Očuvanje kontinuiteta poslovnog procesa i prihvatljive razine sigurnosti informacijskog sustava uslijed havarije

Selec, Ozren

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
V A R A Ž D I N

OZREN SELEC

Očuvanje kontinuiteta poslovnog procesa i prihvatljive razine sigurnosti informacijskog sustava uslijed havarije

Varaždin, 2017.

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
V A R A Ž D I N

Ime i prezime: Ozren Selec

Matični broj: 115/2012

Studij: Menadžment poslovnih sustava

Očuvanje kontinuiteta poslovnog procesa i prihvatljive razine sigurnosti informacijskog sustava uslijed havarije

Specijalistički završni rad

Mentor: prof. dr. sc. Mario Spremić

Varaždin, 2017.

SADRŽAJ

1. UVOD

1.1. Predmet i ciljevi rada

Očuvanje kontinuiteta poslovnog procesa predstavlja vrlo važan poslovni imperativ u raznim industrijama pri čemu često treba udovoljavati različitim zahtjevima (tehnološkim, organizacijskim, regulatornim, sigurnosnim, itd.). Svakodnevna poslovna praksa, ali i brojna istraživanja[1] uočavaju veliku važnost neprekinutosti procesa i očuvanja podataka, osobito u okruženju automatiziranih poslovnih procesa.

Predmet rada je analiza mjera očuvanja kontinuiteta poslovanja i prihvatljive razine informacijske sigurnosti u slučaju havarije.

Glavni ciljevi rada su:

1. Objasniti pojam kontinuiteta poslovanja i prihvatljive razine rizika te prikazati i analizirati model kontinuiteta poslovanja.

2. Analizirati odabrani model očuvanja kontinuiteta poslovanja.

Specifični ciljevi rada su:

a) Prikazati važnosti kontinuiteta poslovnog procesa i informacijske sigurnosti te posljedica koje mogu nastati prekidom poslovnih procesa kod plinskog operatera i istražiti mogućnosti sprečavanja tih scenarija. Uočena je ovisnost većine poslovnih procesa od strane informacijske i komunikacijske tehnološke infrastrukture, kao i kvantitete, kvalitete i dostupnosti informacija koje takva infrastruktura osigurava i podržava. Svaka tvrtka mora opisati svoje poslovne procese pa tako i proces razvoja informacijsko - sigurnosnih rješenja u slučaju havarije ili prekinutosti kontinuiranog poslovnog procesa. Sustavi su podložni rizicima od upada u njih. Potrebna je njegova puna zaštita da bi se ta zaštita održala na profesionalnom poslovnom nivou te zaštićeni samodostatni model optičke mreže koja služi za potrebe operatera kod poslovnog procesa.

b) Opisati načine zaštite sustava, postupke uslijed havarije te prijedlog rješenja uslijed štetnog događaja.

c) Prikazati procesa upravljanja u situacijama havarije, odnosno prekida neometanog protoka informacija u svrhu zaštite podatka i nastavka procesa protoka istih.

d) Ukazati na nužnost upravljanja informacijskom sigurnošću tog zatvorenog sustava sa samodostatnom optičkom mrežom i analizirati model očuvanja njegova kontinuiteta upotrebom sekundarnog načina komuniciranja.

[1] Vukšić, B., Hernaus, V., Kovačić, T. (2008.): „Upravljanje poslovnim procesima - Organizacijski i informacijski pristup“, Školska knjiga, Zagreb.

e) Opisati značajke svjetlovodnih vlakana i svjetlovodnih kabela te navesti primjer greške na izdvojenoj dionici trase plinovoda pod nazivom A-B i kompletan proces opisa tehničkog dijela otklanjanja grešaka kao i prethodno zaštite sustava poslovnog procesa.

f) Prikazati načine uštede vremena i resursa da bi opskrba energentom tekla neprekidno te da bi se poslovni proces odvijao unutar zadanih rokova isporuke.

1.2. Metodologija i struktura rada

U radu će se analizirati posljedice koje mogu nastati prekidom poslovnih procesa kod plinskog operatera i istražiti mogućnosti sprečavanja tih scenarija. Plinski operateri predstavljaju i vrlo važnu, često i kritičnu nacionalnu infrastrukturu kojom se treba upravljati i sa stanovišta informacijske sigurnosti i kontinuiranosti poslovnog procesa. U radu će biti objašnjena zaštita sustava koji je u praksi zatvoren od vanjskih čimbenika, čime se pokušava održati prihvatljiva razina sigurnosti poslovnog procesa. Sigurnost infrastrukture i neprekidnost procesa opskrbe plinom spadaju među najvažnije poslovne ciljeve plinskog operatera, a neplanirani događaji poput havarije trebaju se pokušavati spriječiti ili barem umanjiti šteta koja može nastati.

U rješavanju opisanog problema koristit će se kombinacija sljedećih metoda:

Metoda modeliranja. Ovom metodom želi se modelirati poslovni proces i informacijska sigurnost radi analize i poboljšanja izvođenja postojećeg procesa. Ovom metodom žele se opisati koraci složenog poslovnog procesa kao dio razvojnog procesa, ali životnog ciklusa procesa koji je predmet rada.

Metoda analize. Cilj je prepoznavanje mjesta u kojima se proces može poboljšati. Poslovni proces mora biti neprekinut i zaštićen, te se može na početku napraviti procjena važnosti njegovog kontinuiteta. Analizirat će se zaštićenost sustava informacijske sigurnosti te načina pristupa problemu kod havarije.

Heuristički pristup predstavlja korištenje iskustva, intuicije i vlastite procjene prilikom rješavanja nekog problema. Primjer rješavanja problema bit će dobiven putem razgovora i osobnih iskustava u praksi.

Metoda studije slučaja. Ispituje međuovisnosti svih varijabli pojedinog procesa ili situacije da bi pružili njegovo ukupno razumijevanje. Metoda studija slučaja postavlja pitanja "kako" i "zašto". Studij slučaja koristi se kada se radi o stvarnim problemima stavljenim u kontekst specifičnog okruženja. Navest će se i opisati konkretan problem na izdvojenoj dionici plinskog operatera koja će se zvati A-B.

Induktivna metoda i deduktivna metoda. Na temelju promatrane pojave možemo zaključiti da će slične pojave koje se nisu ispitivale imati ista svojstva kao i pojave koje su se dogodile. Deduktivna metoda polazi od postavke da ono što vrijedi uopće, vrijedi i za jedan poseban slučaj. Promatrat će se i opisati poslovni proces i informacijska sigurnost kod plinskog operatera pod pretpostavkom da se u slučaju havarije prati obrazac postupanja i kod svake sljedeće havarije.

Metoda intervjua**.** Temelj završnoga dijela rada bazirat će se na razgovoru i informacijama s voditeljem optičko-komunikacijskog odjela plinskog operatera kao i primjerom štetnog događaja odnosno havarije na dionici A-B, njezine zaštite i sekundarne komunikacije uslijed havarije.

Metodom analize prikazat će se zaštićenost sustava i prihvatljive razine informacijske sigurnosti u plinskome operateru te način pristupa problemu kod havarije. U radu će se opisati poslovni proces, ukazati na nužnost upravljanja informacijskom sigurnošću tog zatvorenog sustava sa samodostatnom optičkom mrežom i analizirati model očuvanja njegova kontinuiteta.

Metodom studije slučaja i induktivno-deduktivnom metodom prikazat će se konkretan slučaj štetnog događaja te pretpostavka da će se jednak obrazac postupanja koristiti i kod svakog sljedećeg štetnog događaja.

Uslijed havarije dolazi do izražaja neprekidna kontinuiranost poslovnog procesa, opisom primarne i sekundarne komunikacije između dvije stanice, koje će se u radu nazivati A-B, opisat će se načini i postupci rješavanja problema uslijed štetnog događaja.

Metodom heurističkog pristupa te metodom intervjua pokušat će se osobna iskustva zaposlenika plinskog operatera u svakodnevnom radu prenijeti na ovaj rad. Ovaj način primjene sigurnosti i neprekinute komunikacije kod poslovnog procesa može biti primjer i drugim tvrtkama koje se bave distribucijom energenata kako zaštititi svoj poslovni proces i osigurati njegov nesmetani tok čak i kod neplaniranog događaja. Tako će se uštedjeti vrijeme i resursi, te će se opskrba energentom završavati unutar zadanih rokova.

Havarija nije česta pojava, ali kada se dogodi iziskuje pravilan, pravovremen i stručan pristup rješavanju problema unutar zadanog vremenskog roka za što bržu uspostavu primarne komunikacije te razine sigurnosti prije štetnog događaja što se nameće kao ključno mjerilo za uspjeh projekta.

1.3. Doprinos rada

Zbog potreba tržišta i borbe s konkurencijom potrebno je poštovati rokove kao i razinu informacijske sigurnosti, što zahtijeva dobru organizaciju i poznavanje sustava. Za ovakav poslovni proces neometanog protoka informacija u svrhu distribucije energenta potrebno je dobro planiranje, koordiniranje i propisni certifikati te norme informacijske sigurnosti u neprekinutom poslovnom procesu. Svi poslovni procesi trebaju biti opisani, dokumentirani kako bi se mogli optimizirati. U organizaciji gdje je primarna djelatnost distribucija energenta potrebno je sagledati i opisati informacijsku sigurnost sustava, kako bi se smanjila mogućnost od mogućih upada u sustav što će rezultirati kontinuitetom poslovnog procesa i boljom konkurentnošću na tržištu.

Cilj svake organizacije je smanjenje trajanja poslovnog procesa i pojednostavljenje poslovnih procesa. Važno je sagledati poslovni proces i opisati poslovne aktivnosti koje se izvršavaju u njemu. U radu će se opisati poslovni proces i informacijska sigurnost u neprekinutom poslovnom procesu kao i izolirani slučaj neplaniranog događaja i svih njegovih potprocesa, te će se istaknuti svi potencijalni problemi i rješenja pri vraćanju poslovnog procesa u njegov primarni tok. Pretpostavka je da uređeni poslovni proces i planiranje informacijske sigurnosti uvelike pomažu pri poslovnom procesu te da mu daju određenu sigurnost kao i koraci koji se poduzimaju pri neplaniranom događaju koji ga prekida dajući mu prednost i konkurentnost na tržištu. Ovaj rad bi mogao poslužiti kao osnova za sagledavanje sličnih problema u nekoj drugoj tvrtki, te kao model po kojem se dolazi do rješavanja problema.

2. UPRAVLJANJE POSLOVNIM PROCESIMA

U današnjoj svjetskoj ekonomiji, koja pod utjecajem globalizacije širi tržišta, ali i približava konkurenciju, mnoge tvrtke traže načine kako povećati učinkovitost i smanjiti troškove poslovanja. Kao slijed događaja javlja se prihvaćanje procesnog pristupa, kao ključnog elementa poslovanja. Posebno su, za industrijski sektor koji će se opisivati u radu uređenost sustava, hijerarhija, neprekinutost i sigurnost poslovnog procesa kod isporuke energenta.

2.1. Definicija poslovnih procesa

Poslovni procesi (eng. business processes) opisuju način na koji se nešto u organizaciji radi Prema Harringtonu (1991.), Martinu (1994.) i Davenportu (1993.) poslovni proces je niz logičko povezanih aktivnosti koje koriste resurse poduzeća čiji je cilj zadovoljiti potrebu kupaca za proizvodima ili uslugama odgovarajuće kvalitete i cijene, u adekvatnom vremenskom roku, uz istovremeno ostvarivanje neke vrijednosti.

U većini slučajeva poslovni procesi postoje unutar jednog funkcijskog segmenta organizacije. Poslovni procesi nisu mjerljivi numeričkim kriterijima, no oni u najvećem broju slučajeva predstavljaju određenu poslovnu funkciju koja je čvrsto integrirana u radnim zadacima samoga procesa.

Poslovanje je sustav integriranih procesa. Shvaćati kako se odvija poslovanje i komuniciranje u istom između zaposlenika, partnera, kupaca i dobavljača kritična je, konkurentna, poslovna prednost definirana kako su osnovna obilježja poslovnih procesa sljedeća:[2]

- Svaki proces ima svrhu
- Svaki proces ima vlasnika
- Svaki proces ima početak i završetak
- U proces ulaze inputi, a izlaze outputi
- Proces je sastavljen od sekvencijski izvedivih aktivnosti
- Na temelju ulaza i izlaza procesa lako se utvrđuje uspješnost procesa
- Da bi proces opstao treba imati poznate unutarnje i vanjske dobavljače i potrošače
- Unaprjeđenje procesa je neizbježno
- Da bi proces opstao treba imati poznate unutarnje i vanjske dobavljače i potrošače

Ovisno o kontekstu u kojem se poslovni proces spominje postoji nekoliko klasifikacija procesa. Svako poduzeće predstavlja poseban slučaj i mora se promatrati kroz međusobnu povezanost poslovnih procesa i njima pripadajućih dimenzija. Koliko god bila posebna sva poduzeća imaju cijeli niz zajedničkih procesa i poslovnih dimenzija:[3]

- Podjela po organizacijskoj strukturi
- Podjela po vremenskim intervalima
- Podjela po teritoriju
- Podjela po kategorijama produkata i usluga
- Podjela po dobavljačima i kupcima

[2] Business Continuity Institute (2013) BCM Legislations, Regulations and Standards, Caversham: BCI

[3] Business Continuity Institute (2013) BCM Legislations, Regulations and Standards, Caversham: BCI

Prema polju djelovanja procesa unutar organizacije, oni se dijele na tri različite vrste

- Individualni procesi koje obavljaju pojedinci
- Vertikalni (funkcijski) procesi koji su dio funkcijske jedinice ili odjela organizacije
- Horizontalni procesi koji prolaze kroz nekoliko funkcijskih jedinica.

Razlikuju se tri logičke komponente poslovnog procesa

- Upravljački informacijski proces
- Operativni proces
- Upravljački proces

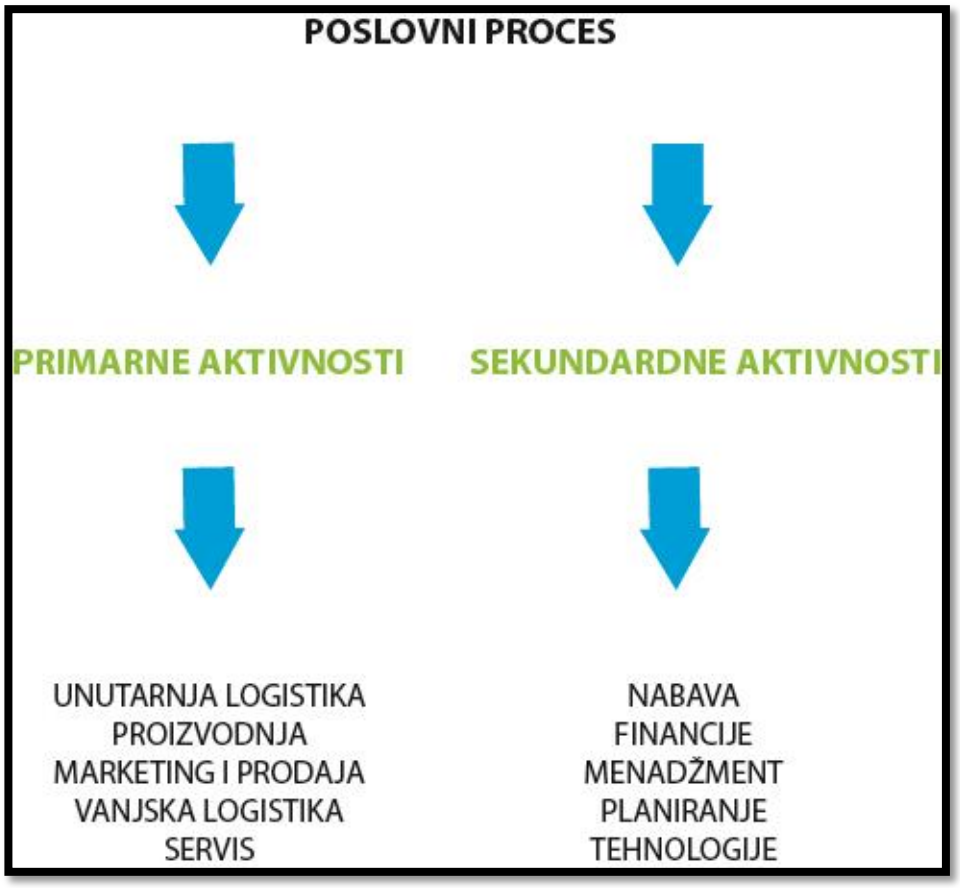
Pod upravljačkim informacijskim procesom podrazumijeva se dio ukupnog upravljačkog informacijskog sustava (UIS-a) koji se odnosi na konkretni poslovni proces. Operativni proces kreira čovjek, a sastoji se od ljudi, opreme, organizacije, politika i procedura, što sve ima za cilj osiguravanje efikasnog rada organizacije. Upravljački proces također kreira čovjek, a sastoji se od ljudi, autoriteta, organizacije, politika i procedura s ciljem planiranja i kontrole aktivnosti koje se odvijaju unutar organizacije.[4]

Pokretačem usmjeravanja pozornosti na poslovne procese smatra se M. E. Porter koji je u knjizi Competitive Advantage: Creating and Sustaining Superior Performance iz 1985. godine iznio koncept poduzeća kao lanca vrijednosti. Lanac vrijednosti obuhvaća više poslovnih procesa, od razvoja novog proizvoda i naručivanja do prodaje kupcu i potpore po završetku prodaje. Prema Porteru lanac vrijednosti sastoji se od primarnih i sekundarnih aktivnosti (Slika 1.). Sve sekundarne aktivnosti moraju biti uključene u jedinstven lanac vrijednosti. Za razliku od primarnih, sekundarne aktivnosti ne ostvaruju izravnu vrijednost za poduzeće, ali su nužne za njegovo funkcioniranje. Proces je dio lanca vrijednosti, a ovisno o složenosti može se podijeliti na manje potprocese.[5]

[4] Business Continuity Institute (2013) BCM Legislations, Regulations and Standards, Caversham: BCI

[5] Elliott D, Swartz E and Herbane B (2010) Business Continuity Management: A Crisis Management Approach, New York: Routledge.

