijom koje rukovoditelji malih i srednjih poduzeća ili vlasnici mikro poduzeća trebaju osigurati podatke poduzeća koji su pod njihovom kontrolom od uništenja u slučaju nastupa incidenta informacijske sigurnosti. U okviru ove mjere potrebno je definirati koji su točno podaci koje je potrebno sačuvati na način da se redovito kreiraju rezervne kopije, koliko često i kojom dinamikom je kopije potrebno izrađivati, na koji način i gdje se rezervne kopije čuvaju.[255]

10. Temeljna razmatranja sigurnosti korištenja **računalne mreže** u poslovanju odnose se na osnovno planiranje mjera sigurnosti uredske računalne mreže, bežičnih računalnih

[250] Sukladno mjerama iz poglavlja A8. standarda ISO 27002.
[251] Sukladno mjerama iz poglavlja A8. standarda ISO 27002.
[252] Sukladno mjerama iz poglavlja A9. standarda ISO 27002.
[253] Sukladno mjerama iz poglavlja A9. standarda ISO 27002.
[254] Sukladno mjerama iz poglavlja A10. standarda ISO 27002.
[255] Sukladno mjerama iz poglavlja A10. standarda ISO 27002.

mreža, distribuiranih računalnih mreža i računalne opreme. Ovo se također odnosi i na sigurnost i politike slanja poruka putem elektroničke pošte, korištenja socijalnih mreža i servisa.[256]

11. **Odgovornosti korisnika** po pitanju implementacije temeljnih mjera osobne informacijske sigurnosti je jedna od najvažnijih obligatornih mjera koje je potrebno provesti čak i u najmanjem poduzeću. Radi se o nekoliko vezanih mjera koje se odnose na kreiranje korisničkog imena i lozinke za svakog korisnika koji koristi informacijsku imovinu, definiraju politiku promjene lozinki te politike „*čistog stola*" i „*čistog ekrana*". [257]

12. Donošenje odluke o **daljinskom pristupu** informacijskoj imovini poduzeća odnosi se na politiku daljinskog pristupa, odnosno radu s udaljenih lokacija uz korištenje informacijske imovine poduzeća, pod kojim uvjetima i na koji način je takav rad dozvoljen ili ne.[258]

13. Analiza **incidenata** informacijske sigurnosti, uključivo njihove korijenske uzroke je mjera kojom rukovoditelji, odnosno vlasnici poduzeća mogu osigurati posebno posvećivanje pažnje čestim uzrocima incidenata sigurnosne sigurnosti te njihovom uklanjanju. Pritom vrijedi pravilo kako je incidente informacijske sigurnosti unutar poduzeća potrebno dokumentirati, analizirati i informacije o njima raspraviti, odnosno diskutirati sa svim zaposlenicima i dionicima ukoliko vlasnici i rukovoditelji procijene kako je to od interesa za poduzeće. [259]

14. Osiguranje **osnovnih mjera** oporavka od katastrofe i kontinuiteta poslovanja. U samom početku formiranja sustava upravljanja informacijskom sigurnošću nije realistično očekivati kako će zaduženi za informacijsku sigurnost kreirati kompleksne sustave oporavka od katastrofe ili kontinuiteta poslovanja, međutim, ukoliko je popisana informacijska imovina, oni mogu donijeti temeljne odluke vezane uz kritične sustave i način njihovog oporavka u slučaju katastrofe, odnosno kreirati katalog poslovnih funkcija s vremenom u kojem poduzeće može funkcionirati bez tih poslovnih funkcija, a koje se odnose na informacijske sustave poduzeća. S vremenom, ukoliko poslovni informacijski sustavi poduzeća dostignu višu razinu kompleksnosti i ukoliko vlasnici i rukovoditelji procjene da su oni ključni za funkcioniranje poduzeća, odnosno da bez njih poduzeću prijeti značajan poremećaj u poslovanju, moguće je provesti i klasičan proces kreiranja, testiranja i održavanja plana oporavka od katastrofe i kontinuiteta poslovanja.[260]

15. Identificiranje i osiguranje **sukladnosti** sa zakonskim zahtjevima po pitanju informacijske sigurnosti [261]

[256] Sukladno mjerama iz poglavlja A10. standarda ISO 27002.
[257] Sukladno mjerama iz poglavlja A11. standarda ISO 27002.
[258] Sukladno mjerama iz poglavlja A11. standarda ISO 27002.
[259] Sukladno mjerama iz poglavlja A13. standarda ISO 27002
[260] Sukladno mjerama iz poglavlja A15. standarda ISO 27002
[261] Sukladno mjerama iz poglavlja A15. standarda ISO 27002

Sve navedene mjere informacijske sigurnosti koriste se u tri navedene **svrhe**, a koji su povezani s ostvarivanjem ciljeva postojanja obaveznih (obligatornih) mjera informacijske sigurnosti:

1. **Postizanje strukturirane organizacije** sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima
2. **Uspostavljanje sustava utemeljenog na obrazovanju** iz područja informacijske sigurnosti koji se širi koncentrično, od vlasnika, ka rukovoditeljima, prema svim radnicima. Ovaj sustav je osobito važan iz razloga sto u malim, a osobito mikro poduzećima, nije realistično očekivati da će poslovna funkcija informacijske sigurnosti zaživjeti s periferije poduzeća ka centru, već upravo obrnuto. Ovu činjenicu čak i kod velikih poduzeća prepoznaju sustavi upravljanja kvalitetom koji u fokus procesa certifikacije stavljaju rukovoditelje koji moraju biti obvezani za postizanje ciljeva upravljanja kvalitetom sustava informacijske sigurnosti.
3. **Zadovoljavanje poslovnih certifikacijskih zahtjeva informacijske sigurnosti**. Radi se o temeljnim zahtjevima poslovne certifikacije koje poduzeće mora ispuniti kako bi moglo poslovati, odnosno ostati na tržištu u zatečenim poslovnim odnosima. To je vrlo heterogena skupina zahtjeva čiji sadržaj ovisi o veličini poduzeća u okviru globalne kategorije malih i srednjih poduzeća, zahtjevima područja (grane) u kojoj se obavlja poslovna aktivnost, razini razvijenosti već implementirane informacijske sigurnosti u poduzećima, korištenim tehnologijama i kanalima nabave i distribucije. U okviru obligatornih mjera informacijske sigurnosti razmatraju se samo oni poslovni certifikacijski zahtjevi bez kojih ne bi bilo moguće obavljati poslovnu aktivnosti, odnosno koji predstavljaju branu pristupa tržištu. Takvi sustavi certifikacije su u ovom kontekstu uobičajeno vezani uz nemogućnost sudjelovanja u dijelovima tržišnog nadmetanja ukoliko poduzeće ne posjeduje odgovarajući certifikat. Takvi **primjeri** mogu biti sljedeći:
    1. ISO 9001:2008 certifikat može biti uvjet za sudjelovanje u postupku nadmetanja javne nabave za dobavljanje određenih dobara i usluga,
    2. PCI:DSS[262] certifikat može biti uvjet za obavljanje poslova kartičnog plaćanja, a osobito ukoliko poduzeće pohranjuje, obrađuje i prosljeđuje podatke o kreditnim karticama klijenata,
    3. ISO 27001:2005 certifikat može biti uvjet malim i srednjim poduzećima za uspostavljanje poslovnih odnosa sa specifičnim klijentima koji imaju posebne zahtjeve za visokom razinom informacijske sigurnosti

[262] *PCI:DSS* je kratica od eng. *„Payment Card Industry Data Security Standard"*. Za detalje cf. PCI Security Standards Council, **https://www.pcisecuritystandards.org/security_standards/index.php** (18.08.2013.)

Obavezne mjere informacijske sigurnosti, a osobito u dijelu organizacije i obrazovanja predstavljaju one mjere za koje čak i najmanja poduzeća ne moraju angažirati značajna financijska sredstva već se trošak uglavnom odnosi na varijabilni trošak rada vlasnika (rukovoditelja) koji je inicijator aktivnosti organizacije. U svojoj suštini, čak i implementacija tehničkih mjera na temeljnoj razini nije povezana uz značajne investicije. Naime, sve do sredine 2000-tih godina, mala i srednja poduzeća morala su zasebno kupovati operativne sustave za računala, antivirusne programe, programe koji štite sustave od *spyware*[263] programa ili malicioznog koda. Od sredine 2000-tih godina takvi su programi u svojim osnovnim inačicama integrirani uz operativne sustave, a zbog razvoja filozofije softvera *otvorenog koda* (besplatnog softvera), moguće je pronaći i koristiti softvere koji ispunjavaju zaštitne kontrole informacijske sigurnosti a koji su besplatni i u komercijalne svrhe u koje ih koriste mala i srednja poduzeća. Zanimljivo je primijetiti da i znanstvena istraživanja potvrđuju kako usprkos raspoloživosti tehnologija, one nisu primijenjene iz razloga što radna snaga ne posjeduje znanje za njihovo korištenje (Kandžija & Lovrić, 2013, p. 106). No, istinita je činjenica kako poslovni certifikacijski zahtjevi, promatrani zasebno, mogu uzrokovati značajne troškove nabave hardvera i softvera malim i srednjim poduzećima, a osobito ukoliko se radi o iznenadnoj aktivnosti implementiranja nekog sustava u nefunkcionalan sustav upravljanja informacijskom sigurnošću. No, ukoliko su u poduzećima već definirani organizacija upravljanja informacijskom sigurnošću i sustav stjecanja dodatnog znanja iz područja informacijske sigurnosti, takva će poduzeća zasigurno već imati implementirane tehničke i organizacijske elemente informacijske sigurnosti i daleko lakše zadovoljiti profesionalne certifikacijske zahtjeve.

Fakultativne mjere informacijske sigurnosti se odnose na dodatne mjere informacijske sigurnosti koje mala i srednja poduzeća mogu poduzeti kako bi poboljšale onu razinu informacijske sigurnosti koja je dostignuta korištenjem obligatornih mjera informacijske sigurnosti poduzetih od strane vlasnika ili rukovoditelja. U ovom dijelu provođenja mjera informacijske sigurnosti mala i srednja poduzeća mogu se koristiti iskustvima velikih poduzeća, te vokabularom informacijske sigurnosti koji ona koriste: radi se o implementaciji djelomičnih ili cjelokupnih procesa informacijske sigurnosti korištenjem strukturiranih sustava najbolje prakse.[264] Osim toga, u provođenju fakultativnih mjera, mala i srednja poduzeća se mogu koristiti klasičnom paradigmom sustavne procjene rizika i uklanjanja rizika raspoloživim kontrolama. **Kontrole** koje su raspoložive malim i srednjim poduzećima se mogu podijeliti na:

[263] Špijunski softver, eng. *„spyware"* je računalni program koji omogućuje prikupljanje informacija o osobama, poduzećima ili organizacijama bez njihovog znanja. Ovi programi često imaju obilježja drugih malicioznih programa poput trojanaca, programa koji prate operativne sustave, šire neželjene reklame ili koriste tehnologiju kolačića (eng. *„cookies*") koji su inače legitimni dio načina funkcioniranja preglednika Interneta.

[264] npr. ITIL, COBIT ili ISO 27001:2005.

1. **Preventivne kontrole**, namijenjene prevenciji nastupa incidenata npr. zabranom pristupa podacima onima koji nemaju dozvoljen pristup od strane poduzeća,
2. **Detekcijske kontrole**, namijenjene identificiranju i karakterizaciji vrste sigurnosnog incidenta koji je već nastao ili je u nastanku, npr. automatska analiza dnevnika pristupa računalnoj mreži koja otkriva pokušaj neovlaštenog pristupa poslovnom informacijskom sustavu iz okoline poduzeća,
3. **Korektivne kontrole**, namijenjene ograničavanju razine štete koju je uzrokovao nastup sigurnosnog incidenta, npr. mjere pohrane rezervnih kopija podataka koji mogu biti vraćeni na izvornu lokaciju ukoliko je došlo do nehotičnog brisanja podataka na datotečnom sustavu poslužitelja poduzeća.

Prema **prirodi**, kontrole informacijske sigurnosti mogu biti kategorizirane na sljedeći način, koji adaptiraju i sustavi najbolje prakse upravljanja informacijskom sigurnošću:

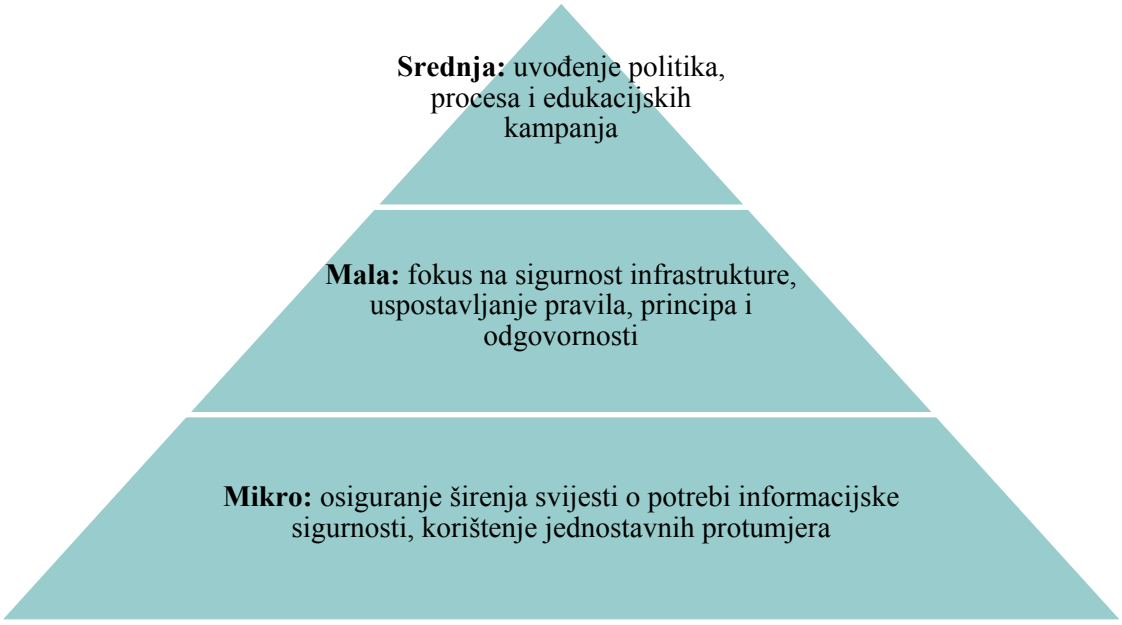
1. **Zakonske kontrole** (regulatorne kontrole ili kontrole suglasnosti), one su kontrole kojima se osigurava sukladnost sa zakonskim propisima koji reguliraju područje privatnosti,
2. **Proceduralne kontrole**, koje definiraju postupanje rukovoditelja ili zaposlenih po pitanju provođenja informacijske sigurnosti, postupanje u slučaju nastupa incidenata informacijske sigurnosti ili preventivne postupke koji sprječavaju nastanak sigurnosnih incidenata,
3. **Fizičke kontrole**, kojima se definira pristup informacijskoj imovini poduzeća, a najčešće ograničavanjem pristupa,
4. **Tehničke kontrole**, kojima se primjenom tehničkih mjera poput softvera ili logičkih mjera, ograničava pristup informacijskim resursima poduzeća. U tehničke kontrole spadaju i logičke kontrole pristupa pojedinoj informacijskoj imovini.

7.1.1.5. Analiza pristupa provođenju informacijske sigurnosti od dna prema vrhu

U praksi se često radi jednostavnosti razdvajaju preporuke za provođenje informacijske sigurnosti u malim i srednjim poduzećima **na tri razine**. (Park , et al., 2008, p. 94) Mjere informacijske sigurnosti su na tim razinama različite, a prilagođene su veličini grupe poduzeća. Tako se na najnižoj razini predlaže osiguranje širenja svijesti o potrebi mjera informacijske sigurnosti i korištenje temeljnih protumjera na razini mikro poduzeća. Za mala poduzeća, optimalnim se smatra pristup s fokusom na tehničku sigurnost infrastrukture, definiranje odgovornosti za informacijsku sigurnost unutar poduzeća na svim razinama, formiranje i uspostavljanje pravila i principa informacijske sigurnosti. Na razini srednjih poduzeća, predviđa se kako je adekvatan pristup koji je usporediv s onim koji koriste velika poduzeća, a to je uvođenje formalnih politika, procesa te provođenje edukacijskih kampanja u poduzeću. Ovakva

piramida pristupa prikazana je na shemi 16. Kod takvog pristupa pozitivna je osobina što se i na razini najmanjih poduzeća informacijska sigurnost prepoznaje kao važna poslovna funkcija, te se primjenjuju temeljne tehničke protumjere što rezultira povećanom razinom informacijske sigurnosti u odnosu na situaciju stohastičkog upravljanja. Također, već od razine srednjih poduzeća formalizira se pristup, i to prvo definiranjem neformalnih procedura kod malih poduzeća, a onda i formalizacijom na razini srednjih poduzeća. Negativna osobina ovakvog pojednostavljenog pristupa je što se isključivo veličina poduzeća uzima za kriterij koji je odlučujući za definiranje pristupa identificiranja mjera informacijske sigurnosti. Tako se npr. posve ignorira dohodovni kriterij, pri čemu poduzeće s manjim brojem zaposlenih ali većom prihodovnom osnovom može imati na raspolaganju sredstva za implementaciju viših razina modela upravljanja informacijskom sigurnošću, kriterij poslovne djelatnosti, ili npr. poduzeće koje ima veći broj zaposlenih ali se bavi primarnim djelatnostima može imati manju potrebu,a možda i raspoloživa financijska sredstva za provođenje mjera informacijske sigurnosti od manjeg pouzeća po kriteriju broja zaposlenih koje se bavi djelatnostima iz kvartarnog ili kvinarnog sektora ali je izrazito produktivno. Međutim, *bottom-up*[265] model ove vrste daje metodologiju koja se može usmjeriti na način da se pojedini čimbenici iz modela preuzmu i adaptiraju neovisno o veličini poduzeća, a da se pritom u obzir uzmu i ostali važni utjecaji od interesa za razvoj informacijske sigurnosti.

Shema 16: Pristup organizaciji i provođenju informacijske sigurnosti u malim i srednjim poduzećima od dna prema vrhu



Izvor: priredio autor

[265] eng. „*bottom-up*“ je uvriježeni izraz za pristup izgradnji sustava od „*dna prema vrhu*“.

Daljim razvojem ovakvog jednostavnog hijerarhijskog modela dolazi se do modela na tri razine koji se može provesti odvjeno u mikro, malim ili srednjim poduzećima, ali jednako tako može biti proveden u poduzeću na tri razine neovisno o njegovoj veličini, ukoliko poduzeće ima potrebu za kompleksnijim obrascem organizacije i upravljanja informacijskom sigurnošću. Ovakva razrada prikazana je na shemi 17. Na **temeljnoj razini** koja ugrubo može odgovarati mikro poduzećima, definiraju se tri **temeljne odrednice:**

1. Budući da su **ograničeni** gotovo svi resursi,a poduzeće orijentirano na vlastiti **opstanak i povećanje prihoda**, od ključne je važnosti direktan angažman vlasnika ili rukovoditelja poduzeća,
2. U ovoj fazi cilj vlasnika ili rukovoditelja nije postizanje visokih razina mjera informacijske sigurnosti kao odgovora na rizik ili prijetnje po informacijsku imovinu. Temeljni cilj treba biti upoznavanje s ispravnom **organizacijom funkcije informacijske sigurnosti** i razumijevanje vlastitih obaveza u osiguravanju te da ispravna primjena te funkcije mora rezultirati smanjenjem razine rizika po informacijske sustave poduzeća,
3. Naposljetku, nužno je provesti neke temeljne **tehničke protumjere** iz **kataloga temeljnih mjera informacijske sigurnosti**. Pritom treba prepoznati kako nije za sve mjere informacijske sigurnosti nužna visoka razina osiguranih financijskih sredstava jer se temeljne mjere mogu provesti korištenjem besplatnog softvera, konfiguriranjem postojećeg softvera a osobito operativnih sustava, te educiranjem direktora i rukovoditelja po pitanju mjera i tehnologije informacijske sigurnosti.

Na **drugoj razini** koja načelno odgovara malim poduzećima, moguće je identificirati sljedeće **korake**, odnosno mjere čija implementacija može biti odgovarajuća na srednjoj razini kompleksnosti i za poduzeća koja ne spadaju nužno u skupinu malih poduzeća prema uobičajenim kriterijima:

1. Jasno definiranje **pravila informacijske sigurnosti** na načelnoj razini korištenjem procedura i inzistiranjem na njihovom adaptiranju u svakodnevnoj praksi, no bez formalizacije u vidu dokumenata,
2. Definiranje **odgovornosti** za provođenje informacijske sigurnosti na način da se informacijska sigurnost provodi po čitavoj vertikalnoj i horizontalnoj razini poduzeća, odnosno da su svi dionici odgovorni za sigurnost informacija u vlastitoj domeni, dok se provedbena koordinacija te aktivnosti obavlja pod kontrolom rukovoditelja odjela ili poslovnih funkcija, odnosno fokusira ka upravljačkom vrhu poduzeća, sve do najviše razine vlasnika ili rukovoditelja,

3. Početak aktivnosti **planiranja oporavka od katastrofe**, kao začetka sveobuhvatnog plana kontinuiteta poslovanja (Tijan, et al., 2009, pp. 252-258), čime se dodatno daje na značaju informacijskoj sigurnosti kao funkciji, i

4. Kreiranje općeg **pregleda informacijske sigur**nosti kroz plan informacijske sigurnosti i uvedenih informacijske sigurnosti kao osnove za dalji razvoj i provođenje.

Na **trećoj razini** moguće je identificirati način provođenja informacijske sigurnosti koji bi okvirno odgovarao srednjim poduzećima, ali se može primjenjivati i u onim poduzećima koja imaju pojačanu potrebu za koherentnim sustavom upravljanja informacijskom sigurnošću neovisno o formalnim kriterijima. U takvim je poduzećima moguće identificirati **korake i mjere** dodatnog učvršćivanja informacijske sigurnosti, koje se izlažu u nastavku.

1. Čvršće definiranje i formaliziranje **politika i procedura** informacijske sigurnosti, ukoliko je moguće, kroz obrasce prepoznate u okviru standarda upravljanja poslovnom informatikom na način kako je to uobičajeno u velikim poduzećima te kroz međunarodne standarde informacijske sigurnosti,

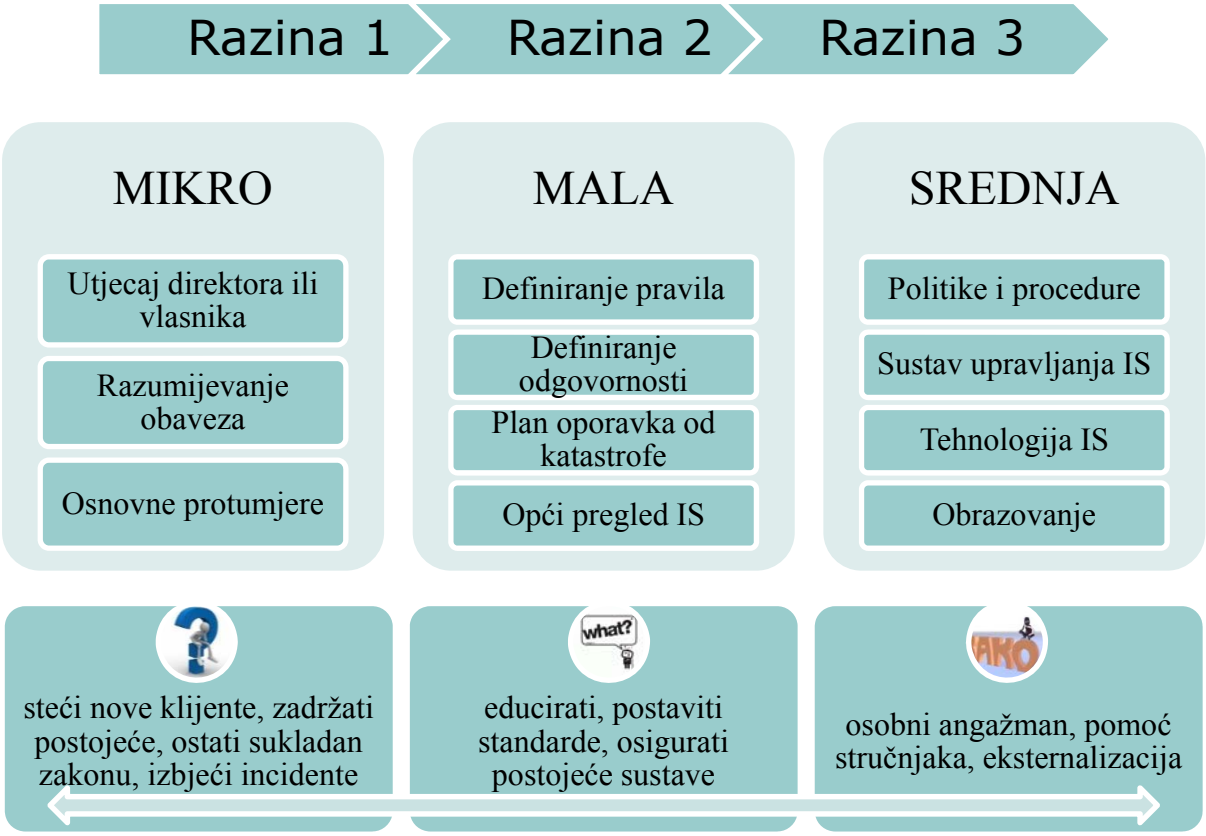
2. Uspostavljanje **sustava upravljanja informacijskom sigurnošću** u svim svojim formalnim elementima,

3. Uvođenje **tehnološke podloge** za upravljanje informacijskom sigurnošću kao odgovora na identificirane rizike informacijske sigurnosti koji se otklanjaju mjerama informacijske sigurnosti i, naposljetku,

4. Konstantno **obrazovanje** u području informacijske sigurnosti, kako vlasnika i rukovoditelja, tako i svih zaposlenika.

Navedeni principi i njihov međuodnos prikazani su na shemi 17. na sljedećoj stranici.

Shema 17: Prijedlog razvojnih koraka implementacije modela informacijske sigurnosti u malim i srednjim poduzećima po razinama



Izvor: priredio autor

Za svaku od tri predložene razine moguće je identificirati i **poveznicu** prema prethodnom, pojednostavljenom hijerarhijsko-piramidalnom modelu, te se to i čini u podnožju sva tri navedena koraka razvojnog modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima.

7.1.1.6. Ekonomsko razmatranje interakcije internog perimetra i okoline malih i srednjih poduzeća u aktivnostima provođenja informacijske sigurnosti

U analizi financijske održivosti sustava informacijske sigurnosti u malim i srednjim poduzećima, iz navedenog slijedi kako je nužno je sučeliti, uz kvantificiranje obje strane, one rizike kojima je izložena informacijska imovina poduzeća, s onim mjerama koje poduzeće poduzima kako bi adresiralo identificirane rizike. Ovaj koncept prikazan je na shemi 18. Svako poduzeće tijekom obavljanja svoje poslovne djelatnosti mora upravljati dvjema **konceptima**:

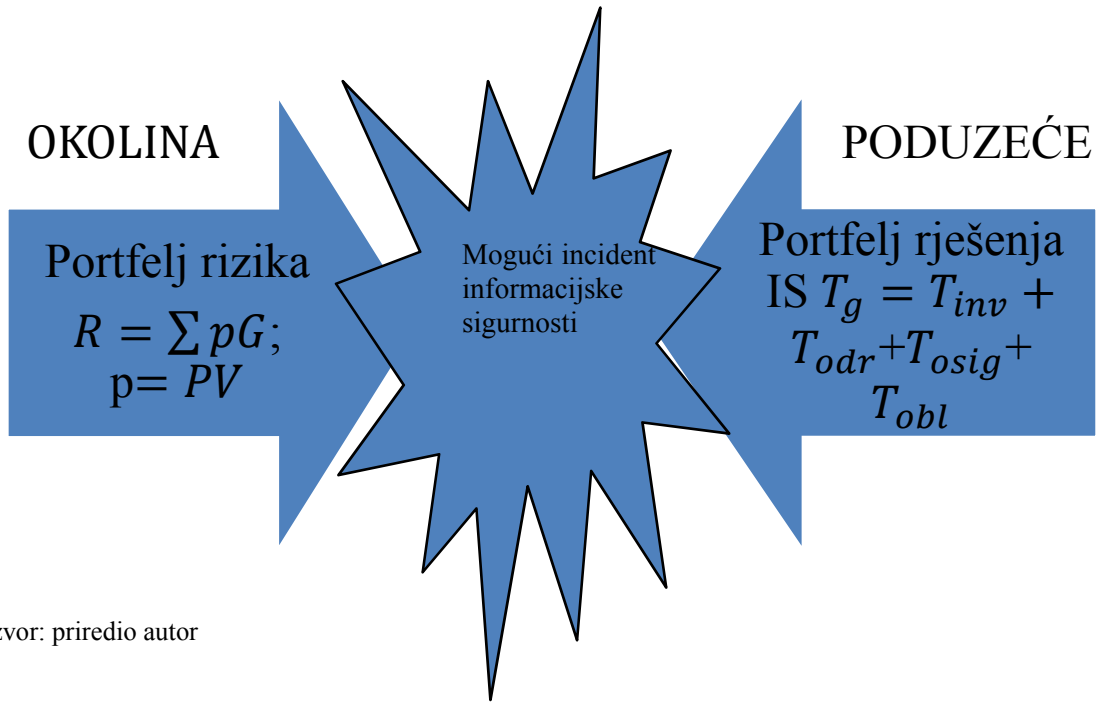
1. **Skup svih rizika informacijske sigurnosti**, koji svoj izvor imaju u ranjivostima informacijske imovine koju poduzeće posjeduje i koristi; ovaj skup rizika u svojoj cjelokupnosti predstavlja **portfelj rizika**. Inherentna osobina portfelja rizika je da poduzeće

rizicima u pravilu ne može upravljati, iako je „*upravljanje rizicima*“ uvriježen pojam u korporativnom upravljanju, već može upravljati isključivo mjerama informacijske sigurnosti kojima se odupire nastupu incidenata informacijske sigurnosti ili umanjuje njihove posljedice. Skup svih rizika informacijske sigurnosti može se smatrati portfeljem rizika. Uobičajeno su procjene rizika informacijske sigurnosti u poduzećima aktivnosti koje su uslijed prirode same aktivnosti kvalitativni pristup procjeni kvantitativnih vrijednosti. Za mala i srednja poduzeća, ključno je kvantificirati rizik u terminima raspoloživih financijskih sredstava za provođenje protumjera.

2. **Skup svih tehničkih, logičkih, organizacijskih i transfernih rješenja** kojima se poduzeće štiti od nastupa i posljedica incidenata informacijske sigurnosti. Ova rješenja su identificirana kao protumjere za korespondirajuće rizike informacijske sigurnosti. Skup svih takvih rješenja predstavlja portfelj rješenja informacijske sigurnosti za koji je također nužno identificirati koliki je njegov ekonomski i financijski utjecaj na poslovanje poduzeća. Inherentna osobina portfelja rješenja informacijske sigurnosti jeste da ona prate istu ekonomsku logiku kao i druga imovina koju poduzeća koriste u svom poslovanju. Također, poduzeća mogu u većini slučajeva birati žele li implementirati rješenja informacijske sigurnosti kroz investicije u vlastitu materijalnu ili nematerijalnu imovinu, ili na način da rješenja informacijske sigurnosti unajmljuju ili koriste kao usluge računalstva „u oblaku“, u slučaju čega ova aktivnost postaje dijelom operativnih troškova poduzeća.

Ova dva koncepta sa svojim sastavnicama prikazani su na shemi 18.