Slika 1. Podjela poslovnih procesa na aktivnosti prema Michaelu Porteru.



Izvor: Cingula,M., Fabac,R., (01.lipanj,2009)[6]

2.2. Koncept upravljanja poslovnim procesima

Poslovanje u svim granama industrije i gospodarstva je pod ogromnim pritiskom velike konkurencije, poslovne okoline koja se brzo mijenja i sve zahtjevnijih kupaca. Postoje tri trenda koja pridonose ovome pritisku, a to su:[7]

- Globalizacija
- Tehnološke, legislativne i regulatorne promjene
- Sve agilnije i fleksibilnije organizacije

Svi ti pritisci stvorili su interes za analiziranjem kako poslovanje može postati fleksibilnije i efektivnije. Svaka organizacija je definirana s puno poslovnih procesa koji opisuju način na koji organizacija provodi svoje poslovanje. Neki procesi su ključni za poslovanje organizacije i čine njenu komparativnu prednost. Neki nisu toliko ključni, ali su i dalje bitni za njeno

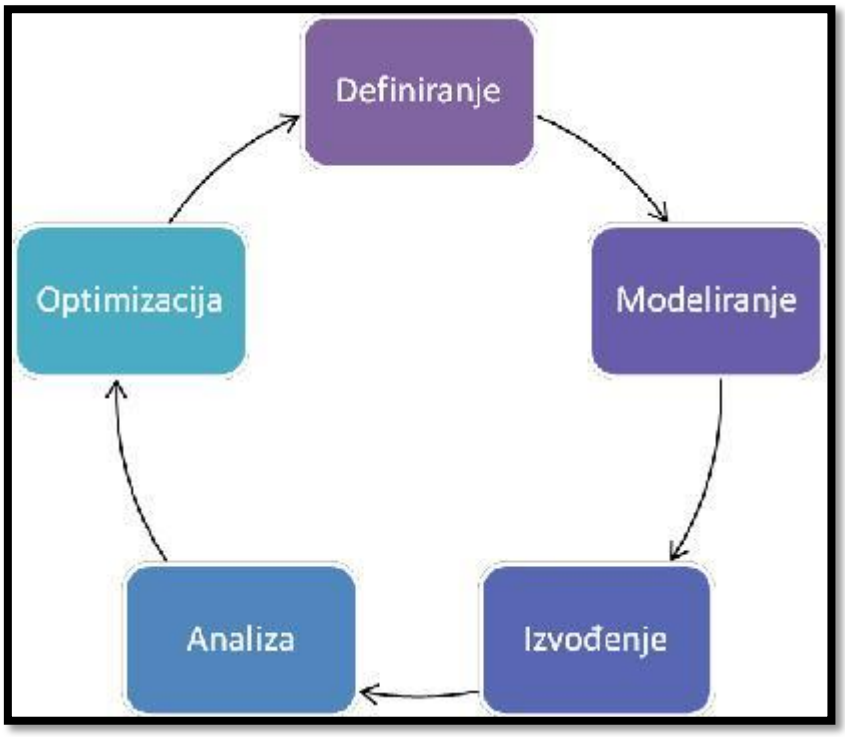
[6] Izvor: Cingula,M., Fabac,R., (01.lipanj,2009)

[7] Elliott D, Swartz E and Herbane B (2010) Business Continuity Management: A Crisis Management Approach, New York: Routledge.

funkcioniranje. Poslovni procesi su, u biti centralni sustav svakog poduzeća i zato je bitno njima upravljati.[8]

Upravljanje poslovnim procesima kombinira menadžerski pristup s odgovarajućom tehnologijom u cilju poboljšavanja performansi poduzeća. Upravljanje poslovnim procesima (eng.Business Process Management, BPM) je sustavan pristup poboljšavanja poslovanja temeljen na oblikovanju, mjerenju, analizi, poboljšanju i upravljanju procesima. Upravljanje poslovnim procesima se oslanja na poslovni pristup upravljanja promjenama zbog unapređivanja poslovnih procesa s konačnim ciljem ostvarenja poslovnih ciljeva, pri čemu promjene obuhvaćaju cijeli životni ciklus procesa: od definiranja i modeliranja do izvođenja, analize i optimizacije procesa (Slika 2.).

Slika 2. Životni ciklus upravljanja poslovnim procesima.



Izvor: Lončar, 2007 str. 15.[9]

Prvi korak u upravljanju poslovnim procesima jest definiranje poslovnih procesa. Vlasnici poslovnih procesa u ovoj fazi imaju najvažniju ulogu jer posjeduju poslovne zahtjeve i dostupne resurse. Sljedeća faza je modeliranje poslovnih procesa i ona uključuje skupljanje dovoljno detalja kako bi se razumjelo kako proces funkcionira te se zatim formalizira tijek poslovnog procesa pomoću dijagrama tijeka poslovnih procesa. Poslovni proces unutar poduzeća se zatim implementira i izvodi te se nadgledanjem prate ključni pokazatelji performansi poduzeća (eng. key performance indicators, KPI). Prikupljeni podaci se analiziraju kako bi se identificiralo neočekivano ponašanje, neoptimizirani tokovi i uska grla te se na temelju toga proces optimizira poslovni proces.

[8] Elliott D, Swartz E and Herbane B (2010) Business Continuity Management: A Crisis Management Approach, New York: Routledge.
[9] Izvor: Lončar, 2007 str. 15.

Upravljanjem poslovnim procesima postižu se:[10]

- Viša kvaliteta
- Kraće vrijeme
- Niži troškovi
- Smanjen je rizik poslovanja

U današnje vrijeme jako je bitno imati jasnu viziju i koncept poslovanja i poslovnog procesa kako bi ostali konkurenti među sve većom i oštrijom konkurencijom.

2.2.1. Koncept razvoja poslovnog procesa

Snažna funkcionalna struktura dovela je do stvaranja izoliranih odjela tzv. silosa poslovanja u kompaniji. Poslovanje i poslovni rezultati praćeni su pojedinačno, na razini odjela i to je dovelo do neefikasnog poslovanja U ranim 1990-tim pažnju akademske zajednice i poslovnog svijeta počeo je privlačiti koncept poslovnih procesa i orijentacije na poslovne procese. Teoretičari procesne filozofije su W.E. Deming, M.E.Porter, T.H. Davenport, M.Hammer, J. Champy, R. Coombs, R.Hull. Prema procesnom tj. horizontalnom pogledu poslovni procesi predstavljaju jezgru funkcioniranja određene organizacije zato što se organizacija primarno sastoji od procesa, a ne proizvoda ili usluga .[11]

Tablica 1. prikazuje razlike u nekim obilježjima između tradicionalnog i procesno orijentiranog poduzeća. Zbog orijentiranosti na poslovne funkcije tradicionalno poduzeće nema jasno definiranu sliku cijeloga procesa, slabo je fokusirano na kupce, postoje nepotrebna uska grla i barijere, loša komunikacija i rivalstvo među organizacijskim jedinicama te konfliktni ciljevi i akcije između različitih odjela. Kod procesno orijentiranih poduzeća usmjerenost na proces osigurava bolju usmjerenost na kupca, utvrđivanjem granica procesa te kupaca i dobavljača procesa postiže se bolja komunikacija, određivanjem vlasnika procesa koji su odgovorni za proces izbjegnuta je tradicionalna rascjepkanost odgovornosti.[12]

[10] Bosilj Vukšić, Hernaus i Kovačić, 2008., str. 7,22

[11] BSi (2012) ISO 22301:2012 Societal Security – Business Continuity Management Systems – Requirements, London: Bsi

[12] BSi (2012) ISO 22301:2012 Societal Security – Business Continuity Management Systems – Requirements, London: Bsi

Tablica 1. Prikaz razlike tradicionalnih i procesno orijentiranih poduzeća

OBILJEŽJA	TRADICIONALNO PODUZEĆE	PROCESNO PODUZEĆE
Poslovni vidik	Poslovna funkcija	Poslovni proces
Organizacijska jedinica	Odjel	Procesni timovi
Radni zadaci, poslovi	Usko definirani	Fleksibilni i opsežni
Fokus djelatnika	Nadređeni, rukovodioci	Kupci
Naknada se temelji na	Provedbi aktivnosti	Postignutim rezultatima
Uloga rukovodstva	Nadzor	Mentorstvo
Ključna osoba	Direktor odjela (poslovne funkcije)	Vlasnik poslovnog procesa
Poslovna kultura	Nadređenost, konflikti	Sudjelovanje, suradnja

Izvor: Bosilj Vukšić, V., Hernaus, T., Kovačić, A. (2008.), str. 53.-55.[13]

2.2.2. Važnost poslovnog procesa.

Postoji mnogo definicija procesne orijentacije (eng. Business Process Orientation, BPO). Bitno je naglasiti:[14]

- Procesna orijentacija nije sinonim za procesnu organizacijsku strukturu. Ona predstavlja razumijevanje tijeka poslovanja i tek je prvi korak ka procesno orijentiranoj organizacijskoj strukturi
- Procesna orijentacija i procesna organizacijska struktura se ne smiju poistovjetiti s reinženjeringom poslovnih procesa (eng. Business Process Reengineering, BPR)

Procesna orijentacija je najvažniji element reinženjeringa poslovnih procesa, a za razliku od BPR-a procesno orijentirana organizacija stavlja naglasak na globalne, socijalne i tehničke

[13] Izvor: Bosilj Vukšić, V., Hernaus, T., Kovačić, A. (2008.), str. 53.-55.

[14] British Standards Institution (2006). Business continuity management-Part 1: Code of practice :London

aspekte ljudske dinamike više nego na tehnologiju, poslovne alate i samu tehniku i to na razini cijele kompanije.

Procesna orijentacija razjašnjava prepreke i aktivnosti koje su nepotrebne i predstavlja alat za buduće promjene i unaprjeđenja. Procesna orijentacija pomaže kompanijama u promišljanju kako njihove aktivnosti i zadaci dodaju ili oduzimaju vrijednost za potrošače i dodaje organizacijskim strukturama novu dimenziju kompleksnosti[15]

Važnost procesne orijentacije najbolje odražava zaključak konzultantske kuće Gartner: "*Upravljanje poslovnim procesima osvaja trostruku krunu: za uštedu vremena, za uštedu novca i za dodavanje vrijednosti.* Ona također širi poslovanje i ističe važnost tehnologije pri osmišljavanju strategije koja osigurava konkurentsku prednost. Konačno, upravljanje procesima kompaniji istovremeno donosi i kratkoročni povrat na investicije i dugoročnu vrijednost na uloženi kapital.

Važnost kontinuiranosti poslovnog procesa biti će prikazan u ovome radu. Opskrba plinskim energentom posebno je važna jer gotovo svaki objekt u Republici Hrvatskoj ima plinski priključak a svaki ispad sustava tretira se kod potrošača negativno u slučaju da energent nije isporučen, što u konačnici dovodi do pada rejtinga kompanije te financijski gubitaka.[16] Najznačajnijom karakteristikom procesne orijentacije, te najznačajnijim principom smatra se identificiranje vlasnika procesa, jer se time nadilazi najveće ograničenje klasične organizacije, a to je pitanje kompetencija i odgovornosti. Procesna orijentacija podrazumijeva da naglasak nije na vertikalnoj distribuciji moći, već na horizontalnoj suradnji radi ostvarivanja željenih performansi procesa. Zato se procesna orijentacija prikazuje kao jedan od uvjeta za osiguravanje visokih performansi. Upravljanje poslovnim procesima zapravo je prihvaćanje procesne orijentacije kao načina realizacije svih zadataka u kompaniji.

2.3. Modeliranje i analiza poslovnih procesa

Modeliranje i analiza poslovnih procesa su od egzistencijalne važnosti za uspjeh inicijativa upravljanja poslovnim procesima. Aktivnosti unutar tih faza životnog ciklusa upravljanja poslovnim procesima razvijaju jasnu definiciju i shvaćanje poslovnih procesa koje vode ka njihovom poboljšanju i optimizaciji

2.3.1. Modeliranje poslovnih procesa

Kod modeliranja poslovnih procesa postoje dva pristupa:[17]

- Grafičke metode (statičko modeliranje)
- Simulacijsko modeliranje (dinamičko modeliranje)

[15] British Standards Institution (2006). Business continuity management-Part 1: Code of practice :London

[16] British Standards Institution (2012). Societal security – Business continuity management Systems – Requirements: London

[17] Business Continuity Institute (2013) BCM Legislations, Regulations and Standards, Caversham: BCI

Grafičko modeliranje poslovnih procesa

- Podrazumijeva formiranje dijagrama koji prikazuju aktivnosti poslovanja i slijed kojim se događaju. Pri izradi modela poslovnog procesa rabe se standardizirani grafički elementi što olakšava komunikaciju različitih sudionika u njihovoj analizi.

Modeliranje poslovnih procesa također omogućava sljedeće:

- Definiranje ključnih poslovnih procesa
- Modeliranje svih ili pojedinih procesa u detalje
- Identificiranje procesa koji traže poboljšanja
- Modeliranje novih procesa prije nego se implementiraju

Grafičke metode za modeliranje se dijele prema sljedećim pristupima (Tablica 2.):[18]

Podatkovni pristup ima težište na entitetima, njihovoj strukturi i povezanosti
Funkcijski pristup se fokusira na aktivnosti i podatke iz njih
Organizacijski pristup prati tko i gdje izvodi aktivnosti
Procesni pristup je fokusiran na pitanja zašto, kada i kako se izvode aktivnosti.

Za modeliranje poslovnih procesa koristi *se Unified Modeling Language* (UML). UML je jezik za modeliranje koji služi za specifikaciju, vizualizaciju, izgradnju i dokumentiranje artefakata sustavnih procesa.

[18] Business Continuity Institute (2013) BCM Legislations, Regulations and Standards, Caversham: BCI

Tablica 2. Pregled različitih pristupa i modeliranja poslovnih procesa

PRISTUP	METODA
Podatkovni	● Dijagram toka podataka ● Dijagram entiteta-veza
Funkcijski	● SDT dijagram ● IDEF dijagram
Organizacijski	● UML dijagram korištenja ● UML dijagram suradnje
Procesni	● UML dijagram aktivnosti ● EEPC DIJAGRAM ● BPMN dijagram

Izvor: Bosilj Vukšić, V., Hernaus, T., Kovaĉiĉ, A., (2008.)., str.152.[19]

Simulacijsko modeliranje poslovnih procesa:[20]

- Simulacija je korisno sredstvo za modeliranje i promjene poslovnih procesa
- Simulacija omogućuje uključivanje slučajnih varijabli u model procesa, eksperimentiranje s modelom i predviđanje učinaka promjena na performanse modela koje su karakteristične za simulacijsko modeliranje
- Repovi čekanja
- Uska grla
- Iskorištenje resursa

[19] Izvor: Bosilj Vukšić, V., Hernaus, T., Kovaĉiĉ, A., (2008.)., str.152

[20] BSi (2012) ISO 22301:2012 Societal Security – Business Continuity Management Systems – Requirements, London: Bsi

Uz očigledne prednosti koje bi mogla donijeti primjena diskretne simulacije u izradi prijedloga poboljšanja postojećih procesa, ona ima i određene nedostatke[21]

- Dug i skup razvoj modela
- Složeno vrednovanje modela i izvođenje eksperimenta
- Potrebno je poznavati velik broj metoda i alata
- Rezultat simulacijskog eksperimenta nije optimalno rješenje, a odabir najboljeg rješenja ovisi o procjeni i odluci članova projektnog tima.