Shema 18: Interakcija internog perimetra i okoline malih i srednjih poduzeća u aktivnostima provođenja informacijske sigurnosti



Izvor: priredio autor

Kao što se vidi iz sheme 18, poduzeće se **portfeljem rješenja**[266] **informacijske sigurnosti**, koja može kontrolirati, suprotstavlja **portfelju rizika** koji dolaze iz okoline poduzeća, ili su posljedica inherentnih osobina (ranjivosti) identificirane informacijske imovine poduzeća.

Ukupna mogućnost nastupa rizika informacijske sigurnosti ekvivalentna je zbroju negativnih utjecaja mogućnosti nastupa pojedinih rizika informacijske sigurnosti. Kvantificiranje rizika nastupa pojedinog incidenta informacijske sigurnosti predstavlja se umnoškom vjerojatnosti nastupa incidenta informacijske sigurnosti i točno određenog ili predviđenog iznosa financijskog gubitka uslijed nastupa incidenta informacijske sigurnosti. Ove **odnose** prikazuje sljedeća formula:

$$R = \sum pG; \text{ gdje je}$$

- R, rizik,
- p, vjerojatnost nastupa incidenta informacijske sigurnosti,
- G, gubitak uslijed nastupa incidenta informacijske sigurnosti.

Vjerojatnost nastupa incidenta informacijske sigurnosti je jednaka umnošku **kvantificirane prijetnje**, odnosno vjerojatnosti nastupa prijetnje informacijskoj sigurnosti i **ranjivosti**, koja je zapravo vjerojatnost iskorištenja identificirane slabosti kao inherentne osobine informacijske imovine. Ove odnose prikazuje sljedeća formula:

$$p = PV;$$

1. P, **prijetnja**, predstavljena vjerojatnošću da će nastupiti prijetnja informacijskoj sigurnosti,
2. V, **ranjivost**, predstavljena vjerojatnošću da će slabost biti iskorištena i rezultirati nastupom incidenta informacijske sigurnosti.

Za mala i srednja poduzeća ključno je točno godišnje proračunsko planiranje raspoloživih financijskih sredstava za provođenje mjera informacijske sigurnosti. U tom smislu, moguće je s obzirom na vrstu utroška identificirati kako je godišnji utrošak za investicijsku sigurnost suma investicijskih troškova, troškova održavanja postojećeg sustava, troškova osiguranja i informacijske sigurnosti računalstva u oblaku. Kod primjera računalstva u oblaku, trošak informacijske sigurnosti se zapravo **transferira** na pružatelje takvih usluga, te se može uzeti kako je on zapravo jednak nuli, odnosno, interni trošak računalstva u oblaku je zapravo jednak

[266] Rješenjima informacijske sigurnosti poduzeća i organizacije pokušavaju adekvatno ispuniti zahtjeve identificiranih mjera informacijske sigurnosti koje je potrebno provesti.

trošku informacijske sigurnosti onih temeljnih informacijsko-komunikacijskih sustava koji služe za korištenje takvih usluga, odnosno već postoje unutar poduzeća. Prema tome:

$$\mathrm{T_g} = \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{T_{inv}} + \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{T_{odr}} + \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{T_{osig}} + \sum_{i=1}^{n} T_{obl} + T_c;$$

$$\mathrm{T_g} = \mathrm{T_{inv}} + \mathrm{T_{odr}} + \mathrm{T_{osig}} + \mathrm{T_{obl}} + T_c;$$

- T_g , godišnji utrošak za informacijsku sigurnost u malom ili srednjem poduzeću,
- T_{inv} , investicijski trošak informacijske sigurnosti,
- T_{odr}, trošak održavanja rješenja informacijske sigurnosti,
- T_{osig}, trošak osiguranja (transfera rizika) informacijske sigurnosti,
- T_{obl}, trošak informacijske sigurnosti računalstva u oblaku ($T_{obl} = 0$),
- T_c, relativno fiksan ostali trošak informacijske sigurnosti (T_c=const.).

Budući kako je objašnjeno da je u uobičajenim okolnostima $\mathrm{T_{obl}} = 0$, može se uzeti da je direktan godišnji trošak informacijske sigurnosti u malim i srednjim poduzećima jednak **sumi** godišnjih investicija, troškova održavanja i troškova osiguranja:

$$\mathrm{T_g} = \mathrm{T_{inv}} + \mathrm{T_{odr}} + \mathrm{T_{osig}} + T_c$$

Ovakvo razmatranje nužno radi pojednostavljenja procesa i prilagodbe realnosti poslovanja malih i srednjih poduzeća dovodi do zanemarivanja nekih vezanih troškova za koje se pretpostavlja kako će ostati relativno konstantni, iz razloga što će mala i srednja poduzeća koristiti postojeće kapacitete za provođenje mjera informacijske sigurnosti, odnosno bit će izloženi isključivo oportunitetnom trošku propuštanja angažiranja rada zaposlenika na drugim radnim zadacima. Priroda ovog oportunitetnog troška je kompleksna, jer on nije u punom iznosu, već u razlici između punog oportunitetnog troška i troška uloženog rada u implementaciju mjera informacijske sigurnosti, ali samo u one rizike koji nisu nastupili. Osim toga, u relativno konstantni trošak informacijske sigurnosti pripada i trošak potrošnog materijala koji koriste zaposlenici koji rade na zadacima vezanim uz implementaciju i održavanje informacijske sigurnosti, trošak uredskog poslovanja[267] i sl. U svrhu ovog modela, uzima se kako je ovakav trošak relativno fiksan. Ovaj dio troška vrlo je komplicirano kvantificirati, ali je njegov udio u ukupnom trošku informacijske sigurnosti također relativno malen.

[267] U ovu skupinu spadaju npr. trošak struje, klimatizacije, vode, najma prostora, te ostali vezani troškovi poslovanja.

Naposljetku, drugi ključan uvjet za ekonomsku održivost ovako postavljenog modela vezan je uz **financijska sredstva** koja su na raspolaganju poduzeću za provođenje poslovne funkcije informacijske sigurnosti:

$$T_g \leq S_{IS},$$

pri čemu je S_{IS} mogući **maksimalni iznos godišnjeg proračuna** malog ili srednjeg poduzeća za svrhu informacijske sigurnosti.

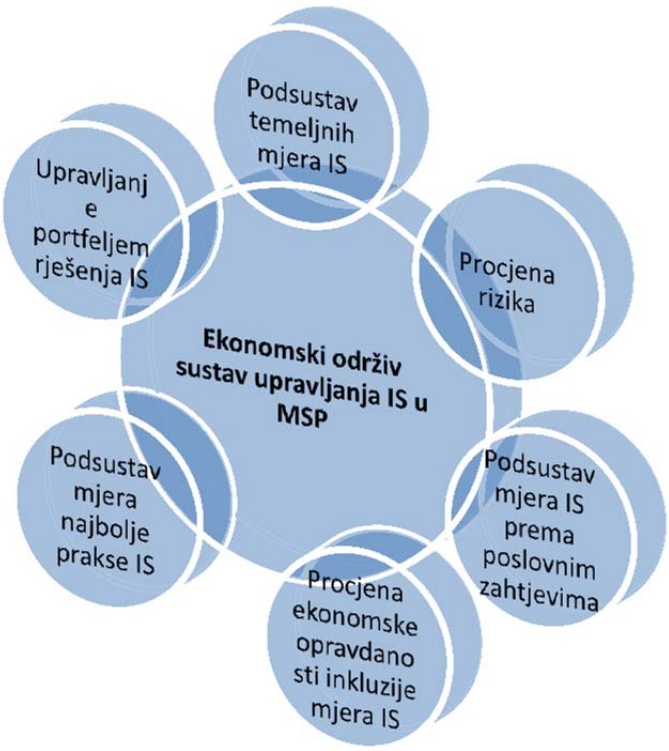
7.1.1.7. Definiranje odrednica modela ekonomski održivog upravljanja informacijskom sigurnošću u malim i srednjim poduzećima

Iz do sada izloženog slijedi kako model ekonomski održivoga upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj sadrži odgovarajući broj temeljnih **odrednica**. Radi se o podsustavima, ili funkcijama, koje moraju biti implementirane na odgovarajući način kako bi se postigla funkcionalnost modela i temeljni cilj informacijske sigurnosti u malim i srednjim poduzećima: osiguravanje informacija poduzeća od neovlaštenog pristupa korištenjem sustavnog upravljačkog pristupa kod kojega se identificirani rizici informacijske sigurnosti umanjuju ili uklanjanju do željene razine primjenom mjera informacijske sigurnosti koje su vlasnicima ili rukovoditeljima poduzeća prihvatljive s obzirom na odnos izmjerene razine rizika i troška implementacije mjera.

Odrednice tog modela definiraju se kako slijedi, a prikazane su na shemi 19 na sljedećoj stranici:

1. Podsustav temeljnih mjera informacijske sigurnosti,
2. Podsustav procjene rizika,
3. Podsustav mjera informacijske sigurnosti prema poslovnim zahtjevima,
4. Podsustav mjera najbolje prakse informacijske sigurnosti,
5. Podsustav ekonomske opravdanosti inkluzije mjera informacijske sigurnosti,
6. Upravljanje portfeljem rješenja informacijske sigurnosti.

Shema 19: Prijedlog sastavnih odrednica modela ekonomski održivog upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj



Izvor: priredio autor

Navedene odrednice modela ekonomski održivog sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima ne nalaze se na istoj hijerarhijskoj razini. Hijerarhijski odnos podsustava prikazan je na shemi 20. Predlaže se implementacija pojednostavljenog sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima koji se sastoji od tri temeljna podsustava:

1. Podsustav temeljne edukacije i provođenja protumjera,
2. Podsustav implementacije sukladnosti, i
3. Podsustav ekonomske evaluacije mjera informacijske sigurnosti

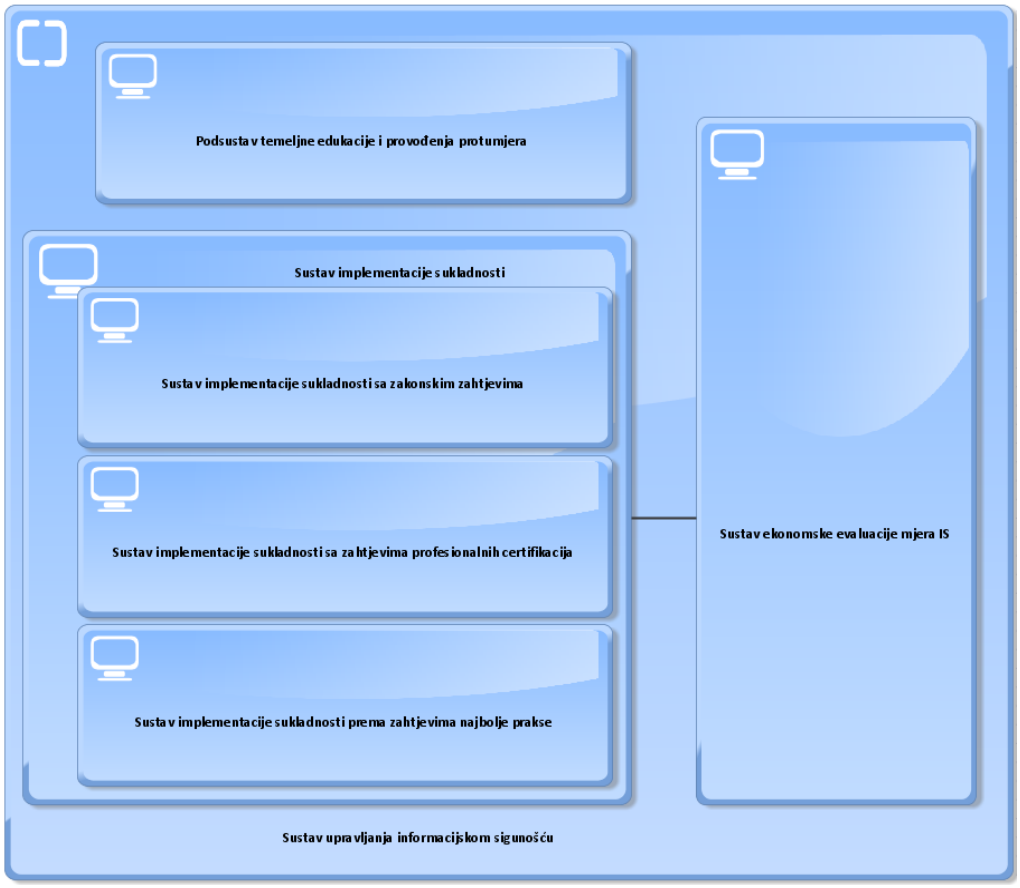
Podsustav implementacije sukladnosti dodatno se sastoji od tri podsustava:

1. Podsustav implementacije sukladnosti sa zakonskim zahtjevima,
2. Podsustav implementacije sukladnosti sa zahtjevima profesionalnih certifikacija,
3. Podsustav implementacije sukladnosti prema zahtjevima najbolje prakse

Podsustav ekonomske evaluacije mjera informacijske sigurnosti prikazan je u shemi 20. na sljedećoj stranici korištenjem *ARIS Express* modela informatičke infrastrukture. Na modelu se vide međuodnosi između pojedinih podsustava modela, kao i činjenica da sustav ekonomske evaluacije mjera informacijske sigurnosti tijesno funkcionira u sprezi sa sva tri podsustava

sustava implementacije sukladnosti. To znači da će podsustavi sustava implementacije sukladnosti tijekom provođenja svojih aktivnosti u svakom koraku pozivati funkcionalnosti sustava ekonomske evaluacije mjera informacijske sigurnosti kako bi se osiguralo da analizirana mjera informacijske sigurnosti osim tehničke opravdanosti u smislu umanjenja ili uklanjanja određenog rizika također bude i dijelom unaprijed određenog proračuna poduzeća odvojenog u tu svrhu, ali i primjeren s obzirom na točno određenu količinu rizika koji otklanja.

Shema 20: Prijedlog podsustava modela ekonomski održivog upravljanja informacijskom sigurnošću u malim i srednjim poduzećima (makro pogled)



Izvor: priredio autor

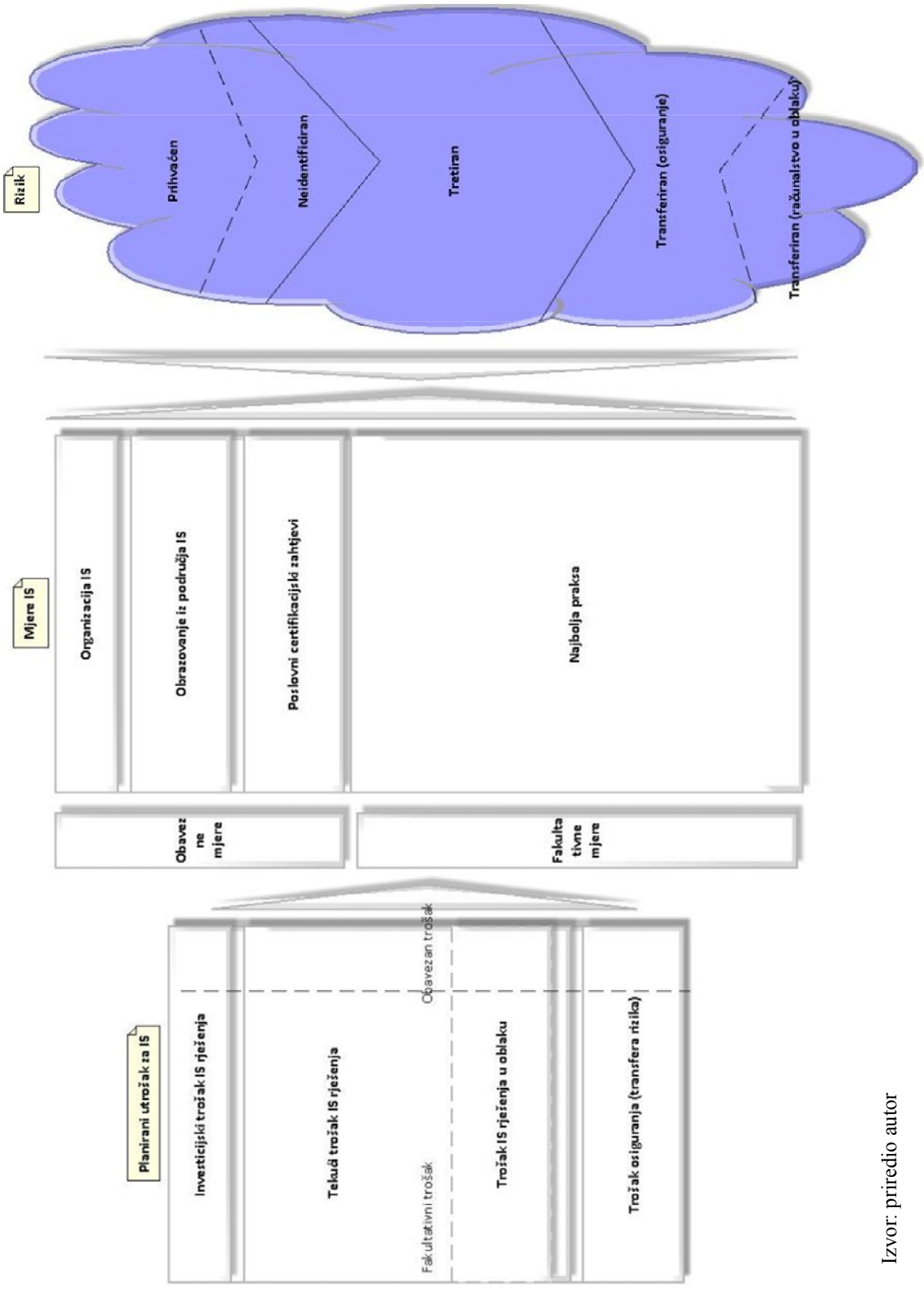
Prema definiciji čimbenika s makro razine koji su zatečeni u okolini i unutar samih i malih poduzeća, definiranju značajnih razlika u organizaciji i provođenju informacijske sigurnosti u velikim u odnosu na mala i srednja poduzeća, dovršetku analize pokretača i motivatora malih i srednjih poduzeća u organizaciji i provođenju informacijske sigurnosti, adaptiranju modificiranog stratificiranog sustava upravljanja na tri razine sukladno klasifikaciji veličine poduzeća, te nakon što su definirane sile koje utječu na odabir mjera informacijske sigurnosti koje tvore portfelj rješenja informacijske sigurnosti i predložene sastavne odrednice modela ekonomski održivog upravljanja informacijskom sigurnošću i njihove organizacije u

podsustave, te po objašnjenju rasporeda i interakcije podsustava modela, moguće je napraviti dodatni korak naprijed i stratificirati sve navedene elemente u tri stupa, te objasniti njihovu međusobnu povezanost. To su:

1. Planirani utrošak za informacijsku sigurnost,
2. Vrste mjera informacijske sigurnosti,
3. Vrste i razine rizika informacijske sigurnosti.

Planirani utrošak za informacijsku sigurnost na godišnjoj razini može se po horizontali podijeliti na trošak investicijskih ulaganja u mjere informacijske sigurnosti, trošak održavanja i korištenja mjera informacijske sigurnosti (uključuje trošak najma ili leasinga rješenja informacijske sigurnosti, osiguranje i korištenje usluga računalstva *„u oblaku"*), te trošak osiguranja od nastupa incidenata informacijske sigurnosti. Po vertikali, a ovisno o fazi implementacije sustava upravljanja informacijskom sigurnošću, ovaj se trošak može podijeliti na obligatorni (obavezni), predstavljen implementacijom onih mjera koje su nužne za postizanje zakonske sukladnosti po pitanju informacijske sigurnosti, te na fakultativne mjere, a to su mjere o kojima rukovoditelji i vlasnici poduzeća mogu odlučivati kako bi postigli ciljeve poslovne certifikacije sustava upravljanja informacijskom sigurnošću ili one koji se odnose na najbolju praksu.

Portfelju rizika informacijske sigurnosti kojima je izložen sustav upravljanja informacijskom sigrnošću suprotstavljen je portfelj informacijsko-sigurnosnih rješenja kojima se pojedini rizici uklanjaju ili umanjuju. Pritom valja napomenuti, kao što je prikazano na elementima s desne strane na shemi 2. na sljedećoj stranici, kako se rizik može podijeliti u nekoliko temeljnih kategorija. Ukupnost rizika bi trebala biti čim više identificirana, a čim manji dio rizika bi trebao biti neidentificiran. Posljedično, čim viša razina ukupnog rizika trebala bi biti tretirana mjerama otklanjanja rizika a čim manje rizika treba biti netretirano ili prihvaćeno.



Izvor: priredio autor

Identificirani rizik se tretira mjerama informacijske sigurnosti, transferira se na treće strane (dionike, npr. dobavljače rješenja informacijske sigurnosti korištenjem softvera kao usluge), ili se transferira na treće strane kroz korištenje usluga računalstva „*u oblaku*“. Ostatak do punog

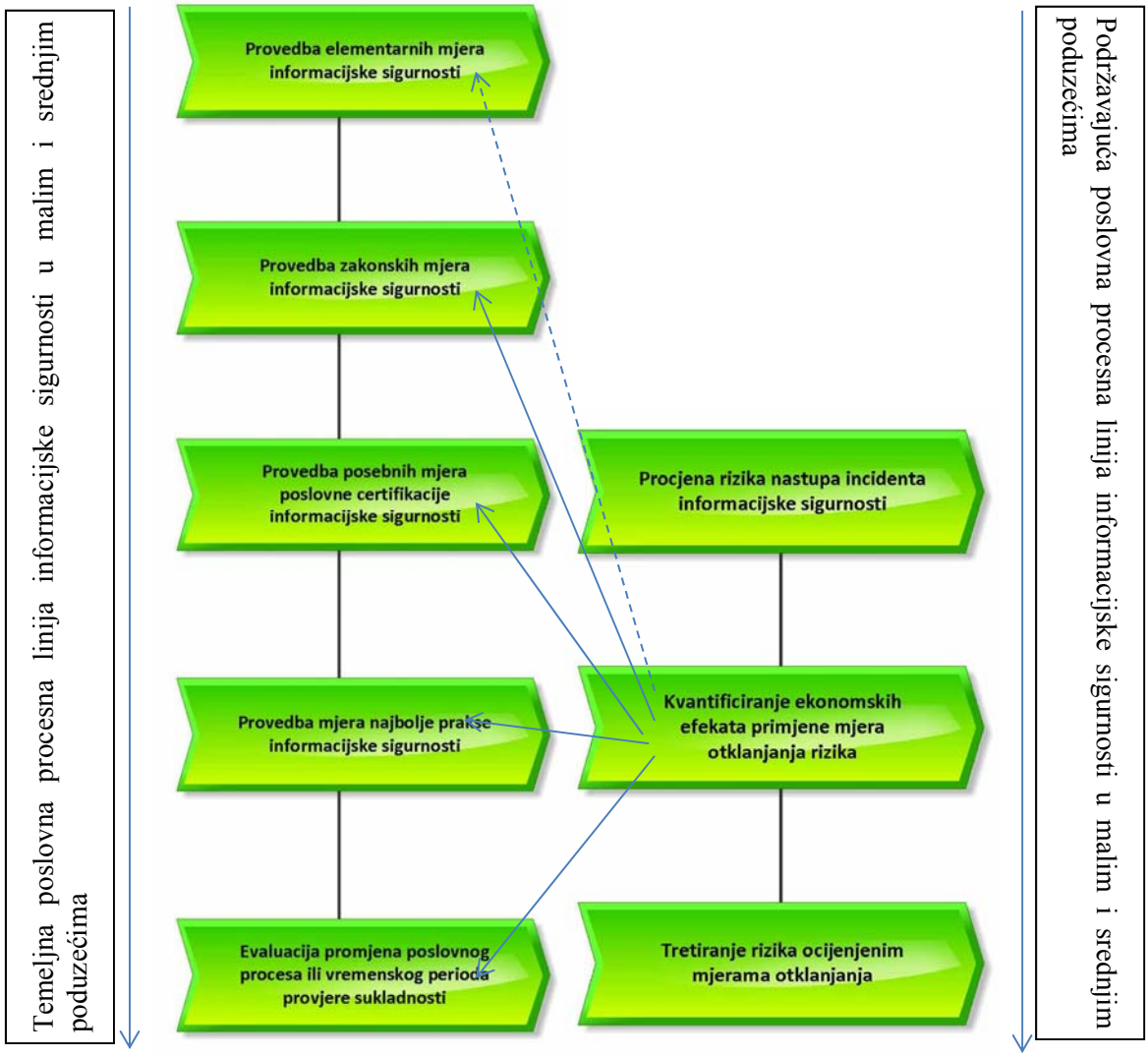
iznosa rizika je prihvaćeni rizik, čije bi uklanjanje ili umanjivanje koštalo više od troška njegovog nastupa.

Mjere informacijske sigurnosti prikazane u centralnom dijelu sheme 21. također se mogu podijeliti na obavezne mjere i fakultativne mjere. Obavezne su mjere one koje se odnose na postizanje zakonske sukladnosti poduzeća te temeljne organizacije poslovne funkcije informacijske sigurnosti i obrazovanja iz područja informacijske sigurnosti, a koje provode neposredno rukovoditelji i vlasnici. Fakultativne mjere se odnose na sukladnost sa sustavima najbolje prakse.

7.1.2. Provedbene aktivnosti i aktivnosti praćenja implementiranog modela

Korištenjem *ARIS Express* modela procesnog krajobraza, ovi se temeljni procesi prikazuju u shemi 22. na sljedećoj stranici. Model procesnog krajobraza specificira one procese u provođenju procesa osiguravanja informacijske sigurnosti koji su primarni čimbenici, odnosno motivatori kreiranja dodane vrijednosti poslovne funkcije informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj. Ovi se procesi, koji se mogu smatrati makro-procesima najviše razine, povezuju u funkcionalnom slijedu koji u svojoj cjelini tvori model procesnih krajobraza. Pritom valja primijetiti kako su u zadanom slučaju navedeni procesi poredani hijerarhijski u navedenom modelu, odnosno održana je procesno orijentirana hijerarhija. U prikazanom modelu procesnih krajobraza, procesna linija s lijeve strane predstavlja one procese koji se izvode u slijedu a koji se izvode **u kontinuitetu**, jer proces upravljanja informacijskom sigurnosti predstavlja aktivnost koja nikada nije dovršena, već se nalazi u ciklusu konstantnog ponovljenog evaluiranja uslijed promjene vrste ili svojstava informacijske imovine, poslovnog procesa ili eksternih zakonskih, odnosno certifikacijskih zahtjeva. S desne strane izloženog modela nalaze se **podržavajuće aktivnosti** temeljnoj aktivnosti koje također imaju svoj hijerarhijski slijed i odnose se na aktivnost procjene informacijskog rizika koji se ekonomski kvantificira, uspoređuje s troškom nastupa rizika te se donose odluke o ulaganju ili propuštanju ulaganja u mjere informacijske sigurnosti.

Shema 22: Temeljna i podržavajuća procesna linija informacijske sigurnosti



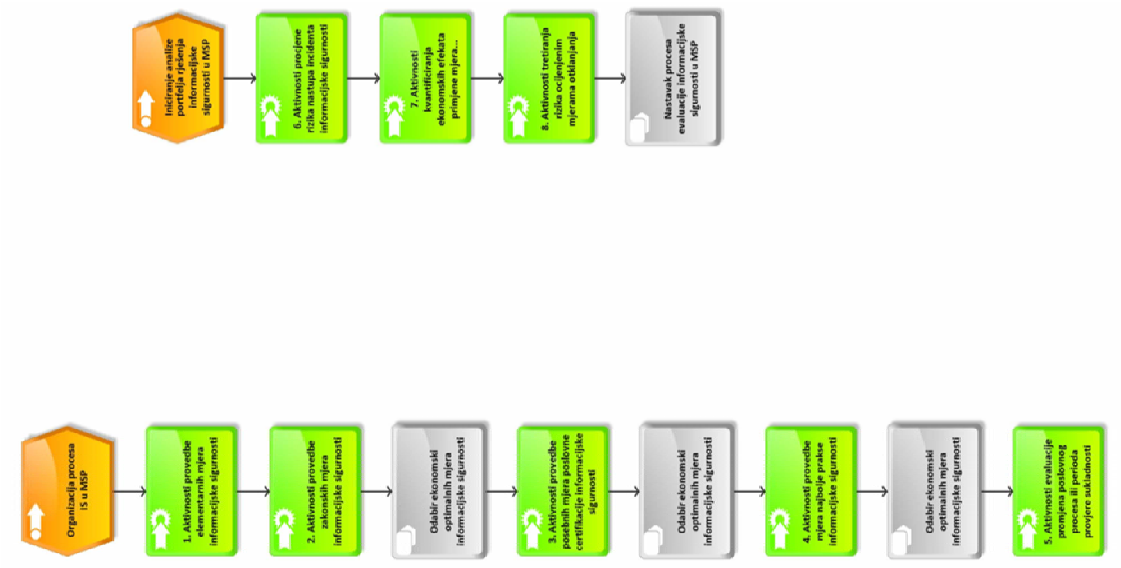
Izvor: priredio autor

Podržavajuće aktivnosti informacijske sigurnosti se odvijaju u svim procesima glavnih procesa informacijske sigurnosti, osim u prvoj – provedbi elementarnih mjera informacijske sigurnosti. Te mjere ne zahtijevaju značajna materijalna sredstava u odnosu na ostala četiri procesa, fokus njihovog provođenja je na osiguravanju pažnje vlasnika i rukovoditelja najviše razine, te primarno ovise o svijesti i volji rukovoditelja i vlasnika kako je poslovna funkcija informacijske sigurnosti jedna od temeljnih poslovnih funkcija koja se prožima sa svim ostalim poslovnim funkcijama te može imati odlučujući pozitivan, ali i negativan utjecaj na temeljno poslovanje poduzeća. Iz tog razloga, evaluacija rizika i kvantificiranje ekonomskih efekata primjene elementarnih mjera informacijske sigurnosti nisu podržavajuće aktivnosti za koje se predviđa kako bi ih u cijelosti trebalo implementirati tijekom provođenja prvog procesa temeljne procesne linije informacijske sigurnosti, iako je metodološki ispravno ostaviti na volju vlasnicima i rukovoditeljima žele li to učiniti. Naime, u samim počecima uvođenja poslovne

funkcije informacijske sigurnosti u okruženja uobičajena za mala i srednja poduzeća nije realistično očekivati kako sami vlasnici i rukovoditelji mogu provesti proces procjene rizika, ekonomske evaluacije mjera i implementacije mjera kojima se rizik uklanja ili umanjuje. Iz tog razloga očekuje se kako je podržavajuću procesnu liniju informacijske sigurnosti moguće implementirati tek po primjeni elementarnih mjera i kada poduzeće te svi dionici dostignu odgovarajuću minimalnu razinu znanja i već uvedenih elementarnih mjera, odnosno kada informacijska sigurnost postane jednim od ključnih čimbenika poslovanja.

Dalja razrada navedenog principa međuodnosa temeljnih procesa informacijske sigurnosti i potpornih procesa prikazana je na shemi 23. Radi jednostavnosti nisu prikazani procesni putevi utjecaja, odnosno inkorporiranja potpornih makro-procesnih aktivnosti na temeljne procese informacijske sigurnosti. Rednim brojevima od 1.-8. su označeni temeljni procesi na obje procesne vertikale a ta će numeracija radi lakše identifikacije biti zadržana i u nastavku. Kao što se vidi, u izradi ovog modela koristi se *ARIS Express* element procesne poveznice. Njegova je svrha uspostavljanje **veze između procesa više razine**, a u ovom slučaju prethodnog procesa i novog procesnog puta, te služi za povezivanje modela, odnosno procesnih puteva iste razine.

Shema 23: Međuodnos temeljnih procesa informacijske sigurnosti i potpornih procesa (rotirano)



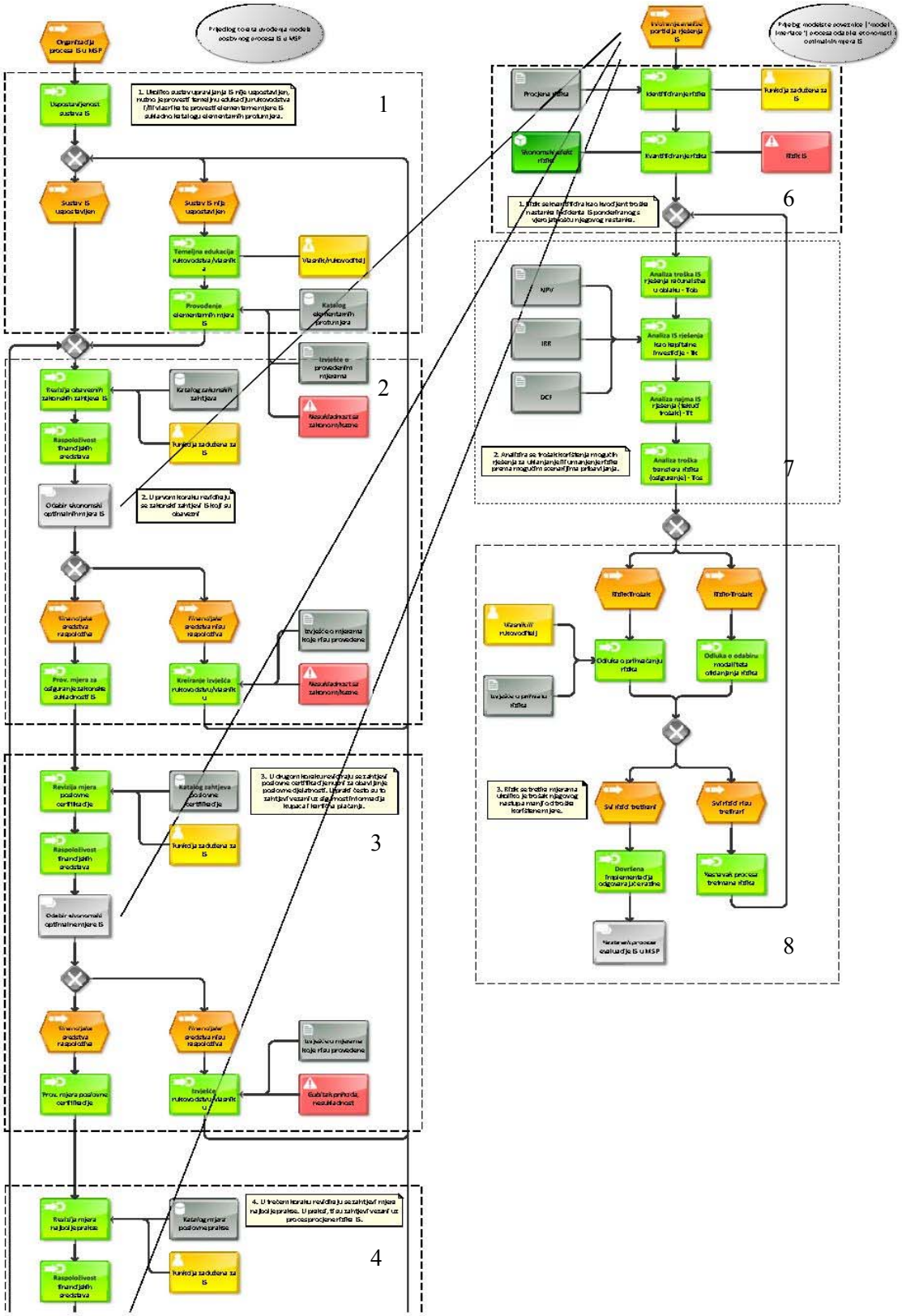
Izvor: priredio autor

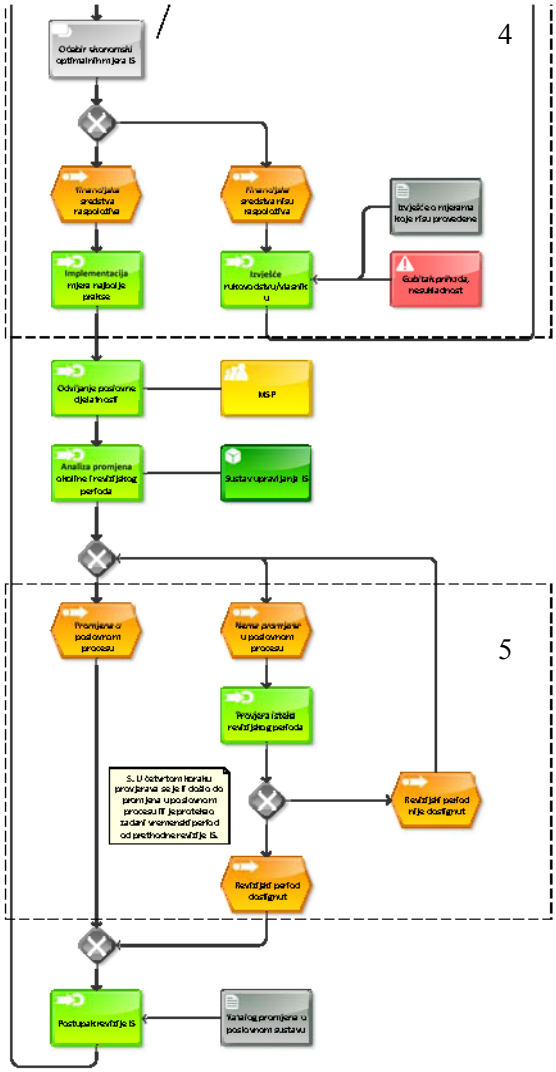
Naposljetku, na shemi 24 prikazana je dodatna **razrada** svih procesa opisanih aktivnosti s **oba procesna puta**. Kao što se vidi, na toj shemi su i dalje zadržana dva procesna puta: temeljni procesi informacijske sigurnosti, označeni brojevima od 1. do 5., te potporni informacijske sigurnosti koji su označeni brojevima 6. do 8. Važno je naglasiti kako se navedeni procesi odnose i na aktivnost uvođenja i kasnijeg provođenja, odnosno održavanja sustava

informacijske sigurnosti u malim i srednjim poduzećima jer je sam *ciklus zatvoren, odnosno nema kraj, već se radi o ciklusu koji je sukladan Demingovom PDCA* ciklusu upravljanja kvalitetom u poduzećima. U odgovarajućim točkama temeljnih procesa informacijske sigurnosti pozivaju se **proceduralni podržavajući procesi** predstavljeni procjenom rizika, financijskom evaluacijom mjera informacijske sigurnosti i njihovog provođenja. Budući da proces implementacije u modelu slijedi nakon procesa ekonomske evaluacije (procjene) uključivosti mjera informacijske sigurnosti u portfelj rješenja informacijske sigurnosti a on slijedi procjenu rizika, u sam model ugrađena je i koncept da niti jedna mjera informacijske sigurnosti, a samim time niti jedan trošak odnosno investicija, ne bi smjeli biti poduzeti ukoliko nisu prošli i proces profesionalne (tehničke) procjene reprezentiran procjenom informacijskog rizika, i proces ekonomske evaluacije. Potrebno je primijetiti kako se u odgovarajućim točkama procesnih puteva koriste, sukladno pravilima modeliranja poslovnih procesa, **operatori** koji odvajaju pojedine grane procesnih puteva ovisno o tome jesu li ili nisu zadovoljeni odgovarajući uvjeti koji su reprezentirani odvijanjem događaja, a zatim se nakon odabira jednog od raspoloživih procesnih puteva izvode odgovarajuće aktivnosti provedbe, odnosno, govoreći jezikom procesnog modeliranja, funkcije. U modelu se navode i mogući **rizici** koje je moguće identificirati u samom procesu uvođenja i provođenja poslovne funkcije informacijske sigurnosti, te neki dokumenti i baze podataka koji mogu biti korišteni u samom procesu.

Sam model izrađen je na način da je orijentiran na **procese** i **metodologiju**, ali **ne na prileţeću tehnologiju**. Ova je zamisao sustavno provedena od samog početka modeliranja, budući da mala i srednja poduzeća među kojima mogu biti najmanja mikro poduzeća koja zapravo nemaju niti jednu zaposlenu osobu već je cjelokupno upravljanje prepušteno vlasnicima često ne posjeduju niti elementarnu informatičku infrastrukturu u terminima kadrova, mrežnih illi hardverskih te nematerijalnih resursa koja je potrebna za organizaciju informacijske sigurnosti. Osim toga, tehnička komponenta informacijske sigurnosti podložna je neprestanim promjenama uslijed promjene svojstava informacijske imovine i rizika.

Shema 24 : Model upravljanja informacijskom sigurnošću u malim i srednjim poduzećima





Izvor: izrada doktorand

Iz navedenog razloga je adaptiran fleksibilan pristup pri kojemu se materijalna stvarnost ne zadaje osim procesno, te kada je to apsolutno nužno, a na vlasnicima i rukovoditeljima ostaje da je organiziraju na način koji je najviše podesan raspoloživim resursima poduzeća i zatečenoj razini razvijenosti informatičke funkcije, prihodovnoj i tržišnoj poziciji te poslovnoj politici i dostignutoj cikličkoj fazi zrelosti u kojoj se poduzeće nalazi. Granice pojedinih makro-procesa naznačene su iscrtanim linijama.

U nastavku se detaljno analiziraju redom svi makro-procesi informacijske sigurnosti u malim i srednjim poduzećima označeni na shemi s 1. do 8., i to na obje procesne vertikalne uvođenja informacijske sigurnosti i potpornih makro-procesa provođenja. Ove su aktivnosti izložene u dvije povezane cjeline: **1) Temeljne aktivnosti** i **2) Podržavajuće aktivnosti.**

7.1.2.1. Temeljne aktivnosti

Izlaganje temeljnih aktivnosti modela zahtijeva objašnjavanje sljedećih međusobno povezanih cjelina: **1) Provedba elementarnih mjera informacijske sigurnosti, 2) Provedba zakonskih mjera informacijske sigurnosti, 3) Provedba posebnih mjera poslovne certifikacije informacijske sigurnosti, 4) Provedba mjera najbolje prakse informacijske sigurnosti** i **5) Evaluacija promjena poslovnih procesa ili vremenskog perioda provjere sukladnosti.**

7.1.2.1.1. Provedba elementarnih mjera informacijske sigurnosti

Oznakom *„1*.“ u shemi 24. prikazan je makro-proces aktivnosti provedbe elementarnih mjera informacijske sigurnosti. Detaljna razrada tog makro-procesa prikazana je u shemi 25. Model procesa započinje događajem odnosno iniciranjem organizacije procesa informacijske sigurnosti u malom ili srednjem poduzeću. Motivatori za taj proces mogu biti različiti a ukoliko se radi o novoosnovanom poduzeću, najčešće su subjektivni jer je u vrlo ograničenom broju konteksta sigurnost poslovnih informacija temeljni proces tijekom organizacije poduzeća. S druge strane, u slučaju već postojećih poduzeća koja obavljaju poslovnu djelatnost, **motivaciju** je moguće identificirati u sljedećem :

1. Prijašnje **iskustvo** vlasnika ili rukovoditelja i želja za uvođenjem osnovnih mjera informacijske sigurnosti,
2. Potreba za **zakonskom sukladnošću**, odnosno poštivanjem zakonskih propisa koji definiraju područje informacijske sigurnosti, a u realnosti malih i srednjih poduzeća najčešće se radi o području sigurnosti osobnih podataka ukoliko ih poduzeća obrađuju,
3. Potreba za **minimumom** postignutih mjera informacijske sigurnosti uslijed zahtjeva vanjske certifikacije u slučaju korištenja sustava kartičnog plaćanja,
4. **Gubici** (neplanirani troškovi) uslijed čestih nastupa incidenata informacijske sigurnosti, odnosno izolirani nastupi incidenata informacijske sigurnosti,
5. **Subjektivni čimbenici** poput iskustava drugih, usporedivih poduzeća, s nastupima incidenata informacijske sigurnosti.

Budući da je ovaj model jednako primjenjiv u slučaju prvog, inicijalnog uvođenja sustava informacijske sigurnosti, te kasnijih cikličkih ili periodički ponovljenih evaluacija, u modelu procesa je potrebno procijeniti je li to inicijalno ili opetovano provođenje temeljnog procesa. Ukoliko se radi o opetovanom provođenju, nije potrebno obavljati aktivnosti (funkcije) provođenja elementarnih protumjera informacijske sigurnosti. Ukoliko se radi o inicijalnom provođenju, tada je potrebno provesti dvije sukcesivne aktivnosti:

1. **Temeljna edukacija rukovoditelja** odnosno vlasnika. Radi se o osnovnoj edukaciji i upoznavanju rukovoditelja i vlasnika s modelom upravljanja informacijskom

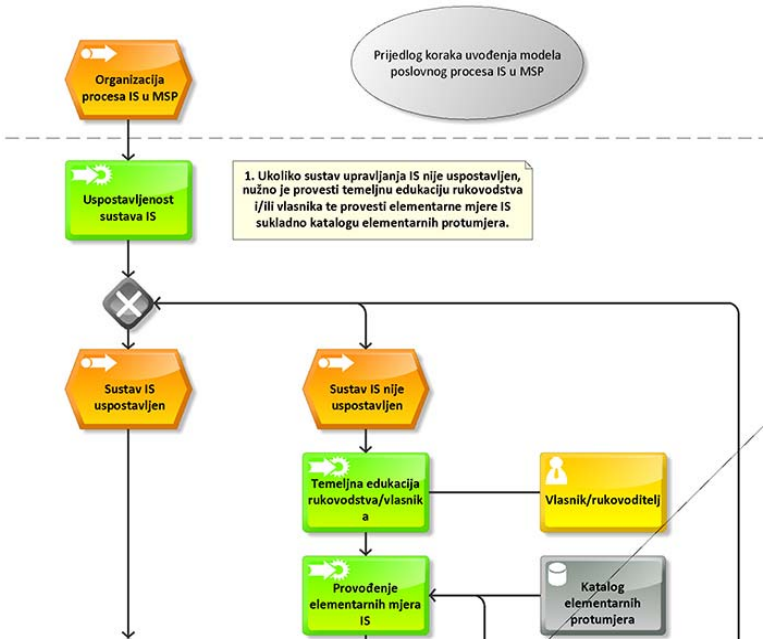
sigurnošću u malim i srednjim poduzećima, prednostima uspostavljanja takvog sustava, vezom koju je moguće uspostaviti između izmjerene ili anticipirane razine rizika i investicija ili troškova sustava upravljanja informacijskom sigurnošću i mogućim posljedicama nastupa incidenata informacijske sigurnosti. Osim toga, dio temeljne edukacije rukovoditelja i vlasnika je i upoznavanje s osnovnim konceptima i terminologijom informacijske sigurnosti, pregled modela najbolje prakse i certifikacije te prepoznavanje onih zakonskih propisa s kojima bi poduzeće moralo osigurati sukladnost u svom poslovnom području, a sukladno djelatnosti kojom se bavi. U zadanom kontekstu, temeljna edukacija može biti samoinicirana aktivnost ili aktivnost koja je svojim dijelom ili u potpunosti eksternalizirana.

2. **Provođenje elementarnih mjera** informacijske sigurnosti. Kao i kod temeljne edukacije, ova aktivnost može biti obavljena unutar poduzeća ili djelomično, odnosno u potpunosti povjerena vanjskom poduzeću, instituciji ili suradniku. Elementarne mjere informacijske sigurnosti za mala i srednja poduzeća imaju nekoliko temeljnih karakteristika: radi se o mjerama koje je moguće poduzeti bez većih troškova a njihov značaj nadilazi rizike koje uklanjaju ili umanjuju te se odnosi i na promicanje kulture informacijske sigurnosti u poduzećima, a osobito u samim počecima provođenja te aktivnosti. Opseg i broj elementarnih mjera informacijske sigurnosti ovisi o čitavom nizu čimbenika među kojima najvažniji utjecaj ima tehničko-tehnološka razina ugroza koje mogu iskazati negativan utjecaj po informacijske sustave poduzeća. Stoga bi bilo poželjno uspostavljanje kataloga elementarnih protumjera koje bi bile primjenjive na ovaj segment hrvatskih poduzeća u području informacijske sigurnosti a koji bi nadziralo neovisno stručno tijelo.[268] Polaznim taksativno nabrojanim elementarnim mjerama mogu se u nedostatku takvog kataloga i tijela smatrati i objašnjene obavezne (obligatorne) mjere informacijske sigurnosti u malim i srednjim poduzećima.

Potrebno je napomenuti kako je u slučaju malih i srednjih poduzeća realno očekivati da će vlasnici, odnosno rukovoditelji moći i delegirati provođenje elementarnih mjera informacijske sigurnosti na odgovarajuće razine unutar poduzeća, osobito u slučaju poduzeća s razvijenijom unutrašnjom strukturom i većim brojem zaposlenih, no i dalje ostaje ključna potreba da čitav proces početka provođenja mjera nadziru vlasnici i vrh rukovodstva kako bi pokazali svoju obvezanost za postizanjem ciljeva provođenja informacijske sigurnosti i uskladili poslovnu funkciju informacijske sigurnosti sa strateškim ciljevima poslovanja. Ovaj makro-proces predviđa kao izlazni dokument **izvješće o poduzetim mjerama** informacijske sigurnosti a sobom nosi rizik zakonske nesukladnosti, odnosno troškova kazni u slučaju nastupa incidenata informacijske sigurnosti. *ARIS BPM* segment ovog procesa prikazan je na shemi 25. na sljedećoj stranici.

[268] npr. stručna udruga uz sudjelovanje ostalih dionika, poput akademske zajednice.

Shema 25: Makro-proces aktivnosti provedbe elementarnih mjera informacijske sigurnosti



Izvor: priredio autor

7.1.2.1.2. Provedba zakonskih mjera informacijske sigurnosti

Po dovršetku inicijalnog provođenja mjera informacijske sigurnosti, odnosno uvođenja elementarnih mjera, modelom procesa predviđen je makro-proces označen brojkom „*2*“. u shemi 24., a radi se o **provedbi zakonskih mjera** informacijske sigurnosti, koje se prikazuju na shemi 26. Na početku provođenja ove faze, poduzeće se nalazi u situaciji da su vlasnici i rukovoditelj vlastitim primjerom i angažmanom uključeni i posvećeni provedbi informacijske sigurnosti, no poduzete mjere su jednostavne, osnovne, nije provedena sustavna procjena rizika niti ekonomska evaluacija utjecaja investicija i troškova informacijske sigurnosti na poslovanje poduzeća. U okviru ovog makro-procesa čije su granice također naznačene iscrtanim linijama, temeljna aktivnost je revizija obaveznih zakonskih zahtjeva informacijske sigurnosti a koju je moguće derivirati iz drugog oformljenog repozitorija koji predviđa model a to je **katalog zakonskih zahtjeva** informacijske sigurnosti za mala i srednja poduzeća. U ovoj fazi provođenja modela, moguće je kako su tijekom provođenja elementarnih mjera vlasnici i rukovoditelji već identificirali i imenovali jednu osobu koja će biti zadužena za koordinaciju mjera informacijske sigurnosti, a ukoliko takva osoba ili funkcija nije određena, provođenje mjera i odvijanje i dalje nadziru vlasnici i rukovoditelji, te se stoga u ovoj točki predviđa u modelu definiranje navedene uloge[269]. Spominje se funkcija a ne osoba iz razloga što je u

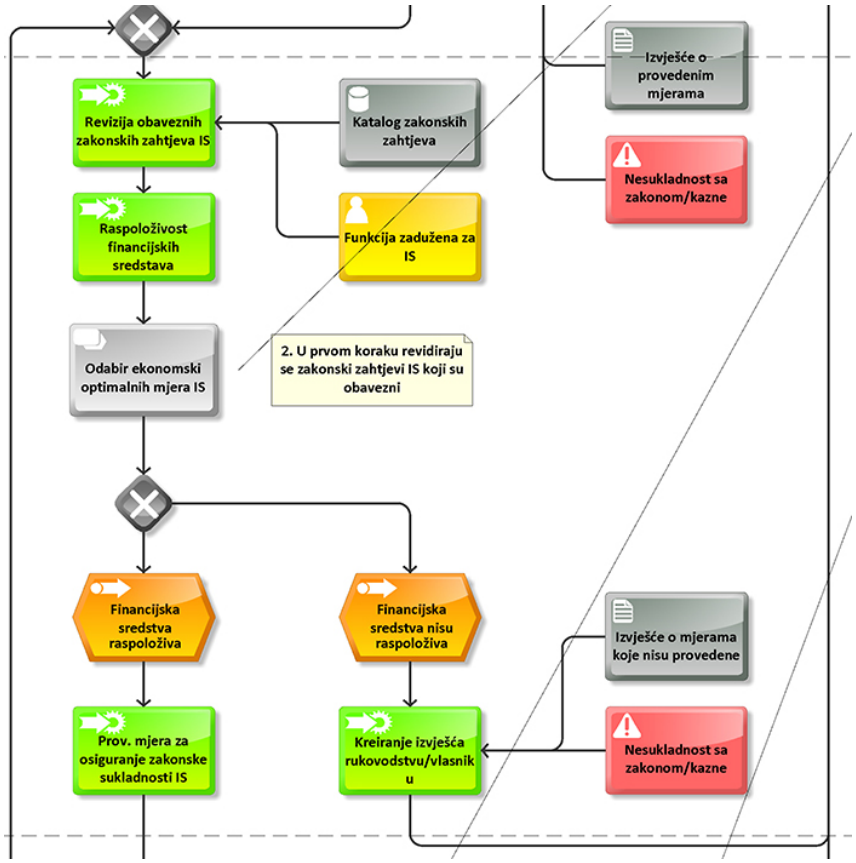
[269] U ovom kontekstu pod „*ulogom*“ se smatra „*funkcija zadužena za informacijsku sigurnost*“, od eng. „*role*“.

kompleksnijim okruženjima čest slučaj delegiranja provođenja na odjel, više osoba, ili eksternalizacija funkcije.

Po reviziji, odnosno kreiranju liste primjenjivih zakonskih zahtjeva koji sa sobom donose i potrebu kreiranja i provedbe odgovarajućih mjera informacijske sigurnosti, u modelu se po prvi put provodi proceduralni poziv potpornih (prileţećih) aktivnosti prikazanih na shemama 23. i 24, a koje se odnose odabira ekonomski optimalnih mjera informacijske sigurnosti. Kod te aktivnosti potrebno je procijeniti rizik koji je kod zakonskih zahtjeva razmjerno jednostavno ustanoviti budući da je po nastupu jednog incidenta informacijske sigurnosti jednak zakonski određenoj kazni (ili rasponu), no u tom slučaju radi se samo o trošku nepoštivanja regulatornih zahtjeva. Model pretpostavlja da se trošak nastupa incidenta informacijske sigurnosti uslijed nepoštivanja regulatornih i zakonskih zahtjeva treba zasebno procjenjivati kao i nastup bilo kojeg drugog incidenta informacijske sigurnosti, s time da je njegov temeljni uzrok nepoštivanje zakonskih propisa.[270] Potrebno je napomenuti i činjenicu kako je odabir ekonomski optimalne mjere informacijske sigurnosti u potpornoj procesnoj vertikali proces koji **nije opterećen raspoloživošću financijskih sredstava** za financiranje troška ili investicije u informacijsku sigurnost. Cilj tog odabira je **identificiranje ekonomski povoljne alternative** i usporedba kvantificirane razine rizika s troškom nastupa sigurnosnog incidenta. Usporedba apsolutnog iznosa odabrane alternative obavlja se u glavnoj procesnoj vertikali modela, te se u njoj analizira jesu li financijska sredstva raspoloživa ili ne. U slučaju da jesu, obavlja se dobava i implementacija mjere ili mjera informacijske sigurnosti. Iako se metodološki uglavnom uzima kako je sukladnost sa zakonskim zahtjevima nužan uvjet poslovanja, model uzima u obzir realno postojeću situaciju u kojoj je izvjesno kako postoje mala i srednja poduzeća u kojima ne postoje raspoloživa dovoljna financijska sredstva za osiguravanje sukladnosti sa zakonskim zahtjevima a koja i dalje posluju. Rezultat ovog procesa je dokument – **izvješće o mjerama sukladnosti** sa zakonskim propisima koje nisu provedene zbog nedostatka financijskih sredstava i identificirani rizik nesukladnosti sa zakonom, odnosno plaćanja iznosa kazne. U svakoj sljedećoj iteraciji provođenja modela, na vrh popisa mjera koje treba poduzeti su one mjere koje su identificirane, odnose se na zakonsku sukladnost a nisu provedene zbog nedostatka financijskih sredstava i to neovisno o tome što možda neprovođenje neke druge mjere ili uklanjanja drugog rizika sobom nosi apsolutno viši iznos nastupa incidenta informacijske sigurnosti.

[270] Naime, u ovom slučaju je rizik nastupa incidenta informacijske sigurnosti toliki da je čak i zakonodavac, provevši procjenu rizika, ustanovio da protumjeru treba prikazati obaveznom i uobličiti je u zakonski propis.

Shema 26: Makro-proces provedbi zakonskih mjera informacijske sigurnosti



Izvor: priredio autor

7.1.2.1.3. Provedba posebnih mjera poslovne certifikacije informacijske sigurnosti

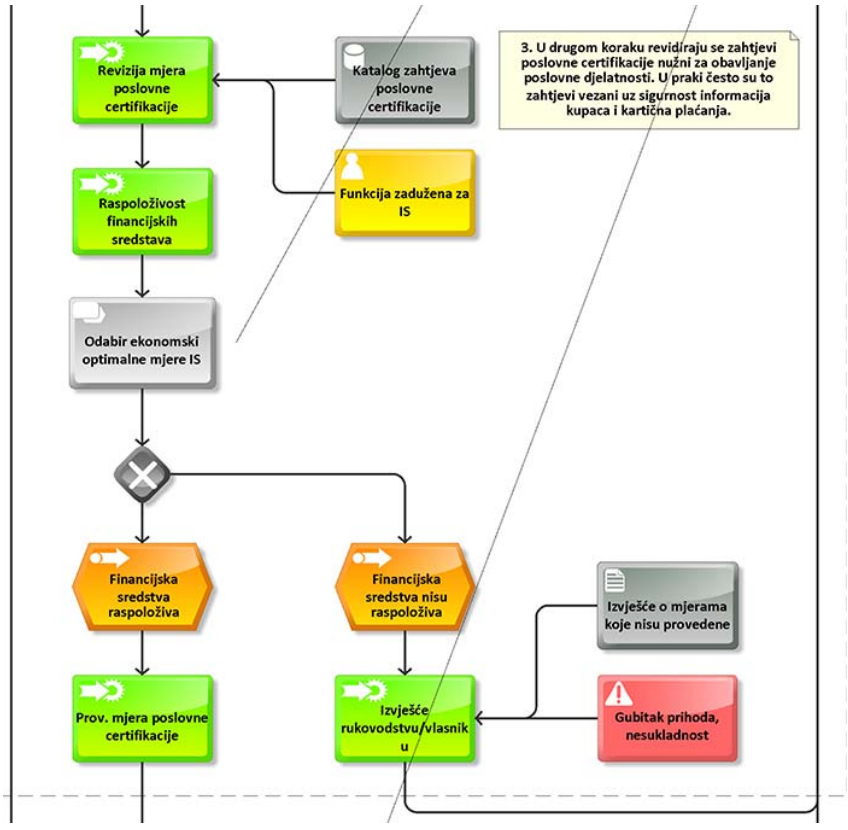
Po dovršetku provedbe makro-procesa provedbi zakonskih mjera informacijske sigurnosti, prelazi se na treći makro-proces modela, a radi se o **provedbi posebnih mjera** poslovne certifikacije informacijske sigurnosti poduzeća. Kao što je već rečeno, radi se o posebnim mjerama koje zahtijevaju dobavljači ili klijenti radi nesmetanog odvijanja poslovne aktivnosti, a uglavnom se radi o certifikacijskim zahtjevima unutar malog ili srednjeg poduzeća kojim se ne povećava razina informacijske sigurnosti samo unutar njega, već se tim mjerama štite suradnja i informacijski sustavi poduzeća-suradnika. Ovaj je proces, označen brojkom „3“. u shemi 24, u cijelosti prikazan shemom 27.

Slično kao i u prethodnim fazama uvođenja i provođenja poslovne funkcije informacijske sigurnosti, moguće je identificirati dvije temeljne slijedne aktivnosti, a to su kreiranje referentnog kataloga mjera informacijske sigurnosti koje su potrebne za osiguranje sukladnosti sa zahtjevima poslovne certificiranosti, te analiza raspoloživosti financijskih sredstava za implementiranje onih mjera informacijske sigurnosti koje su identificirane u okviru podržavajuće procesne vertikale ekonomske evaluacije mjera informacijske sigurnosti. Pritom se definira treća potporna baza podataka potrebna za funkcioniranje ovog modela, a to je

katalog zahtjeva poslovne certifikacije. U slučaju da poduzeće za odvijanje svoje centralne poslovne aktivnosti mora biti sukladno s više sustava poslovne certifikacije, tada će se raditi o više kataloga zahtjeva koji se odnose na više sustava poslovne certifikacije, a pred funkciju zaduženu za uvođenje informacijske sigurnosti postavljen je izazov da se usporedive ili identične mjere provedu samo jednom, odnosno da se napravi usporedna analiza kataloga zahtjeva dva ili više sustava poslovne certifikacije.

U slučaju raspoloživosti financijskih sredstava za provođenje sukladnosti s identificiranim sustavima poslovne certifikacije, određene se mjere provode, dok se u slučaju neraspoloživosti, provodi aktivnost kreiranja izvješća rukovodstvu, odnosno vlasniku, te je izvješće o takvim neprovedenim mjerama sljedeći dokument koji se identificira kao izlazni dokument modela procesa. Uz ovakav ishod veže se i rizik koji je moguće identificirati a radi se o gubitku prihoda uslijed nesukladnosti sa zahtjevima poslovne certifikacije. Kao i kod zakonskih zahtjeva po pitanju informacijske sigurnosti, prednost u sljedećoj iteraciji mjera informacijske sigurnosti imaju one mjere koje zbog nedostatka financijskih sredstava nisu provedene u prethodnim iteracijama modela. Radi se o provedbi mjera najbolje prakse informacijske sigurnosti.