2.3.2. Analiza poslovnih procesa

Analizom poslovnih procesa pronalaze se: aktivnosti koje ne dodaju vrijednost, redundantne aktivnosti, neprimjerene upotrebe tehnologije, neprikladna pravila i procedure te se pronalaze načini davanja povratne informacije i veze između procesa koje nedostaju. Postoji mnogo pristupa analizi poslovnih procesa ali dvije glavne kategorije uključuju top-down i bottom-up metodologiju.[22]

Top-down metodologiji određuje se opseg procesa, identificiraju se procesi i njihovi ciljevi te aktivnosti i koraci od kojih se procesi sastoje. Prilikom analize, analiziraju se procesi do najniže razine, izvođači procesa i čitav niz performansi

Bottom-up metodologija uobičajeno uključuje razvoj dva modela poslovnih procesa. Prvi jest stanje postojećih poslovnih procesa i identifikacija šansi za poboljšanje (AS-IS). Drugi model se razvija u svrhu definiranja novih, željenih poslovnih procesa (TO-BE). Odabir metodologije ovisi o samome cilju analize. Nužni koraci prilikom analize procesa su

- Definirati cilj aktivnosti i analizirati korake od kojih se aktivnost sastoji
- Otkriti da li aktivnost dodaje vrijednost ili ne
- Definirati mjere za rezultate aktivnosti
- Definirati znanje koje je potrebno kako bi se aktivnost mogla izvesti
- Odrediti tko izvodi aktivnosti
- Definirati troškove, resurse i vrijeme trajanja aktivnosti
- Simulirati proces

Pri analizi poslovnih procesa često se primjenjuju:

- Mapiranje poslovnih procesa
- Korelacijska matrica
- Pareto analiza
- Analiza kulturnih čimbenika
- Analiza dodane vrijednosti
- Analiza kritičnog puta

[21] Business Continuity Institute (2013) BCM Legislations, Regulations and Standards, Caversham: BCI

[22] Spring, J., Kern, S., Summers, A. (2015). "Global adversarial capability modeling". *2015 APWG Symposium on Electronic Crime Research (eCrime)*: 1–21.

Najpopularniji alat za analizu poslovnih procesa jest mapiranje poslovnih procesa. Mapiranje procesa se koristi za vizualni prikaz procesa.[23]

Postoje tri tehnike mapiranja poslovnih procesa:

- Relacijske mape
- Međufunkcionalne mape
- Dijagrami toka

Relacijske mape prikazuju relacije isporučitelj-kupac. Međufunkcionalne mape prikazuju funkcije, korake, niz koraka, ulaze i izlaze za određeni dio procesa. Dijagrami toka prikazuju aktivnosti, niz aktivnosti, ulaze i izlaze za određeni dio procesa. Osnovna upotreba mapa jest prikaz kako se obavlja ili kako bi se trebao obavljati tekući proces.

[23] Spring, J., Kern, S., Summers, A. (2015). "Global adversarial capability modeling". *2015 APWG Symposium on Electronic Crime Research (eCrime)*: 1–21.

3. POJAM INFORMACIJSKE SIGURNOSTI I INFORMACIJSKA SIGURNOST U POSLOVNOM PROCESU

3.1. Pojam informacijske sigurnosti

Nema sumnje da informacijska sigurnost postaje sve značajnija infrastruktura u uvjetima suvremenog poslovanja. Suvremeni subjekti[24] uvelike su vezani za računalnu i komunikacijsku infrastrukturu. Pod samim pojmom informacijske sigurnosti misli se na zaštitu informacija od pojavnih oblika prijetnji (unutarnjih i vanjskih), kako bi se omogućio poslovni tijek, smanjio rizik, te povećala količina poslovnih prilika i povrat uloženih ulaganja. Ljudska bića svoj život, odluke i djelovanja, organiziraju na osnovama dostupnih informacija. Prikaz realnosti zato postaje njihova realnost, koja se doživljava kao točnija i pouzdanija nego realnost sama. Nešto se dogodilo, nešto postoji samo ako postoji u informacijskom prostoru, tj. kao informacija.[25]

Pojam informacijske sigurnosti ne odnosi se samo na tehničke mjere zaštite[26], nego podrazumijeva administrativne[27] i fizičke[28] mjere. Na taj način, informacijsku sigurnost promatramo kao: način promišljanja, beskonačan proces, upravljanje rizikom, garantiranje poslovnog uspjeha i kao odgovornost svakog radnika. Informacija predstavlja imovinu i kao takvu ju je potrebno na odgovarajući način i zaštititi, kako bi se postiglo uspješno poslovanje tvrtke odnosno svake druge organizacije. Taj zahtjev sve je značajniji u poslovnom svijetu zbog distribuiranosti poduzetničke okoline, jer su u takvom okruženju informacije izložene većem broju prijetnji i ranjivosti. Posebno je to bitno kod industrijskog sektora gdje je sigurnost sustava i zaštićenost podataka primat. Bez obzira u kojem je obliku pohranjena informacija, ona uvijek mora biti prikladno zaštićena, sigurnosno osigurana i namjenski korištena. Informacije i podatci vrijedan su kapital koji tvrtkama osiguravaju opstanak i uspjeh na tržištu. Svjedoci smo različitih oblika krađe poslovnih podataka i informacija u privatnom, javnom i korporativnom sektoru čime im se nanosi ogromna šteta.

Uzroci krađe i gubitka uglavnom su u slaboj organizaciji informacijske sigurnosti kao i nedovoljnog investiranja u zaštitu poslovnog procesa. U današnjem suvremenom poslovanju u vrijeme tržišne ekonomije i suvremenih tehnoloških rješenja informacijska sigurnost postaje ključan faktor poslovne usklađenosti. Računalna i komunikacijska infrastruktura kreiraju odnosno olakšavaju protok ogromne količine informacija. Te informacije u isto vrijeme su izložene mnogim prijetnjama na koje je nužno pravovremeno reagirati s ciljem izbjegavanja štetnih posljedica.[29] Današnje tvrtke suočavaju se s ogromnim sigurnosnim prijetnjama kao što su računalne prijevare, špijuniranja, sabotaže, vandalizmi i itd. Šteta nanesena tvrtki u obliku računalnog hakiranja i uskraćivanja usluge je predstavlja moderni kriminalni oblik u segmentu poslovanja.

[24] Kao što su državni i gospodarski.
[25] Tuđman, M. (2008). „Informacijsko ratište i informacijska znanost“, Zagreb, 2008.
[26] Korisnička imena, zaporke, i itd.
[27] Sigurnosne politike, pravilnici, procedure
[28] Video nadzor, zaštita prostorija, fizička kontrola pristupa itd
[29] Gugić A. (2014). Poslovne sigurnosne politike i procedure; predavanje Veleučilište Marko Marulić, Knin.

Informacijska sigurnost jednako je značajna javnim i privatnim subjektima. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uvjetima oblici centralizirane kontrole nisu učinkoviti. Upravljanje i usklađenost poslovanja kroz organizacijski i upravljački sklad podržavan informacijskom sigurnošću zahtjeva učešće svih zaposlenika organizacije, a često je potrebna pomoć konzultanta izvan organizacije.[30] U sljedećoj tablici (Tablica 3.) navedeni su sigurnosni segmenti informacijskih sustava.[31]

Tablica 3. Sigurnosni segmenti informacijskih sustava

SIGURNOSNI SEGMENTI INFORMACIJSKIH SUSTAVA		
	SEGMENTI	**SADRŽAJ SEGMENATA**
1	Svijest informacijskoj sigurnosti	**Važno je biti svjestan potrebe za sigurnošću informacijskih sustava i zaštitnim sigurnosnim mjerama.**
2	Odgovornost	**Svi članovi organizacije su odgovorni za sigurnost informacijskih sustava.**
3	Odziv	**Svi članovi organizacije trebaju pravovremeno i kooperativno sudjelovati u sprječavanju, detekciji i rješavanju sigurnosnih incidenata.**
4	Etika	**Svi članovi organizacije trebaju postupati respektivno prema legitimnim interesima ostalih.**
5	Demokracija	**Sigurnost informacijskih sustava treba biti u skladu s pravilima demokratskog društva.**
6	Procjena rizika	**Potrebno je provoditi procjene rizika.**
7	Dizajn implementacija sigurnosnih mjera	**Sigurnosne kontrole trebaju biti sastavni dio informacijskih sustava.**
8	Upravljanje sigurnošću	**Organizacija treba uspostaviti jasan pristup upravljanju sigurnošću.**
9	Promjene	**Organizacija treba redovito nadzirati sustav informacijske sigurnosti i izvoditi potrebne modifikacije sigurnosnih politika, mjera, procedura.**

Izvor: Kempis, R. D., Ringbeck, J. (1998). "Manufacturing use and abuse of IT", The McKinsey Quarterly, 1998, No.1[32]

Sigurnost informacijskih sustava objedinjuje primjenu aktivnosti i radnji u svrhu zaštite podataka koji su u tijeku obrade ili su sačuvani odnosno pohranjeni, ili se nalaze u fazi prijenosa, od gubitka povjerljivosti, cjelovitosti i dostupnosti, te zbog sprečavanja gubitaka cjelovitosti ili dostupnosti samih sustava.[33]

[30] Rimljak, J. (2015). Informacijska sigurnost u suvremenom poslovanju. Veleučilište „Marko Marulić" u Kninu.
[31] Kotler, P., Lee, N. (2009). „Društveno odgovorno ponašanje", MEP CONSULT, Zagreb, 2009.
[32] Izvor: Kempis, R. D., Ringbeck, J. (1998). "Manufacturing use and abuse of IT", The McKinsey Quarterly, 1998, No.1
[33] Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X., Ratick, S. (1988). "The social amplification of risk: A conceptual framework". *Risk Analysis*. **8** (2)

Sigurnosne mjere uključuje mehanizme i procese koji se trebaju implementirati s ciljem odvraćanja, sprečavanja, uočavanja i oporavka od utjecaja havarije odnosno incidenta koji djeluju na povjerljivost, cjelovitost i dostupnost podataka i pratećih sustavnih servisa i potencijala, uključujući i izvještavanje o sigurnosnim prijetnjama odnosno havarijama. To je ustvari proces upravljanja rizikom koji se koristi za procjenu, nadgledanje, otklanjanje, izbjegavanje, transferiranje ili prihvaćanje rizika.

3.1.1. Prihvatljiva razina informacijske sigurnosti

Sustav upravljanja informacijskom sigurnošću (ISMS) je skup politika koje se bave upravljanjem informacijskom sigurnošću ili IT povezanim rizicima. Ovi idiomi su nastali prvenstveno iz BS-a 7799. Upravni princip iza ISMS je da organizacija treba oblikovati, implementirati i održavati koherentan skup pravila, procesa i sustava za upravljanje rizicima svoje informacijske imovine, čime se osigurava prihvatljiva razine informacijske sigurnosti rizika

Kao i kod svih procesa upravljanja, ISMS mora ostati i učinkovit dugoročno, prilagođavajući se promjenama u unutarnjem ustroju i vanjskoj okolini. ISO / IEC 27001: 2005, dakle, ugradio je "Plan-Do-Check-Act" (PDCA) ili Deming ciklus pristup:[34]

- Faza planiranja je o projektiranju ISMS-a, procjena informacija sigurnosnih rizika i odabirom odgovarajuće kontrole
- DO faza ili radna faza uključuje provedbu i operativne kontrole
- Cilj faze provjere je pregledati i procijeniti učinkovitost (efikasnost i djelotvornost) ISMS-a
- U fazi djelovanja promjene se vrše kada je to potrebno kako bi se ISMS vratio na vrhunac svoje učinkovitosti

ISO / IEC 27001: 2005 je standard koji se temelji na riziku informacija, što znači da organizacije moraju imati proces upravljanja rizicima. Proces upravljanja rizicima uklapa u PDCA model. Međutim, najnoviji standard, ISO / IEC 27001: 2013, ne naglašava Deming ciklus više. ISMS korisnik je slobodan koristiti bilo koji proces upravljanja (poboljšanje) pristupa kao PDCA ili šest Sigma DMAIC.

Još jedan konkurencijski ISMS je standard dobre prakse (SOGP). Više je temeljen na dobroj praksi s obzirom na to da dolazi iz iskustva ISF-a industrije. Neki najpoznatiji ISMS-ovi za certifikaciju računalne sigurnosti su: Common Criteria (CC) međunarodni standard i njegovi prethodnici Information Technology Security Evaluation Criteria (ITSEC) i Trusted Computer System Evaluation Criteria (TCSEC).[35]

Drugi okviri, kao što su COBIT i ITIL dotiču se sigurnosnih pitanja, ali uglavnom su usmjereni prema stvaranju okvira upravljanja za podatke i općenito. COBIT ima sudružni okvir koji se naziva Risk IT koji se odnosi na informacijske sigurnosti. Postoji niz inicijativa usmjerenih na problematiku upravljanja i organizacijskog osiguravanja informacijskih sustava imajući u vidu da je poslovni i organizacijski problem, a ne samo tehnički problem:

[34] Spring, J., Kern, S., Summers, A. (2015). "Global adversarial capability modeling". *2015 APWG Symposium on Electronic Crime Research (eCrime)*: 1–21.

[35] Spring, J., Kern, S., Summers, A. (2015). "Global adversarial capability modeling". *2015 APWG Symposium on Electronic Crime Research (eCrime)*: 1–21.

- Savezni Zakon upravljanja informacijskom sigurnošću od 2002. godine američki je savezni zakon donesen 2002. godine koji je prepoznao važnost informacijske sigurnosti u ekonomskim i nacionalnim sigurnosnim interesima SAD-a. Zakon zahtijeva od svake savezne agencije da razvija, dokumentira i provodi agencijski program za pružanje informacijske sigurnosti za informacije i informacijske sustave koji podržavaju poslovanje i imovinu agencije, uključujući i one koji pruža ili upravlja drugim agencijama, izvođačima ili drugim izvorima
- Priručnik za implementaciju sigurnosti poduzeća s Carnegie Mellon Software Engineering Institute CERT je osmišljen kako bi pomogao poslovnim liderima provoditi učinkovit program upravljanja informacijskim tehnologijama i informacijskom sigurnosti
- Capability Maturity Model (CMM) za sigurnost sustava inženjeringa je standardiziran u ISO / IEC 21827
- Information Security Management Maturity Model (poznat kao ISM-kub ili ISM3) je još jedan oblik ISMS. ISM3 se temelji na standardima kao što su ISO 20000, ISO 9001, CMM, ISO / IEC 27001 i opće informacije upravljanja i sigurnosti koncepata. ISM3 se može koristiti kao predložak za ISO 9001. Dok ISO / IEC 27001 kontrola na bazi, ISM3 je postupak koji se temelji i uključuje proces metrike. ISM3 je standard za upravljanje sigurnošću (kako se postiže misija organizacije unatoč greškama, napadima i nesrećama s određenom proračunom). Razlika između ISM3 i ISO / IEC 21827 je da ISM3 je usmjerena na upravljanje, ISO 21287 na inženjering

3.1.2. Potreba za sustavom upravljanja informacijskom sigurnošću

Sigurnosni stručnjaci kažu:[36]

- Administratori sigurnosti informacijskih tehnologija bi trebali posvetiti otprilike jednu trećinu svog vremena adresiranja tehničkih aspekta. Preostale dvije trećine trebale bi biti potrošene u razvoju politike i procedure, obavljanje sigurnosne recenzija i analizu rizika, osvrćući se na planiranja za slučaj nepredviđenih situacija i promicanju sigurnosti svijesti
- Sigurnost ovisi o ljudima više nego o tehnologiji
- Zaposlenici su daleko veća prijetnja sigurnosti informacija nego vanjski čimbenici
- Sigurnost je poput lanca, jaka je koliko i njegova najslabija karika
- Stupanj sigurnosti ovisi o tri čimbenika: rizik koji ste spremni preuzeti, funkcionalnost sustava i troškovi koje ste spremni platiti
- Sigurnost nije status ili snimak, nego proces koji je u tijeku