Shema 27: Makro-proces provedbe posebnih mjera poslovne certifikacije informacijske sigurnosti



Izvor: priredio autor

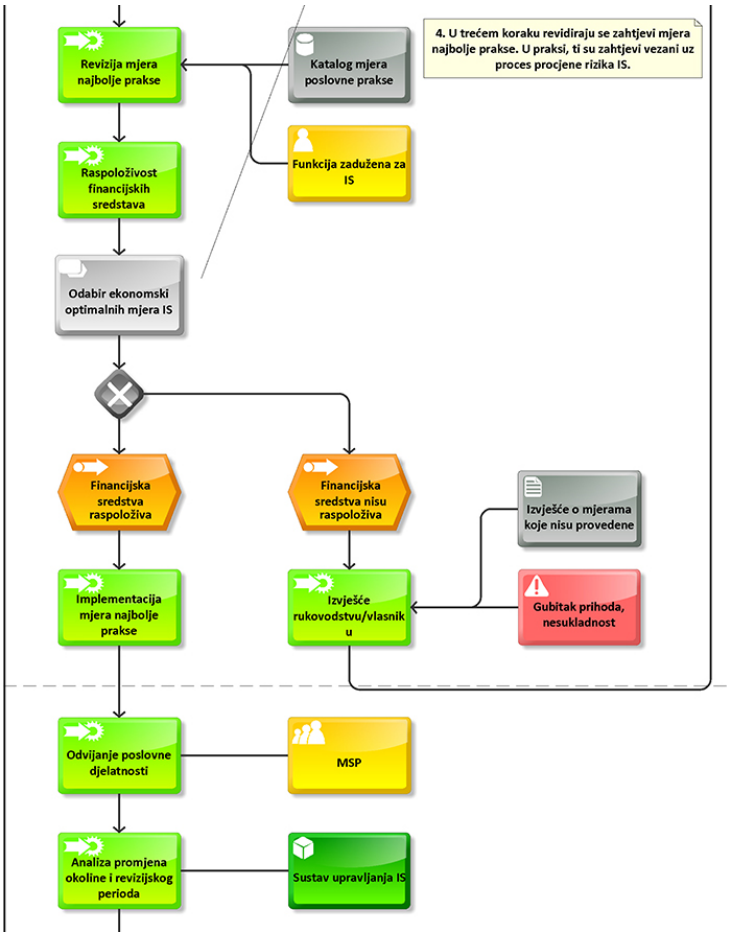
7.1.2.1.4. Provedba mjera najbolje prakse informacijske sigurnosti

Kao što je vidljivo iz modela, drugi i treći makro-proces modela procesa informacijske sigurnosti u malim i srednjim poduzećima imaju povratnu vezu na početak pod-procesa koji se trenutačno implementira iz razloga da sustavnim procesom provođenja zakonske sukladnosti te profesionalne certifikacije budu obuhvaćeni svi identificirani rizici. Tek u točki u kojoj su svi identificirani rizici provedeni, model se nastavlja sljedećim makro-procesom, koji je u modelu u shemi 24. označen brojem „*4*“., a detaljno razložen u shemi 28.

Na ulazu u ovaj makro-proces, malo ili srednje poduzeće već je prešlo velik put od početne točke koji je obilježen provedenim elementarnim mjerama informacijske sigurnosti, uključenošću vlasnika i rukovoditelja, obavljenom procjenom rizika, postignutom sukladnošću sa zakonskim propisima i temeljnim poslovnim certifikacijskim zahtjevima, odnosno pripremljenim izvješćima o mjerama koje su trebale biti provedene a nisu uslijed nedostatka financijskih sredstava. U ovoj točki, poduzeće je provelo određeni broj mjera informacijske sigurnosti i značajno napredovalo u osiguranju informacijske imovine poduzeća od nastupa incidenata informacijske sigurnosti, ali nije provelo sve mjere, već samo one koje je bilo obavezno provesti, i to prema zahtjevima države ili certifikacijskih tijela koja iznose zahtjeve koji većim dijelom štite interese trećih strana.

Makro proces implementacije mjera najbolje prakse najsličniji je uobičajenim mjerama koje se provode kod uvođenja certificiranog sustava upravljanja kvalitetom sustava informacijske sigurnosti. Treći definirani repozitorij koji zahtijeva ovako postavljen model je **katalog mjera poslovne prakse**. Takav katalog može biti preuzet od strane sustava najbolje prakse ili certifikacije poput *ISO 27002*, ili može biti sastavljen interno, unutar poduzeća, korištenjem vlastitih resursa, a osobito znanja i iskustva osoba zaduženih za upravljanje i provođenje informacijske sigurnosti. I u ovom koraku u glavnu procesnu vertikalu proceduralno se poziva podržavajuća vertikala ekonomske procjene efekata provođenja mjera najbolje prakse te se zatim financijska sredstva potrebna za provođenje mjera uspoređuju s onima koja su proračunski raspoloživa. Izlazni dokument ovog procesa je izvješće rukovodstvu o mjerama koje nisu provedene, dok izlaz iz ovog makro-procesa također pokazuje cirkularnost dokle god nisu provedene sve anticipirane mjere najbolje prakse. **Rizik** koji je moguće identificirati u ovoj fazi je povezan uz mogućnost nastupa sigurnosnih incidenata kao posljedica nesukladnosti s identificiranim rizicima koji prijete informacijskoj imovini a koji nisu otklonjeni. Ovaj makro proces prikazuje se na shemi 28.

Shema 28: Makro-proces provedbe mjera najbolje prakse informacijske sigurnosti



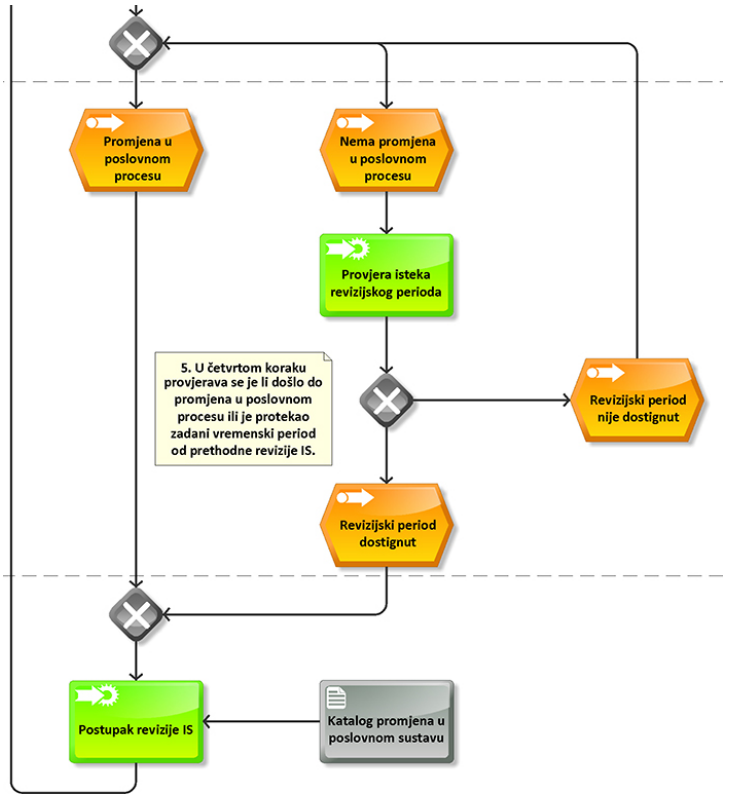
Izvor: priredio autor

7.1.2.1.5. Evaluacija promjena poslovnih procesa ili vremenskog perioda provjere sukladnosti

Sljedeći, peti korak uvođenja i provođenja sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, koji je u modelu u shemi 24. označen brojem „5“., detaljno se obrazlaže u shemi 29. na sljedećoj stranici. Taj se peti makro-proces naziva **aktivnostima evaluacije promjene poslovnog procesa** ili **perioda provjere sukladnosti**. Nakon što je poduzeće provelo inicijalno ili iterativno uvođenje informacijske sigurnosti prema katalogu elementarnih mjera, zakonskim zahtjevima i najboljoj praksi, rukovoditelji i vlasnici poduzeća trebaju u točno definiranim vremenskim razmacima ponoviti proces od točke 2. - provedbe zakonskih mjera informacijske sigurnosti nadalje. Vremenski period mora biti točno i formalno određen a može se radi pogodnosti podudarati s ostalim važnim periodičkim poslovnim događajima poput podnošenja periodičkih financijskih izvješća. Osim u slučaju opsežnih promjena u poslovnom procesu ili zakonskim zahtjevima, očekuje se kako će svaka sljedeća iteracija ovog procesa biti vremenski kraća za provođenje, a mjerama manje opsežna, jer ne bi trebala otkloniti ukupnost preostalih rizika po uvođenju elementarnih

mjera informacijske sigurnosti u okviru početnog makro-procesa, već samo novonastale rizike, i osigurati sukladnost sa novim zakonskim propisima i novonastalim tehničko-tehnološkim zahtjevima. Isto tako, poduzeća trebaju pažljivo procijeniti jesu li promjene u poslovnom procesu rezultirale povećanim ili promijenjenim zahtjevima po pitanju informacijske sigurnosti. Čak i ukoliko značajnijih promjena u okviru trajanja predefiniranog revizijskog perioda nije bilo, provođenje ove aktivnosti je značajno zbog procesnog pristupa, održavanja kulture informacijske sigurnosti i sustavnog pristupa organizaciji te funkcije. Opisani se ciklus ponavlja sve dok nije dostignut ili **zadani vremenski revizijski period** ili dok ne dođe do takve značajne **promjene u poslovnom procesu** koja zahtijeva ponovnu procjenu rizika i sukladnosti prema navedenim razinama makro-procesa u okviru modela.

Shema 29: Makro-proces evaluacije promjena poslovnih procesa ili vremenskog perioda provjere sukladnosti



Izvor: priredio autor

Kako bi poduzeće u svakom trenutku imalo spoznaju o tome u kojem stanju se nalazi njegova informacijska imovina te jesu li promjene u poslovnom procesu imale toliki utjecaj i značaj da poduzeće treba iznova provesti procesnu vertikalu, model predviđa **interni katalog promjena u poslovnom sustavu** koji vlasnicima i rukovoditeljima može poslužiti kao polazna osnova ovakve procjene.

7.1.2.2. Podržavajuće aktivnosti

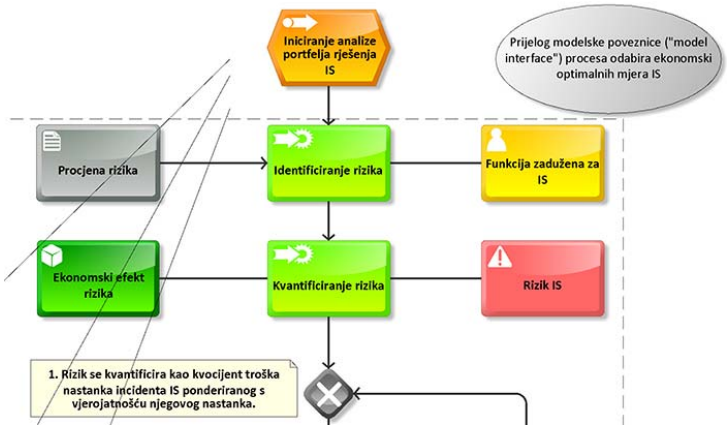
U nastavku se objašnjavaju značaj i provedbeni koraci **podržavajuće procesne vertikale** poslovne funkcije informacijske sigurnosti u malim i srednjim poduzećima. Kao što je već pojašnjeno u shemi 24., ova se procesna vertikala proceduralno poziva tijekom provođenja osiguranja sukladnosti sa zakonskim propisima, zahtjevima poslovne certifikacije i primjene mjera najbolje prakse. To je prikazano korištenjem elementa procesne poveznice koja reprezentira uvođenje drugog modela procesa iste razine u postojeći model. Podržavajuća procesna vertikala koja se sastoji od tri makro procesa označena na shemi 22. brojevima 6., 7. i 8. proceduralno se poziva svaki put kada treba procijeniti ekonomski, odnosno financijski utjecaj i opravdanost provođenja mjera informacijske sigurnosti u malom ili srednjem poduzeću prema predloženom modelu. Izlaganje ovih aktivnosti obavlja se kroz sljedeća poglavlja: **1) Procjena rizika nastupa incidenta informacijske sigurnosti, 2) Kvantificiranje ekonomskih efekata (učinaka) primjene mjera otklanjanja rizika** i **3) Tretiranje rizika ocijenjenim mjerama otklanjanja.**

7.1.2.2.1. Procjena rizika nastupa incidenta informacijske sigurnosti

Na shemi 30. na sljedećoj stranici prikazan je makro-proces označen brojkom „*6*“ iz sheme 24., koji je ujedno **početni podržavajući proces** informacijske sigurnosti u modelu posebno prilagođenom malim i srednjim poduzećima. Početni događaj koji aktivira podržavajuću procesnu vertikalu je **iniciranje analize portfelja rješenja** informacijske sigurnosti, jer je početna aktivnost ovog makro-procesa zapravo identificiranje da li svojim izdvojenim djelovanjem ili međudjelovanjem neke od već implementiranih mjera informacijske sigurnosti na dovoljnoj razini uklanjaju zakonski zahtjev informacijske sigurnosti, certifikacijski zahtjev ili zahtjev najbolje prakse kroz rizik koji se percipira novim ali je već postojeći i tretiran. Razina rizika identificira se kroz aktivnost identificiranja rizika a zatim i njegovog kvantificiranja. Radi se o aktivnosti koja se prepušta funkciji zaduženoj za informacijsku sigurnost. Kvantificiranjem razine rizika procjenjuje se koji je maksimalni iznos troška (u financijskom smislu) koji može biti posljedica nastupa incidenta informacijske sigurnosti u slučaju da mjere po navedenoj identificiranoj ranjivosti informacijske imovine nisu provedene. *ARIS* element rizika koji se može u ovoj točki identificirati je rizik informacijske sigurnosti a *ARIS* element „*proizvod*“[271] je – ekonomski efekt rizika. **Proizvod** je procesni element koji podržavajuća procesna vertikala predaje osnovnoj kao jedan od svojih izlaznih rezultata.

[271] „*Proizvod*“ od eng. „*product*“, a radi se o jednom od elemenata procesa *ARIS Expressa*.

Shema 30: Makro-proces procjene rizika nastupa incidenta informacijske sigurnosti



Izvor: priredio autor

7.1.2.2.2. Kvantificiranje ekonomskih efekata (učinaka) primjene mjera otklanjanja rizika

Na shemi 31. na sljedećoj stranici prikazan je makro-proces označen brojkom „*7*“. iz sheme 24, koji slijedi procjenu rizika, a koji nosi naziv „*Aktivnosti kvantificiranja ekonomskih efekata (učinaka) primjene mjera otklanjanja rizika*.“ Cilj ovih aktivnosti je suprotstaviti više raspoloživih **mogućnosti** operativnog tretmana i **financijskih učinaka** korištenja mjera informacijske sigurnosti. Malim i srednjim poduzeća u Republici Hrvatskoj na dostignutom stupnju tehničko-tehnološkog razvoja i tržišta rješenja informacijske sigurnosti stoje na raspolaganju četiri temeljna identificirana **oblika** operativnog provođenja informacijske sigurnosti:

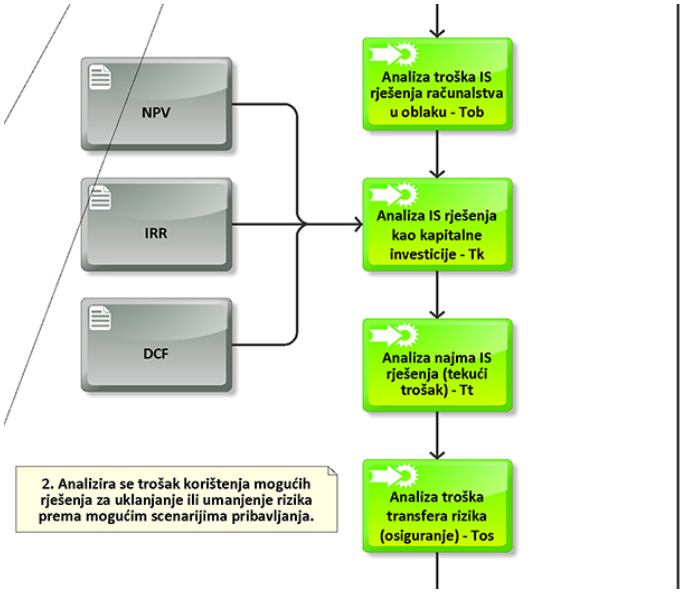
1. Implementacija mjera informacijske sigurnosti korištenjem rješenja računalstva **„u oblaku**“,
2. Implementacija mjera informacijske sigurnosti korištenjem rješenja koja su pribavljena kao **vlastite investicije**,[272]
3. Implementacija mjera informacijske sigurnosti koje su pribavljene **najmom rješenja**,
4. Implementacija transfera posljedica nastupa rizika incidenta informacijske sigurnosti na treću stranu korištenjem **osiguranja** od rizika.

Rezultat ovog makro-procesa su **ekonomski** i **financijski pokazatelji** koji jasno uspoređuju moguće istovjetne alternative implementacije mjere ili mjera informacijske sigurnosti koje otklanjaju ili na željenoj razini umanjuju nastup incidenta informacijske sigurnosti. Pritom je važno napomenuti da rukovoditelji, vlasnici i instance poduzeća zadužene za provođenje mjera informacijske sigurnosti, a osobito oni koji odlučuju o načinu i razini investicija u te mjere,

[272] Kapitalne investicije, u smislu investicijskih ulaganja u trajnu imovinu.

moraju paziti da rješenja koja se uspoređuju otklanjaju rizike otprilike u istoj razini, odnosno da se ne uspoređuju ona rješenja koja to rade npr. djelomično ali su jeftinija s onima koja to čine u potpunosti ili čak i izvan opsega određenog identificiranog rizika, ali je njihov trošak korištenja ili nabave viši.

Shema 31: Makro-proces kvantificiranja ekonomskih efekata (učinaka) primjene mjera otklanjanja rizika



Izvor: priredio autor

Prigodom analize sheme 31. potrebno je primijetiti kako se mjere informacijske sigurnosti korištenjem računalstva u oblaku, najma ili transfera rizika računovodstveno tretiraju kao operativni trošak dok je analiza rješenja kao kapitalne investicije reprezentirana trima izlaznim pokazateljima analize (Bezić, et al., 2011, p. 252), a to su analiza neto sadašnje vrijednosti investicije (*NPV*)[273], interne stopa povrata (*IRR*)[274] i diskontiranih novčanih tijekova (*DCF*)[275].

7.1.2.2.3. Tretiranje rizika ocijenjenim mjerama otklanjanja

Posljednji makro proces podržavajuće procesne vertikale uvođenja i provođenja informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj prikazan je na shemi 32., a radi se o procesu označenom brojkom „*8.*“ u shemi 24. Ovaj makro proces predstavlja posljednju točku prije nego se procesna linija razgranate procesne poveznice sa svim svojim izlazima vrati natrag u osnovnu, odnosno primarnu procesnu vertikalu te aktivnosti,

[273] *NPV* – kratica od eng. „*Net present value*“, neto sadašnja vrijednost investicije skupa novčanih tijekova reprezentirana sumom sadašniih vrijednosti pozitivnih i negativnih novčanih tijekova.
[274] *IRR* - kratica od eng. „*Internal rate of return*“, interna stopa povrata investicije korištena za usporedbu profitabilnosti investicija.
[275] *DCF* - kratica od eng. „*Discounted cash flow*“, diskontirani novčani tijekovi, pozitivni i negativni, svedeni na određeni datum.

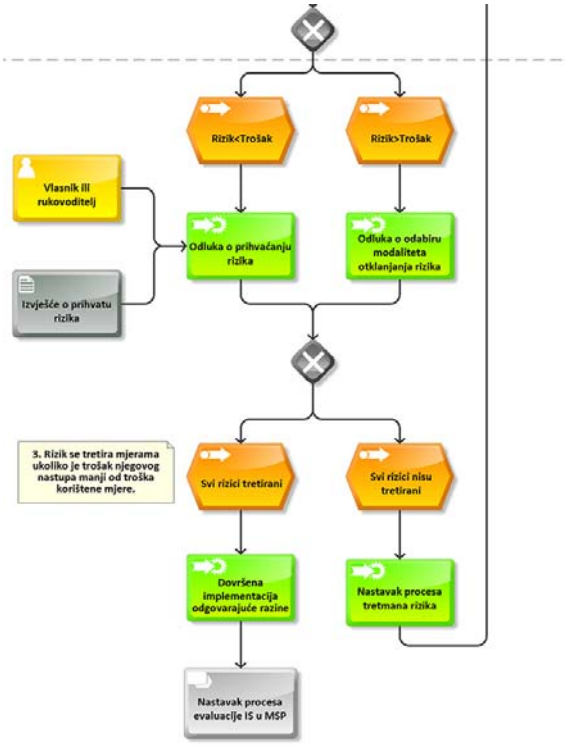
identificirane lijevo na shemi 24. **Ulazni parametri** ove točke su jasno identificirani relevantni rizici, njihovi kvantificirani iznosi, moguće mjere njihovog uklanjanja, te sve mogućnosti njihovog provođenja u operativnom smislu (korištenjem najma, vlastitom kupovinom, korištenjem rješenja, odnosno usluga računalstva u oblaku ili osiguranjem).

Cilj odvijanja ovog makro procesa je dvojak:

1. U njegovom okviru kvantificirani **rizik** bit će **uspoređen s troškom** implementacije mjera informacijske sigurnosti kojima se rizik otklanja te će biti donesena odluka o tome je li financijski isplativo otklanjati rizik ili ga treba prihvatiti,
2. Ocijenit će se jesu li **obuhvaćeni svi rizici** informacijske sigurnosti u ovom koraku implementacije unutar poduzeća. Ukoliko nisu, podržavajuća se procesna vertikala iznova odvija dokle god taj zahtjev nije zadovoljen.

U slučaju da je kvantificirana razina nastupa rizika manja od troška potrebnog za implementaciju mjera kojima će se taj trošak ukloniti, financijski gledano, nije isplativo na tim razinama rizika i troška provoditi mjere informacijske sigurnosti. Takva odluka mora nužno biti formalizirana od strane vlasnika ili rukovoditelja, a modelom procesa predviđa se dokument **izvješća prihvaćanja rizika**. U svakoj sljedećoj iteraciji korištenja podržavajuće procesne vertikale, nužno je uzeti u obzir kako uslijed proteka vremena ili promjena načina odvijanja poslovne aktivnosti, utjecaja rizika, a samim time i njegove razine, kao i zbog pada troška uvođenja i korištenja pojedinih mjera informacijske sigurnosti, dobiveni rezultati nisu konstantni već varijabilni i privremeni. Ovime se dodatno podupire mehanizam periodičkog ponavljanja postupka provođenja poslovne funkcije informacijske sigurnosti u malim i srednjim poduzećima. Naime, okruženje poduzeća, te promjene unutar samih poduzeća nužno nalažu periodičke revizije obavljanja ove aktivnosti. Ovo je osobito izraženo u onim poduzećima koja imaju kompleksnije **zahtjeve** za mjerama informacijske sigurnosti jer su zbog prirode svog posla izloženija nastupu sigurnosnih incidenata, u onim poduzećima koja imaju značajnu informacijsku imovinu pod upravljanjem ili u svom vlasništvu te u poduzećima u kojima se proces odvija inicijalno (prvi put) ili ukoliko je došlo do značajnih promjena u poslovnoj djelatnosti, procesima, obliku organizacije, okruženju poduzeća ili internim odnosima ili u poduzeću korištenoj tehnologiji.

Shema 32: Makro-proces tretiranja rizika ocijenjenim mjerama otklanjanja



Izvor: priredio autor

Opisom posljednjeg, sedmog makro procesa, opisana je cjelokupnost prijedloga inicijalnog uvođenja i kasnijeg provođenja poslovne funkcije informacijske sigurnosti u malom i srednjem poduzeću koja je utemeljena na cikličkom odvijanju aktivnosti, nekoliko vanjskih repozitorija (katalog) potrebnih informacija, vrlo malom, ograničenom skupu internih proizvoda procesne vertikale i kreiranih dokumenata, što je osobito prikladno za korištenje u malim i srednjim poduzećima i ekonomsko-financijsko utemeljenom donošenju odluka o investicijama i troškovima ove poslovne funkcije.

7.2. UČINCI PRIMJENE EKONOMSKI ODRŽIVOG MODELA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU MALIH I SREDNJIH PODUZEĆA

Očekivani učinci primjene ekonomski održivog modela upravljanja informacijskom sigurnošću malih i srednjih poduzeća objašnjavaju se u pet međusobno povezanih cjelina: **1) Usklađenost sa zakonskim propisima, najboljom praksom i certifikacijskim standardima i sustavima, 2) Izbjegavanje troškova nastupa sigurnosnih incidenata, 3) Zaštita informacijskog kapitala, 4) Povećanje imidža malih i srednjih poduzeća** i **5) Dostupnost izvora financiranja.**

7.2.1. Usklađenost sa zakonskim propisima, najboljom praksom i certifikacijskim standardima i sustavima

Kao što je vidljivo iz sheme 24. na kojoj su predstavljene temeljna i podržavajuća procesna vertikala informacijske sigurnosti, drugi element modela za svoj cilj ima postizanje usklađenosti sa zakonskim propisima. Prema prvom „*Global Compact*“[276] principu Ujedinjenih naroda, poduzeća moraju podržavati i poštovati internacionalno određena ljudska prava, te promovirati poštovanje vladavine prava. Ovaj princip moguće je povezati uz pravo pristupu Internetu[277], a dalje i uz prava i slobodu izražavanja mišljenja. Iz navedenog razloga, većina država donijela je i zakonske propise koji reguliraju zaštitu privatnih informacija osoba te su taj i vezani zakonski propisi uobičajena osnova na kojoj države izgrađuju svoju legislativu povezanu uz informacijsku sigurnost.

Vladavina prava[278] definira se kao utjecaj zakona unutar društva putem nametanja ograničenja ponašanja, uključujući ponašanje izabranih koji vladaju društvom. Taj se koncept može pratiti još od antičke Grčke, od Aristotela[279], a populariziran je u 19. stoljeću od strane britanskog profesora i teoretičara ustavnog prava Alberta Venna Diceya[280]. Iz navedenog razloga, poštovanje vladavine prava primijenjenog na digitalnu domenu, a osobito područje zaštite privatnih podataka, te zakonske propise koji reguliraju pojedina poslovna područja predstavlja temeljnu civilizacijsku tekovinu modernog društva. U Europskoj uniji posluje preko 23 milijuna malih i srednjih poduzeća koji predstavljaju 99 % ukupnog poslovnog sektora (European Commission, 2013), te je jasno kako će pristupom Republike Hrvatske suradnja nešto više od 80.000 hrvatskih poduzeća koja pripadaju istoj kategoriji s poduzećima izvan nacionalnih granica biti još tješnja. Budući da je hrvatsko zakonodavstvo u pretpristupnim pregovorima za pridruženje Republike Hrvatske Europskoj uniji u potpunosti usklađeno sa zahtjevima iste, može se zaključiti kako će poštivanje regulative koja se odnosi na informacijsku sigurnost u Republici Hrvatskoj omogućiti, zahvaljujući zajedničkom pravnom okviru, zadovoljenje i zahtjeva u zemljama Europske unije na koju je Republika Hrvatska politički i ekonomski nužno i primarno orijentirana.

---

[276] Za detalje cf. United Nations Global Compact, **http://www.unglobalcompact.org/** (20.08.2013.)
[277] Pravo pristupa Internetu se u kontekstu ljudskih prava prvi put spominje tijekom svjetskog summita o informacijskom društvu u prosincu 2003. godine. Za detalje cf. World Summit on the Information Society, **http://www.itu.int/wsis/index.html** (18.07.2013.)
[278] Vladavina prava naziva se još i „*nomokracija*“, od grč. „*nomos*“, zakon.
[279] Aristotel je poznat prema izreci „*Zakon treba vladati“*.
[280] Albert Venn Dicey (1835-1922) je bio autor principa na kojima se temelji Ustav Velike Britanije. Za detalje cf. Encyclopaedia Britannica, Albert Venn Dicey,
http://www.britannica.com/EBchecked/topic/162050/Albert-Venn-Dicey (18.08.2013.)

Temeljni zakonski propisi koji reguliraju ovo područje u pravilu nisu previše zahtjevni, a osobito ne u tehničkom smislu, niti zahtijevaju značajnije investicije, pa čak niti napore malih i srednjih poduzeća koji bi se mogli preslikati u troškove, bilo za tehnička rješenja informacijske sigurnosti u nekom od mogućih oblika[281], bilo u smislu varijabilnog troška rada utrošenog za postizanje sukladnosti sa zakonskim propisima. U pravilu se radi o mjerama i akcijama koje mala i srednja poduzeća moraju poduzeti kako bi osigurala minimum sukladnosti sa zakonom i to isključivo vezano uz sigurnost osobnih podataka sukladno zakonskoj definiciji, ukoliko ih obrađuju. U svjetlu navedenoga čudi činjenica da samo 27 % malih i srednjih poduzeća u Republici Hrvatskoj prati svoje zakonske obaveze po pitanju informacijske sigurnosti, a samo dodatnih 10 % takvih poduzeća ih još nije pratilo, ali je planiralo početi baviti se tom problematikom u bližoj budućnosti. Preostaje 63 % malih i srednjih poduzeća, ili njih više od 53.000, koja svoje zakonske obaveze uopće ne poznaju, te je samim time više nego upitno koliko ih poštuju[282]. Potrebno je napomenuti i kako je za izvršitelje obrade te voditelje zbirke podataka koji podatke prikupljaju ili obrađuju protivno Zakonu o zaštiti osobnih podataka zapriječena kazna u iznosu od 20.000 do 40.000 Kn a za odgovornu osobu u pravnoj osobi u iznosu od 5.000 do 10.000 Kn. Trenutačno zakonodavac ne inzistira provođenjem nadzornih radnja previše po pitanju ovog zakona, no u svakom slučaju su mala i srednja poduzeća izložena ovoj vrsti troška ukoliko ne poštivaju navedeni zakon.

Očekuje se kako će primjena navedenog modela rezultirati i prije formalne certifikacije po nekom od certifikacijskih sustava upravljanja informacijskom sigurnošću visokim razinama sukladnosti s formalnim zahtjevima jer su u izgradnji modela korišteni modeli i postupci tipični za te sustave, poput *PDCA* ciklusa i operativnih mjera informacijske sigurnosti. reprezentiranih katalogom temeljnih mjera. Osim formalne sukladnosti sa zahtjevima najbolje prakse, primjena predloženog modela rezultirati će i povećanom razinom pažnje vlasnika i rukovoditelja usmjerenoj ka poslovnoj funkciji informacijske sigurnosti, ali i poslovnoj informatici. Budući da je trenutačno aktualan zaokret od poslovne informatike kao poslovne funkcije koja upravlja informacijskom imovinom ka poslovnoj funkciji koja planira i koordinira svim poslovnim procesima u poduzeću, korištenje ovog modela može se uzeti kao **početna točka** u usklađivanju poduzeća takvoj preobrazbi, ali i značajnom koraku prema uvođenju nekih od profesionalnih certifikacija informacijske sigurnosti (npr. *ISO 27001:2005*).

Naposljetku, implementacija ovakvog modela može predstavljati osnovu za uvođenje standarda profesionalne certifikacije kao što je *PCI DSS*, koji je standard informacijske sigurnosti za

[281] npr. kroz investicije u vlastitu trajnu imovinu, najam ili leasing rješenja ili korištenjem usluga računalstva u oblaku.
[282] Naime, uvijek je moguće da su uslijed slučajnog upravljanja ili malog broja zahtjeva zakonski propisi poštovani.

organizacije i poduzeća koja pohranjuju i upravljaju informacijama o vlasnicima kreditnih i debitnih kartica. Za očekivati je kako je ovo prvi standard s kojim će se susresti većina malih i srednjih poduzeća, a osobito onih koja posluju u bilo kojem obliku maloprodajne ili direktne uslužne djelatnosti. Kontrolni ciljevi *PCI DSS* sustava[283] se u potpunosti poklapaju sa temeljnim sastavnicama modela, odnosno mogu se njima postići. Za očekivati je da ono poduzeće koje uspostavi sustav upravljanja informacijskom sigurnošću sukladan predloženom modelu, bez većih poteškoća može implementirati i *PCI DSS* sukladnost.

7.2.2. Izbjegavanje troškova nastupa sigurnosnih incidenata

Najvažniji potencijalni učinak uvođenja modela koji će zasigurno inicijalno intrigirati rukovoditelje i vlasnike malih i srednjih poduzeća je izbjegavanje troškova nastupa sigurnosnih incidenata. Kao što je pokazano u ovom istraživanju, u Republici Hrvatskoj u malim i srednjim poduzećima nastupe incidenata informacijske sigurnosti bilježi 30 % anketiranih poduzeća. U njima je prosječan broj incidenata informacijske sigurnosti mjeren medijanom 3, a aritmetičkom sredinom 4,8 uz standardnu devijaciju od 4,84; pri čemu je financijski mjeren trošak nastupa takvih incidenata više nego značajan: 4 % poduzeća iznosi kako je on u rasponu od 4-6 % godišnjeg prihoda, 7 % bilježi taj trošak u rasponu od 2 do 4 % godišnjeg prihoda dok nažalost čak 23 % poduzeća sustavno ne analizira trošak njihovog nastupa.

U referentnim godišnjim izvješćima o regionalnom i globalnom stanju informacijske sigurnosti u poduzećima te trošku incidenata informacijske sigurnosti, uvriježeno je iskazivanje troška incidenta informacijske sigurnosti izraženo u odnosu na **jedan podatkovni zapis** koji je kompromitiran, pri čemu većina organizacija koje se bave takvom vrstom analize iz nje isključuje ona poduzeća u kojima je kompromitirano više od 100.000 zapisa jer se smatraju nereferentnina. Tako je u Njemačkoj u 2012. godini trošak kompromitiranja jednog zapisa iznosio 199 $, a u analiziranim poduzećima je u prosjeku bilo kompromitirano 23,647 zapisa. Prosječan trošak detekcije i eskalacije incidenta informacijske sigurnosti u Sjedinjenim Američkim Državama iznosi 1,3 mil. $, a u Australiji 1,2 mil. $. (Symantec, 2013) U Sjedinjenim Američkim Državama je najveća redukcija troškova uočena kod onih poduzeća koja vode brigu o informacijskoj sigurnosti u svakodnevnom radu, imaju plan odgovora na sigurnosne incidente i imenovanu osobu zaduženu za informacijsku sigurnost, a trošak nastupa incidenta raste ukoliko su o njemu obaviješteni oni na koje se kompromitirani podaci odnose, regulator i ostali dionici.

[283] U zadnjoj inačici od 26.10.2013. godine.

Važno je napomenuti kako je trošak naknadnog oporavka od incidenta informacijske sigurnosti u Sjedinjenim Američkim Državama 2,5 puta **veći** od proaktivnih mjera kojima se njegov nastup mogao spriječiti, a u Njemačkoj je čak 4 puta veći. (Ponemon Institute, 2013, p. 13)

U Ujedinjenom Kraljevstvu preko 80 % malih i srednjih poduzeća bilježi incidente informacijske sigurnosti, a njihov je ukupan trošak između 35.000 i 65.000 britanskih funti po poduzeću. Taj trošak sastoji se od 3 do 5 radnih dana izgubljenih uslijed nastupa incidenta informacijske sigurnosti koji se procjenjuju na trošak od 30 do 50.000 funti, odgovora na incident informacijske sigurnosti koji košta 2.000 do 6.000 funti, izgubljene poslovne prigode u iznosu 300 do 600 funti, gubitak informacijske imovine u iznosu 150 do 300 funti i trošak gubitka reputacije od 1500 do 8000 funti. (Schutte, 2013)

Trošak incidenta informacijske sigurnosti je u apsolutnomiznosu niži za mala i srednja poduzeća niži nego za velika poduzeća, no upravo zbog veličine i neotpornosti na vanjske stresove, taj trošak može predstavljati za mala i srednja poduzeća takav udarac od kojega se mnoga niti ne oporave i prestaju poslovati. Prema studiji Kaspersky Labsa čiji rezultati su prikazani u tablici 52., prosječni gubitak uslijed nastupa incidenta informacijske sigurnosti u takvim poduzećima iznosi 50.000 $, pri čemu se 36.000 $ odnosi na direktne troškove incidenta a 14.000 $ na ostale povezane troškove. Najniži prosjek troškova incidenta informacijske sigurnosti zabilježen je u Ruskoj Federaciji i iznosi 21.000 $, a najviši u Sjevernoj Americi (82.000 $) i pacifičkom dijelu Azije (96.000 $). Ovo istraživanje pokazuje kako posljedice nastupa incidenata informacijske sigurnosti u malim i srednjim poduzećima iznose i do 5 % njihovih godišnjih prihoda, a u jednom od anketiranih poduzeća zabilježeno je kako je poduzeće izgubilo kompletnu poslovnu djelatnost u regiji gdje je prije nastupa incidenta informacijske sigurnosti poslovalo vrlo uspješno. Trošak ciljanog napada za mala i srednja poduzeća je gotovo dvostruko viši od prosjeka nastupa incidenta informacijske sigurnosti i iznosi 92.000 $. Zaključak izvješća je da su svi, pa i oni najdestruktivniji napadi na informacijske sustave mogli biti prevenirani da su rukovoditelji upravljali informacijskom imovinom i sigurnosnim rješenjima na adekvatan način. (Kaspersky Lab, 2013).

Tablica 52: Prosječni utjecaj nastupa incidenta informacijske sigurnosti u malim i srednjim poduzećima po regijama u 2012. (u $)

Vrsta	Ukupno	Sjeverna Amerika	Šire područje Europe	Ruska Federacija	Azija (Pacifički dio)	Azija, Afrika i Latinska Amerika
Ukupna očekivana šteta	36.000	59.000	38.000	14.000	74.000	35.000
Trošak reakcije	14.000	23.000	17.000	7.000	22.000	10.000

Ukupni financijski efekt	50.000	82.000	55.000	21.000	96.000	45.000

Izvor: prilagodio autor prema Kaspersky Labs: **„Global IT Security Risks Survey Report 2013.“**, 2013.

Temeljem vlastitih istraživanja incidenata informacijske sigurnosti, u suradnji Symanteca i Ponemon Instituta stvoren je ekspertni sustav koji se slobodno može koristiti preko Interneta. [284] Ekspertni sustav uzima u obzir podatke iz vlastite baze, te ulaze od strane korisnika i kao rezultat daje procjenu vjerojatnosti nastupa incidenta informacijske sigurnosti i njegov trošak.

Ulazi koje u ekspertni sustav unosi korisnik su sljedeći:

1. Industrijska klasifikacija poduzeća[285],
2. Karakteristike politike zaštite privatnosti i podataka u poduzeću,
3. Vrsta podataka koje obrađuje poduzeće,
4. Subjektivna percepcija mogućnosti nastupa incidenta informacijske sigurnosti,
5. Pohrana podataka poduzeća na prijenosnim računalima i podatkovnim medijima,
6. Korištenje enkripcije na prijenosnim računalima i podatkovnim medijima,
7. Imenovana osoba zadužena za informacijsku sigurnost,
8. Broj zaposlenika,
9. Geografske operacije poduzeća[286],
10. Dozvola udaljenog pristupa informacijskom sustavu poduzeća,
11. Korištenje mjera enkripcije za pristup informacijskim sustavima poduzeća,
12. Geografska lokacija sjedišta poduzeća,
13. Samoprocjena broja zapisa koji mogu biti ugroženi uslijed nastupa incidenta informacijske sigurnosti.

Ukoliko se simulira scenarij malog ili srednjeg poduzeća u Republici Hrvatskoj sukladno rezultatima dobivenim anketnim istraživanjem, te se u ekspertni sustav unese poduzeće klasifikacije „*Ostalo*“ koje nema politiku zaštite privatnosti i podataka, posjeduje podatke o klijentima i dobavljačima, ima percepciju kako su vjerojatni nastupi incidenata informacijske sigurnosti uslijed nemara i nepažnje, pohranjuje podatke bez korištenja enkripcije, nema imenovanu osobu zaduženu za informacijsku sigurnost, posluje samo u Republici Hrvatskoj, dozvoljava daljinski pristup informacijskim sustavima ali ne koristi enkripciju te upravlja s 5.000 do 10.000 zapisa koji mogu biti ugroženi, sustav provodi simulaciju temeljem postojećih

[284] Internet adresa za pristup ekspertnom sustavu (kalkulatoru) mogućeg troška nastupa incidenta informacijske sigurnosti je cf.: **https://databreachcalculator.com/** (30.08.2013.)
[285] Radi se o ekvivalentu *Nacionalne klasifikacije djelatnosti*, ali s jednostavnijom podjelom u jedanaest područja i „*Ostalo*“.
[286] npr. Operacije u državi, regija, na kontinentu ili globalno.

podataka i kao rezultat dobiva se izračun prema kojemu takvo hipotetsko poduzeće koje odgovara u suštini idealnom prosječnom profilu poduzeća iz anketnog uzorka, ima vjerojatnost od 9,4 % za nastupom incidenta informacijske sigurnosti i trošak nastupa takvog incidenta od 139 $ po zapisu, sve na godišnjoj razini.

Budući da predloženi model inkorporira sve odrednice koje su ključne za smanjenje troška mogućih incidenata informacijske sigurnosti, razumno je očekivati kako će sustavni pristup koji je primijenjen pri izradi modela i prijedlogu koraka za njegovo uvođenje, a koji je osobito prilagođen kategoriji malih i srednjih poduzeća, rezultirati **smanjenjem,** kako pojavnosti incidenata informacijske sigurnosti, tako i troška oporavka i povratka poslovne djelatnosti u normalne parametre.

7.2.3. Zaštita informacijskog kapitala

Kao što je već detaljno obrazloženo u poglavlju posvećenom informacijskom kapitalu malih i srednjih poduzeća, postoji značajna razlika između svih informacija koje poduzeće koristi i onih informacija koje predstavljaju nematerijalni informacijski kapital poduzeća, a čije korištenje može rezultirati poboljšanjem poslovnih procesa ili konkurentskim prednostima. Upravljanje informacijskim kapitalom provodi se operativnim korištenjem metodologije klasifikacije podataka i upravljanja njihovim životnim ciklusom. Pritom je nužno da se navedene mjere primjenjuju isključivo u odnosu na one informacije i podatke koji su identificirani kao informacijski kapital poduzeća. Naime, u slučaju da se te mjere primjenjuju neselektivno, te ukoliko informacijski kapital poduzeća nije točno identificiran, nije moguće izvesti objektivno argumentaciju o opravdanosti povećanja investicija u informacijsku infrastrukturu.

Prema Coaseovim[287] spoznajama objavljenim u njegovom poznatom članku *„The nature of the Firm*“, moguće je odgovoriti na nekoliko **temeljnih pitanja iz teorije poduzeća**, a to su:

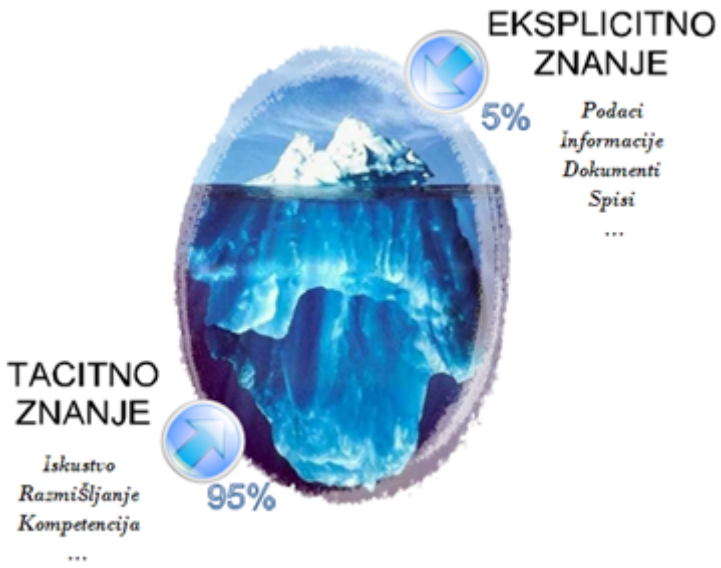
1. Zašto poduzeća nisu veća?
2. Zašto postoje poduzeća?

Naime, Coase objašnjava ovu problematiku kroz svoju teoriju transakcijskih i ugovornih troškova koji ograničavaju veličinu poduzeća. Uloga informacijskih tehnologija je u tome da smanjuju transakcijske troškove i na taj način omogućavaju rast (povećanje veličine) poduzeća te da povećavaju efikasnost malih poduzeća i kreiraju jaču konkurenciju većim poduzećima –

[287] Ronald Harry Coase (r. 1910. godine) je britanski ekonomist koji djeluje u Sjedinjenim Američkim Državama i dobitnik Nobelove nagrade iz ekonomije 1991. godine. Poznat je po svojoj teoriji transakcijskih troškovak kojima objašnjava granice širenja poduzeća, te obradi problema eksternalija. Osnivač je Ronald Coase Instituta. Za detalje cf. The Ronald Coase Institute, **http://www.coase.org/** (22.08.2013.)

što u konačnici može rezultirati smanjenjem veličine postojećih velikih poduzeća. (Coase, 1937, p. 404) Prema tome, informacijske tehnologije koje predstavljaju osnovna operativna sredstva kojima se osigurava informacijski kapital poduzeća, omogućavaju malim i srednjim poduzećima dodatni rast koji bi bez njih bio otežan ili nemoguć, a u okviru cikličkog procesa kretanja poduzeća, omogućuju rast do te mjere da uklanjaju barijere pristupa tržištu koja postavljaju velika poduzeća korištenjem ekonomije obujma. Budući da su najpropulzivnija poduzeća iz kojih često potiču inovacije uglavnom mala i srednja poduzeća, kod njih je ključno inzistiranje na očuvanju i opredmećenju *tacitnog* znanja. Radi se o znanju koje predstavlja okosnicu informacijskog kapitala poduzeća, a koje je derivirano iz direktnog iskustva i ne može se formalizirati ili lako imitirati od strane konkurencije i traži dug vremenski period za stjecanje od konkurencije. Utjecaj tacitnog znanja na istraživanje i razvoj u malim i srednjim poduzećima, a samim time i na informacijski kapital poduzeća je od odsutnog značaja. (Birkinshaw & Fey, 2005) Uobičajena metafora međuodnosa između **eksplicitnog znanja**[288] i **tacitnog znanja**[289] prikazuje se simbolički putem ledenjaka na ilustraciji 3., pri čemu se ispod površine vode nalazi samo manji udio ukupnog akumuliranog informacijskog kapitala poduzeća, a ispod nje nalazi se veći dio predstavljen tacitnim znanjem.

Ilustracija 3: Odnos eksplicitnog i tacitnog znanja u poduzeću



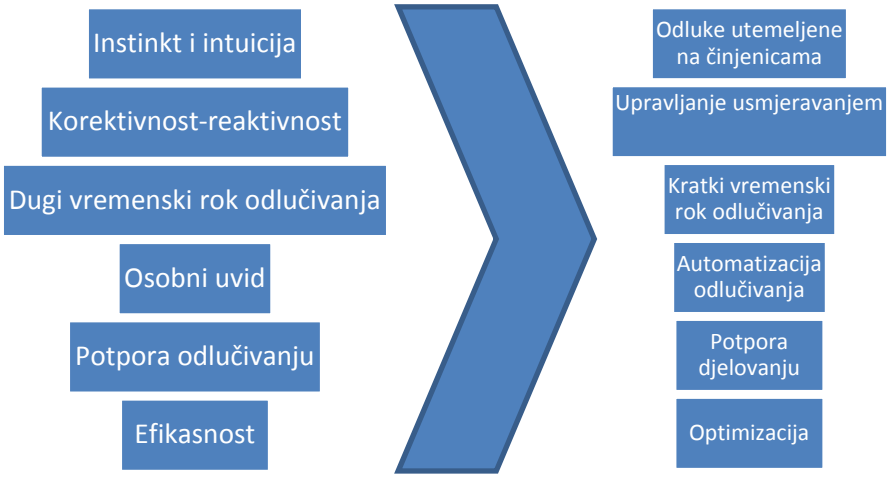
Izvor: **http://autopoiesis.foi.hr/** (04.08.2013.)

Implementacija novog modela upravljanja informacijskom sigurnošću poduzeća koji je osobito prilagođen malim i srednjim poduzećima omogućit će im upravljanje na način koji je svojstven velikim poduzećima. Naime, vlasnici i rukovoditelj malih poduzeća često koriste instinkt i

[288] Odnosno, informacija i podataka sadržanih u informacijskom sustavu poduzeća.
[289] Odnosno, informacijskog kapitala poduzeća.

intuiciju, čak i u trenucima kada oni nisu utemeljeni, umjesto upravljanje temeljem činjenica, pri čemu isključivo informacijski kapital koji je potpunog integriteta, sačuvan od neovlaštenog otkrivanja (a osobito konkurenciji) i raspoloživ kada je to potrebno može pomoći poduzeću u postizanju konkurentskih prednosti u poduzeću. Upravljanje informacijskim kapitalom poduzeća omogućiti će da tradicionalni **korektivni** (*reaktivni*) model upravljanja bude zamijenjen novim, **direktivnim** (*proaktivnim*). Naposljetku, primjena modela ekonomski održive informacijske sigurnosti omogućiti će smanjenje vremena potrebnog za upravljanje i donošenje odluka, te optimizirati procese u poduzeću. Ovakva promjena paradigme shematski je prikazana na shemi 33.

Shema 33: Tradicionalni pristup i novi pristup informacijskoj sigurnosti u malim i srednjim poduzećima



Izvor: prilagodio autor prema IBM Global Business Services**: „Business Analytics and Optimization for the Intelligent Enterprise“**, **http://mds.ricoh.com/change/optimizing_information,** 2009. (13.07.2013.)

7.2.4. Povećanje imidža malih i srednjih poduzeća

Kao što je do sada objašnjeno, čak i velika poduzeća nailaze na značajne probleme kod provođenja poslovne funkcije informacijske sigurnosti. Njihovi su poslovni informacijski sustavi inherentno vrlo kompleksni, a prema Mooreovom zakonu s protekom vremena postaju još kompleksniji. Osim internih čimbenika ove vrste, sama korištena informacijska tehnologija postaje toliko složena, da se značajno povećavaju inherentna svojstva koja rezultiraju ranjivostima korištene informacijske imovine a koje mogu biti iskorištene i rezultirati nastupom incidenta informacijske sigurnosti.

Međutim, mala poduzeća imaju tu komparativnu prednost u odnosu na velika poduzeća da imaju značajno manju količinu informacijske imovine, ukupna količina ranjivosti, pa samim time i prijetnji je manja, apsolutni iznos moguće štete uslijed nastupa incidenta informacijske

sigurnosti je manji, a poslovni procesi su jednostavniji. Upravljanje promjenama u manjim sustavima inherentno je jednostavnije nego u velikim sustavima. Uslijed toga, ukoliko ta poduzeća od samog početka svog poslovanja posvete dovoljnu pažnju informacijskoj mogućnosti, moći će pratiti rast i razvoj poduzeća, a budući da predloženi model inkorporira i zakonske zahtjeve i zahtjeve poslovne certifikacije i one najbolje prakse, mala i srednja poduzeća mogu zbog manjih zahtjeva i kraćeg potrebnog vremena za provođenje mjera informacijske sigurnosti postati i uzorom velikim poduzećima u organizaciji i upravljanju tom poslovnom funkcijom.

Imidž poduzeća je kategorija koju je teško procijeniti a tradicionalno se promatra kroz pojam *goodwilla*. *Goodwill* je predstavljen u nematerijalnom obliku prednošću u odnosu na konkurenciju koju je pouzeće steklo kroz svoje robne marke i reputaciju, vrijednošću projiciranih i budućih prihoda koje poduzeće može očekivati iznad svoje knjigovodstvene cijene, a osobito u slučaju prodaje dijela ili cijelog poduzeća. (Merriam-Webster, 2013)

Štoviše, moguće je pretpostaviti kako bi ovaj model mogao biti primjenjiv i za velika poduzeća koja su do sada upravljala informacijskom sigurnošću na stohastičan način ili slučajnim upravljanjem, od slučaja do slučaja. Bilo bi preporučljivo da takva velika poduzeća prođu kroz jedan ciklus uvođenja informacijske sigurnosti, od uključenja rukovoditelja i vlasnika do implementacije svih predviđenih mjera na ekonomski održiv način, a kada je taj sustav jednom uspostavljen, primjena modela upravljanja informacijskom sigurnošću na način koji je primjeren velikim poduzećima, formalnom certifikacijom, može biti proveden daleko jednostavnije.

Jedna od mogućnosti dodatnog povećanja imidža malih i srednjih poduzeća po implementaciji predloženog modela informacijske sigurnosti postojala bi u slučaju posjedovanja posebnog neprofitnog organizacijskog tijela koje bi izdavalo **certifikate o suglasnosti** s predloženim modelom, ali i vodilo brigu o daljem razvoju modela, sukladno zahtjevima koji proizlaze iz razvoja okruženja. Osim toga, minimalni zahtjevi elementarnih mjera informacijske sigurnosti koji su predstavljeni katalogom elementarnih mjera informacijske sigurnosti moraju biti konstantno održavani sukladno promjenama tehnologije i procesa. Takvo tijelo, po mogućnosti formirano unutar sustava ministarstva zaduženog za gospodarstvo i obrt, ili u okviru neke od vezanih agencija, a uz suradnju obrazovnog sektora, moglo bi obavljati poslove temeljne revizije mjera informacijske sigurnosti u malim i srednjim poduzećima, te izdavati certifikate o sukladnosti s jednostavnim mjerama, a također bi uz poštovanje razdvajanja odgovornosti između savjetodavnog i revizorsko-certifikacijskog tijela, moglo obavljati i poslove savjetovanja malih i srednjih poduzeća vezano uz napore poboljšanja dostignute razine informacijske sigurnosti. Certifikat ove vrste mogao bi služiti kao uvjerenje bankama,

upraviteljima fondova rizičnog kapitala, investitorima u početnoj fazi, ali i samim rukovoditeljima i vlasnicima poduzeća o tome kako je sustav informacijske sigurnosti uspostavljen sukladno ovome modelu, a samim time i da su informacijski sustav i kapital poduzeća adekvatno zaštićeni na dostignutoj razini rizika, karakteristika korištene informacijske imovine i njene ranjivosti.

7.2.5. Dostupnost izvora vanjskog financiranja

Mala i srednje poduzeća **financiraju** se iz dva glavna izvora, a to su vlastiti kapital[290] i vanjsko financiranje. Vanjsko financiranje najčešće poprima oblik bankovnog zajma, ali i može poprimiti i druge **hibridne** oblike poput:

1. **Trgovačkog kredita**, odnosno odgođenog plaćanja dobavljača,
2. **Faktoringa**, odnosno prodaje potraživanja,
3. **Okvirnog kredita** po poslovnom računu koji je efektivno prekoračenje odobreno od strane banke.

Posebna vrsta financiranja malih i srednjih poduzeća koje se veže uz rane faze njihovog poslovanja, a osobito se odnosi na poduzeća za koja se očekuje visok potencijal ostvarivanja prihoda i povrata na početni kapital, ali i vrlo visok rizik neuspjeha je tzv. financiranje rizičnim kapitalom[291]. Radi se o načinu financiranja koji je u Sjedinjenim Američkim Državama vrlo uobičajen još od početka osamdesetih godina prošlog stoljeća i vrlo prisutan u tehnološkom, informatičkom i biomedicinskom sektoru, te je prema nekima čak i jednim od čimbenika koji su doveli do više ciklusa burzovnih špekulativnih balona. Postoji više različitih tipova ovog oblika financiranja malih i srednjih poduzeća, no oni se uglavnom odnose na financiranje brzorastućih poduzeća koja koriste nove ideje i tehnologije u poslovanju, pri čemu oni koji financiraju takve poduhvate obično traže vlasnički udio u budućem poduzeću. Naposljetku, ciklus financiranja novih poduhvata rizičnim kapitalom završava inicijalnom ponudom i prodajom vlasničkog udjela. Kako bi se stekao dojam o utjecaju i veličini ovakvog oblika ulaganja, procjenjuje se kako je 2009. godine bilo između 4,000 i 6,000 investicija ove vrste u Ujedinjenom Kraljevstvu a prosječna investicija iznosila je 42,000 britanskih funti. Svaki investitor dobio je udio od 8 % u poslovnom poduhvatu. 35 % investicija generiralo je povrat u iznosu od 100-500 % a 9 % više od 1000 %. Srednji povrat svih investicija iznosio je 220 % u 3,6 godina a prosječna interna stopa povrata je bila 22 % bruto. (Wiltbank, 2009, p. 15)

[290] Često korišteni sinonim za „*vlastiti kapital*“ je i „*vlasnički kapital*“, a ponekad i „*upisani kapital*“. Njih treba razlikovati od „*temeljnog kapitala*“, koji je zapravo upisani kapital od strane udjelničara ili dioničara u trenutku osnivanja poduzeća.

[291] Ovaj način financiranja naziva se još i financiranje pothvatnim kapitalom od eng. *„venture capital financing“*. Za detalje cf, Investopedia, **http://www.investopedia.com/terms/v/vcfund.asp** (20.08.2013.)

U Republici Hrvatskoj u zadnjih nekoliko godina financirano je nekoliko ovakvih početnih poduzetničkih poduhvata, te je razvijena scena anđela-investitora i rizičnog kapitala, no marketinška prezentacija takvih projekata trenutačno je daleko jača od stvarnog utjecaja rizičnog kapitala na poslovne poduhvate ove vrste.

Za razliku od velikih poduzeća, a osobito onih koja se financiraju s tržišta kapitala emitiranjem dužničkih vrijednosnih papira ili izdavanjem redovnih ili preferencijalnih dionica, financiranje malih i srednjih poduzeća značajno je drugačijeg karaktera . Zbog veće rizičnosti poslovanja malih i srednjih poduzeća te činjenice kako ona su ona često inicijalno kapitalizirana ispod razine optimalne za poslovanje (Fliess, 2007, p. 5), ona ne posjeduju zadovoljavajuće poslovne planove, a samim time nemaju mogućnost davanja kolaterala za zajmove u opsegu koji zahtijevaju banke. Stoga je malim i srednjim poduzećima često zapriječen pristup izvorima financiranja. Ova je činjenica osobito dokumentirana i dokazana u ekonomijama u razvoju i znanstveno potvrđena.[292] Osim toga, mala i srednja poduzeća u fazi ubrzanog rasta često **ne posjeduju** dovoljnu profitabilnost, likvidnost, stabilnost poslovanja i ne posluju u dovoljno dugačkom vremenskom periodu kako bi zadovoljila zahtjeve banaka za odobravanjem kredita.

Mala i srednja poduzeća zbog svog značaja, udjela u nacionalnim ekonomijama i činjenice da su pokretači najuspješnijih gospodarstava svijeta, nalaze se pod posebnom paskom ministarstava zaduženih za malo gospodarstvo u većini nacionalnih ekonomija. Tako je i u Republici Hrvatskoj, te mala i srednja poduzeća tijekom pretpristupnih pregovora i nakon ulaska u Europsku uniju imaju na raspolaganju čitav niz različitih izvora vanjskog financiranja, a koji su povoljniji od tržišnih izvora financiranja, ili su utemeljeni na korištenju sredstava Europskih fondova, bilo direktno, bilo putem državnih agencija, ili se radi o direktnim potporama. (Ministarstvo poduzetništva i obrta Republike Hrvatske, 2013) Između njih moguće je izdvojiti sljedeće, prikazane u tablici 53. na sljedećoj stranici.

[292] Poduzeća s ovim karakteristikama se od radionice održane u Ženevi u srpnju 2008. godine pod naslovom „The Network for Governance, Entrepreneurship & Development (GE&D)“ nazivaju – Small Growing Businesses (eng. kratica „SGB“) – mala rastuća poduzeća.

Tablica 53: Mogućnosti potpora i poticaja malim i srednjim poduzećima u Republici Hrvatskoj

R.Br.	Pružatelj	Vrsta programa (potpore)
1.	Ministarstvo poduzetništva i obrta	Program „Poduzetnički impuls“ Mjera A: Razvoj mikropoduzetništva i obrta 1. Aktivnost A1: Mikropoduzetništvo i obrt, 2. Aktivnost A2: Poduzetništvo kreativnih industrija 3. Aktivnost A3: Mladi i početnici u poduzetništvu 4. Aktivnost A5: Jačanje poslovne konkurentnosti klastera Mjera: B Jačanje poslovne konkurentnosti poduzetnika i obrtnika 5. Aktivnost B1: Jačanje konkurentnosti poduzetnika i obrtnika 6. Aktivnost B3: Poticanje inovativnog poduzetništva
2.	Hrvatska banka za obnovu i razvitak	7. Program kreditiranja poduzetnika početnika 8. Program kreditiranja financijskog restrukturiranja 9. Program kreditiranja za poboljšanje likvidnosti 10. Program kreditiranja projekata zaštite okoliša 11. Program kreditiranja nove proizvodnje 12. Program kreditiranja razvitka malog i srednjeg poduzetništva 13. Program kreditiranja proizvodnje 14. Program financiranja pronalazaka 15. Program kreditiranja turističkog sektora 16. Program kreditiranja pripreme turističke sezone
3.	Hrvatska agencija za malo gospodarstvo i investicije	- Jamstveni program za nove poduzetnike (pismo namjere za izdavanje jamstva) - Mikrokreditiranje - Jamstveni program „Likvidnost“ - Jamstveni program Leasing - Jamstveni program Investicijom do uspjeha - Jamstveni program Rast - Jamstveni program Inovacije - Jamstveni program „Rast“
4.	Hrvatski zavod za zapošljavanje	- Mjere samozapošljavanja u okviru Programa stručnog osposobljavanja i zapošljavanja - Mjere potpore za proširenje postojeće djelatnosti
5.	Agencija za plaćanja u poljoprivredi, ribarstvu i ruralnom razvoju	- Proizvodno vezana plaćanja - Specifična plaćanja - Plaćanja u iznimno osjetljivim sektorima - Potpore za mjere ruralnog razvoja
6.	Hrvatski zavod za zapošljavanje	- „Mobilni timovi Zavoda za zapošljavanje“ – usluge poslodavcima u restrukturiranju ili u teškoćama
7.	Ministarstvo gospodarstva	- Otvoreni javni poziv iz programa „Razvoj energetskog sustava“ - Operativni program potpora sektorima prerađivačke industrije za 2013. godinu
8.	Fond za zaštitu okoliša i energetsku učinkovitost	- Sredstva fonda za sufinanciranje projekata korištenja obnovljivih izvora energije - Sredstva fonda za sufinanciranje projekata korištenja obnovljivih izvora energije - Sufinanciranje projekata energetske učinkovitosti u zgradarstvu
9.	Poslovno inovacijska agencija Republike	- Provjera inovativnog koncepta za poduzetnike (PoC Private) : Javni poziv za podnošenje prijava za

	Hrvatske	sufinanciranje inicijalne faze inovativnih znanstveno-poduzetničkih projekata - Sjemenski kapital za razvoj novog proizvoda – RAZUM Program za istraživanje i razvoj – IRCRO (Natječaj zatvoren.) - Programi razvoja tehnologijske infrastrukture – TEHCRO i TEST
10.	Ministarstvo turizma	- Program poticanja razvoja turizma na turistički nerazvijenim područjima u 2013. godini - Program poticanja slobodnog pristupa internetu u turističkim destinacijama - Dodjela bespovratnih sredstava manifestacijama u funkciji razvoja turizma u 2013. - Program poticanja inovacija u turizmu "INOVATIVNI TURIZAM"

Izvor: priredio doktorand prema podacima sa Internet stranice Ministarstva poduzetništva i obrta, **http://poticaji.minpo.hr/** (15.08.2013.)

Za očekivati je kako će u skoroj budućnosti, a osobito za poduzeća koja se bave djelatnostima s visokotehnološkom i dodanom vrijednošću, i banke i investitori u rizični kapital, zahtijevati dodatne **garancije** u smislu očuvanja **integriteta informacijskih sustava** i **informacijskog kapitala** takvih poduzeća. Ovo je osobito moguće očekivati za ona poduzeća koja razvijaju nove tehnologije, a koje mogu potencijalno rezultirati novim izumima, patentima ili postupcima, kod kojih je tajnost, odnosno barijera pristupa tim podacima u odnosu na konkurenciju, temeljna aktivnost kojom se u fazi prije patentiranja poduzeća štite od disruptivnih radnji konkurencije ili otkrivanja informacija koje predstavljaju temelj razvoja njihovog poslovanja. Osim toga, i država bi kao stvaratelj okvira za uspješno poslovanje malih i srednjih poduzeća trebala prepoznati značaj informacijske sigurnosti u svim fazama rasta i poslovanja malih i srednjih poduzeća te bi trebala postaviti dodatne formalne zahtjeve pred ta poduzeća u fazi dodjele potpora ili preferencijalnog financiranja kako bi osigurala svrsishodnost korištenja dodijeljenih sredstava.