Ove činjenice neminovno mogu dovesti do zaključka da je sigurnosna administracija pitanje upravljanja, a ne čisto tehničko pitanje. Uspostava, održavanje i kontinuirano ažuriranje nekog ISMS-a pružaju jak pokazatelj da tvrtka koristi sustavni pristup identifikaciji, procjeni i upravljanju rizika informacijske sigurnosti. Kritični faktori ISMS-a su sljedeći:

- Povjerljivost: zaštita podataka od neovlaštenih stranki
- Integritet: zaštita podataka od modifikacije od strane neovlaštenih korisnika
- Dostupnost: izrada dostupne informacije ovlaštenim korisnicima

[36] Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X., Ratick, S. (1988). "The social amplification of risk: A conceptual framework". *Risk Analysis*. **8** (2)

Tvrtka će biti u stanju uspješno se baviti zahtjevima informacijske povjerljivosti, cjelovitosti i dostupnosti (CIA) koji pak imaju implikacije:[37]

- Kontinuitet poslovanja
- Minimiziranje štete i gubitaka
- Konkurentnost
- Profitabilnost i novčani tijek
- Zakonska usklađenost

Glavni cilj upravljanja informacijskom sigurnošću je provesti odgovarajuće mjere kako bi se uklonili ili smanjili utjecaji koji razne prijetnje vezane za sigurnost i ranjivosti mogu imati na organizaciju. Na taj način, upravljanje informacijskom sigurnošću će omogućiti provedbu željene kvalitativne karakteristike usluge koju nude organizacije (tj dostupnost usluga, očuvanja povjerljivosti i integriteta podataka i sl.). Sprečavanjem i umanjivanjem utjecaja sigurnosnih incidenata, ISMS osigurava kontinuitet poslovanja, povjerenje klijenata, zaštitu poslovne investicije i mogućnosti, ili smanjuje štetu na poslu.[38]

Velike industrijske organizacije, banke i financijske ustanove, telekomunikacijski operateri, bolnica i zdravstvene institucije i državna i javna tijela imaju mnogo razloga za razmatranje informacijske sigurnosti vrlo ozbiljno. Pravni i regulatorni zahtjevi kojima je cilj zaštita osjetljivih ili osobnih podataka, kao i opći uvjeti javne sigurnosti tjeraju ih da posvete najveću pažnju i prioritet riziku informacijske sigurnosti. Pod tim okolnostima, razvoj i provedba odvojenog neovisnog procesa upravljanja, ISMS je jedina alternativa. Razvoj ISMS okvira na temelju ISO / IEC 27001: 2005 za sobom povlači sljedećih šest koraka:[39]

- Definicija sigurnosne politike
- Definicija opsega ISMS
- Procjena rizika (kao dio upravljanja rizicima)
- Upravljanje rizicima
- Odabir odgovarajućih kontrola
- Izjava o primjenjivosti

3.1.3. Kritični faktori uspjeha sustava upravljanja informacijskom sigurnšću

Da bi bio djelotvoran, ISMS mora:

- Imati stalnu, nepokolebljivu i vidljivu podršku i predanost rukovodstva organizacije
- Njime se mora upravljati centralizirano, na temelju zajedničke strategije i politike preko cijele organizacije
- Biti sastavni dio cjelokupnog upravljanja organizacijom u vezi s te odražavajući pristup organizacije upravljanja rizicima, ciljevi upravljanja i kontrole i stupanj osiguranja

[37] Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X., Ratick, S. (1988). "The social amplification of risk: A conceptual framework". *Risk Analysis*. **8** (2)

[38] Hallenbeck, W. H. (1986). *Quantitative risk assessment for environmental and occupational health.* Chelsea, Mich.: Lewis Publishers

[39] Hallenbeck, W. H. (1986). *Quantitative risk assessment for environmental and occupational health.* Chelsea, Mich.: Lewis Publishers

- Imati sigurnosne ciljeve i aktivnosti koje će se temeljiti na poslovnim ciljevima i zahtjevima, a na čelu poslovnog upravljanja
- Poduzeti samo nužne zadatke i izbjegavati prekomjernu kontrolu i otpad vrijednih resursa
- U potpunosti mora biti u skladu s filozofijom organizacije i razmišljanja organizacije osiguravanjem sustava koji umjesto da spriječi ljude da rade ono što su zaposleni učiniti
- Temelji se na kontinuiranom osposobljavanju i svijesti osoblja i izbjegava korištenje disciplinskih mjera i "policijske" ili "vojne" prakse
- Biti proces koji nikada ne završava

3.1.4. Prihvatljive razine rizika

Procjena rizika je utvrđivanje kvantitativnih ili kvalitativnih procjena rizika vezanih za dobro definirane situacije i priznate prijetnje (koje se nazivaju i opasnosti). Kvantitativna procjena rizika zahtijeva izračune dvije komponenti rizika (R) magnituda potencijalnog gubitka (L), i vjerojatnost (P) da će se pojaviti gubitak. Prihvatljivi rizik je rizik koji se razumije i tolerira obično jer cijena ili poteškoće u provedbi učinkovite protumjere za povezane ranjivosti premašuje očekivanja gubitku. Procjena rizika uključuje varijacije kao što su vrsta rizika kao i vrsta i težina odgovora, s ili bez konteksta vjerojatnosti.[40]

U svim vrstama inženjeringa kompleksnih sustava sofisticirane procjene rizika često su izrađene u okviru sigurnosne tehnike i pouzdanosti inženjeringa, kada se radi o prijetnji za život, okoliš i funkcioniranje stroja. Nuklearne, zrakoplovne, uljne, željezničke i vojne industrije imaju dugu povijest koja se bavi procjenom rizika. Isto tako, medicinske, bolnica, socijalna služba i prehrambene industrije imaju kontrolu rizika i obavljanje procjene rizika na trajnoj osnovi. Metode za procjenu rizika mogu se razlikovati između industrije i odnose se na opće financijske odluke ili procjene zdravstvenog rizika okoliša.

Procjena rizika sastoji se od objektivne procjene rizika u kojem se pretpostavke i neizvjesnosti jasno sagledaju i predstavljaju. Dio poteškoća u upravljanju rizikom je da su i količine kojima se bavi procjena rizika, potencijalni gubitak i vjerojatnost pojave mogu se vrlo teško mjeriti. Vjerojatnost pogreške u mjerenju ta dva pojma je visoka. Rizik s velikim potencijalnim gubitkom i mala vjerojatnost su pojave, često se različito tretira od jednog s niskim potencijalnim gubitkom i velikom vjerojatnošću pojave. U teoriji, obje su blizu kada je u pitanju prioritet, ali u praksi ovime može biti vrlo teško upravljati kada je suočen s nedostatka resursa, posebno vremena, u kojem se provode proces upravljanja rizicima.[41]

3.1.5. Prihvatljivi kriteriji rizika

Ideja nepovećavanja životnog vijeka rizika za više od jedan u milijun je postala uobičajena u javnom zdravstvenom diskursu i politici. To je heuristička mjera. Ona omogućuje numeričku osnovu za uspostavu zanemarivog porasta rizika. Odlučivanje o okolišu omogućuje neku diskreciju smatrajući pojedine rizike potencijalno "prihvatljivima" ako je manje od jedan u deset tisuća šanse za povećanim rizikom su doživotne. Niski kriteriji rizika kao što su ovi

[40] Hallenbeck, W. H. (1986). *Quantitative risk assessment for environmental and occupational health.* Chelsea, Mich.: Lewis Publishers

[41] O'Brien, M., (2002), *Making better environmental decisions: an alternative to risk assessment*, Cambridge, Massachusetts: MIT Press

pružaju određenu zaštitu za slučaj gdje pojedinci mogu biti izloženi čimbenik.[42] Inteligentna misao o razumno cijelom setu opcija je bitna. Dakle, nije neobično da postoji iterativan proces između analize, uzimajući u obzir mogućnosti i popratnu analizu.

3.1.6. Sigurnost informacija i procjena rizika

Procjena informacijskog rizika može biti izvedena od strane kvalitativnog ili kvantitativnog pristupa, sljedeći različite metodologije. Jedna važna razlika u procjenama rizika u području informacijske sigurnosti je modificiranje modela prijetnji za činjenicu da bilo koji neprijateljski sustav spojen na internet ima pristup i mogućnost da bude prijetnja bilo kojem povezanom sustavu. Procjena rizika, dakle, možda se može mijenjati kako bi se u obzir uzele prijetnje od svih protivnika, a ne samo one s razumnim pristupom, kako je učinjeno u drugim područjima.

Druga značajna razlika je strateška priroda procjene informacijskog rizika. Za razliku od taktičkih procjena ranjivosti i ispitivanja penetracije kojima je cilj identificirati i zatvoriti određene nedostatke u sigurnosti, procjene rizika su funkcionalne na izvršnoj razini ispitati širu sliku za upravljanje informacijskim rizicima.

3.1.7. Kvantitativna procjena rizika

Kvantitativna procjena rizika uključuje izračun jedinstvenog očekivanog gubitka (SLE) imovine. Jedinstveno očekivani gubitak može se definirati kao gubitak vrijednosti za imovinu na temelju jednog sigurnosnog incidenta. Tim je zatim izračunava na godišnjoj razini stope pojavljivanja (ARO) od ugroženosti imovine. ARO je procjena na temelju podataka o tome koliko često prijetnja bi bila uspješna u iskorištavanju ranjivosti. Iz ovih podataka, na godišnjoj razini očekivani (ALE) može se izračunati. Godišnji očekivani gubitak je izračun jednog očekivanog gubitka pomnožen sa stopom nastanka, odnosno koliko bi organizacija mogla procijeniti gubitak imovine na temelju rizika, prijetnji i ranjivosti. To onda postaje moguće iz financijske perspektive kako bi opravdali troškove za provedbu protumjere za zaštitu imovine.

[42] Humphreys, E., (2011). "Information security management system standards". *Datenschutz und Datensicherheit - DuD*. **35** (1)

3.2. Komponente sigurnosti informacijskih sustava

Unutar komponenti sigurnosti informacijskih sustava uključuju se autentifikacija, enkripcija, kontrolirani pristup i neospornost. Pod autentifikacijom podrazumijeva se utvrđivanje autentičnosti korisnika, poruke, naslovnika i sl. Uloga enkripcije je ta da sam podatak na transportnom mehanizmu predstavlja nečitljivim[43]. Kontrolirani pristup omogućuje pristup zaštićenom okružju isključivo autoriziranim korisnicima. Kontrolirani pristup ne osigurava podatke koje jednom omogućeni pristupnik skuplja i šalje u otpremu. Neospornost u svojoj biti izvodi se odobrenjem digitalnog odnosno elektroničkog potpisa, određuje izvornika potpisanog podatka i jamči autentičnost potpisanog dokumenta. Jedna od najosjetljivijih etapa sigurnosnog sustava predstavlja generiranje i distribuiranje enkripcijskih ključeva na prostorno udaljena mjesta.[44]

Sukladno zahtjevima korisnika i potrebama osigurane infrastrukture, nužno je izabrati najbolji algoritam enkripcije, te kreirati sustav lokalnih master ključeva te otpremanja parova enkripcijskih ključeva. Generirane ključeve nužno je spremiti na lokaciju koja je posve sigurna za njih. Uslijed toga, čista programska rješenja nisu u dovoljnoj mjeri sigurna zbog toga što najmanje jedan korisnik u osiguranom sustavu ima znanje i alate za proboj osiguranog sustava. Za osiguranje financijskog okruženja, svjetski standardi (ITSEC) predviđaju neki nivo osiguranja koji bi trebao biti kreiran tako da korisnik osiguranog okružja posjeduje potpunu kontrolu nad okružjem[45]. Svi događaji trebaju biti evidentirani i osigurani od promjena.

Verzije master ključeva morali bi se limitirati tako da nije moguće izvršiti ponavljanje radnje[46], a prijelomi kriptiranog ključa razdijeljeni su ključarima s ciljem smanjenja mogućnost prekršaja i povećanja sigurnosti. Generirani parovi ključeva za enkripciju ključeva[47] i parova ključeva za izvršenje enkripcije podataka moraju biti raspoređeni tako da ih je nemoguće otkriti odnosno dešifrirati. Kao jedno od rješenja koje se pokazalo najboljim predstavlja korištenje infrastrukture javnog ključa. Kao najviši stupanj povjerenja u poretku autentikacije ovlaštenja predstavlja *Trusted Third Party,* koja predstavlja neovisnu organizaciju koja je u stanju da potpisuje autentičnosti ovlaštenja nižeg stupnja. Tako je svaki od sudionika u stanju provjeriti ispravnost odnosno originalnost ovlaštenja na sigurnosnom stupnju koji upotrebljava u otpremanju ključeva i podataka u svom zaštićenom djelokrugu.[48]

ISO/IEC 27000 je dio rastuće obitelji ISO/IEC standarda informacijskih sustava za upravljanje sigurnošću (ISMS) - ISO/IEC 27000 serije. ISO/IEC 27000 je međunarodni standard pod nazivom: Informacijska tehnologija - Sigurnosne tehnike - Sustavi upravljanja sigurnošću informacija - Pregled i vokabular. Standard je razvijen od strane pododbora 27 (SC27) prvog Zajedničkog tehničkog odbora (JTC1) Međunarodne organizacije za normizaciju i Međunarodne elektrotehničke komisije.

[43] Ne autenticira izvornika niti naslovnika, te ne garantira autentičnost podataka
[44] Kempis, R. D., Ringbeck, J. (1998). "Manufacturing use and abuse of IT", The McKinsey Quarterly, 1998, No.1.
[45] Pristupom, generiranjem i otpremanjem ključeva, prometom na transportnom sustavu.
[46] U pravilu korištenjem mehanizma generatora od slučajnih brojeva kao triger
[47] Distribucija ključeva za deskripciju ključeva za podatke
[48] Kempis, R. D., Ringbeck, J. (1998). "Manufacturing use and abuse of IT", The McKinsey Quarterly, 1998, No.1.

ISO/IEC 27000 omogućuje:

- Pregled i uvod u cijelu ISO/IEC 27000 obitelj standarda informacijskih sustava za upravljanje sigurnošću (ISMS)
- Objašnjenje ili vokabular temeljnih pojmova i definicija koji se koriste u ISO/IEC 27000 obitelji

ISO / IEC 27000 je dostupan putem ITTF web stranice.

PCI DSS (Payment Card Industry Data Security Standard) je standard kojem je cilj osigurati što bolje sigurnosne mjere u kartičnim sustavima i zaštiti krajnjih korisnika u kartičnom plaćanju uključujući Visa, Master Card, American Express, Discover i JCB. PCI standard pod mandatom je brandova kartica i njime upravlja vijeće sigurnosnih standarda za platne kartice. Standard je stvoren da se poveća kontrola podataka na karticama kako bi se smanjile prijevare na kreditnim karticama.

Provjera sukladnosti provodi se jednom godišnje, bilo od strane vanjskog kvalificiranog procjenitelja (*QSA*) ili od strane specifičnog unutarnjeg procjenitelja sigurnosti (ISA) koji pravi izvješće o sukladnosti (ROC) za organizacije koje upravljaju velikim količinama transakcija.

PCI Data Security standard specificira dvanaest zahtjeva za sukladnost, raspoređenih u šest logički povezanih grupa pod nazivom "ciljevi kontrole". Svaka verzija PCI DSS je podijelila ovih dvanaest zahtjeva u nekoliko pod zahtjeva na drugačiji način, ali dvanaest zahtjeva na visokoj razini nisu se promijenili od početka standarda.

Iako PCI DSS mora biti proveden od strane svih subjekata koji obrađuju, pohranjuju ili prenose podatke kartica, formalno priznavanje PCI DSS usklađenosti nije obvezno za sve subjekte. Trenutno i Visa i Master Card zahtijevaju da i trgovci i pružatelji usluga moraju biti potvrđeni u skladu s PCI DSS standardom. Visa nudi alternativni program pod nazivom „Tehnološki inovacijski program“ (TIP) koji omogućuje kvalificiranim trgovcima da prekinu godišnju PCI DSS procjenu valjanosti. Ovi trgovci su kvalificirani ako poduzimaju alternativne mjere protiv krivotvorenja prijevare kao što je korištenje EMV ili od točke do točke šifriranja (P2PE) tehnologiju, no od njih se i dalje traži da budu podređeni PCI DSS-u. Manji trgovci i pružatelji usluga ne moraju izričito potvrditi sukladnost sa svakom od kontrola propisanih PCI DSS iako ove organizacije još uvijek moraju provesti sve kontrole kako bi se održala sigurna luke i izbjegla potencijalnu odgovornost u slučaju prijevare povezane s krađom podataka kartice.[49]

Banke koje izdaju kartice ne moraju proći kroz PCI DSS validaciju, iako oni još uvijek moraju osigurati osjetljive podatke na kompatibilan način putem PCI DSS. Banke moraju biti u skladu s PCI DSS, kao i da se njihova usklađenost potvrdi pomoću revizije. U slučaju povrede sigurnosti, bilo koji ugroženi entitet koji nije PCI DSS sukladan u vrijeme povrede će biti predmet dodatnih kazni povezanih s karticama, kao što su novčane kazne.