8. ZAKLJUČAK

U Republici Hrvatskoj preko 99 % svih poduzeća pripada kategoriji malih i srednjih poduzeća, u njima radi dvije trećine svih zaposlenih, u njima se stvara oko polovice bruto domaćeg proizvoda i preko 40 % ukupnog izvoza. Prema relativnom udjelu malih i srednjih poduzeća u ukupnosti privredne aktivnosti nacionalne ekonomije, ova je struktura slična onoj u Europskoj uniji i Sjedinjenim Američkim Državama. Sva ta poduzeća neovisno o svojoj veličini, pa i poslovnoj djelatnosti, od samog početka svog poslovanja koriste informacijske sustave kao potporu poslovanju, ili su pojedine informacijske tehnologije čak i predmetom njihovog poslovanja ukoliko takva poduzeća razvijaju nove tehnologije ili usluge s visokom dodanom vrijednošću ili poslovne informacijske sustave.

Informacijski sustavi koje koriste poduzeća sastoje se od informacijske imovine, koja je predstavljena skupom materijalne i nematerijalne imovine koju poduzeće koristi u poslovnom procesu, a koja inherentno posjeduje svojstva ranjivosti koja proistječu iz njenih osobina. Takve ranjivosti moguće je eksploatirati na način da prijetnje koje dolaze iz okoline poduzeća ili iz samog poduzeća iskoriste navedene ranjivosti informacijske imovine, a što rezultira nastupom incidenta informacijske sigurnosti.

Mala i srednja poduzeća su u području upravljanja informacijskom sigurnošću specifična u odnosu na velika poduzeća prema više pokazatelja. Njihovi su informacijski sustavi u pravilu manje razine kompleksnosti, posjeduju manju količinu informacijske imovine, te je apsolutni trošak nastanka incidenta informacijske sigurnosti uobičajeno manji. Međutim, velika poduzeća imaju na raspolaganju veće materijalne i ljudske resurse za implementiranje informacijskih tehnologija, pa tako i sustava upravljanja informacijskom sigurnošću, te za razliku od malih i srednjih poduzeća, postoje profesionalni i certifikacijski sustavi koji su dobro prilagođeni njihovim specifičnostima. Iako su takvi profesionalni i certifikacijski sustavi nazivno nediskriminatorni i mogu se jednako koristiti i za mala i srednja poduzeća, u svojim temeljnim pretpostavkama podrazumijevaju relativno kompleksne obrasce zaštite informacija i instance u poduzeću koje su zadužene za provedbu mjera informacijske sigurnosti (osoba ili odjel zaduženi za informacijsku sigurnost). Iz tog razloga, oni nisu primjereni za upotrebu u malim i srednjim poduzećima u kojima je funkcija poslovne informatike često povjerena jednoj osobi unutar poduzeća, eksternalizirana ili je čak obavlja jedan od rukovoditelja ili vlasnika uz sve ostale radne zadatke.

Ulaskom u Europsku uniju u Republici Hrvatskoj završio je proces prilagodbe nacionalnog zakonodavstva zakonima Europske unije, pa je tako u posljednjih pet do šest godina donesen čitav niz zakona i uredbi kojima se uređuje područje informacijske sigurnosti. Međutim,

sukladno istovjetnim procesima u Europskoj uniji, niti u Republici Hrvatskoj područje informacijske sigurnosti u malim i srednjim poduzećima nije uređivano zakonima. Oni uglavnom reguliraju zaštitu privatnosti i osobnih podataka, dok je zaštita informacijskih sustava prepuštena organizacijama koje se profesionalno bave informacijskom sigurnošću i certifikacijskim postupcima koji su u pravilu previše kompleksni, previše skupi i neprilagođeni realnosti malih i srednjih poduzeća, a osobito mikro i malih poduzeća. Iz praktičnih i teorijskih spoznaja slijedi kako se specifičnosti poslovne funkcije informacijske sigurnosti malih i srednjih poduzeća ne uzimaju uobzir od strane zakonodavca ili certifikacijskih tijela. Vrlo često su ona prepuštena dobavljačima rješenja informacijske sigurnosti, a tako uspostavljeni sustavi informacijske sigurnosti zasigurno nisu optimalni prema svojim parametrima, odnosno stupnju otklanjanja rizika informacijske sigurnosti.

Uobičajeni pristup organizaciji informacijske sigurnosti kreće od obvezivanja rukovoditelja, tj. uprava poduzeća za provođenje ciljeva informacijske sigurnosti, zatim ide određivanja opsega tj. dohvata informacijske sigurnosti i ide preko procesa popisivanja informacijske imovine i procjene rizika do određivanja mjera kojima će se ti rizici ukloniti ili umanjiti. Dobrim dijelom te mjere su organizacijske, ali i zahtijevaju značajne investicije u rješenja informacijske sigurnosti. Budući da većina certifikacijskih mjera sadrži stotine različitih rizika u katalogu rizika kojima korespondira isto toliko ili više različitih rješenja i mjera informacijske sigurnosti, jasno je kako se radi o vrlo kompleksnom procesu koji je gotovo neprovediv u realnosti malih i srednjih poduzeća. Međutim, čak i u uvjetima u kojima su financijska sredstva raspoloživa, certifikacijski sustavi i sustavi najbolje prakse često ne uzimaju u obzir ekonomsku isplativost implementacije takvih mjera, odnosno, je li ekonomski i financijski primjereno implementirati odgovarajuće mjere, za koje se s tehničkog aspekta procjene rizika smatra kako bi trebale biti provedene. Naime, odluku o implementaciji potrebnih mjera u pravilu se prepušta upravi poduzeća, smatrajući kako one imaju sve potrebne informacije kako bi odlučivali o ovako strateškim potezima, dok u praksi to nije tako.

Kako bi se predložio novi model informacijske sigurnosti koji je ekonomski održiv, što znači da bi sadržavao i analizu isplativosti uvođenja mjera informacijske sigurnosti u odnosu na kvantificirani rizik, bilo je potrebno analizirati koje su temeljne odrednice informacijske sigurnosti kao ravnopravne poslovne funkcije, njen strateški značaj u upravljanju poduzećem i kakav utjecaj ima rizik po informacijsku sigurnost. Razvoj mjera informacijske sigurnosti prati razvoj informacijskih sustava, koji su pak posljedica uvođenja informacijsko-telekomunikacijskih tehnologija u svakodnevno poslovanje poduzeća nakon Drugog svjetskog rata. Ova je poslovna funkcija doživjela svoj iznenadni razvoj po pitanju kompleksnosti u trenutku kada su računala unutar poduzeća umrežena u interne mreže, *Intranete*, odnosno kada

su se poduzeća umrežila korištenjem svojih *Ekstraneta*, odnosno *business to business* informatičkih sustava, a sve korištenjem Internet tehnologija od sredine devedesetih godina prošlog stoljeća. Štoviše, informatička je sigurnost postala strateškom poslovnom funkcijom iz tog razloga što ona predstavlja barijeru koju poduzeće postavlja konkurenciji kako ona ne bi imala pristup svim informacijama koje posjeduje to poduzeće, a koje s druge strane predstavljaju konkurentsku prednost za to poduzeće. Ovaj je proces osobito važan za ona mala i srednja poduzeća koja u svom poslovanju pokušavaju na tržište plasirati nove proizvode, usluge i koncepte, jer njihov opstanak ovisi o tome da informacije kojima upravljaju ostanu tajne do faze patentiranja proizvoda. Međutim, čak i ostala poduzeća koja se bave primarnim ili sekundarnim djelatnostima mogu izvući pozitivne efekte iz uvođenja novog ekonomski održivog sustava upravljanja informacijskom sigurnošću, jer mogu izbjeći maliciozne napada iz unutrašnjosti ili iz okoline poduzeća, ili troškove uslijed nastupa različitih incidenata informacijske sigurnosti, poput napada na informacijske sustava ili ostalih oblika ukidanja raspoloživosti, povjerljivosti i integriteta informacija pohranjenih u informacijskim sustavima poduzeća. Pritom je potrebno prepoznati kako poduzeća u upravljanju informacijskom sigurnošću zapravo ne štite sve informacije koje posjeduju već trebaju identificirati koji je informacijski kapital poduzeća koji je ključan za njegovo poslovanje, a radi se o onim informacijama i znanju koji djeluju katalitički u proizvodnji dobara i usluga, a koji su klasificirani u informacijskim i dokumentacijskim sustavima poduzeća, no koji su ujedno dijelom sustava upravljanja životnim ciklusom podataka i informacija. Teorijskom analizom svih navedenih koncepata i njihovim pažljivim stavljanjem u međusobni odnos, potvrđuje se prva potporna hipoteza doktorske disertacije.

Proces kreiranja novog modela informacijske sigurnosti za mala i srednja poduzeća nastavljen je analizom zakonskih zahtjeva koji su postavljeni pred taj segment poduzeća a pritom se referentnim zakonskim sustavima uzimaju sustavi država i državnih zajednica koje su postigle najviši stupanj regulative informacijske sigurnosti . Međutim, detaljno su analizirani i zakonski sustavi ostalih država s kojima Republika Hrvatska ostvaruje značajnu trgovinsku razmjenu, a to su primarno države koje su s Republikom Hrvatskom tvorile SFRJ, odnosno njene bivše republike a sada samostalne države. Naime, način reguliranja područja informacijske sigurnosti u državama s kojima Republika Hrvatska ostvaruje značajne ekonomske odnose bitan je i za mala i srednja poduzeća u Republici Hrvatskoj, jer se na taj način može anticipirati zahtjeve koji su pred njih postavljeni. Analizirane zemlje nemaju posebne zakone koji bi individualno ciljali mala i srednja poduzeća, već je zakonska regulativa uglavnom usmjerena ka propisivanju mjera i načina upravljanja, zaštite, korištenja i obrade osobnih podataka u državnim poduzećima i tijelima koja ih obrađuju, odnosno klasifikaciji podataka kojima upravlja država. U Republici Hrvatskoj, ali i drugim državama je informacijska sigurnost detaljnije regulirana za financijski

sektor, međutim mala i srednja poduzeća su izuzeta iz ovih mjera jer poduzeća koja posluju u financijskom sektoru po automatizmu definicije pripadaju velikim poduzećima neovisno o broju zaposlenih, prihodima ili iznosu bilance. Međutim, kazneni zakoni svih analiziranih država prepoznaju veliki niz kaznenih djela koja se odnose na informacijske sustave a po pojavnim oblicima, načinima počinjenja i opisu odgovaraju uobičajenim načinima nastupa incidenata informacijske sigurnosti.

Osim zakonskih zahtjeva, za postavljanje novog modela nužno je proučiti i smjernice, standarde i najbolju praksu pri uspostavljanju i korištenju sustava upravljanja informacijskom sigurnošću. Radi se o sustavima koji su vezani uz isporuku informatičkih usluga te su dijelom uobičajene prakse u velikim poduzećima, ali su jednako primjenjivi i na mala i srednja poduzeća. Osim sustava upravljanja pojedinim domenama poslovne informatike, u ovu skupinu sustava normizacije pripadaju i referentni sustavi upravljanja kvalitetom, i to *ISO 9001* te *ISO 27001:2005* koji opisuje upravljanje sustavom kvalitete informacijske sigurnosti. Pojedine smjernice, mjere i postupci navedenih sustava i standarda mogu se adaptirati i koristiti i u upravljanju informacijskom sigurnošću u malim i srednjim poduzećima. Tako je upravljanje ciljevima i ključnim pokazateljima informacijske sigurnosti moguće organizirati u okviru sustava *ISO 9001*, pojedine mjere iz aneksa A informacijske sigurnosti izvanredno se mogu uklopiti u katalog mjera informacijske sigurnosti za mala i srednja poduzeća dok se sustavi upravljanja isporukom informacijskih usluga *ITIL* i sustav upravljanja poslovnom informatikom *COBIT* mogu u potpunosti ili u najvažnijim dijelovima implementirati za upravljanje poslovnom informatikom, a u okviru nje i informacijskom sigurnošću. Uvođenje sustava upravljanja informacijskom sigurnošću korištenjem metodologije *PRINCE2* i sličnih projektnih metodologija povećat će uspješnost uvođenja takvih sustava. Međutim, niti jedan od navedenih sustava najbolje prakse i standarda nije prilagođen samo korištenju u malim i srednjim poduzećima, a činjenica je kako usprkos tome što takvi sustavi ne diskriminiraju između poduzeća prema veličini, oni zahtijevaju značajne financijske i organizacijske resurse, kako za uvođenje, tako i za njihovo održavanje. Iz navedenog razloga, sami po sebi ovakvi sustavi normiranja nisu adekvatni za korištenje u malim i srednjim poduzećima, ali pružaju značajne smjernice po pitanju načina na koji je poslovnu funkciju informacijske sigurnosti moguće u njima organizirati. Ovime je potvrđena potporna hipoteza kako je za uspostavljanje ekonomski održivog sustava upravljanja informacijskom sigurnošću potrebno sagledati i relevantne zakonske propise i najbolju strukovnu praksu.

Mjere informacijske sigurnosti predstavljene su organizacijskim i tehničkim obrascima kojima se informacijska imovina, odnosno informacijski kapital poduzeća štite od nastupa rizika informacijske sigurnosti koji prijete iskoristiti njihovu ranjivost. Kao što je u disertaciji detaljno

objašnjeno, mjere informacijske sigurnosti koje predlažu sustavi najbolje prakse ne uzimaju u obzir financijsku poziciju poduzeća, njihovu poslovnu strategiju niti dostignuti stupanj razvijenosti funkcija poslovne informatike i informacijske sigurnosti već pristup utemeljen na apsolutnom riziku jednako primjenjuju na sva poduzeća i sve prilike. Ovakav tehnički pristup glavna je zamjerka postojećem uvriježenom sustavu upravljanja informacijskom sigurnošću i jedan od vjerojatnih uzroka zbog kojih je sigurnost informacijskih sustava u malim i srednjim poduzećima tradicionalno značajno niža od one u velikim poduzećima koja imaju više iskustva i veće resurse na raspolaganju za provođenje potrebnih mjera. Kako bi se predložili instrumenti za kasniju uporabu kvantitativnih metoda koje su pogodne za upotrebu u malim i srednjim poduzećima, pomno su proučena dosadašnja znanstvena istraživanja iz novog područja mikroekonomike – ekonomike informacijske sigurnosti, te se tim postupkom pokušalo doći do onih kvantitativnih metoda koje bi bile pogodne za upotrebu u malim i srednjim poduzećima. U teorijskom smislu, veći broj znanstvenika bavio se u zadnjih petnaestak godina problematikom isplativosti ulaganja u informacijsku sigurnost a zajednički su im pokušaji određivanja optimuma ulaganja u informacijsku sigurnost u odnosu na razinu proračunatog rizika koji prijeti informacijskim sustavima. Pritom se koriste vrlo kompleksnim matematički instrumentarijem, te poslovnu funkciju promatraju u okviru teorije igara pri čemu je informacijska sigurnost igra između napadača koji uzrokuju incidente i rukovoditelja sustavom informacijske sigurnosti koji donose protumjere, odnosno pokušavaju odrediti koja je točka do koje poduzeća mogu opravdati investicije u informacijsku sigurnost.

Kako bi mala i srednja poduzeća imala točan uvid u svoju informacijsku imovinu, njene osobine i rizike, nužno je da održavaju njen točan popis, ali i pretpostavljane iznose utroška u sustav upravljanja informacijskom sigurnošću na godišnjoj razini, i to prema investicijama (ulaganjima) u sustav i troškovima njegovog održavanja, te dodatno razrađen prema pojavnim oblicima takvih troškova, odnosno prema tehničkim disciplinama i mjerama informacijske sigurnosti. Tek kada mala i srednja poduzeća na ovaj način sistematiziraju svoje upravljanje sustavom informacijske sigurnosti, moguće je očekivati da mogu nastaviti s korištenjem metoda financijske analize pri odlučivanju o pojedinim investicijama i troškovima. U disertaciji je pokazano kako se za analizu investicijskih ulaganja u sustave upravljanja informacijskom sigurnošću može koristiti klasična financijska analiza kapitalnih investicija te izračun pokazatelja povrata na inicijalnu investiciju *(ROI)*, neto sadašnje vrijednosti investicije u informacijsku sigurnost *(NPV)* i interne stope povrata *(IRR)*, a dobivene rezultate je potrebno pažljivo protumačiti sukladno ulaznim parametrima i okolnostima. Čest je slučaj da poduzeća moraju birati između više alternativa, a u kontekstu informacijske sigurnosti radi se o gotovo apsolutnoj supstitutivnosti investicija rješenjima najma ili korištenjem usluga računalstva u oblaku čime se djelomično ili u potpunosti trošak informacijske sigurnosti prebacuje na

pružatelja usluga. Budući da takav odabir predstavlja kvalitativno odlučivanje o kvantitativnim odrednicama poslovanja, jer iskazuje preferencije rukovoditelja, odnosno vlasnika poduzeća u odnosu na jednu ili drugu vrstu rješenja koja se ne može nužno objektivno kvantificirati, malim i srednjim poduzećima preporuča se korištenje provjerene metode analitičkih hijerarhijskih procesa *(AHP)* jer je u disertaciji pokazano kako se ona može koristiti za odlučivanje o investiranju u jednu od više mogućih alternativa (mjera) informacijske sigurnosti, te da daje najbolje rezultate ukoliko je odlučivanje između parova kriterija i alternativa konzistentno, a mjeru konzistencije moguće je kao korektiv točno matematički odrediti.

Kako bi se ocijenilo stanje sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, u prvoj polovici 2013. godine provedeno je anketno istraživanje na slučajno odabranom uzorku svih malih i srednjih poduzeća te su dobiveni rezultati statistički značajni za čitavu populaciju. Istraživanju je prethodilo kreiranje modela za ocjenu dostignutog stupnja zrelosti sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, a koji u sebi inkorporira sve bitne elemente te funkcije, od provođenja operativnih mjera informacijske sigurnosti do uključenosti rukovodstva i vlasnika u upravljanje. Model za ocjenu kreiran je korištenjem odrednica sustava upravljanja poslovnom funkcijom informatike *COBIT*, sustava isporuke informatičkih usluga *ITIL*, aneksa A sustava kontrole kvalitete upravljanja informacijskom sigurnošću *ISO 27001:2005* i ostalih sustava najbolje prakse informacijske sigurnosti. Na ovaj način kreiran je model za ocjenu koji predviđa pet razina funkcionalnosti (zrelosti) sustava upravljanja informacijskom sigurnošću, a koje su poredane u hijerarhijskom odnosu. Opisani model je kreiran na način da srednja, treća razina modela obuhvaća najviše mjera operativne informacijske sigurnosti iz razloga što su one preduvjet za postizanje viših razina funkcionalnosti sustava, odnosno sustav je asimetričan, što odgovara praktičnoj vizuri sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima. Iz dobivenih rezultata može se zaključiti kako je zatečena i dostignuta razina zrelosti (funkcionalnosti) sustava upravljanja informacijskom sigurnošću u malim i srednjim poduzećima više nego nezadovoljavajuća. Ukupna implementacija sustava upravljanja informacijskom sigurnošću iznosi između 19,79 % (mjereno medijanom) do 22,32 % (mjereno aritmetičkom sredinom). Pritom čak 4,3 % anketiranih poduzeća nema implementiranu niti jednu mjeru informacijske sigurnosti. Ovi, i dodatni analitički rezultati koji se odnose na percepciju upravljanja informacijskom sigurnošću kao strateškom aktivnosti, opravdali su pomoćnu hipotezu prema kojoj je zatečeno stanje potrebno korigirati putem novog modela utemeljenog na ekonomskim principima procjene investicija u sustav upravljanja informacijskom sigurnošću. Osim ocjene razine funkcionalnosti sustava, anketa je pružila prigodu i za kreiranje instrumenta analize ostalih čimbenika koji se odnose na incidente informacijske sigurnosti te upravljanje informacijskom sigurnošću i dostignuti stupanj kulture

informacijske sigurnosti u malim i srednjim poduzećima. Svi dobiveni pokazatelji ukazuju na neadekvatnost načina na koji je ta funkcija organizirana u malim i srednjim poduzećima u Republici Hrvatskoj pri čemu je dokazano kako se uzorak mikro, malih i srednjih poduzeća može promatrati kao homogen budući da se samo između 5,5 i 6,5 % varijance u ukupnoj dostignutoj funkcionalnosti može atribuirati pripadnosti grupaciji sukladno kriterijiima raspona broja zaposlenih, iznosa bilance i ukupnog prihoda.

U nastavku, od velike je važnosti bilo identificirati one nezavisne varijable koje su od najvećeg utjecaja na zavisnu varijablu - dostignutu ukupnu razinu funkcionalnosti (zrelosti) modela upravljanja informacijskom sigurnošću u malim i srednjim poduzećima u Republici Hrvatskoj, te na dihotomnu zavisnu varijablu – strateško upravljanje informacijskom sigurnošću. Regresijskom analizom ustanovljeno je kako je u prvom slučaju moguće identificirati pet nezavisnih varijabli koje opisuju 84,3 % varijance u zavisnoj varijabli, a to su zrelost operativnog upravljanja informacijskom sigurnošću, poštivanje propisa, politika i standarda, posvećenost rukovodstva strateškoj informacijskoj sigurnosti i mjera percepcija posljedica nastupa incidenata informacijske sigurnosti. Interesantno je kako nezavisna varijabla mjere zrelosti odlučivanja o investiranju u informacijsku sigurnost ne poboljšava model te je stoga iz njega izbačena a vjerojatan razlog tome je stihijsko upravljanje vlasnika i rukovoditelja koje ne rezultira dovoljnim poboljšanjima koja bi se reflektirala u poboljšanjima ukupnog funkcioniranja modela. U drugom slučaju, obavljena je regresijska analiza dihotomne zavisne varijable strateškog upravljanja informacijskom sigurnošću te šest nezavisnih varijabli za koje se pretpostavlja kako mogu objasniti kretanje zavisne varijable. Na taj način je od šest nezavisnih varijabli identificirano četiri koje kreiraju predikcijski model koji ispravno predviđa 77,5 % pojava u odnosu na nul model, dok se za varijable uvedenost operativnih mjera informacijske sigurnost i uvedenost sustava *ISO 9001* ne nalazi da bi poboljšale model. Ova je situacija zapravo i očekivana, budući da mala i srednja poduzeća ne posjeduju znanja o tome kako iskoristiti sustav *ISO 9001* i u njega inkorporirati upravljanje informacijskom sigurnošću. Iznenađujuće je kako predikcijski model ne uključuje strateške mjere informacijske sigurnosti ali uključuje posjedovanje pisanih procedura vezanih uz informacijsku sigurnost. Ova se činjenica može objasniti time da je informacijska sigurnost u malim i srednjim poduzećima u Republici Hrvatskoj na vrlo niskim razinama, te su samim time primijenjene operativne mjere uvedene slučajnim upravljanjem, na prijedlog dobavljača rješenja ili isu implementirane zbog iskustva i na prijedlog zaduženih za informacijske sustave poduzeća, a nisu rezultat strateškog promišljanja.

Nakon što je izrađeni model potvrdio hipotezu o neprilagođenosti potrebama malih i srednjih poduzeća i niskoj razini funkcionalnosti, predloženi su koraci za reinženjering postojećih

procesa na način da su predložene aktivnosti implementacije novog modela upravljanja informacijskom sigurnošću, i to u pripremnom i provedbenom dijelu. Korištenjem *ARIS BPM* metodologije modeliranja procesa predložen je model provedbe koji se sastoji od dvije procesne vertikale, pri čemu se u prvoj predlažu konkretni koraci inicijalne ili opetovane implementacije modela informacijske sigurnosti koji je osobito prilagođen za mala i srednja poduzeća. Na samom početku, provedbene aktivnosti obavljaju sam vlasnik ili vrh rukovodstva poduzeća što zahtijeva značajna financijska sredstva, a što je uz nepoznavanje obaveza jedna od glavnih prepreka povećanju razine funkcionalnosti informacijske sigurnosti. Nakon toga, aktivnosti se razlažu u nekoliko makro-ciklusa za koje se predlaže uvođenje slijedom važnosne hijerarhije, a to su osiguravanje sukladnosti sa zakonskim zahtjevima, osiguravanje sukladnosti s profesionalnim certifikacijskim zahtjevima i naposljetku, osiguravanje sukladnosti sa sustavima najbolje prakse informacijske sigurnosti. Proces se ciklički ponavlja ukoliko je dostignut rok za provjeru sukladnosti ili je došlo do takvih promjena u poslovnom procesu, informacijskoj imovini ili rizicima da je ponovna provedba procesa nužna. Potpornu procesnu vertikalu čini proces evaluacije rizika po informacijsku imovinu i ekonomske evaluacije mjera, odlučivanja o investicijama (pri čemu su primjerene metode klasične financijske analize) ili o najmu informacijsko-sigurnosnih rješenja, odnosno korištenju usluga računalstva u oblaku. Modelom je predviđeno i nekoliko repozitorija mjera i informacija vezanih uz upravljanje informacijskom sigurnošću poduzeća a među njima je ključaj katalog elementarnih mjera informacijske sigurnosti za koji bi bilo preporučljivo da ga održava vanjska strukovna organizacija ili državna agencija, budući da se radi o elementarnim mjerama koje ne zahtijevaju značajna financijska sredstva a provode se u prvom koraku modela.

Zaključno, identificirani su učinci primjene ovako izloženog ekonomski održivog modela upravljanja informacijskom sigurnošću malih i srednjih poduzeća. Ekonomska održivost takvog modela ogleda se u tome kako je primjena svake mjere informacijske sigurnosti pod povećalom instrumentarija ekonomske analize, odnosno uspoređuje se u jednoj dimenziji u odnosu na paradigmu, tj. trilemu „*investicija-najam-korištenje usluge računalstva u oblaku*“, a u drugoj dimenziji s obzirom na financijske pokazatelje implementacije neke od mjera. Očekuje se kako bi korištenje opisanog modela moglo u praksi rezultirati povećanom razinom usklađenosti sa zakonskim propisima, certifikacijskim standardima i sustavima i najboljom praksom, a sve navedeno je temelj nastavka poslovne djelatnosti malih i srednjih poduzeća, a osobito u segmentu prodaje, odnosno *b2c* segmentu odnosa s kupcima, kao i postizanju viših razina strukovne usklađenosti i potencijalno, formalne certifikacije sustava upravljanja informacijskom sigurnošću. Zasigurno najznačajniji, te vlasnicima i rukovoditeljima najlakše i najbrže uočljiv učinak primjene biti će izbjegavanje troška nastupa incidenata informacijske sigurnosti, te povećana razina zaštite informacijskog kapitala, što je osobito značajan učinak za ona poduzeća

koja razvijaju nove proizvode, usluge i postupke koji rezultiraju patentima. Mala i srednja poduzeća mogla bi primjenom ovakvog modela postati liderima u odnosu na velika poduzeća koja imaju na raspolaganju značajnije resurse za upravljanje informacijskom sigurnošću ali je tom funkcijom teže upravljati zbog inercije i kompleksnosti sustava. Također, povećana razina informacijske sigurnosti može rezultirati i lakšom dostupnošću izvora vanjskog financiranja, kako na direktan način, kod apliciranja na projekte financirane iz sredstava fondova Europske unije, tako i indirektno, kroz poboljšanje poslovnih pokazatelja malih i srednjih poduzeća u postupku dokazivanja sposobnosti za bankovno kreditiranje ili prijave na razne državne programe poticaja i potpora.

Rezultati znanstvenoga istraživanja koji su prezentirani u petom i šestom poglavlju ovog doktorskog rada te prijedlog koraka uvođenja novog modela izložen u sedmom poglavlju, **potvrdili su temeljnu znanstvenu hipotezu**: **Upotrebom utemeljenih spoznaja ekonomske znanosti, te uz uvažavanje zakonom određenih zahtjeva, i međunarodno prihvaćenih normi najbolje prakse, moguće je predložiti ekonomski utemeljen model upravljanja sustavom informacijske sigurnosti koji je posebno prilagođen potrebama malih i srednjih poduzeća u Republici Hrvatskoj, a koji će osigurati poboljšanje poslovnog rezultata, te povećati razinu sukladnosti sa zakonskim propisima i predmetnim međunarodnim standardima.** Dokazano je da je zatečena razina informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj vrlo niska i definirani su glavni čimbenici uspješnog povećanja razine funkcionalnosti poslovne funkcije informacijske sigurnosti. Predloženi su i koraci te makro-procesi poboljšanja poslovne funkcije informacijske sigurnosti koji su utemeljeni na ekonomskoj analizi rizika i učinaka te posebno prilagođeni okolnostima oskudnosti resursa u kojima posluju mala i srednja poduzeća. Uvođenjem ovakvog modela mogu se očekivati značajne direktne i indirektne uštede.

LITERATURA

KNJIGE

1. **„Oracle® Data Mining Concepts 11g Release 1 (11.1)“**, Oracle, 2008.
2. Alberts, C., Dorofee A.: **"Managing Information Security Risks: The OCTAVE (SM) Approach"**, Addison-Wesley Professional, Boston, 2002.
3. Anderson, R.: **„Why Information Security is Hard“**, Applied Computer Security Associates, New Orleans, 2001.
4. Bazavan, V. I., Lim I**.: "Information Security Cost Management"**, Auerbach Publications, New York, 2006.
5. Biba, K. J. **"Integrity Considerations for Secure Computer Systems"**, MTR-3153, The Mitre Corporation, 1977.
6. Birchler, U., Buetler, M.: **"Information Economics“,**Routledge Advanced Texts in Economics and Finance, Routledge, Oxon, 2007.
7. Canzer, B.: **„E-Business: Strategic Thinking and Practice“**, 2nd edition, South-Western College Pub., Boston, 2005.
8. Delišimunović, D: **"Management zaštite i sigurnosti"**, Pragmatekh, Zagreb, 2006.
9. Elton, E. J. et. a.: **“Modern Portfolio Theory and Investment Analysis“**, Wiley, Bognor Regis, 2009.
10. Fahramand, F. et. a.: **„Managing vulnerabilities of information systems to security incidents“**,ICEC, New York, 2003.
11. Fliess, B**.:**“**External impediments to SME access to international markets: What are they and how can they be reduced?“**, OECD, Ženeva, 2007.
12. Hai, J. C: **„Fundamental of development administration“,** Scholar Press, Puchong, 2007.
13. Hamidović, H.: **"Standardi informacijske sigurnosti"**, Info Press, Zagreb, 2006.
14. Hefferna, S.: **„Modern Banking in Theory and Practice“,** John Wiley&Sons Ltd., Chicester, 1996.
15. Hirshleifer, J.: **"The Analytics of Uncertainty and Information"**, Cambridge University Press, Cambridge, 1992.
16. Huffmire, T. et.al: **“Handbook of FPGA Design Security“**, High Assurance Software Lessons and Techniques, Springer, Berlin, 2010.
17. Ivandić-Vidović, D., Karlović, L., Ostojić, A.: **"Korporativna sigurnost"**, UHMS, Zagreb, 2011.
18. Johnson, M. Eric: **"Managing Information Risk and the Economics of Security"**, Springer, Berlin, 2009.