[49] Humphreys, E., (2011). "Information security management system standards". *Datenschutz und Datensicherheit - DuD*. **35** (1)

Dok su PCI DSS standardi vrlo eksplicitni kada su u pitanju uvjeti za krajnju pohranu i pristup KBS (Card Holder podacima), vijeće standarda sigurnosti platnih kartica reklo je vrlo malo o prikupljanju tih podataka na prednjem kraju, bilo kroz web, interaktivne govorne sustave ili agente call centara. To je iznenađujuće, s obzirom na visoku potencijal opasnosti za prijevare s kreditnim karticama i kompromisa koje predstavljaju call centri.[50]

U pozivnom centru, kupci čitaju njihove podatke s kreditne kartice, CVV kod i datum isteka agentima pozivnih centara. Postoji nekoliko kontrola koje sprečavaju snimanje (prijevare s kreditnim karticama) te podatke s uređajem za snimanje ili računalom ili prepisivanjem na papirić. Štoviše, gotovo svi pozivni centri implementiraju nekakav softver za snimanje poziva, koji prikuplja i pohranjuje sve ove osjetljive podatke potrošača. Ove snimke su dostupne mnoštvu osoblja pozivnog centra, često nekodirane, a uglavnom ne spadaju pod PCI DSS standard koji smo naveli. Telefonski agenti koji su smješteni kod kuće predstavljaju dodatnu razinu izazova, zahtijevajući off tvrtke da osiguraju kanal od kućnog agenta putem pozivnog centra do hub-a, prodavača aplikacija.[51]

SANS Institut (službeno Escal Institute of Advanced Technologies) je privatna tvrtka u USA osnovana 1989. godine koja je specijalizirana za informacijsku sigurnost i cybersecurity treninge. Teme koje se nalaze na raspolaganju za trening uključuju cyber i mrežnu obranu, ispitivanje penetracije, odgovor u slučaju incidenta, digitalnu forenziku i revizije. Tečajevi o sigurnosti informacija su razvijeni kroz proces konsenzusa koji uključuje administratora, menadžera sigurnosti i profesionalaca informacijske sigurnosti. Tečajevi pokrivaju sigurnosne osnove i tehničke aspekte informacijske sigurnosti. Institut je poznat po svojim programima obuke i programima certificiranja. SANS se zalaže za reviziju, mreže i sigurnost.

COBIT (kontrolni ciljevi za informacije i srodne tehnologije) je dobar okvir prakse izrađen od strane međunarodnog strukovnog udruženja ISACA za informacijske tehnologije upravljanje i IT upravljanja. COBIT pruža provedive setove kontrola nad informacijskim tehnologijama, te ih organizira oko logičkog okvira povezanih procesa i aktivatora informacijskih tehnologija.

Poslovna orijentacija COBIT-a sastoji se od povezivanja poslovnih ciljeva do ciljeva informacijskih tehnologija, pružajući metrike i modele zrelosti za mjerenje postignuća, te identificiranje povezane odgovornosti poslovnih i procesa vlasnika informacijskih tehnologija.[52]

Procesni fokus COBIT-a je prikazan modelom procesa koja ga dijeli na četiri područja (u planiranje i organizacija, stjecanje i primjena, dostava i podrška, te praćenje i procjena) i 34 procesne stavke s odgovornošću na područjima planiranja, izrade, pokretanja i praćenja. Nalazi se na visokoj razini i usklađen je s drugim, detaljnijim standardima informacijskih tehnologija i dobrim praksama, kao što su COSO, ITIL, BISL, ISO 27000, CMMI, TOGAF i PMBOK. COBIT djeluje kao integrator tih različitih materijala za navođenje, sumirajući ključne ciljeve pod jedan kišobran koje povezuju modele dobre prakse u upravljanju i poslovnim zahtjevima.

[50] Jo, H., Kim, S., Won, D., (2011). "Advanced information security management evaluation system". *KSII Transactions on Internet and Information Systems*. **5**(6)

[51] Jo, H., Kim, S., Won, D., (2011). "Advanced information security management evaluation system". *KSII Transactions on Internet and Information Systems*. **5**(6)

[52] Cabinet Office. (2004). overview of the Act. In: Civil Contingencies Secretariat Civil Contingencies Act 2004: a short. London: Civil Contingencies Secretariat

COBIT 5 dodatno je učvrstio i integrirao COBIT 4.1, Val IT 2.0 i izvukao iz okvira ISACA IT Assurance (ITAF) i poslovni model za informacijske sigurnosti (BMIS).

Okvir i njegovi dijelovi mogu, prilikom dobre uporabe, također pridonositi osiguravanju propisa. To može potaknuti umanjeno rasipanje upravljanja informacijama, poboljšati zadržavanje rasporeda, povećati poslovnu agilnost i niže troškove, a biti bolje u skladu sa zadržavanjem podataka i pravilima o upravljanju.

COBIT komponente uključuju:[53]

Okvir: organizira ciljeve upravljanja i dobre prakse putem domena i procesa informacijskih tehnologija i povezuje ih s poslovnim zahtjevima.

Procesni opis: referentni model procesa i zajednički jezik za sve u organizaciji.

Kontrolni ciljevi: pruža potpuni skup zahtjeva visoke razine koji razmatra uprava za učinkovitu kontrolu svakog procesa informacijske tehnologije.

Smjernice za upravljanje: pomaže dodijeliti odgovornost, dogovor o ciljevima, mjerenje performansi ilustriraju uzajamnom odnosu s drugim procesima.

Modeli: procjenjuje zrelost i sposobnost za proces i pomaže u rješavanju nedostataka.

3.3. Komunikacija u svrhu sigurnosti

Komunikacija u svrhu sigurnosti može se podijeliti na: informatički djelokrug, telefonski sustav, program i prijenos funkcija kontrola. Elementi koje treba poštivati u sklopu informatičkog mrežnog djelokruga su ispitivanje ranjivosti mrežne infrastrukture i Qualys Guard Express solucije.[54]

Pod informatičkim okruženjem podrazumijeva se:[55]

- Kreiranje sigurnosno-sustavnih načina
- Kontroliranje prometa i firewall
- Kreiranje mrežnih veza
- Enkripcija
- Odabir načina odnosno enkripcijskog metoda
- Različite varijante enkripcije
- Računalna (dial up) veza
- Preuzimanje podataka s poslužitelja

[53] Cabinet Office. (2004). overview of the Act. In: Civil Contingencies Secretariat Civil Contingencies Act 2004: a short. London: Civil Contingencies Secretariat

[54] Brumec, J. (1996). Projektiranje i metodika razvoja informacijskog sustava, Euro Data, Zagreb, 1996.

[55] Pintar, D. (2009). Model uslužno orijentirane arhitekture za stvarno vremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva., str. 211-214.

Pod telefonskim sustavima podrazumijevaju se:[56]

- Sustavi e-pošte
- Standardi telekomunikacija
- Internet veze
- Intranet ispravke
- Extranet ispravke
- Sustavi elektroničkog naplaćivanja i financijskog poslovanja.

Program i prijenos kontrolnih funkcija objedinjuju:[57]

- Računalni virusi
- Tijek izrade
- Tijek razmjene funkcija kontrole
- Sudjelovanje trećih strana u kreiranju sustava
- Računalne radnje.

Segmenti koje bi trebalo poštivati u sklopu informatičkog mrežnog sustava su:[58]

- Instaliranje komponenti koje odgovaraju potrebama i politici sigurnosti
- Prilagođavanje informatičkih mrežnih sustava
- Određivanje poslužitelja
- Spajanje ovlasti u podjeli potencijala
- Određivanja točaka pristupa
- Određivanje komunikacijskih postulata
  - dijeljenje identificiranja i autoriziranje s pristupnicima
  - vođenje i monitoring akreditivnih pristupnika
  - sporedne metode u slučaju nužde
  - podatkovno kriptiranje na prijevoznom sustavu
- Određivanje elemenata firewalla
- Nadziranje mreže, ažuriranje SW/FW u skladu s prijedlozima proizvođača
- Kontroliranje ulaza i izlaza
- Protekcija
  - radna postaja, pristup
  - mreža, podjela potencijala
  - poslužitelji, autentifikacija
  - poslužitelji, kriptiranje podataka unutar baze
  - firewall, određivanje odobrenja u prometu
  - router, odobrenja, pristupna lozinka i sl.
- Ispitivanje osjetljivosti mrežne infrastrukture
- Analiziranje rezultata i posao na provođenju predloženih radnji

[56] Pintar, D. (2009). Model uslužno orjentirane arhitekture za stvarnovremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva., str. 211-214.
[57] Pintar, D. (2009). Model uslužno orjentirane arhitekture za stvarnovremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva., str. 211-214.
[58] Pintar, D. (2009). Model uslužno orjentirane arhitekture za stvarnovremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva., str. 211-214.

- Ponovno ispitivanje ranjivosti
- Ispitivanje probojnosti odnosno etičko hakiranje

Kada se govori o ispitivanju ranjivosti mrežne infrastrukture situacija je sljedeća. Pod tezom da se radi o mreži koja je uobličena[59], kao prvi potez u manevriranju mrežnom infrastrukturom, nužno je potvrditi sigurnosni status mrežnog djelokruga. Postoji nekolicina proizvođača softverske opreme koja pruža otkrivanje sigurnosnih mrežnih propusta uz nuđenje adekvatnih rješenja. Kao vodećeg proizvođača u tom području može se izdvojiti tvrtka Qualys, koja je sa svojim proizvodima poznata s ispitnim alatom kod značajnog broja PCI revizora.[60] Qualys Guard Express solucija predstavlja sustav za tzv "*on demand vulnerabillity management*" odličan za potrebe mrežnog okruženja informacijskih tehnologija, upotrebljiv korištenjem običnog, odnosno grafičkog sučelja. Qualys Guard Express solucija sustav je koji je odabrao plinski operater za potrebe svog umreženog sustava.

3.4. Primjeri prijetnji po informacijski sustav

Informacijska sigurnost vrlo je važna dok sa s raznih strana nalaze eventualne opasnosti po njega. Sigurnost informacijskih sustava može se narušiti na razne načine. Ključnu podjelu prijetnji koje mogu narušiti sigurnost sustava dijele se na one koji dolaze izvana, one koji se nalaze unutra i one koji djeluju u kombinaciji unutarnjih i vanjskih. Opće je poznata činjenica da su ljudski potencijali poduzeća odnosno tvrtke najveća prijetnja informacijske sigurnosti. Oni ugrožavaju informacijske potencijale bilo slučajnim pogreškama ili namjernim nastojanjima zabranjenih aktivnosti. Sukladno podacima Instituta za nacionalnu sigurnost[61] skoro 3/4 sigurnosnih prekršaja događa se "interno". Iako rijetki, no napadi koji uglavnom uzrokuju najveće posljedice predstavljaju napade koji dolaze "izvana" odnosno eksterno. Oni sudjeluju u značajno malom omjeru, a namjera im je doći do informacija, mijenjanje informacija ili njihovo uništenje. Sustav se od takvih napada štiti kontroliranjem prometa s interneta sukladno sustavu i kontra, putem onemogućenja instaliranja programa u operacijski sustav ili izvršenjem kriptiranja podataka. Implementiranjem ovakvih mjera u informacijskim sustavima poboljšava se njegova razina sigurnosti, a mogućnost izvršenja opasnih radnji svodi se na najnižu moguću razinu.[62]

3.4.1. Prijetnja po sigurnost informacijskog sustava

Prijetnja predstavlja mogućnost izvorišta prijetnje da se okoristi nekom ranjivošću odnosno slabošću sustava[63]. Izvor prijetnje predstavlja namjeru i način koji je usmjeren ka iskorištenju ranjivosti odnosno slabosti ili priliku i metodu odnosno način koji slučajno može aktivirati određenu slabost odnosno ranjivost. Sam izvor prijetnje ne predstavlja opasnost ako ne postoji ranjivosti koja može biti iskorištena. Kako bi se utvrdila mogućnost određene prijetnje treba se uzeti u obzir samo izvorište prijetnje, moguće ranjivosti i aktualne kontrole odnosno zaštite. Prijetnje se mogu grupirati u one prijetnje koje dolaze od osoba a to su ustvari namjerne prijetnje, te prijetnje od osoba koje mogu biti nenamjerne prijetnje i na koncu

[59] Postavljeni su mreni elementi, osigurani komunikacijski i pristupni putovi, definirana pravila itd
[60] Jurison, J. (1995). "The Role of Risk and Return in Information Technology Outsourcing Decisions, Journal of Information Technology", 1995, 10.
[61] National Security Institute, SAD
[62] Gugić A. (2014). Poslovne sigurnosne politike i procedure; predavanje Veleučilište Marko Marulić, Knin.
[63] Slučajnim aktiviranjem ili namjernom eksploatacijom

prirodne nesreće te prijetnje koje dolaze od slabo zaštićene i kvalitetne opreme.[64] Primjer koji će se kasnije opisivati u radu plod je ljudske nemarnosti i nepažnje koja spada u grupu nenamjernih prijetnji.

Namjerne prijetnje mogu se realizirati kroz sljedeće aktivnosti:[65]

- Aktivnosti zavaravanja
- Aktivnosti pregleda
- Aktivnosti prisluškivanja
- Aktivnosti čišćenja
- Kroz neželjenu e-poštu
- Kroz preusmjeravanje

I pored toga što mnogi vjeruju da prijetnje sigurnosti sustava uglavnom dolaze eksterno (van tvrtke), istraživanja koja su izvršena, a potom i objavljena u knjizi "Computer Crime A Crimefighter's Handbook", O'Reilly & Associates ukazuju na skroz suprotne faktore. U tim rezultatima pokazano je da najvećim postotkom probleme sigurnosti uzrokuju greške ljudske prirode. One se uglavnom događaju uslijed nedovoljne pažnje i obuke radnika. Također, veliki uzrok grešaka u sustavima predstavlja kvar opreme, slijede radnici koji svoj položaj u poduzeću koriste za osobnu korist i radnici koji na ovaj način izražavaju vlastito nezadovoljstvo prema tvrtki ili primjerice nadređenome u toj tvrtki.