19. Kirkwood, C. W.: **„Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets“**, Duxbury Press, Belmont, 1997.
20. Krause, M. & Tipton, H. F.: **„Handbook of Information Security Management“**, 5th edition ,CRC Press, New York,2005.
21. Malik, Krishan A**., „Petroleum Project Evaluation & Investment Decision Making“**, Institute for Petroleum Development, Austin, 2011.
22. Mason, A.: **„Overview of VPNs and VPN Technologies“,** Pearson Education, Cisco Press, Indianapolis, 2002.
23. McGraw, G.: **„Bulding security in“**, Addison-Wesley Professional, Boston, 2006.
24. Meixner, H. R.: **„An illustrated guide to the Analytic Hierarchy Process“**, University of Natural Resources and Applied Life Sciences, Institute of Marketing & Innovation, Beč, Austrija, 2011.
25. Meyer, Paul J.: **„Attitude is Everything“**, The Leading Edge Publishing, Merced, 2006.
26. National Research Council of the National Academies: **„Government data centers: meeting increasing demands“**, The National Academy Press, Washington D.C., 2003.
27. Nilsen, Odd: **„Protection of Information Assets“**, SANS Institute InfoSec Reading Room, SANS Institute, 2002.
28. Norman, L.T.: **„Integrated Security Systems Design: Concepts, Specifications, and Implementation“** , Butterworth-Heinemann , Oxford, 2011.
29. Osten, M. & Kanter, B.: „**How to cost and fund ICT“**, NCVO , London, 2007.
30. Petz, B.: **„Osnovne statističke metode za nematematičare“**, Naklada Slap, Jastrebarsko, 2002.
31. Roberts, M, Russo R..: **„A Student's Guide to Analysis of Variance“**, Routledge, London, Velika Britanija, 1999.
32. Samarati, P. &, Capitani di Vimercati, S.: **„Access Control: Policies, Models and Mechanisms“**, Instituto de Computação – UNICAMP, 2007.
33. Scheer, A. W.: **„Architecture of Integrated Information Systems: Foundations of Enterprise Modelling“** softcover reprint of the original 1st ed.,Springer Verlag, Berlin, 1992.
34. Schneier, B.: **„Secrets & Lies - Digital Security in a Networked World“**,. 2nd ed., Hoboken, John Wiley & Sons, Hoboken, 2004.
35. Short, J. E.: **„Information Lifecycle Management Concepts, Practices, and Value“**, University of California, San Diego, 2007.
36. Srića, V., Spremić, M: **"Informacijskom tehnologijom do poslovnog uspjeha"**, Sinergija, Zagreb, 2000.

37. Stamp, M.:„**Information security principles and practice“**, Wiley-Interscience, New York, 2006.
38. Tipton, H. F. & Nozaki, M. K.:.**“Information Security Management Handbook“,** 5th ed., Auerbach Publications, Chicago, 2006.
39. Wiltbank, R. E.: **„Siding with the Angels, Business angel investing - promising outcomes and effective strategies“**, British Business Angels Association, London, 2009.

ČLANCI, STUDIJE I ZBORNICI RADOVA

40. Acquisti, A., Friedman, A. & Telang, R.: „**Is there a cost to privacy breaches? An event study.“,** Cambridge, Velika Britanija, Twenty Seventh International Conference on Information Systems, Milwaukee, 2006.
41. Bell, D. E.: **“Looking Back at the Bell-La Padula Model“**, ACSAC '05, Proceedings of the 21st Annual Computer Security Applications Conference, IEEE Computer Society, Washington DC, 2005.
42. Bezić, H., Tijan, E..Aksentijević, S.:.**“ Port community system - economic feasibility evaluation“** Ekonomski vjesnik br. 2/2011.
43. Birkinshaw, J., Fey, C. F.: **„External sources of knowledge and performance in r&d organizations“,** Academy of Management Journal, 31(4),2005.
44. Blakley, B., McDermott, E., Geer, D.:**“ Information Security Is Information Risk Management“**, Proceedings of the 2001 workshop on New security paradigms - NSPW '01, 2001.
45. Bojanc , R. & Jerman-Blažič, B.: **„An economic modelling approach to information security risk management“**, International Journal of Information Management, 28(5),2008.
46. Bojanc, R. & Jerman-Blažič, B.: **„Towards a standard approach for quantifying an ICT security investment“**, Computer Standards & Interfaces, 30(4), 2007.
47. Cavusoglu, H., Cavusoglu, H, Raghunathan,S.: **„Economics of IT Security Management: four improvements to current security Practices“,** Communications of the Association for Information Systems, Volume 14, 2004.
48. Coase, R. H.: **„The Nature of the Firm“**, Economica, 4(16), 1937.
49. Čičin-Šain, M., Vukmirović, S., Čapko, Z.: **„Methodological Framework of Business Reengineering within Logistics System“,** Journal of Computing and Information Technology - CIT 12, Issue 2, 2004.
50. Dollinger, R.: **„Database Security Models - A Case Study“**, 8th IEEE International Conference on Intelligent Engineering systems, Cluj-Napoca, 2004.

51. Garbin-Praničević, D. & Srića, V.:“**AHP support to estimation of the information system (IS) significance to the business performance, particularly the hospitality performance“**, Croatian Operational Research Review (CRORR), Svezak 4., Zagreb, 2013.
52. Gordon, L. A. & Loeb, M. P. : **„Using information security as a response to competitor analysis systems“**, Communications of the ACM 44(9), New York, 2001.
53. Gordon, L. A. & Loeb, M. P.: **“The economics of information security investment“**, ACM Transactions on Information and System Security (TISSEC), 5(4), New York, 2002.
54. Heras, I. et.al..: **“ISO 9000 registration's impact on sales and profitability: A longitudinal analysis of performance before and after accreditation“**, International Journal of Quality & Reliability Management, Issue 19., 2002.
55. Hlača, B., Aksentijević, S. i Tijan, E: **„Influence of ISO 27001:2005 on the Port of Rijeka security“**, Pomorstvo, Scientific Journal of Maritime Research, Pomorski fakultet u Rijeci, 22(2),2008.
56. Hlača, B., Aksentijević, S., Tijan, E.:**“Influence of ISO 27001:2005 on the Port of Rijeka security”,** Pomorstvo, Scientific Journal of Maritime Research, 22(2), Pomorski fakultet u Rijeci, 2008.
57. Kandžija, V., Lovrić, L.: **„Ekonomski rast tranzicijskih zemalja u procesu globalizacije“,** Ekonomska misao i praksa, Broj 1, Sveučilište u Dubrovniku,2013.
58. Lawrence, G. A. & Loeb, M. P.: **„Using information security as a response to competitor analysis systems“**, Communications of the ACM, 44(9),New York, 2001.
59. Lientz, P. B., Swanson, E. B. , Tompkins, G. E**.: “Characteristics of application software maintenance“**, Communications of the ACM, 21(6), New York, 1978.
60. Lo, C. K., Cheng, A. C.,Edwin, T.: **„Impact of ISO 9000 on time-based performance: An event study“**. World Academy of Science, Engineering and Technology, Issue 7, Las Cruces, 2001.
61. O'Bryan, S. K.: **„Critical Elements of Information Security Program Success“**, Information Systems Control Journal, Information Systems Audit and Control Association (ISACA) Svezak 3., 2006.
62. Park , J.-Y. et al.: **„IT Security Strategies for SME’s“**, International Journal of Software Engineering and Its Applications, 2(3), Science & Engineering Research Support society, Sandy Bay, 2008.
63. Rodgers, J. L. & Nicewander, A.: **„Thirteen Ways to Look at the Correlation Coefficient“**, The American Statistician, 42(1), An Official Journal of the American Statistical Association, 1988.

64. Rowley, Jennifer: **„The wisdom hierarchy: representation of the DIKW hierarchy“**, Journal of Information Science 33(2), 2007.
65. Ryan, J. & Ryan, D. J.: **„Expected benefits of information security investments“,** Computers & Security, 25(8), 2006.
66. Sroufe, R. & Curkovic, S.: „**An examination of ISO 9000:2000 and supply chain quality assurance“,** Journal of Operations Management, 26(4), 2008.
67. Tijan, E., Kos, S. & Ogrizović, D.: **„Disaster recovery and business continuity in port community systems“**, Pomorstvo, Scientific Journal of Maritime Research, 23(1), Pomorski fakultet u Rijeci, 2009.
68. Tijan, E.: **„Data classification and information lifecycle management in port community systems“**, Pomorstvo, 23(2), Scientific Journal of Maritime Research , Pomorski fakultet u Rijeci, 2009.
69. Wilemson, J.: „**On the Gordon and Loeb Model for Information Security Investment**“, The Fifth Workshop on the Economics of Information Security (WEIS 2006),Cambridge, 2006.
70. Wilson, V:.**“Research Methods: Focus Groups”,** Evidence Based Library and Information Practice, 07(01), 2012.
71. Yokakul, N., Zawdie, G, Booth, P.: **“The role social capital, knowledge exchange and the growth of indigenous knowledge-based industry in the Triple Helix system: the case of SMEs in Thailand“**, Proceedings Papers of the Triple Helix IX Conference, Stanford University, Stanford, 2011.

ZAKONSKI PROPISI

72. „**The Sarbanex-Oxley Act**“, http://www.soxlaw.com/index.htm, Addison-Hewitt Associates, B2B Consultancy, 2002. (08.04.2013.)
73. **Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures**, Official Journal of the European Union 13/ 19.01.2000.
74. **Direktiva 2002/58/EC o privatnosti i elektroničkim komunikacijama**, Official Journal of the European Union 201/31.07.2002.
75. **Direktiva 2003/4/EC**, Official Journal of the European Union 41/14.02.2003.
76. **Direktiva 95/46/EZ o zaštiti osoba s obzirom na obradu osobnih podataka i slobodno kretanje takvih podataka,** Official Journal of the European Union, 281/23.11.1995.
77. **Direktiva o zadržavanju podataka 2006/24/EC**, Official Journal of the European Union 105/13.04.2006.

78. **Direktiva o zaštiti telekomunikacijskih podataka 97/66/EC**, Official Journal of the European Union 24/30.01.1998.
79. **Hrvatski standardi financijskog izvješćivanja HSFI 6.3.**,Narodne novine 30/2008.
80. **Instrukcija o načinu provjere obrade ličnih podataka prije uspostavljanja zbirke ličnih podataka**, Službeni glasnik BiH 76/2009.
81. **Izmjene i dopune zakona o poticanju razvoja malog gospodarstva,** Narodne novine 53/2012.
82. **Krivični Zakonik Republike Srbije, Službeni glasnik Republike Srbije** 85,88/2005., ispr. 107/2005., 72, 111/2009., 121/2012.
83. **Memorandum o razumijevanju između Republike Hrvatske i europske zajednice o sudjelovanju Republike Hrvatske u programu Zajednice o interoperabilnom pružanju europskih prekograničnih elektroničkih usluga javne vlasti javnim upravama, poduzetnicima i građanima (IDABC)**, Međunarodni ugovori 2/2007.
84. **Zakon o potvrđivanju ugovora između Republike Hrvatske i Europske unije o sigurnosnim postupcima za razmjenu tajnih podataka,** Međunarodni ugovori 9/2006.
85. **Nacionalna klasifikacija djelatnosti**, Narodne novine 28/2007., 6/1995., 3/1997., 13/2003.
86. **Odluka 1151/2003/EC o borbi protiv ilegalnog i štetnog sadržaja na globalnim mrežama**, Official Journal of The European Union 162/01.07.2003.
87. **Odluka Europskog parlamenta i Odluka Vijeća Europe 854/2005/EC o promociji sigurnijeg korištenja Interneta**, Official Journal of the European Union 149/11.06.2005.
88. **Odluka o primjerenom upravljanju informacijskim sustavom,** Narodne novine 80/2007.
89. **Odluka Vijeća Europe 92/242/EEC u području sigurnosti informacija**, Official Journal of the European Union 123/31.03.1992.
90. **Opći porezni zakon**, Narodne novine 147/08, 18/11, 78/12, 136/12, 73/13
91. **Pravilnik o detaljnom obliku i najmanjem opsegu te sadržaju revizorskog prijedloga i revizorskog izvješća s obzirom na specifičnosti poslova osiguranja i reosiguranja**, Narodne novine 119/2009.
92. **Pravilnik o inspekcijskom nadzoru u oblasti zaštite ličnih podataka**, Službeni glasnik BiH 51/2009.
93. **Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost**, Narodne novine 30/2011.
94. **Pravilnik o načinu čuvanja i posebnim mjerama tehničke zaštite ličnih podataka**, Službeni glasnik BiH 67/2009.

95. **Pravilnik o načinu vođenja i obrascu evidencije o zbirkama ličnih podataka**, Službeni glasnik BiH 52/2009.
96. **Pravilnik o postupku po prigovoru nosioca podataka u Agenciji za zaštitu ličnih podataka u Bosni i Hercegovini**, Službeni glasnik BiH 51/2009.
97. **Preporuka EU-a 2003/36,** Official Journal of the European Union 156/25.06.2003.
98. **Rezolucija Vijeća 2000/C 293/02 o organizaciji i upravljanju Internetom**, Official Journal of the European Union 43/28.01.2002.
99. **Rezolucija Vijeća Europe o zajedničkom pristupu i specifičnim akcijama u području sigurnosti mreža i informacija**, Official Journal of the European Union 43/14.10.2000.
100. **„Sarbanes-Oxley Act",** University of Cincinnati, College of Law, http://taft.law.uc.edu/CCL/SOact/soact.pdf ,2002. (10.08.2013.)
101. **Sigurnosna politika 2001/264/EC**, Official Journal of the European Communities 101/11.04.2011.
102. **Uredba Br. 1007/2008.**, Official Journal of the European Union 293/31.10.2008.
103. **Uredba Br. 526/2013.**, Official Journal of the European Union 165/18.06.2013.
104. **Uredba Europske komisije Br. 460/2004**., Official Journal of the European Union 77/13.03.2004.
105. **Uredba o mjerama informacijske sigurnosti**, Narodne novine 46/2008.
106. **Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka**, Narodne novine 139/2004.
107. **Zakon o bankama**, Narodne novine 84/2002.
108. **Zakon o elektroničkim komunikacijama**, Služben vesnik 13/2006.
109. **Zakon o elektronskoj trgovini**, Službeni List Republike Crne Gore 80/2004.
110. **Zakon o elektronskom dokumentu**, Službeni List Republike Crne Gore 5/2008..
111. **Zakon o elektronskom potpisu**, Službeni list Republike Crne Gore 31/2005.
112. **Zakon o informacijskoj sigurnosti**, Narodne novine 79/2007.
113. **Zakon o informacionoj bezbjednosti Republike Crne Gore**, Službeni list Crne Gore 14/2010.
114. **Zakon o izmjenama i dopunama zakona o elektronskom potpisu,** Službeni list Republike Crne Gore 21/2008.
115. **Zakon o klasificiranim informacijama**, Služben vesnik 9/2004.
116. **Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminaliteta** , Službeni glasnik Republike Srbije 61/2005.
117. **Zakon o osiguranju**, Narodne novine 151/2005.
118. **Zakon o poticanju razvoja malog gospodarstva,** Narodne novine 56/2013.
119. **Zakon o računovodstvu**, Narodne novine 109/07, 144/12, 54/13

120. **Zakon o slobodnom pristupu informacijama od javnog značaja**, Služben vesnik 13/2005.
121. **Zakon o zaštiti ličnih podataka**, Službeni glasnik BiH 49/2006.
122. **Zakon o zaštiti na radu**, Narodne novine 143/2012., 59/1996., 94/1996., 114/2003., 100/2004., 86/2008., 116/2008., 75/2009.
123. **Zakon o zaštiti osobnih podataka**, Narodne novine 106/2012.
124. **Zakon o zaštiti osobnih podataka**, Služben vesnik 103/2008.
125. **Zakon o zaštiti podataka o ličnosti**, Službeni glasnik Republike Srbije 97/2008.

OSTALI IZVORI

126. Agencija za elektronski komunikacii, http://www.aec.mk/ (18.08.2013.)
127. Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, http://www.azlp.gov.ba/ (19.08.2013.)
128. Agencija za zaštitu osobnih podataka, http://www.azop.hr (03.08.2013.)
129. Aksentijević, S.: **"Integralna zaštitna funkcija unutar poduzeća i sustav upravljanja informacijskom sigurnošću – Saipem Mediteran Usluge d.o.o, Rijeka"**, završni rad poslijediplomskog specijalističkog studija, Ekonomski fakultet, Rijeka, 2008, (neobjavljen)
130. Aksentijević, S.: **„Operative Information Protection Plan, WI-SMS-ICT-105-E rev1.",** radna uputa sustava ISO 9001:2008, Saipem S.p.A., podružnica u Republici Hrvatskoj, Rijeka, 2012.
131. Aksentijević, S.:**"Informacijska sigurnost u funkciji upravljanja informacijskim kapitalom poduzeća"**, metodološki seminarski rad, predmet „Metodologija znanstvenog istraživanja", Ekonomski fakultet u Rijeci, Rijeka, 2010. (neobjavljeno)
132. ARIS Community, IDS Scheer AG, http://www.ariscommunity.com/aris-express, 2013. (14.2.2013)
133. Arveson, P.: **„The Deming Cycle"**, Balanced Scorecard Institute, http://www.balancedscorecard.org/thedemingcycle/tabid/112/default.aspx, 2013. (09.07.2013.)
134. ASIS International: **„Safeguarding Intangible Drivers of Company Value"**, https://www.asisonline.org/Education-Events/Education-Programs/Webinars/Pages/Safeguarding-Intangible-Drivers-of-Company-Value.aspx, 2013. (11.07.2013.)
135. Bank for International Settlements, http://www.bis.org/bcbs/about.htm (14.08.2013.)
136. Bank for International Settlements: **„Basel II: Revised international capital framework",** http://www.bis.org/publ/bcbsca.htm, 2005. (14.08.2013)

137. Bank for International Settlements: **„International regulatory framework for banks (Basel III)“**, http://www.bis.org/bcbs/basel3.htm,, 2011. (14.08.2013.)
138. **„British standard (BS) 5750--quality assurance?“**, PUBMed, http://www.ncbi.nlm.nih.gov/pubmed/7617456 ,1995.(21.08.2013.)
139. **„Business Analytics and Optimization for the Intelligent Enterprise“**, IBM Global Business Services, http://mds.ricoh.com/change/optimizing_information ,2009. (13.07.2013.)
140. Cambridge Dictionaries, http://dictionary.cambridge.org/dictionary/business-english/buy-in (18.08.2013.)
141. CEPOR - Centar za politiku razvoja malih i srednjih poduzeća i poduzetništva: **„Izvješće o malim i srednjim poduzećima u Hrvatskoj - 2012.“**,CEPOR, Zagreb, 2012.
142. CIRT, http://www.cirt.me/ (18.08.2013.)
143. Commission of the European Communities, http://eur-lex.europa.eu/LexUriServ/site/en/com/2004/com2004_0028en01.pdf, 2004. (01.08.2013.)
144. Commission of the European Communities, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF,2005. (25.07.2013.)
145. Committee of sponsoring organizations of the Treadway Commission, COSO, http://www.coso.org/, 2013. (11.07.2013.)
146. Cornell Information, Legal Information Institute , http://www.law.cornell.edu/ (19.05.2013)
147. **„Cost of Data Breach 2013.“**, Ponemon Institute, Traverse City, 2013.
148. Curphey, M.:**“A Guide to Building Secure Web Applications“,** The Open Web Application Security Project (OWASP), http://www.cgisecurity.com/owasp/html/ch08s02.html, 2013 (14.7.2013.)
149. Čapko, Z: **„Elektroničko poslovanje“**, skripta, Ekonomski fakultet u Rijeci, Rijeka, 2008. (neobjavljeno)
150. Deloitte, http://www.deloitte.com/view/en_GR/gr/services/enterprise-risk-services/risk-consulting-services/financial-risk-assessment/index.htm (11.07.2013)
151. Department of Defense, Online Information for the Defense Community, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf , 2003. (02.08.2013.)
152. EIF - European Interoperability Framework for pan-European eGovernment services, http://ec.europa.eu/idabc/en/document/2319/5644.html (14.07.2013.)
153. Encyclopaedia Britannica, http://www.britannica.com/EBchecked/topic/162050/Albert-Venn-Dicey (18.08.2013.)

154. EUbusiness - Single European Information Space, http://www.eubusiness.com/topics/internet/i2010 (14.11.2012.)
155. European Commission, http://ec.europa.eu/enterprise/policies/sme/index_en.htm (7.8.2013)
156. Europe's Information Society Thematic PortalSafer Internet Programme**: „Empowering and Protecting Children Online“**, http://ec.europa.eu/information_society/activities/sip/index_en.htm , 2013. (29.07.2013.)
157. Federation of American Scientists, http://www.fas.org/irp/program/process/echelon.htm (25.03.2013)
158. Financijska agencija, http://www.fina.hr/Default.aspx?sec=896 (11.08.2013.)
159. Fin-In, http://www.in-fin.info/krediti-i-leasing/ (21.08.2013.)
160. Forbes, http://www.forbes.com/2002/07/01/0701topnews.html (01.06.2013.)
161. FREE BSD: **„The Power to Serve“**, http://www.freebsd.org/cgi/man.cgi?mac_biba ,2013. (14.02.2013)
162. Gartner IT Glossary, http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/ (22.08.2013).
163. Glynn, F.: **„Guide to Data Loss Prevention, Data Loss and Data Leakage“**, http://www.veracode.com/security/data-loss-prevention, 2012. (11.07.2013.)
164. Google Docs, https:// docs.google.com/ (20.08.2013.)
165. Gordon, L. & Richardson, R.: **“Bank Systems & Technology“**, http://www.banktech.com/management-strategies/the-new-economics-of-information-securit/18901266 ,2004. (21.08.2013)
166. Harvey, B.: **„What is a hacker?“**, http://www.cs.berkeley.edu/~bh/hacker.html, 1985. (11.07.2013)
167. Heggeseth, A. G., Lome, O. B**.:“ The Growth of SMEs: An Empirical Investigation of Norwegian Exporters“**, thesis, Norwegian University of Science and Technology, Trondheim, 2012.
168. Hoo, S.: **„How Much Is Enough? A Risk-Management Approach“,** www.cl.cam.ac.uk/~rja14/econws/06.doc , 2010. (14.07.2013)
169. Hrvatska akademska i istraživačka mreža, http://www.carnet.hr/ (14.07.2013.)
170. Hrvatska gospodarska komora, http://www.hgk.hr/o-hgk (11.08.2013.)
171. Hrvatska gospodarska komora: **“Gospodarska kretanja 04. 2013.“**, http://www.hgk.hr/wp-content/blogs.dir/1/files_mf/gospodarska_kretanja_0485.pdf.(08.08.2013)
172. http://autopoiesis.foi.hr/ (04.08.2013.).
173. http://poticaji.minpo.hr/ (15.08.2013.)

174. http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx (14.06.2013.)
175. http://www.123ahp.com/PrimjerDocs/SWOT_en/SWOT_and_AHP_123ahp.jpg , (24.12.2011.)
176. http://www.ahpacus.com/OMetodi.aspx , (24.12.2011.)
177. http://www.isaca.org/COBIT/Pages/default.aspx (14.06.2013.)
178. http://www.noxglobe.com/blog/itil/itil-v3-processes/ (04.08.2013.)
179. IBM SPSS, http://www-01.ibm.com/software/analytics/spss/ (23.08.2013.)
180. **„In Defense of Data - Views from the Frontlines of Data Protection“**, Symantec, http://www.indefenseofdata.com/data-breach-trends-stats/ (30.0 7.2013.)
181. **„Instruction Number 8500.2: Information Assurance (IA) Implementation“**, Department of Defense, Sjedinjene Američke Države, 6.2.2003.
182. **„International Standard ISO/IEC 27001 - Information technology — Security techniques — Information security management systems — Requirements“**, SAI GLOBAL, Index House, 2007.
183. Internet stranice agencije za zaštitu osobnih podataka, http://www.azop.hr (03.08.2013.)
184. Investopedia**,** http://www.investopedia.com/terms/i/industrial-espionage.asp (19.08.2013.)
185. Investopedia, http://www.investopedia.com/terms/v/vcfund.asp (20.08.2013.)
186. **„ISO Standards Translated Into Plain English“**, Praxiom Research Group limited, http://www.praxiom.com/iso-17799-objectives.htm , 2013. (18.03.2013.)
187. **„ISO/IEC 27001 Information Security Management standard“**, BSI, London, Velika Britanija, 2013.
188. ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management, http://www.iso.org/iso/catalogue_detail?csnumber=50297 (12.08.2013.)
189. **„ISSA-UK 5173 - Information Security for Small and Medium Sized Enterprises"**, Information Systems Security Association, ožujak 2011.
190. Itillious: **„The Information Security Organization's Identity Crisis“**, http://www.itillious.com/insight/articles/ciso.html, 2013. (11.08.2013)
191. itSMF - The IT Service Management Forum: **„An Introductory Overview of ITIL V3.“**, IT Service Management Forum Limited. ,London, 2007.
192. Kaspersky Lab: **„The high cost of a security breach: one serious incident could cost $649k“**, Kaspersky Lab, Moskva, 2013.
193. Kilpatrick, I.: **„Enterprise Innovation“**, http://enterpriseinnovation.net/article/ten-growth-areas-it-security-2010 , 2013. (21.08.2013)

194. Klaić, A.: **„EU's information security expectations“**, konferencija infosecweek, Zagreb, 14-18. svibanj 2007. (neobjavljeno)
195. Košutić, D.: **“Elementi procjene i upravljanja informacijskim rizicima”**, Kvadra Savjetovanje d.o.o, Zagreb, 2007. (neobjavljeno)
196. LimeSurvey, https://www.limesurvey.org/ (20.08.2013.)
197. LinkedIn, http://www.linkedin.com (25.08.2013.)
198. Merriam-Webster, http://www.merriam-webster.com/dictionary/goodwill (10.8.2013.)
199. Microsoft Safety & Security Center, http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx , 2013. (09.04.2013.)
200. Ministarstvo poduzetništva i obrta Republike Hrvatske, 2013., http://poticaji.minpo.hr/ (14.07.2013.)
201. Ministry of Defense: **„ASQ, 1959. MIL-Q-9858A, the Origin of ISO 9001.“**, http://asq.org/fdc/2012/06/mil-q-9858a-the-origin-of-iso-9001.html?shl=109629 (21.08.2013.)
202. Mogull, R.: **„Securosis - Information Security Research and Analysis“**, htps://securosis.com/blog/data-classification-is-dead , 2013.(29.04.2013.)
203. Moj izbor - moja odluka, INIT, http://www.mojizbormojaodluka.net/ , 2007. (05.02.2012)
204. Nacionalni CERT, http://www.cert.hr/ (14.07.2013.)
205. National Institute of Standards and Technology - Information Technology Laboratory, http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf ,2013. (29.05.2013.)
206. Nissen Consulting - IT Service Management, ITSM Partner d.o.o., http://www.itsm.hr/itil-itsm-metodologija/metodologija-cobit.php, 2007. (14.06.2013)
207. Oracle Java – Make the Future Java, http://www.oracle.com/us/technologies/java/overview/index.html (22.08.2013.)
208. Ovum’s multi-market Q4 2012 BYOD survey, http://cxounplugged.com/2012/11/ovum_byod_research-findings-released/ (14.08.2013.)
209. PCI Security Standards Council, https://www.pcisecuritystandards.org/security_standards/index.php (18.08.2013.)
210. **Program poticanja poduzetništva i obrta "Poduzetnički impuls 2013.”**, Ministarstvo gospodarstva RH, siječanj 2013., Zagreb
211. **„Recommended Security Controls for Federal Information Systems and Organizations – NIST Special Publication 800-53“**, U.S. Department of Commerce, National Institute od Standards and Technology, Gaithersburg, 2009.

212. Republička agencija za elektronske telekomunikacije, http://www.ratel.rs (08.08.2013.)
213. Rogalski, J**.: "Risk Assessment Framework for Online Channel: Learn from an Expert"** ,webinar, 2013.
214. SANS Institute, InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-effective-information-security-program-protecting-data-assets-of-1398 ,2004. (11.05.2013.)
215. Schutte, S.: **„What does a security breach really cost an SME?"**, http://realbusiness.co.uk/article/20838-what-does-a-security-breach-really-cost-an-sme, 2013. (14.08.2013.)
216. SearchCloudComputing, http://searchcloudcomputing.techtarget.com/definition/XaaS-anything-as-a-service (22.08.2013).
217. SearchSecurity, http://searchsecurity.techtarget.com/definition/Carnivore , 2013. (11.04.2013.)
218. SecretCodeBreaker.com, 2013. Secret code breaker - online cryptanalyst's handbook, http://www.secretcodebreaker.com/history2.html (14.06.2013.)
219. **„ISO/IEC 27001 Information Security Management standard"**, BSI, London, Velika Britanija, 2013.
220. Telecom Cloud, http://www.telecom-cloud.net/network-as-a-service/ (22.08.2013.)
221. **„The BS7799 Security Standard"**, C&A Systems Security Ltd., Cheshire, http://www.riskserver.co.uk/bs7799/contact.htm ,2002. (11.08.2013.)
222. The free dictionary by Farlex, http://www.thefreedictionary.com/wan (21.08.2013.)
223. **„The ISO 27000 Directory"**, http://www.27000.org/ismsprocess.htm (15.08.2013.)
224. **„The ISO Survey of Management System Standard Certifications (1993.-2011.)"**, ISO, www.iso.org (11.07.2013.)
225. The ITSM Encyclopedia, ITSM, http://itsm.certification.info/itilfree.html , 2013.(08.08.2013)
226. The Ronald Coase Institute, http://www.coase.org/ (22.08.2013.)
227. Tijan, E.: **„Integralni model elektroničke razmjene podataka u lučkom klasteru"**, doktorska disertacija, Pomorski fakultet u Rijeci, Rijeka, 2011.
228. United Nations Global Compact, http://www.unglobalcompact.org/ (20.08.2013.)
229. Ured vijeća za nacionalnu sigurnost, http://www.uvns.hr/ (14.07.2013.)
230. Webopedia, http://www.webopedia.com/TERM/C/cloud_computing.html (22.08.2013).
231. Webopedia, http://www.webopedia.com/TERM/S/SaaS.html (22.08.2013.)
232. Webopedia, http://www.webopedia.com/TERM/S/Service_Level_Agreement.html (11.08.2013.)

233. Workshop on the Economics of Information Security 2013., http://www.weis2013.econinfosec.org/ (17.07.2013.)
234. World Summit on the Information Society, http://www.itu.int/wsis/index.html (18.07.2013.)
235. Zavod za sigurnost informacijskih sustava, http://www.zsis.hr (14.07.2013.)
236. Zečević, Z., http://www.scribd.com/doc/75998229/Metode-Za-Ocjenu-Financijske-Efikasnosti , 2011. (09.01.2012.)

POPIS TABLICA

POPIS SHEMA

POPIS GRAFIKONA

POPIS ILUSTRACIJA

POPIS PRILOGA

PRILOZI

Prilog br. 1: Ispitni listić anketnog istraživanja

Anketu možete popuniti i na Internetu koristeći adresu:

http://alturl.com/3rkc9

ANKETNI UPITNIK

Poštovani,

U sklopu izrade doktorske disertacije na doktorskom studiju Poslovne ekonomije pri Ekonomskom fakultetu u Rijeci provodim istraživanje o osobitostima upravljanja sustavima informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj. Molim Vas da odvojite desetak minuta i ispunite ovu anketu. Broj poduzeća koja treba anketirati je velik i bez Vaše pomoći ova anketa ne može uspjeti.

Sva pitanja odnose se na poduzeće u kojemu radite. Na neka pitanja potrebno je odgovoriti zaokruživanjem jednog broja na skali 1-5 gdje broj 1 označava *„vrlo slabo, vrlo malo, ne slažem se"* dok broj 5 označava *„vrlo jako, izrazito, slažem se"*. Kod pitanja s višestrukim izborom odaberite samo jednu ponuđenu mogućnost, osim ako nije drugačije navedeno.