S ciljem sprječavanja mogućnosti izvršenja ovakvih neželjenih događaja plinski operater implementirao je konkretne mjere i protokole rada. Mjerama kao što je obuka radnika snižava se mogućnost njihove pogreške kojima bi mogli narušiti sigurnost informacijskih sustava.[66] Smještanjem opreme na kojima se pohranjuju podaci u poseban prostor, propisima putem kojih se vrši određivanje tko ima pravo pristupa istoj, kontroliranjem uvjeta u takvoj prostoriji poput temperature i vlage, omogućuje se duži životni vijek opremi a tako i sigurniji rad samoga sustava. Implementiranje kontroliranog pristupa podacima i određivanjem kazni onim korisnicima koji se ne pridržavaju unaprijed utvrđenih načela minimizira se zlouporaba sustava od strane radnika u poduzeću. Kako bi se realizirala krajnja sigurnost sustava nužno je obratiti pozornost na:[67]

- Fizički aspekt sigurnosti
- Mjere sigurnosti za zaposlene
- Komunikacijsku sigurnost
- Sigurnost u pogledu radnji

Osnova fizičke sigurnosti predstavlja zaštitu fizičkog dijela informacijske infrastrukture, postrojenja u kojima je ona postavljena, uređaja za spremanje podataka i opreme u svrhu komunikacija. Mjere fizičke sigurnosti uključuju sve mjere koje služe za obranu a koje su

[64] Bubić V., Šmidl, I. (2008). Risk Managment of Working Capital Requirements, CECIIS 2008 Proceedings, Faculty of Organization and Informatics, Varaždin, 2008.
[65] Pintar, D. (2009). Model uslužno orjentirane arhitekture za stvarnovremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva., str. 31-32.
[66] Campbell. K. et al. (2003). "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," J. Computer Security, vol. 11, no. 3, 2003
[67] Pintar, D. (2009). Model uslužno orjentirane arhitekture za stvarnovremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva., str 35-37.

poduzete s ciljem zaštite kompjutorske infrastrukture od prirodnih nesreća, poteškoća u okolini, incidenata i namjernih propusta. Fizičku sigurnost sustava mogu narušiti prirodne nesreće poput poplava, udara munje odnosno potresa, prijetnje iz djelokruga kao što je zagrijavanje, hladnoća ili strujni udari, na posljetku korisnici odnosno radnici na sustavu ili osobe koje nemaju pravo na pristup sustavu. Prirodne nesreće u stanju su imati ogroman utjecaj po sigurnost informacijskih sustava. Računalna oprema vrlo je osjetljiva na dim, prašinu, vlagu i sl, te ako ne egzistira potrebni nivo zaštite pri njihovom djelovanju može se desiti da se sustav uništi, a tako i podaci mogu nestati. Električna energija predstavlja prijetnju koja može ugroziti bilo koji informacijski sustav. Računalna je infrastruktura slaba na promjene napona električne energije. U trenutcima neadekvatne pokrivenosti električnom energijom može se javiti oštećenje sustava ili cjelokupno brisanje podataka. Elektronička oprema vrlo je slaba i na temperaturu pri uvjetima u kojima djeluje, te je nužno vršiti kontrolu temperature i vlažnosti zraka u sobama u kojima je oprema smještena. Kako bi se postigla adekvatna fizička sigurnost s obzirom na opasno djelovanje osoba, kružni pristup računalnoj opremi jedna je od osnovnih faza koja je predmet razmatranja.[68] Najveće prijetnje informacijskim sustavima predstavljaju osobe odnosno ljudi, Tablica 4. koji s njim rade, putem redovnog rada ili putem povremenog održavanja. Neke osobe (radno osoblje) nisu dovoljno obučene za neki posao te se može javiti da takav radnik u poduzeću nenamjerno uništi podatke te tako ugrozi informacijski sustav. Ugrožavanje sustava također je moguće putem namjernog djelovanja radnika na sustavu. Svako poduzeće mora se oslanjati na snažne i pouzdane sigurnosne mjere za osoblje, te je tako veoma važno uz punu pažnju izvršiti odabir zaposlenika, što podrazumijeva da se u obzir trebaju uzimati i najsitniji segmenti.[69] Promatranjem radnji unutar poduzeća i izvan njega, moguće je na vrijeme spriječiti moguće opasnosti i poboljšati mjere sigurnosti. Poduzeće koje ima problema sa svojim radnicima može vrlo lako postati metom napada radnika ili osoba izvan poduzeća koji će se eventualno solidarizirati s radnikom.

Komunikacija između računala dovodi do povećanja snage sustava, brzine procesiranja podataka, dostupnosti, ali što se više putem računala vrši komunikacija s drugim računalima to uvjetuje kreiranju značajnih rizika poslovnom procesu, a time i osjetljivosti sustava. Komunikacija mrežom može se postići sigurnijom i opreznijom kontrolom pristupanja, kriptiranjem podataka, tehničkom protekcijom i sigurnosnim radnjama te drugim mjerama fizičke sigurnosti. Kontrola pristupa važan je faktor u realiziranju sigurnosti informacijskog sustava unutar mrežnog okružja. Mnogi informacijski sustavi rabe šifre u pogledu osiguranja kontroliranog pristupa, svatko tko zna točnu šifru posjeduje dozvoljen pristup informacijskom sustavu.[70]

Logička sigurnost obuhvaća dva standardna faktora sigurnosti informacijskih sustava. Prvi standard se odnosi na uvećanje svijesti sigurnosne kulture i samozaštite među mogućim žrtvama. Drugi standard čini načini na koji se računalni prijestupnici mogu onemogućiti u počinjenju prekršaja. Povećanje svijesti postiže tako da kad god je to moguće radnici budu uključeni u program sigurnosti te ih po potrebi obučavati na koji način je sigurnosti zaprijećeno i kako svi vrše podjelu rizika i odgovornosti.

[68] Kempis, R. D., Ringbeck, J. (1998). "Manufacturing use and abuse of IT", The McKinsey Quarterly, 1998, No.1.
[69] Kotler, P., Lee, N. (2009). „Društveno odgovorno ponašanje", MEP CONSULT, Zagreb, 2009.
[70] Battles, B. E., Mark, D., Ryan, C. (1996). "An Open Letter to CEOs: How Otherwise Good Managers Spend Too Much on Information Technology", The McKinsey Quarterly, 1996, No. 3.

Poslovna sigurnost uvjetovana je informacijskim sustavima u ogromnoj mjeri tako da ne postoji mogućnost realizirati bilo koji format sigurnosti ili nivo usklađenosti poslovanja bez informacijskih sustava. Bez informacijskih sustava nisu zamislivi sigurnosni integrirani modeli, bez kojih ne postoji uspješno poslovanje. Sigurnosti informacijskih sustava pridajemo značaj kroz planiranje i provođenje, prije nego se dogodi izvanredno stanje. Nužno je oblikovati učinkovit dijagnostički sustav koji će alarmirati na sve eventualne komunikacijske tokove s ciljem da se na vrijeme vidi eventualna sigurnosna opasnost.[71]

Tablica 4. Prijetnje koje prouzrokuju osobe

Izvori prijetnji	Motiv	Akcije
Hakerski napad	• **Izazov** • **Ego** • **Pobuna**	• **Hakiranje** • **Socijalni inženjering** • **Upad sustav** • **Neautoriziran pristup sustavu**
Računalni kriminal	• **Uništenje informacija** • **Ilegalno otkrivanje podataka** • **Novčani dobitak** • **Ilegalna izmjena podataka**	• **Kompjuterski kriminal** • **Neovlaštene radnje** • **Podmetanje informacija**
Teroristi	• **Uništavanje informacija** • **Ucjene, izrabljivanje** • **Osveta**	• **Bombaški napadi** • **Rat informacijama** • **Probijanje u sustav** • **Uplitanje u sustav**
Poslovna špijunaža	• **Prednost u poslovanju** • **Ekonomska špijunaža** • **Korist**	• **Ekonomsko iskorištavanje** • **Krađa informacija** • **Upad u privatnost** • **Neautorizirani upad u sustav**
Insiders	• **Radoznalost** • **Ego** • **Snalažljivost** • **Osveta** • **Novac**	• **Napad na djelatnike, ucjena** • **Brisanje podataka** • **Prijevare i krađe** • **Presretanje** • **Sabotaža**

Izvor:http://www.veleri.hr/files/datoteke/nastavni_materijali/k_sigurnost_s2/sigurnost_informacijskih_ sustava.pdf (pristupljeno: 30.03.2016.)[72]

3.4.2. Slabosti informacijskih sustava

Ranjivost odnosno slabost predstavlja nedostatak u sigurnosnim pogledima sustava, primjeni ili internim kontrolama koja se može realizirati i rezultirati povredom sigurnosti ili

[71] Tuđman, M. (2008). „Informacijsko ratište i informacijska znanost“, Zagreb, 2008.

[72] Izvor:http://www.veleri.hr/files/datoteke/nastavni_materijali/k_sigurnost_s2/sigurnost_informacijskih_ sustava.pdf (pristupljeno: 30.03.2016.)

ugrožavanjem politike sigurnosti. Podaci o tehničkim i drugim (netehničkim) ranjivostima sustava mogu se pribavljati na više načina:[73]

- Kroz anketni upitnik stručnjaci iz segmenta sigurnosti mogu kreirati anketu koju treba dodijeliti odgovarajućim radnicima koji su u dodiru s tehničkim i netehničkim komponentama sustava koji je predmet ispitivanja
- Kroz intervju intervjuiranje odgovarajućih radnika u sklopu sektora organizacije pruža pomoć pribavljanju informacija o fizičkoj i operacijskoj komponenti informacijskih sustava
- Kroz pregledavanje dokumenata pregled politika sigurnosti, sustavske dokumentacije i drugih dokumenta koji se odnose na sigurnost može pružiti uvid u kontrole sigurnosti i pomoći pri uočavanju slabosti
- Uporaba alata za pregled sustava

Kod plinskog operatera iskustvo na terenu najbitnija je za detektiranje slabosti poslovnog informacijskog sustava. Proaktivne tehničke metode pružaju kvalitetan uvid o sustavu i veoma su učinkovite u pribavljanju podataka o osjetljivostima sustava. Najzastupljenije metode predstavljaju penetracijska ispitivanja[74], ST&E[75] i alati koji imaju automatizirane sustave za otkrivanje slabosti. Učestali pregled web stranica na kojima se objavljuju uočene slabosti, zakrpe[76], uslužni paketi[77] i sl. pružaju uvid u trenutne slabosti. Ako informacijski sustav još nije kreiran traganje za ranjivostima trebala bi se usmjeriti na organizacijsko-sigurnosnu politiku, utvrđene sigurnosne etape i sustavske sigurnosne zahtjeve.

3.4.3. Procjena rizika

Zahtjevi za sigurnošću identificiraju se putem metodičke procjene sigurnosnih rizika. Proširenje sigurnosnih kontrola treba biti jednako šteti koju propusti sigurnosti nanose poduzeću. Rezultati procjene rizika pružaju pomoć u određivanju prioriteta i adekvatnih akcija kod upravljanja rizicima. Procjena rizika treba se realizirati u razdobljima s ciljem da se u procjenu uvedu bilo koja vrsta promjena koje bi mogle utjecati na rizik. Bez jasne analize ranjivosti, skoro nije moguće jasno izvršiti definiranje sigurnosnog rizika.[78]

Više metoda egzistira koje idu u smjeru procjenjivanja rizika. Korisno je izabrati metodu koja pruža rezultate koji se ponavljaju. Postoji mogućnost da se odabere neka od metoda koju pružaju adekvatni alati. Pri tome je važno paziti da je alat ispravno instaliran i konfiguriran. Pri odabiru metodologije za procjenu rizika nužno je utvrditi ljestvicu za izbor odnosno mjerenje rizika. Ljestvica može biti realizirana na više načina. Korisno je da skala posjeduje barem nekoliko vrijednosti. Ako egzistiraju samo tri vrijednosti, postoji opasnost da se većini potencijala dodijeli srednja vrijednost, a tako se gubi na ispravnosti rezultata procjene.

[73] Brumec, J. (1996). Projektiranje i metodika razvoja informacijskog sustava, Euro Data, Zagreb, 1996.m str. 37-45.
[74] engl. penetration testing
[75] engl. Security Test & Evaluation
[76] engl. patch
[77] engl. service packs
[78] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5.

Metodologiju sačinjavaju sljedeće aktivnosti:[79]

- Aktivnosti pripreme
- Aktivnosti procjenjivanja opasnosti i osjetljivosti sustava
- Aktivnosti procjene rizika
- Aktivnosti izračuna rizika koji je preostao

Mogućnost lošeg događaja prikazuje se indeksom koji posjeduje vrijednosti od 1 do 5 te bi ih trebalo promatrati u definiranim vremenskim razdobljima. Mogućnosti su svedene na ponavljanje događaja u tijeku jedne godine. Indeks mogućnosti odnosno vjerojatnosti može se procijeniti izravnom procjenom mogućnosti određenog događaja ili putem procjene dodatnih parametara koji utječu na mogućnost pojave događaja. Za definiranje indeksa mogućnosti kroz dodatne mjere uzimaju se četiri čimbenika koji utječu na mogućnost događaja, a kao indeks mogućnosti odnosno vjerojatnosti uzima se njihova srednja (aritmetička) vrijednost ili najveća zasebna vrijednost.[80] Što su manji zahtjevi za potencijalima koji su potrebni za iskorištavanje osjetljivosti sustava, to je i veća mogućnost da će netko nastojati iskoristiti navedenu slabost. Nužni potencijali mogu biti jaka računalna infrastruktura za upad i prijelaz preko enkripcijskih ključeva, specijalna komunikacijska oprema za praćenje informacijske linije ili programski alati za detekciju zaporke.[81] Poslije identificiranja sigurnosnih zahtjeva i izvršene procjene rizika, nužno je odabrati i provesti jasne kontrole kako bi se rizik sveo na odgovarajući nivo. Izbor kontrole isključivo ovisi o poduzeću, ali također i o državnim i međunarodnim načelima, pravima i obvezama. Kontrole koje u stvarnosti pokazuju zadovoljavajuće rezultate kod primijene informacijske sigurnosti predstavljaju kontrole:[82]

- Politike sigurnosti
- Podjele odgovornosti sigurnosti informacija
- Svijest o informacijske sigurnosti, obrazovanje i obuka
- Točno procesiranje podataka u programima
- Upravljanje osjetljivostima
- Upravljanje poslovnom dosljednošću
- Upravljanje sigurnosnim propustima i unaprjeđenjem sustava

3.4.3.1. Upravljanje rizicima informacijskih sustava

Upravljanje rizicima informacijskih sustava temelji se na uočavanju i razumijevanju poslovnih rizika koji su se javili kao rezultat slabosti i slabe zaštite informacijskih sustava. Poslovna sigurnost podržanog informacijskog sustava u izravnoj je vezi s ispravnim procjenama rizika koji se javljaju iz korištenja informacijskih sustava. Analiza rizika posjeduje zadatak koji treba pružiti odgovore na to:[83]

[79] Jurison, J. (1995). "The Role of Risk and Return in Information Technology Outsourcing Decisions, Journal of Information Technology", 1995, 10. , str 54.
[80] 1. Vještine i znanja 2. Jednostavnost pristupa 3. Motivacija 4.
[81] Clark, T. D., Zmud, R. W., McCray, G. E. (1995). "The Outsourcing of Information Services: Transforming the Nature of Business in the Information Industry", Journal of Information Technology,1995., 10.
[82] Bubić V., Šmidl, I. (2008). Risk Managment of Working Capital Requirements, CECIIS 2008 Proceedings, Faculty of Organization and Informatics, Varaždin, 2008., str 64.
[83] Bysinger, B., Knight, K. (1996). "Investing in Information Technology", Van Nostrand Reinhold, 1996., str. 132.

- Što bi se moglo dogoditi?
- Ako se propust dogodi kakve će posljedice uslijediti?
- Koliko je moguće da će se propust dogoditi?

Upravljanje rizicima informacijskih sustava objedinjuje zaštitu potencijala odnosno resursa i smanjenje eventualnih gubitaka od sljedećih primarnih opasnosti: prirodnih nesreća, grešaka osoblja te namjernog počinjenja štete. Ogroman je raspon eventualnih štetnih posljedica, od uklanjanja određenog podatka do cjelovitog uništenja računalnog središta, od nemarnog postupka radnika do komplicirane, namjeravane akcije špijuniranja ili sabotiranja. Uvećavanje poslovne učinkovitosti, a tako i kompliciranosti sigurnosnih prilika, uvećava konstantan trend porasta kriminalnih aktivnosti čiji su cilj informacijski sustavi. Dodatni čimbenici koji utječu na povećanje rizika predstavljaju razvoj informacijskih sustava, laka pristupačnost jeftinoj računalnoj opremi i ogromni broj korisnika javnih mreža kojima su dostupni alati za upad i prelazak zaštitnih umreženih računalnih sustava. Namjera analize rizika predstavlja procjenu rizika u segmentu informacijskih sustava i njegovog djelokruga, putem analize mogućih opasnosti i identificiranja slabosti, s ciljem izbora mjere zaštite za eventualne propuste odnosno incidente.[84] Analiza rizika predstavlja kompliciran postupak koji pruža popis rizika evaluiranih po određenim svojstvima odnosno karakteristikama. Na osnovu prepoznatih rizika moguće je poduzeti akcije za smanjenje rizika i eliminiranje mogućih opasnosti za poslovni proces. Kreiranjem mjera zaštite, rizici se mogu umanjiti do razumne i ne toliko opasne razine. Sigurnost informacijskih sustava podrazumijeva, uočavanje, kvantifikaciju i redoslijed odnosno, stupanj ugroženosti informacijskih sustava kako bi se izabrale adekvatne zaštitne mjere, čijom se primjenom minimizira rizik od opasnih događaja na razumnu odnosno odgovarajuću razinu. Ispravno upravljanje potencijalima informacijskih sustava predstavlja uvjet uspješne uporabe sustava za potporu poslovnim procesima.

U potencijale informacijskog sustava uključuju se:

- Fizički potencijali poput hardvera i oprema
- Podaci poput dokumenata
- Softver
- Radna snaga

Potencijali posjeduju vrijednost za poduzeće i nužno ih je osigurati, kao što treba osigurati odnosno zaštititi i svu drugu imovinu u poduzeću. Za izbor i primjenu mjera zaštite nužno je uočiti potencijale informacijskih sustava. Nivo detalja popisa potencijala treba biti usklađen s namjerama zaštite. Rizik je resurs da će se neka prijetnja ostvariti i pokrenuti događaj koji je u stanju izazvati loše posljedice. Zbivanje rizika opisuje način na koji neka prijetnja ili skupina prijetnji može rezultirati incidentom i kakvo će biti djelovanje na sustav. Svaka promjena u informacijskom sustavu ili njegovoj okolini može imati utjecaja na nivo rizika. Na taj način, rana detekcija ili spoznaja o promjeni u sustavu ili okruženju, uvećava mogućnost pravovremene i odgovarajuće akcije s namjerom umanjenja odnosno minimiziranja rizika. Mjere zaštite čine organizacijske korake odnosno akciju ili metode koji su u stanju sustav štititi od opasnosti, minimizirati njegovu osjetljivost, ograničiti radnje opasnih radnji, detektirati sigurnosne propuste i popraviti njegove potencijale. Kvalitetna zaštita uglavnom zahtjeva spregu više zaštitnih mjera.

[84] Dvorak, R. E., Hollen, E., Mark, D., Meehan, W. F. (1996). "Six Principles of High-Performance IT", The McKinsey Quarterly, 1997, No. 3.

Generalno, mjere protekcije izvršavaju neke od radnji poput:[85]

- Prevencije od štetnih prilika
- Obrane od opasnih prilika
- Pronalaženja opasnih događaja
- Popravke štete koja je uslijedila uslijed štetnih događaja
- Obnove potencijala poslije realizacije štetnih posljedica
- Monitoring nad procesom
- Alarmiranje

Izbor prikladnih mjera zaštite od ogromnog su značaja za njihovu ispravnu primjenu. Mnoge od njih u stanju su pokrivati mnogo segmenata istovremeno. Često je bolje odabrati mjere koje će djelovati u više segmenata u isto vrijeme. Neki od primjera tih mjera zaštite odnosno sigurnosti su:[86]

- Sustavi kontroliranog prava pristupa
- Anti-virusni program
- Enkripcija podataka
- Elektronički potpis
- Vatreni zid
- Sustavi za nadziranje i analiziranje

Poslije vrednovanja i izbora koraka zaštite predstoji njihova primjena, što obuhvaća nabavu i instaliranje sigurnosnih mjera, određivanje pravila i koraka za uporabu, educiranje osoblja i ispitivanje. Povremena educiranja rabe se za ispitivanje koraka i dobivanje povratnih informacija o kvaliteti i manama usvojenih mjera.[87]

3.5. Organizacija informacijske sigurnosti i uloga vođe

3.5.1. Osnovni ciljevi organiziranja informacijskih sustava sigurnosti

Na najvišem nivou upravljanja u nekoj tvrtki imenuje se specijalni odbor koji će odobriti politiku informacijske sigurnosti, pripisati uloge u tijeku zaštite i upravljati implementacijom zaštite u tvrtki. Kako bi se održao tempo s aktualnim stanjem, te se osiguralo praćenje standarda i metoda procjenjivanja sigurnosti kao ispravno djelovalo na propuste nužno je utemeljiti organizacijski i upravljački spektar kroz propise o informacijske sigurnosti.

Na ovaj način se postiže multidisciplinirani pristup osiguranja kroz suradnju djelatnika u poduzeću, korisnika i osoblja za sigurnost kao i stručnjaka za segmente poput upravljanja kvalitetom i sigurnosnim rizikom.[88] Naredni značajan cilj je osiguranje zaštite sustava za procesuiranje informacijama i zaštite informacija koje su dostupne zainteresiranim stranama.

[85] Dempsey, J. (1998). Dvorak, R. E., Holen, E., Mark, D., Meehan, W. F. III: "A hard and soft look at IT investment", The Mc KinseyQuarterly, 1998, No. 1., str. 34.
[86] Dempsey, J. (1998). Dvorak, R. E., Holen, E., Mark, D., Meehan, W. F. III: "A hard and soft look at IT investment", The Mc KinseyQuarterly, 1998, No. 1., str. 35.
[87] Gugić A. (2014). Poslovne sigurnosne politike i procedure; predavanje Veleučilište Marko Marulić, Knin.
[88] Kempis, R. D., Ringbeck, J. (1998). "Manufacturing use and abuse of IT", The McKinsey Quarterly, 1998, No.1.

Pristup poslovnih partnera informacijskim resursima nužno je kontrolirati putem provjera i procjena sigurnosnog rizika s ciljem evidentiranja eventualnih posljedica po sigurnost. Ugovori koji određuju pristup poslovnog partnera informacijskim resursima trebaju regulirati i pitanje pristupanja drugih sudionika koje je uveo poslovni suradnik. Posljednji cilj odnosi se na očuvanje informacijske sigurnosti u prilikama kada se odgovornost za procesiranje podataka transferira na eksternog partnera. Ugovori s eksternim dobavljačima usluga obrade podataka moraju obuhvaćati rizike, sigurnosne mjere i segmente zaštite koje se odnose na informacijske sustave, mreže i sl.

3.5.2. Opća organizacija modela zaštite informacijskih sustava

Model je prilagođen s organizacijskom strukturom poduzeća odnosno poslovne organizacije kao i primarnim postulatima koji su navedeni u politici informacijske sigurnosti. Funkcije zaštite informacijskog sustava izvršavaju se putem više organizacijskih struktura odnosno koncepata. Na osnovu skupine poslova i odgovornosti postoje sljedeće grupe:[89]

- Stručna tijela i nadzor
- Odgovorna osoba operativnog nivoa
- Indirektni izvršitelji poslova osiguranja

U upravljanju softverom sigurnosti informacijskih sustava, od strateškog planiranja i kontrole na najvišem poslovnom nivou do stručnog rada na višestrukim projektima i zaključcima, poslovi se dijele na sljedeće kategorije:[90]

- Sponzorski tim uprave odnosno odbora
- Širi tim za zaštitu informacijskih sustava
- Uži tim za zaštitu informacijskih sustava

Hijerarhijska struktura indirektnih izvršitelja poslovne sigurnosti informacijskih sustava posjeduje strukturu: [91]

- Voditelj sigurnosti poslovne organizacije odnosno poduzeća
- Administratori zaštite u određenim tehnološkim i organizacijskim aspektima
- Korisnici informacijskih sustava

Zaštita informacijskih sustava je multidisciplinarna, a određeni segmenti i poslovi u izravnoj su vezi više organizacijskih sektora i radnika. Za njihovo usklađeno izvršavanje i ispunjenje ciljeva zaštite nužno je izvršiti konkretno razdvajanje poslova i odgovornosti, kreiranje vertikalne crte obavljanja poslova zaštite, kao i horizontalnih povezanosti između izvršitelja radnji iz više organizacijskih sektora.

[89] Jurison, J. (1995). "The Role of Risk and Return in Information Technology Outsourcing Decisions, Journal of Information Technology", 1995, 10. str. 34-42.
[90] Jurison, J. (1995). "The Role of Risk and Return in Information Technology Outsourcing Decisions, Journal of Information Technology", 1995, 10. str. 34-42.
[91] Dempsey, J. (1998). Dvorak, R. E., Holen, E., Mark, D., Meehan, W. F. III: "A hard and soft look at IT investment", The Mc KinseyQuarterly, 1998, No. 1., str. 36-37.

Uprava poduzeća odnosno tvrtke osniva na svojoj najvišoj poslovnoj razini odbor za zaštitu informacijskih sustava, kao operativno tijelo za upravljanje informacijskim sigurnostima. U sustav odbora uključuju se:[92]

- Top menadžment odnosno uprava
- Voditelj informacijskih poslova
- Voditelj osiguranja
- Voditelj za kvalitetu
- Project menadžer
- Voditelj općih poslova

Povjerenstvo predstavlja stručno operativno tijelo za upravljanje sigurnošću informacijskih sustava poduzeća. Povjerenstvo vrši okupljanje operativnih rukovoditelja i eksperte angažirane na radnjama zaštite informacijskih sustava. Povjerenstvo za zaštitu informacijskih sustava sudjeluje u određivanju potreba i analize ponuda informacijskog sustava iz segmenta sigurnosti informacijskih sustava. Saziva se i radi u potpunom sastavu ili u smanjenom sastavu, kada se rješavaju posebni problemi. Radom povjerenstva upravlja voditelj sigurnosti ili osoba koja je zadužena za kvalitetu. Korisnici su svakako uključeni u podjelu njihovih podataka.[93]

Povjerenstvo vodi raspravu i daje prijedloge rješenja i odluke u slučaju:[94]

- Podjele uloga i odgovornosti za poslove osiguranja informacijskih sustava kod organizacijskih segmenata
- Dogovaranja i donošenja posebnih metodologija i procesa u svrhu zaštite informacijskih sustava
- Stručne potpore poslovima zaštite na nivou poduzeća, kao što je program edukacije za zaštitu informacijskih sustava
- Procjene novih mjera i rješenje koje vodi zaštita informacijskih sustava i koordinacije kod primjene
- Razgovaranje o sigurnosnim propustima
- Promoviranja zaštite informacijskih sustava
- Analize promjene sustavnih rješenja, ulaganja i kreiranja planova
- Prihvaćanje prijedloga pravilnika za segment osiguranja i zaštite
- Analiziranja utjecaja osiguranja poslovne funkcije poduzeća

Voditelj sigurnosti bira se na temelju posebnih znanja nužnih za stvaranje zaštite i osiguranja. Poslovi voditelja sigurnosti podrazumijevaju:[95]

[92] Jurison, J. (1995). "The Role of Risk and Return in Information Technology Outsourcing Decisions, Journal of Information Technology", 1995, 10. str. 34-42.
[93] Battles, B. E., Mark, D., Ryan, C. (1996). "An Open Letter to CEOs: How Otherwise Good Managers Spend Too Much on Information Technology", The McKinsey Quarterly, 1996, No. 3.
[94] Gugić A. (2014). Poslovne sigurnosne politike i procedure; predavanje Veleučilište Marko Marulić, Knin., str. 14.
[95] Jurison, J. (1995). "The Role of Risk and Return in Information Technology Outsourcing Decisions, Journal of Information Technology", 1995, 10. str. 34-42.

- Procjenjivanje rizika za određene cjeline informacijskih sustava
- Određivanje nužnih mjera zaštite i sudjelovanje u njihovom implementiranju
- Vršenje provjere provođenja aktualnih mjera sigurnosti
- Sudjelovanje u stopiranju loših aktivnosti i analiziranje sigurnosnih propusta
- Pratnja aktualnosti, referenci i produkata za segment zaštite informacijskih sustava
- Pripremu pravilnika i koraka za zaštitu informacijskih sustava
- Izradu planova za očuvanje dosljednosti obavljanja poslova
- Određivanje potreba zaštite i provjera primjene u novim produktima i programima
- Ispitivanje svojstva osiguranja za nove produkte i programe

Uz posebnu obuku svih radnika koji sudjeluju u kreiranju i održanju mjera osiguranja, nadređeni voditelj provodi konstantnu obuku radnika poduzeća za zaštitu informacijskih sustava. Voditelj sigurnosti osigurava strogu specifikaciju programa zaštite te vodi projekte osiguranja informacijskih sustava. Poslovi voditelja sigurnosti veoma su komplicirani, oni su organizacijske i izvršne prirode iz pogleda sigurnosti informacijskih sustava.

Politika informacijske sigurnosti primjenjuje se na sve potencijale u razvoju, korištenju i održavanju poslovnog sustava tvrtke odnosno poslovne organizacije, kao i korake, procedure i usluge njegove implementacije, upotrebe i redovnog održavanja. Potencijali čine informacije, tehnološku odnosno tehničku podršku za njihovo pribavljanje, procesiranje, spremanje i prijenos te radnike koji održavaju i upotrebljavaju sustav. Informacije mogu biti pohranjene i prikazane u različitim formatima kao što su: magnetski medij, baze podataka, datoteke i sl. U tehnološku potporu ubrajaju se sva kompjutorska i komunikacijska oprema te pripadna programska potpora koja se rabi u segmentu poslovnog sustava.[96] Politika informacijske sigurnosti se pored na radnike tvrtke odnosno poslovne organizacije upotrebljava i u slučajevima eksternih korisnika, dobavljača, poslovnih partnera i drugih strana koje koriste informacijski sustav ili posjeduju pravo pristupa. Sve informacije koje se upotrebljavaju smatraju se imovinom i trebaju se zaštiti od bilo kakvog uništenja, zlouporabe ili nezakonitog odavanja. Granice opsega informacijskih sustava definirane su potencijalima, pravima i ovlastima djelovanja unutar tvrtke odnosno poslovne organizacije.[97]

3.5.3. Segmenti politike informacijskih sustava sigurnosti

Svaki radnik odnosno korisnik na poslovnom sustavu u tvrtki odnosno poslovnoj organizaciji treba razumjeti svoje mjesto i odgovornosti prema osiguranju informacija te štititi potencijale samoga sustava. Nepoštivanje načela politike informacijske sigurnosti i smjernica koja iz njih proizlaze može dovesti do disciplinskog postupka, podrazumijevajući prestanak radnog odnosa ili postupak pred sudom u skladu s važećim zakonima. Svako nepoštivanje ili sumnja u nepridržavanje pravila sigurnosti, koje može rezultirati gubitkom povjerljivosti, integriteta ili raspoloživosti, trebalo bi biti prijavljeno nadležnoj osobi unutar poduzeća koja je odgovorna za provođenje mjera sigurnosti.[98]

[96] Battles, B. E., Mark, D., Ryan, C. (1996). "An Open Letter to CEOs: How Otherwise Good Managers Spend Too Much on Information Technology", The McKinsey Quarterly, 1996, No. 3.
[97] Rimljak, J. (2015). Informacijska sigurnost u suvremenom poslovanju. Veleučilište „Marko Marulić" u Kninu.
[98] Pintar, D. (2009). Model uslužno orjentirane arhitekture za stvarnovremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva.

3.6. Politika informacijske sigurnosti u suvremenom poslovanju

Konstantan i vrlo brz razvoj elektroničke vrste poslovanja poduzećima, ali i radnicima unutar poduzeća kao i poslovnim partnerima nudi pristup do informacija odnosno podataka iz ureda, lokacije korisnika ili iz doma. To podrazumijeva sve veću ovisnost poslovanja o informacijskim sustavima kao podršku razvoju, operativnom radu i poslovnim segmentima. Razvoj informacijskog sustava koja daje potporu takve vrste rada, kao i globalizacija komunikacija uvode nove moguće opasnosti i ranjivosti informacijskih sustava. Sigurnosni propusti koji su posljedica tih ranjivosti mogu ozbiljno ugroziti informacijski sustav i odvijanje procesa rada tvrtke te sam njezin ugled ili ugled njezinih radnika.[99] Politika informacijske sigurnosti predstavlja primarni dokument koji definira namjenu tvrtke za određenje koraka i kreiranje pravila i organizacije te provođenje nužnih mjera sigurnosti u realiziranju programa rada tvrtke. Na osnovu načela iz politike sigurnosti vrši se razrađivanje potrebnih naputaka i koraka te ostalih dokumenata koji se odnose na segment sigurnosti poslovnog sustava neke tvrtke.[100] (Tablica 5: Segmenti obuhvaćeni politikom informacijske sigurnosti.)

Tablica 5. Segmenti obuhvaćeni politikom informacijske sigurnosti

SEGMENTI OBUHVAĆENI POLITIKOM INFORMACIJSKE SIGURNOSTI	
POLITIKE ZAŠTITE	**POLITIKE SIGURNOSTI**
Fizička zaštita	**Opća politika i informacijske sigurnost**
Zaštita operativnih sustava	**Klasificiranje informacija**
Antivirusna sigurnost	**Privatnost podataka**
Zaštita autorskog prava	**Individualna odgovornost**
Sigurnost radnika	**Osiguranje operativnih sustava**
Zaštita resursa u transportu	**Planiranje kontinuiteta poslovanja**
Zaštita mrežne arhitekture	**Uporaba sustava**
Zaštita od eksternih mreža	**Kontroliranje prava pristupa**
Zaštita na Internetu	**Prava pristupa sustavu izvana**
Zaštita u razvoju programa	**Uporaba elektroničkih komunikacija**
Prihvatljiva uporaba Interneta	**Odgovori na incidente**

Izvor: http://www.snt.hr/boxcontent/news/Propisi_sigurnost.pdf (pristupljeno: 29.03.2016.)[101]

[99] Dutta S., Bilbao-Osorio B. (2012). *The Global Information Technology Report 2012: Living in a Hyperconnected World*, Geneva, World Economic Forum.
[100] Dempsey, J. S. (2008). Introduction to private security. Belmont, CA: Thomson Wadsworth.
[101] Izvor: http://www.snt.hr/boxcontent/news/Propisi_sigurnost.pdf (pristupljeno: 29.03.2016.)