Ispunjenu anketu možete vratiti na e-mail adresu sasa.aksentijevic@gmail.com .

Istraživanje je anonimno i nema komercijalni karakter. Dobiveni podaci će biti prikazani u relativnim odnosima i isključivo u znanstvene svrhe. Ime tvrtke traži se isključivo kako, u slučaju da anketu popuni više ispitanika u istoj tvrtci, ne bi došlo do udvostručavanja podataka i posljedično do iskrivljenih rezultata istraživanja. Email adresu dostavite ukoliko želite primiti obrađene rezultate ankete.

Unaprijed se zahvaljujem na Vašoj suradnji.

S poštovanjem, Saša Aksentijević

I. OPĆI PODACI

1. Naziv poduzeća _____

2. Vaša e-mail adresa *(u slučaju da želite primiti rezultate ankete)*: _____

3. Poslovna djelatnost *(zaokružiti jedno slovo)*:

A Poljoprivreda, šumarstvo i ribarstvo
B Rudarstvo i vađenje
C Prerađivačka industrija
D Opskrba električnom energijom, plinom, parom i klimatizacija
E Opskrba vodom; uklanjanje otpadnih voda, gospodarenje otpadom te djelatnosti sanacije okoliša
F Građevinarstvo
G Trgovina na veliko i malo; popravak motornih vozila i motocikala
H Prijevoz i skladištenje
I Djelatnosti pružanja smještaja te pripreme i usluživanja hrane
J Informacije i komunikacije
K Financijske djelatnosti i djelatnosti osiguranja
L Poslovanje nekretninama
M Stručne, znanstvene i tehničke djelatnosti
N Administrativne i pomoćne uslužne djelatnosti
O Javna uprava i obrana; obvezno socijalno osiguranje
P Obrazovanje
Q Djelatnosti zdravstvene zaštite i socijalne skrbi
R Umjetnost, zabava i rekreacija
S Ostale uslužne djelatnosti
T Djelatnosti kućanstva kao poslodavca; djelatnosti kućanstava koja proizvode različitu robu i obavljaju različite usluge za vlastite potrebe
U Djelatnosti izvanteritorijalnih organizacija i tijela

4. Prosječan broj zaposlenih u 2012. godini:
   a) 0-9
   b) 10-49
   c) 50-249

5. Ukupan prihod u 2012. godini:
   a) ≤2 mil. EUR
   b) 2-10 mil. EUR
   c) 10-50 mil. EUR

6. Ukupan iznos bilance u 2012. godini:
   a) ≤2 mil. EUR
   b) 2-10 mil. EUR
   c) 10-43 mil. EUR

7. Vaša funkcija u poduzeću:
   a) Član Uprave
   b) Direktor ili prokurist poduzeća
   c) Rukovoditelj odjela informatike
   d) Rukovoditelj odgovoran za upravljanje informacijskom sigurnošću
   e) Ostalo (*napisati funkciju*): _____

II. PITANJA O UPRAVLJANJU INFORMACIJSKOM SIGURNOŠĆU

8. Postoji li u poduzeću zaposlenik ili odjel zadužen za informatičku potporu?
   a) DA
   b) NE
   c) NE, ali je imamo u planu zaposliti/organizirati takav odjel

9. Posjeduje li poduzeće uspostavljen sustav upravljanja informacijskom sigurnošću:
   a) DA
   b) NE
   c) NE, ali imamo u planu uspostaviti ga

10. Koristi li poduzeće ključne indikatore za određivanje efikasnosti sustava upravljanja informacijskom sigurnošću?
    a) DA
    b) NE
    c) Ne, ali imamo u planu uvesti njihovo korištenje

11. Organizira li se u poduzeću stjecanje novih znanja za rukovodstvo poduzeća iz područja informacijske sigurnosti (npr. tečajevi, seminari, savjetovanja)?
    a) DA
    b) NE
    c) NE, ali imamo u planu organizirati dodatnu edukaciju rukovodstva po tom pitanju

12. Organizira li se u poduzeću stjecanje novih znanja za zaposlenike poduzeća iz područja informacijske sigurnosti (npr. tečajevi, seminari, savjetovanja)?
    a) DA
    b) NE
    c) NE, ali imamo u planu organizirati dodatnu edukaciju zaposlenika po tom pitanju

13. Je li u poduzeću imenovana osoba zadužena za provođenje mjera informacijske sigurnosti?
    a) DA
    b) NE
    c) NE, ali je namjeravamo imenovati

14. Ukoliko je odgovor na prethodno pitanje potvrdan, provodi li mjere informacijske sigurnosti isključivo ta osoba?
    a) DA
    b) NE

15. Postoji li u poduzeću odjel zadužen za funkciju informacijske sigurnosti?
    a) DA
    b) NE
    c) NE, ali je u postupku organizacije i uskoro ćemo ga imati

16. Provode li se mjere informacijske sigurnosti u poduzeću isključivo diskrecionim upravljanjem (donošenjem mjera, akcija, odluka) od strane rukovoditelja?
    a) DA
    b) NE

17. Provode li se mjere informacijske sigurnosti u poduzeću isključivo reaktivnim rješavanjem posljedica informacijsko sigurnosnih incidenata (tek kada oni nastanu)?
    a) DA
    b) NE

18. Planiraju li se mjere informacijske sigurnosti na godišnjoj razini?
    a) DA
    b) NE
    c) NE, ali ih imamo namjeru početi planirati na godišnjoj razini

19. Ima li poduzeće usvojenu dokumentiranu politiku informacijske sigurnosti?
    a) DA
    b) NE
    c) NE, ali je planiramo usvojiti

20. Prati li poduzeće odvojeno ulaganja u informacijsko sigurnosna rješenja od troška njihovog održavanja?
    a) DA, izdvojeno se prate obje navedene kategorije
    b) DJELOMIČNO, analizira se iznos investicijskih ulaganja ali ne i troškova održavanja
    c) DJELOMIČNO, analizira se iznos troškova održavanja ali ne i investicijskih ulaganja
    d) NE, ne analizira se niti jedna navedena kategorija
    e) NE, ali planiramo uskoro uvesti analizu investicijskih ulaganja
    f) NE, ali planiramo uskoro uvesti analizu troškova održavanje
    g) NE, ali planiramo uskoro uvesti analizu obje navedene kategorije

21. Koristi li poduzeće kvantitativne metode (npr. kapitalno budžetiranje) pri odlučivanju o nabavi novih informacijsko sigurnosnih rješenja?
    a) DA
    b) NE
    c) NE, ali planiramo početi koristiti kvantitativne metode pri takvom odlučivanju

22. Postoji li u poduzeću definiran skup procedura vezanih uz operativno provođenje informacijske sigurnosti?
    a) DA, u pisanom obliku
    b) DA, radi se o neformalnim procedurama
    c) NE, nemamo niti pisane niti neformalne procedure
    d) NE, ali ih namjeravamo razviti

23. Je li u poduzeću provedena procjena informacijskog rizika (identificiranje informacijske imovine, njene ranjivosti i rizika)?
    a) DA
    b) NE, ali namjeravamo obaviti identifikaciju informacijske imovine, ranjivosti i rizika
    c) NE

24. Je li u poduzeće uveden sustav upravljanja fizičkom sigurnošću zaposlenika i imovine?
    a) DA
    b) NE
    c) NE, ali ga namjeravamo uvesti

25. Je li u poduzeće uveden sustav praćenja promjena i nadzora nad komunikacijskim sustavom (mreža, telefoni)?
    a) DA
    b) NE
    c) NE, ali namjeravamo uvesti takav sustav

26. Je li u poduzeće uveden sustav logičke kontrole pristupa informatičkim resursima, sukladno dodijeljenoj razini ovlasti pojedinim zaposlenicima („autorizacija prije korištenja")?
    a) DA
    b) NE
    c) NE, ali uskoro namjeravamo uvesti takav sustav kontrole pristupa

27. Prati li se u poduzeću sigurnost informacijskih sustava tijekom njihovog cijelog životnog vijeka (od nabave, razvoja i korištenja do održavanja)?
    a) DA
    b) NE
    c) NE, ali namjeravamo početi pratiti sigurnost informacija tijekom tih procesa

28. Posjeduje li poduzeće sustav učenja i poboljšanja informacijskog sustava nakon nastupa sigurnosnih incidenata?
    a) DA
    b) NE
    c) NE, ali namjeravamo uvesti sustav učenja i poboljšanja sustava učenjem iz sigurnosnih incidenata

29. Je li u poduzeće uveden sustav kriznog upravljanja po nastupu informacijsko-sigurnosnih incidenata?
    a) DA
    b) NE
    c) NE, ali ga namjeravamo uvesti

30. Je li u poduzeću razvijen plan oporavka u slučaju katastrofe?
    a) DA
    b) NE
    c) NE, ali namjeravamo razviti takav plan

31. Je li u poduzeću razvijen plan kontinuiteta poslovanja?
    a) DA
    b) NE
    c) NE, ali namjeravamo razviti takav plan

32. Je li u poduzeće uveden sustav praćenja sukladnosti sa zakonskim zahtjevima po pitanju informacijske sigurnosti?
    a) DA
    b) NE
    c) NE, ali namjeravamo uvesti sustav praćenja zakonskih zahtjeva informacijske sigurnosti

33. Je li za upravu poduzeća (vlasnike, rukovoditelje) upravljanje informacijskom sigurnošću jedna od ključnih poslovnih funkcija u postizanju poslovnih ciljeva?
    a) DA
    b) NE
    c) NE, ali planiramo da će postati ključna u srednjem roku (1-3 godine)
    d) NE, ali planiramo da će postati ključna u dužem roku (>3 godine)

34. Je li u poduzeće uveden sustav operativnih mjera informacijske sigurnosti)?
    a) DA
    b) NE
    c) NE, ali ga namjeravamo uvesti

35. Ukoliko je odgovor na prethodno pitanje potvrdan, molim odgovorite kako je provođenje operativnih mjera organizirano:
    a) Reaktivnim rješavanjem posljedica informacijsko sigurnosnih incidenata — VRLO MALO 1 2 3 4 5 IZRAZITO
    b) Osobnom inicijativom zaposlenika — VRLO MALO 1 2 3 4 5 IZRAZITO
    c) Direktnim mjerama upravljanja od strane rukovoditelja-vlasnika — VRLO MALO 1 2 3 4 5 IZRAZITO
    d) Aktivnostima odjela informatičke podrške — VRLO MALO 1 2 3 4 5 IZRAZITO
    e) Putem osobe imenovane za upravljanje informacijskom sigurnošću — VRLO MALO 1 2 3 4 5 IZRAZITO
    f) Aktivnostima odjela za informacijsku sigurnost — VRLO MALO 1 2 3 4 5 IZRAZITO
    g) Planiranjem mjera informacijske sigurnosti na godišnjoj razini — VRLO MALO 1 2 3 4 5 IZRAZITO

36. Posjeduje li poduzeće sustav upravljanja kvalitetom sukladan normi ISO 9001?
    a) DA
    b) NE
    c) NE, ali ga planiramo uvesti

37. Ukoliko je odgovor na prethodno pitanje potvrdan, mjere li se ključni pokazatelji u okviru sustava ISO 9001?
    a) DA
    b) NE
    c) NE, ali ih planiramo početi pratiti kroz normu ISO 9001

38. Posjeduje li poduzeće certificirani sustav upravljanja informacijskom sigurnošću sukladan normi ISO 27001:2005?
    a) DA
    b) NE
    c) NE, ali sustav namjeravamo certificirati sukladno toj normi

39. Poduzeće upravlja informacijskom sigurnošću:
    a) Korištenjem internih resursa
    b) Korištenjem eksternih resursa (usluge vanjskih poduzeća)
    c) Kombinirano, korištenjem internih i eksternih resursa

40. Poduzeće je u 2012. godini za obrazovanje po pitanju informacijske sigurnosti potrošilo _____ Kn.

41. U 2012. godini poduzeće je u nabavu novih komponenti sustava za upravljanje informacijskom sigurnošću uložilo:
    a) 0-0,5 % godišnjeg prihoda
    b) 0,5-1 % godišnjeg prihoda
    c) 1-1,5 % godišnjeg prihoda
    d) 1,5-2 % godišnjeg prihoda
    e) Ostalo (upisati postotak): _____ %

42. U 2012. godini poduzeće je u održavanje postojećih komponenti sustava za upravljanje informacijskom sigurnošću uložilo:
    a) 0-0,5 % godišnjeg prihoda
    b) 0,5-1 % godišnjeg prihoda
    c) 1-1,5 % godišnjeg prihoda
    d) 1,5-2 % godišnjeg prihoda
    e) Ostalo (upisati postotak): _____ %

III. PITANJA VEZANA UZ DOMENE UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

43. U poduzeću u kojemu sam zaposlen:
    a) Rukovoditelji dovoljno inzistiraju na provođenju sigurnosnih politika SLABO 1 2 3 4 5 IZRAZITO
    b) Zaposlenici poštuju donesene mjere informacijske sigurnosti SLABO 1 2 3 4 5 IZRAZITO
    c) Rukovoditelji poduzeća su upoznati sa zakonskim zahtjevima postavljenim pred poduzeće po pitanju upravljanja informacijskom sigurnošću SLABO 1 2 3 4 5 IZRAZITO

44. U poduzeću se odlučuje o investiranju u komponente sustava upravljanja informacijskom sigurnošću temeljem:
    a) Inicijative rukovoditelja NE SLAŽEM SE 1 2 3 4 5 SLAŽEM SE
    b) Nastupa informacijsko-sigurnosnog incidenta NE SLAŽEM SE 1 2 3 4 5 SLAŽEM SE
    c) Prijedloga dobavljača informacijsko-sigurnosnog rješenja NE SLAŽEM SE 1 2 3 4 5 SLAŽEM SE
    d) Profesionalnih zahtjeva uslijed procjene rizika NE SLAŽEM SE 1 2 3 4 5 SLAŽEM SE
    e) Slučajnog (stihijskog) odlučivanja NE SLAŽEM SE 1 2 3 4 5 SLAŽEM SE
    f) Kvantitativne procjene povrata ulaganja u informacijsku sigurnost NE SLAŽEM SE 1 2 3 4 5 SLAŽEM SE

45. Stav rukovoditelja po pitanju informacijske sigurnosti u poduzeću je sljedeći:
    a) Informacijska sigurnost je strateška poslovna funkcija u postizanju ciljeva poduzeća NE SLAŽEM SE 5 4 3 2 1 SLAŽEM SE
    b) Ulaganje u postizanje ciljeva informacijske sigurnosti je prioritet poduzeća NE SLAŽEM SE 5 4 3 2 1 SLAŽEM SE
    c) Ulaganje u informacijsku sigurnost treba održavati na najnižim mogućim razinama NE SLAŽEM SE 5 4 3 2 1 SLAŽEM SE
    d) Funkcije poduzeća odgovorne za informacijsku sigurnost svakodnevno inzistiraju na poboljšanju dostignute razine informacijske sigurnosti NE SLAŽEM SE 5 4 3 2 1 SLAŽEM SE
    e) Funkcije poduzeća odgovorne za odlučivanje o investiranju u mjere informacijske sigurnosti imaju na raspolaganju dovoljno informacija za uspješno obavljanje te zadaće NE SLAŽEM SE 5 4 3 2 1 SLAŽEM SE
    f) Poduzeće dovoljno ulaže u obrazovanje zaposlenika po pitanju informacijske sigurnosti NE SLAŽEM SE 5 4 3 2 1 SLAŽEM SE

46. Planira li poduzeće investicije i trošak sustava upravljanja informacijskom sigurnošću na godišnjoj razini?
    a) DA
    b) NE
    c) NE, ali ih planiramo početi pratiti na godišnjoj razini

47. Smatrate li kako bi poduzeće imalo dodatnu korist od povećanja razine ulaganja u sustav upravljanja informacijskom sigurnošću?
    a) DA
    b) NE

48. Ukoliko je odgovor na prethodno pitanje pozitivan, koji je razlog da su ulaganja u sustave upravljanja informacijskom sigurnošću na nižoj razini od one koju percipirate optimalnom?
    a) Nedostatak financijskih sredstava
    b) Nedostatak znanja o sustavima upravljanja informacijskom sigurnošću
    c) Nedostatak ljudskih resursa obučenih za upravljanje funkcijom informacijske sigurnosti
    d) Poslovna politika poduzeća zahtijeva koncentraciju na druga područja poslovanja
    e) OSTALO (navedite što)_____

49. U 2013. godini ulaganja u sustave upravljanja informacijskom sigurnošću bit će:
    a) Smanjena u odnosu na 2012. godinu
    b) Na istoj razini kao u 2012. godini
    c) Povećana u odnosu na 2012. godinu

IV. PITANJA VEZANA UZ OPERATIVNE MJERE INFORMACIJSKE SIGURNOSTI I SIGURNOSNE INCIDENTE

50. Poduzeće koristi sljedeće operativne mjere informacijske sigurnosti: *(zaokružiti sve korištene mjere)*
    a) Odvojena korisnička imena i lozinke za sve korisnike
    b) Antivirusnu zaštitu na svim računalima
    c) Vatrozid *(firewall)* koji odvaja unutrašnju mrežu poduzeća od Interneta
    d) Najnovije sigurnosne zakrpe za računalnu opremu i programe
    e) Praćenje i analiza mrežnog komunikacijskog prometa u poduzeću
    f) Filtriranje (selektivni pristup) Internet sadržajima
    g) Odvajanje pristupa podacima po grupama ovlaštenih korisnika (npr. odjeli, organizacijske jedinice)

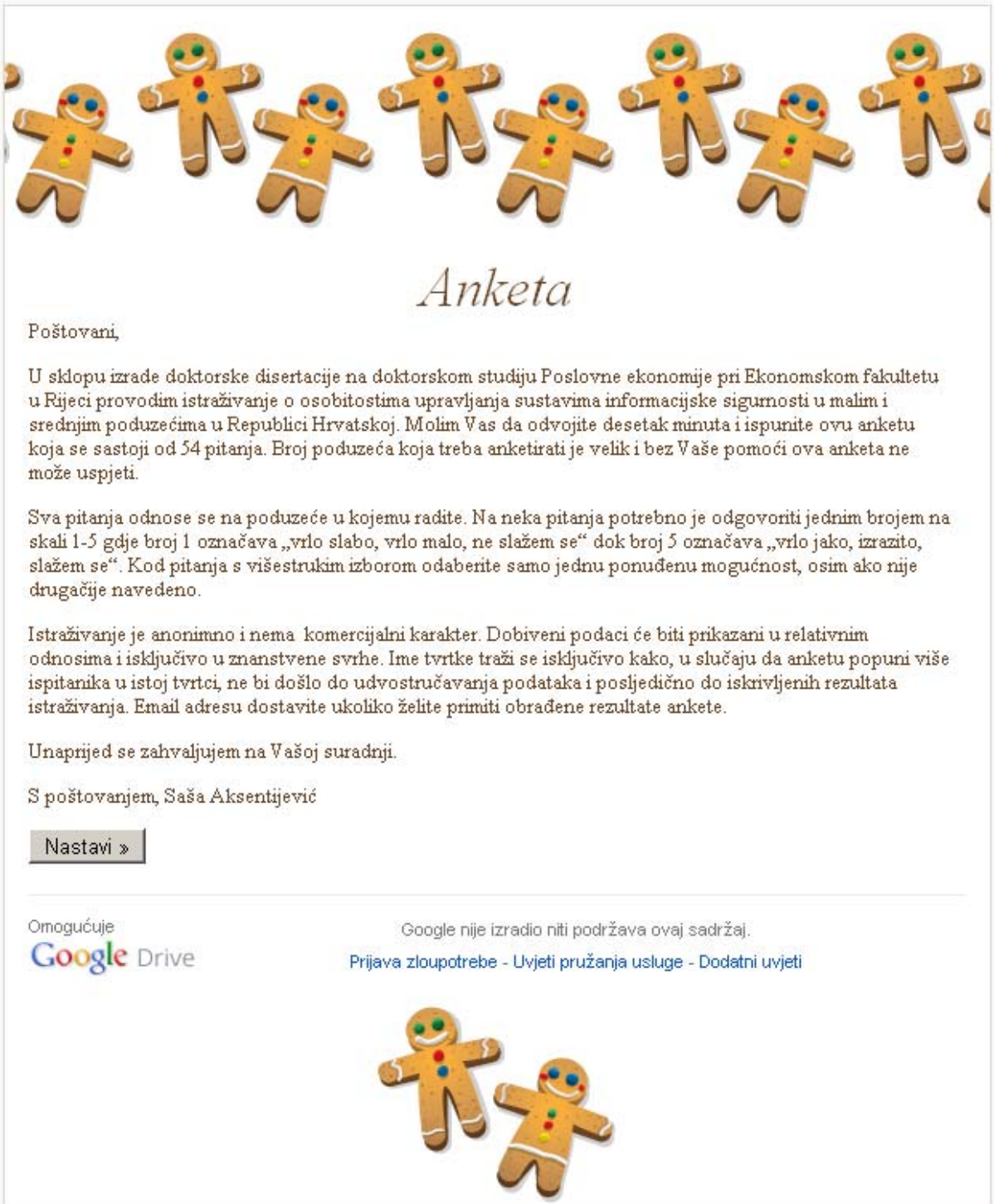
51. Je li poduzeće je u 2012. godini zabilježilo pojavu informacijsko-sigurnosnih incidenata?
    a) DA
    b) NE

52. Ukoliko je odgovor na prethodno pitanje potvrdan, koji je bio broj sigurnosnih incidenata u 2012. godini? _____

53. Ukoliko je odgovor na pitanje br. 51 pozitivan, koliki je bio ukupan trošak u 2012. godini uzrokovan nastupom takvih incidenata?
    a) 0-2 % prihoda
    b) 2-4 % prihoda
    c) 4-6 % prihoda
    d) 6-8 % prihoda
    e) 8-10 % prihoda
    f) Ostalo (upisati postotak): _____ %
    g) Poduzeće ne bilježi i ne posjeduje takve podatke

54. Smatrate li da pojava informacijsko-sigurnosnih incidenata u poduzeću može imati negativan utjecaj po:
    a) Poslovni rezultat poduzeća VRLO MALO 1 2 3 4 5 IZRAZITO PUNO
    b) Imidž poduzeća među zaposlenicima VRLO MALO 1 2 3 4 5 IZRAZITO PUNO
    c) Imidž poduzeća među partnerima i klijentima VRLO MALO 1 2 3 4 5 IZRAZITO PUNO
    d) Opstanak poduzeća na tržištu VRLO MALO 1 2 3 4 5 IZRAZITO PUNO
    e) Ostalo (navedite): _____

Prilog br. 2: Uvodna stranica Internet sustava anketnog istraživanja (http://alturl.com/3rkc9, 27.06.2013)



Anketa

Poštovani,

U sklopu izrade doktorske disertacije na doktorskom studiju Poslovne ekonomije pri Ekonomskom fakultetu u Rijeci provodim istraživanje o osobitostima upravljanja sustavima informacijske sigurnosti u malim i srednjim poduzećima u Republici Hrvatskoj. Molim Vas da odvojite desetak minuta i ispunite ovu anketu koja se sastoji od 54 pitanja. Broj poduzeća koja treba anketirati je velik i bez Vaše pomoći ova anketa ne može uspjeti.

Sva pitanja odnose se na poduzeće u kojemu radite. Na neka pitanja potrebno je odgovoriti jednim brojem na skali 1-5 gdje broj 1 označava „vrlo slabo, vrlo malo, ne slažem se" dok broj 5 označava „vrlo jako, izrazito, slažem se". Kod pitanja s višestrukim izborom odaberite samo jednu ponuđenu mogućnost, osim ako nije drugačije navedeno.

Istraživanje je anonimno i nema komercijalni karakter. Dobiveni podaci će biti prikazani u relativnim odnosima i isključivo u znanstvene svrhe. Ime tvrtke traži se isključivo kako, u slučaju da anketu popuni više ispitanika u istoj tvrtci, ne bi došlo do udvostručavanja podataka i posljedično do iskrivljenih rezultata istraživanja. Email adresu dostavite ukoliko želite primiti obrađene rezultate ankete.

Unaprijed se zahvaljujem na Vašoj suradnji.

S poštovanjem, Saša Aksentijević

Nastavi »

Prilog br. 3: Detaljna analiza karakteristika distribucije varijable „Mjera zrelosti funkcije operativnog upravljanja informacijskom sigurnošću“ (X_1)

Descriptives

			Statistic	Std. Error
Mjera zrelosti funkcije operativnog upravljanja IS	Mean		3,3365766	,07359634
	95% Confidence Interval for Mean	Lower Bound	3,1907259	
		Upper Bound	3,4824272	
	5% Trimmed Mean		3,3282332	
	Median		3,1400000	
	Variance		,601	
	Std. Deviation		,77538553	
	Minimum		1,00000	
	Maximum		5,00000	
	Range		4,00000	
	Interquartile Range		1,00000	
	Skewness		,233	,229
	Kurtosis		,572	,455

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mjera zrelosti funkcije operativnog upravljanja IS	,141	111	,000	,953	111	,001

a. Lilliefors Significance Correction

Prilog br. 4: Detaljna analiza karakteristika distribucije varijable „Mjera dostignute razine poštivanja zakonskih propisa, politika i najboljih standarda informacijske sigurnosti“ (X_2)

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Mjera razine postivanja propisa, politika i standarda IS	347	100,0%	0	0,0%	347	100,0%

Descriptives

			Statistic	Std. Error
Mjera razine postivanja propisa, politika i standarda IS	Mean		2,7511527	,05616550
	95% Confidence Interval for Mean	Lower Bound	2,6406840	
		Upper Bound	2,8616215	
	5% Trimmed Mean		2,7249296	
	Median		2,6700000	
	Variance		1,095	
	Std. Deviation		1,04624727	
	Minimum		1,00000	
	Maximum		5,00000	
	Range		4,00000	
	Interquartile Range		1,33000	
	Skewness		,267	,131
	Kurtosis		-,436	,261

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mjera razine postivanja propisa, politika i standarda IS	,089	347	,000	,965	347	,000

a. Lilliefors Significance Correction

Prilog br. 5: Detaljna analiza karakteristika distribucije varijable „Mjera uključenosti i posvećenosti rukovodstva poduzeća postizanju strateških ciljeva informacijske sigurnosti“ (X_3)

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Mjera uključenosti i posvećenosti rukovodstva strateškoj IS	347	100,0%	0	0,0%	347	100,0%

Descriptives

			Statistic	Std. Error
Mjera uključenosti i posvećenosti rukovodstva strateškoj IS	Mean		2,7855908	,04832384
	95% Confidence Interval for Mean	Lower Bound	2,6905453	
		Upper Bound	2,8806362	
	5% Trimmed Mean		2,7722382	
	Median		2,8000000	
	Variance		,810	
	Std. Deviation		,90017332	
	Minimum		1,00000	
	Maximum		5,00000	
	Range		4,00000	
	Interquartile Range		1,20000	
	Skewness		,226	,131
	Kurtosis		-,290	,261

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mjera uključenosti i posvećenosti rukovodstva strateškoj IS	,066	347	,001	,985	347	,001

a. Lilliefors Significance Correction

Prilog br. 6: Detaljna analiza karakteristika distribucije varijable „Mjera percepcije posljedica nastupa informacijsko-sigurnosnih incidenata u poduzeću na imidž i poslovni rezultat poduzeća“ (X_4)

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Mjera percepcije posljedica nastupa incidenata IS	347	100,0%	0	0,0%	347	100,0%

Descriptives

			Statistic	Std. Error
Mjera percepcije posljedica nastupa incidenata IS	Mean		3,2132565	,05289892
	95% Confidence Interval for Mean	Lower Bound	3,1092126	
		Upper Bound	3,3173004	
	5% Trimmed Mean		3,2342699	
	Median		3,2500000	
	Variance		,971	
	Std. Deviation		,98539775	
	Minimum		1,00000	
	Maximum		5,00000	
	Range		4,00000	
	Interquartile Range		1,50000	
	Skewness		-,299	,131
	Kurtosis		-,495	,261

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mjera percepcije posljedica nastupa incidenata IS	,093	347	,000	,975	347	,000

a. Lilliefors Significance Correction

Prilog br. 7: Detaljna analiza karakteristika distribucije varijable „Mjera zrelosti sustava odlučivanja o investicijama u komponente sustava upravljanja informacijskom sigurnošću konstruirana kao aritmetička sredina ocjene obilježja“ (X_5)

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Mjera zrelosti modela odlučivanja o investicijama u IS	347	100,0%	0	0,0%	347	100,0%

Descriptives

			Statistic	Std. Error
Mjera zrelosti modela odlučivanja o investicijama u IS	Mean		2,8486167	,03776397
	95% Confidence Interval for Mean	Lower Bound	2,7743409	
		Upper Bound	2,9228926	
	5% Trimmed Mean		2,8406196	
	Median		2,8300000	
	Variance		,495	
	Std. Deviation		,70346487	
	Minimum		1,00000	
	Maximum		5,00000	
	Range		4,00000	
	Interquartile Range		1,00000	
	Skewness		,198	,131
	Kurtosis		,710	,261

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mjera zrelosti modela odlučivanja o investicijama u IS	,095	347	,000	,983	347	,000

a. Lilliefors Significance Correction

Prilog br. 8: Detaljna analiza karakteristika distribucije varijable „Trošak obrazovanja za IS u 2012.“

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Trošak obrazovanja za IS	347	100,0%	0	0,0%	347	100,0%

Descriptives

			Statistic	Std. Error
Trošak obrazovanja za IS	Mean		22667,0910086	6509,82451695
	95% Confidence Interval for Mean	Lower Bound	9863,2823791	
		Upper Bound	35470,8996382	
	5% Trimmed Mean		4252,2593020	
	Median		0E-7	
	Variance		14705101888,797	
	Std. Deviation		121264,59453936	
	Minimum		,00000	
	Maximum		1,00000E+006	
	Range		1000000,00000	
	Interquartile Range		5000,00000	
	Skewness		7,645	,131
	Kurtosis		59,069	,261

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Trošak obrazovanja za IS	,426	347	,000	,170	347	,000

a. Lilliefors Significance Correction

Prilog br. 9: Detaljna analiza karakteristika distribucije varijable „Broj incidenata IS u 2012."

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Broj incidenata IS u 2012.	104	30,0%	243	70,0%	347	100,0%

Descriptives

			Statistic	Std. Error
Broj incidenata IS u 2012.	Mean		3,3846	,36314
	95% Confidence Interval for Mean	Lower Bound	2,6644	
		Upper Bound	4,1048	
	5% Trimmed Mean		2,8611	
	Median		2,0000	
	Variance		13,715	
	Std. Deviation		3,70334	
	Minimum		1,00	
	Maximum		25,00	
	Range		24,00	
	Interquartile Range		1,00	
	Skewness		3,066	,237
	Kurtosis		12,004	,469

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Ukupna razina funkcionalnosti	,104	347	,000	,923	347	,000

a. Lilliefors Significance Correction

Prilog br. 10: Detaljna analiza karakteristika distribucije varijable „Ukupna razina funkcionalnosti upravljanja informacijskom sigurnošću (Y)“

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Ukupna razina funkcionalnosti	347	100,0%	0	0,0%	347	100,0%

Descriptives

			Statistic	Std. Error
Ukupna razina funkcionalnosti	Mean		21,43	,912
	95% Confidence Interval for Mean	Lower Bound	19,63	
		Upper Bound	23,22	
	5% Trimmed Mean		20,11	
	Median		19,00	
	Variance		288,338	
	Std. Deviation		16,981	
	Minimum		0	
	Maximum		80	
	Range		80	
	Interquartile Range		23	
	Skewness		1,000	,131
	Kurtosis		,839	,261

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Ukupna razina funkcionalnosti	,104	347	,000	,923	347	,000

a. Lilliefors Significance Correction