3.6.1. Sigurnosna politika informacijskih sustava

Politika sigurnosti informacijskih sustava bazira se na organizacijskom i menadžerskom skladu, gdje se striktno zna tko je za nešto zadužen. Politiku sigurnosti informacija realiziraju stručna tijela za upravljanje sigurnost preko korisnika informacijskih sustava, korisnici informacijskih sustava svrstavaju se na one koji upotrebljavaju usluge i one koji nude usluge. Informacijski sustavi objedinjuju podatke kojima se koriste ovlašteni korisnici i koji služe s ciljem da korisnicima omoguće uporabu sustava. Kako takvi podaci ne bi smjeli biti dostupni javno, ne smiju se mijenjati bez odobrenja te ne smiju biti van domašaja korisnicima, bitno je realizirati određene faze sigurnosti kako bi navedeni uvjeti uvijek bili ispunjeni. Sigurnosna politika predstavlja cjelinu pravila, smjernica i radnji koja određuju na koji način informacijski sustav omogućiti sigurnim i kako osigurati njegove tehnološke i informacijske vrijednosti.

Sigurnosnom politikom određena su pravila odnosno koraci koji podrazumijevaju:[102]

- Svu kompjutorsku opremu poduzeća
- Osobe koje su odgovorne za rad informacijskih sustava
- Sve radnike i korisnike sustava, odnosno radnike koji imaju pravo pristupanja
- Eksterne suradnike

Sigurnosnom politikom objedinjeni su veći segmenti mjera sigurnosti, ali nisu svi segmenti politike nužni određenim grupama korisnika. Primjerice, radnici koji rade na sustavu ne trebaju poznavati segment politike koji se odnosi na sigurnost tehničke opreme ili onaj segment koji je namijenjen eksternim korisnicima. Tako je preporučljivo sigurnosnu politiku kreirati u više cjelina.[103] Oni korisnici, kojima je politika sigurnosti i namijenjena, uglavnom ne posjeduju dovoljno strpljenja da čitaju veliki broj stranica sadržaja.[104] Oni često imaju veoma slaba znanja u pogledu tehnologija koje koriste pri svome radu i uslijed toga je potrebno odrediti sigurnosnu politiku na način da bude sažeta i koncizna, kreirana tako da gdje će je korisnici moći lako razumjeti. Politiku napisanu koja je napisana stručnim jezikom i koja je opširna običan radnik nije u stanju razumjeti te je nije u stanju ni poštovati.[105]

3.6.2. Značaj sigurnosne politike u izvršenju procjene rizika

Sigurnost informacijskih sustava zasniva se na osobama odnosno radnicima unutar poduzeća. Putem tehnologije nije moguće u cijelosti omogućiti sigurnost sustava i stoga je bitno implementirati dopunske mjere, a prvi korak ka tome predstavlja određivanje sigurnosne politike. Osnovna uloga sigurnosne politike predstavlja kreiranje s jedne strane prihvatljivog i s druge strane neprihvatljivog načina ponašanja s ciljem zaštite vrijednosti informacijskih

[102] Bysinger, B., Knight, K. (1996). "Investing in Information Technology", Van Nostrand Reinhold, 1996., str. 72.
[103] Alter, S. (1996). "Information Systems-A Management Perspective", The Benjamins/ Cummings Publishing Company Inc, 1996.
[104] Rimljak, J. (2015). Informacijska sigurnost u suvremenom poslovanju. Veleučilište „Marko Marulić" u Kninu.
[105] Dvorak, R. E., Hollen, E., Mark, D., Meehan, W. F. (1996). "Six Principles of High-Performance IT", The McKinsey Quarterly, 1997, No. 3.

sustava, uz opremu, programsku potporu i podatke. Na osnovu pravila određenih, njen je zadatak pružiti tri osnovne vrste informacija:[106]

- Tajnost informacija
- Informacijski integritet
- Dostupnost informacija

Povjerljivost predstavlja zaštita podataka koja objedinjuje sustav sigurnosti od zlonamjernog pristupa koji može biti ugrožen na više načina od kojih se izdvajaju oni koji se tijekom poslovanja događaju više puta:[107]

- Hakerski upadi
- Lažno predstavljanje
- Protuzakonita aktivnost
- Preuzimanje podataka bez zaštite
- Lokalne mreže
- Virusi

Pod integritetom se ovdje misli na spašavanje odnosno čuvanje podataka bilo od namjerne ili pak slučajne (bez ovlasti) promjene. Kao i kod slučaja povjerljivosti, integritet se može ugroziti hakerskim upadima, lažnim predstavljanjem, neovlaštenim aktivnostima i nedozvoljenim pristupom i ostalim aktivnostima koje mogu rezultirati neovlaštenim mijenjanjem podataka. Postoje tri primarna postulata zasnivanja integriteta kontrole:

- Dodjeljivanje isključivo osnovnih pristupnih prava[108]

Korisnicima je potrebno omogućiti pravo pristupa isključivo na one datoteke i softvere koji su im nužni da bi izvršavali svoju poslovnu funkciju u poduzeću. Pristup proizvodnim podacima i izvornoj šifri treba posebno ograničiti dobro određenim transakcijama koje pružaju odnosno omogućuju da korisnici mogu izmijeniti podatke na striktno kontroliran način s ciljem zaštite integriteta. Kako se od korisnika očekuje da učinkovito obavlja svoj dio posla, pristupne mogućnosti moraju biti razumno dodijeljene s ciljem da se s korisnicima omogući prilagodljivost u radu. Sigurnosne mjere trebaju uravnotežiti sigurnosne zahtjeve s praktičnom produktivnosti.[109]

- Odvajanje dužnosti i obveza[110]

Korisno je izvršiti osiguranje da nijedan radnik ne posjeduje kontrolu nad transakcijom od samoga početka pa sve do kraja. Dvije ili više osoba moraju biti odgovorne za izvođenje transakcije primjerice: netko tko ima mogućnost da kreiranja transakciju ne bi trebao imati mogućnost za njezinu realizaciju.

---

[106] Dutta S., Bilbao-Osorio B. (2012). *The Global Information Technology Report 2012: Living in a Hyperconnected World,* Geneva, World Economic Forum., str. 65-66.
[107] Dutta S., Bilbao-Osorio B. (2012). *The Global Information Technology Report 2012: Living in a Hyperconnected World,* Geneva, World Economic Forum., str. 66.
[108] engl. need-to-know basis
[109] Dvorak, R. E., Hollen, E., Mark, D., Meehan, W. F. (1996). "Six Principles of High-Performance IT", The McKinsey Quarterly, 1997, No. 3.
[110] engl. separation of duties

- Rotiranje dužnosti[111]

Poslovne operacije bi se trebale mijenjati vremenom tako da korisnicima bude teže zlonamjerno preuzimati kontrolu nad transakcijama. Ovaj pristup efikasan je kada se upotrebljava u sprezi sa separiranjem dužnosti. Ipak, tvrtke koje posjeduju manjak radnika ili slabije obučene radnike, teško izvršavaju rotiranje dužnosti.

Modeli integriteta vrše opis načina realizacije integritetne politike. Postoje tri cilja integriteta, gdje ih modeli postižu na više načina:[112]

- Onemogućenje neovlaštenih korisnika da mijenjaju podatke odnosno programe
- Onemogućenje ovlaštenih korisnika da mijenjaju podatke odnosno programe na neodgovarajući i zabranjen način
- Održavanje interne i eksterne konzistentnosti kako podataka tako i programa

Dostupnost predstavlja jamstvo ovlaštenim korisnicima sustava da će im isti biti na raspolaganju u bilo kojem momentu kada za to budu imali potrebu. Postoje dva osnovna uzroka neraspoloživosti sustava:

- Uskraćivanje usluge[113]
- Gubitak sposobnosti obrade podataka uslijed prirodnih nezgoda

Kada se govori o uskraćivanju usluge govori se o načinu napada u kojemu se uglavnom namjernim generiranjem ogromne količine mrežnog prometa pokušava zagušiti odnosno začepiti mrežna oprema i poslužitelji odnosno server. Informacijske tehnologije postaju u tolikoj mjeri opterećene da više nisu u mogućnosti procesirati normalan promet što na koncu donosi poslijedice da redovni korisnici nisu u stanju koristiti mrežne usluge.[114]

Pod gubitkom sposobnosti obrade podataka kao rezultata prirodnih nesreća ili akcija osoba misli se na gubitke koji se prate planiranjem izvanrednih prilika što pomaže smanjenju vremena nedostupnosti sredstava za obradu podataka. Izvršenje planiranja nepredviđenih prilika, koje može obuhvaćati planiranje oporavka od nesreće planiranje obnove poslovnih procesa itd, omogućuje sporedne načine obrade podataka.[115]

Sigurnosne mjere putem kojih se osigurava dostupnost mogu biti podijeljene na:[116]

- Fizičke elemente koji obuhvaćaju onemogućenje neovlaštenih korisnika da pristupe sredstvima za obradu podataka, razne zaštitne sustave za obranu od požara, poplave itd.
- Tehničke elemente koji predstavljaju sustave otporne na pogreške i redundantnost sklopovlja, programe za kontroliranje pristupanja i sl.

---

[111] engl. rotation of duties

[112] Battles, B. E., Mark, D., Ryan, C. (1996). "An Open Letter to CEOs: How Otherwise Good Managers Spend Too Much on Information Technology", The McKinsey Quarterly, 1996, No. 3., str. 23.

[113] eng. Denial Of Service

[114] Rimljak, J. (2015). Informacijska sigurnost u suvremenom poslovanju. Veleučilište „Marko Marulić" u Kninu.

[115] Bysinger, B., Knight, K. (1996). "Investing in Information Technology", Van Nostrand Reinhold, 1996.

[116] Gugić A. (2014). Poslovne sigurnosne politike i procedure; predavanje Veleučilište Marko Marulić, Knin., str. 34.

- Administrativne elemente koji obuhvaćaju politiku pristupne kontrole, operativnog protokola, planiranja neredovnih prilika i educiranje korisnika.

3.7. Upravljanje kontinuitetom poslovanje (BC) i njegov razvoj

Upravljanje kontinuitetom poslovanja, Slika 3. (eng. Business Continuity Planning, BCP ili Business Continuity Management, BCM) je proces izrade plana koji opisuje načine i korake o tome kako izbjeći, ublažiti ili oporaviti poslovanje nakon kraha uzrokovanog nezgodom. Za donošenje logističkog plana za upravljanje poslovnim procesima tvrtke prilikom događaja koji mogu negativno utjecati na poslovanje, treba proći kroz nekoliko ključnih radnji. Odnosno, u ciklusima treba prolaziti redovito kroz sljedeće radnje: analizu, izradu rješenja, provedbu rješenja, provjeru rješenja i prilagodbu rješenja.

Slika 3. Model upravljanja kontinuitetom poslovanja

Izvor: Centar informacijske sigurnosti: "Upravljanje kontinuitetom poslovnih procesa", pristup: 18.10.2016.[117]

Pojam "osiguranje kontinuiteta poslovanja" podrazumijeva, dakle, niz procesa i akcija kojima je cilj na vrijeme identificirati potencijalne prijetnje za poslovanje kompanije, odnosno poslovne organizacije. Upravljanjem kontinuitetom poslovanja osigurava se temelj učinkovite i pravodobne reakciju koja će zaštiti interese kompanije.

Upravljanje kontinuitetom poslovanja uključuje: upravljanje kriznim i hitnim situacijama, predlaganje mjera i aktivnosti za minimaliziranje potencijalne štete u slučaju incidenta, te minimaliziranje učinka štete na daljnje poslovanje.

U brojnim poslovnim procesima i najmanji je oblik prekida normalnog kontinuiranog rada izuzetno štetan, a sanacija štete je dugotrajna i skupa, a često i neizvjesna. U tim slučajevima je upravljanje kontinuitetom poslovanja od izuzetne važnosti, no ovaj je proces važan i kada potencijalna šteta ne znači nužne i katastrofalne gubitke u poslovanju.

[117] Izvor: Centar informacijske sigurnosti: "Upravljanje kontinuitetom poslovnih procesa", pristup: 18.10.2016

Upravljanje kontinuitetom poslovanja važno je, stoga, za sve tvrtke, bez obzira na vrstu djelatnosti kojom se kompanija bavi, jedina je razlika u tome što je u nekim poslovnim procesima to više, a u drugima manje važno, odnosno za jedne potencijalna šteta znači goleme gubitke, za druge manje, ali se u svakom slučaju radi o gubicima, bilo financijskim bilo nekim drugim kao što je imidž kompanije i sl.

Prema propisanim normama (BS 25999-1 i BS 25999-2) objavljenim 2006. plan kontinuiteta poslovanja mora se sastojati od:

1. Plana odaziva na incident, koji se obično sastoji od jedinstvenog plana koji se odnosi na cijelu organizaciju i opisuje radnje koje se moraju poduzeti odmah nakon pojave havarije – smanjenje posljedica incidenta, komunikacija sa službama za hitne slučajeve, evakuacija zgrade, okupljanje na zbornim mjestima, organizacija transporta na rezervnu lokaciju i sl.

2. Plana oporavka koji se obično piše zasebno za svaku kritičnu aktivnost i mora obuhvaćati sljedeće korake: vrijeme i način na koji se komunicira s raznim zainteresiranim stranama (zaposlenicima i njihovim obiteljima, dioničarima, klijentima, partnerima, državnim službama, javnim medijima i dr.), princip sastavljanja tima, provođenje oporavka infrastrukture, provjera funkcionalnosti aplikacija i kontrole pristupa, provjera podataka koji nedostaju i utvrđivanje svega što je oštećeno u havariji, oporavak podataka i uspostava normalnih aktivnosti.

Prema recentnim istraživanja, jedna od pet kompanija godišnje doživi neki oblik poremećaja procesa poslovanja, a važnost upravljanja poslovnim procesima je danas u uvjetima globalnog tržišta i jake konkurencije važnija nego ikad prije.

Iako je važno prepoznati da postoji holistički pristup onome što se može nazvati "Organizacijska Otpornost", te da postoje sličnosti i komplementarni pristupi funkcija koje će omogućiti podršku za organizaciju, postoje i jasne razlike u pristupu nekim područjima. Kontinuiteta poslovanja (BC) mnogi vide kao specijalnost i temeljenu funkciju informacijske tehnologije nego ono što je on postao. Definicija kontinuiteta poslovanja koja je prikladno za primjenu na ove bilješke je iz ISO 22301: 2012 (Društvena Sigurnost - Business Continuity sustavi upravljanja - zahtjevi) pri čemu je kontinuitet poslovanja holistički proces upravljanja koji identificira potencijalne prijetnje organizacija i utjecaja na poslovanje te prijetnje, koji može uzrokovati i koji pruža okvir za izgradnju organizacijske otpornosti s mogućnošću učinkovitog odgovora koja štiti interese svojih ključnih dionika, ugled, brendove i aktivnosti stvaranja vrijednosti.[118]

Kao definiranje područja koja kontinuitet poslovanja pokriva i njegovih ciljevi, ovo je prikladno polazište za daljnje ispitivanje i analize. Nećemo u ovoj fazi razbiti definiciju u riječi i komponente, međutim to je korisno za usmjeravanje misli prema ideji što kontinuitet poslovanja nastoji postići i gdje se mogu uklopiti s drugim organizacijskim elastičnim pod-funkcijama. Postoje mnogi a neki su, oporavak od havarije (kontinuitet informacijske tehnologije) upravljanja sigurnošću, analiza rizika, upravljanje krizom i hitnim slučajevima te planiranje. Svi su komplementarni i svi doprinose kontinuitetu poslovanja. U razmatranju

[118] International Organization for Standardization (ISO), (2005). Code of Practice for Information Security Management, ISO/IEC 17799, Switzerland

"primata", tj. koja funkcija podržava druge strane; organizacije i praktičari ne moraju biti jasni o tome što je važno i gdje se uklapaju zajedno.

Ako netko ima subjektivnu točku gledišta, ponekad može biti teško procijeniti s bilo kakvom točnošću pravu vrijednost poslovnog kontinuiteta organizacije.

Postoji zbunjenost, interes i aktivnost koja će uvijek izvrtati pristranost jednoj funkciji nad drugom u organizacijskoj hijerarhiji. Međutim, za profesionalne prakse (na nepristrane i analitičke akademije), procjena vrijednosti organizacijama i doprinos funkciji poslovnog kontinuiteta i njegovih ostalih dijelova koji doprinose za organizaciju, treba uzeti u obzir u smislu svoje obradivosti, djelotvornosti svojih funkcija i njegovu sposobnost da se osigura kontinuitet usluga. Perspektiva koja se temelji na vrijednosti je u pitanju manja s usklađenosti, pravilima, tehnologijom neuspjeha nego s potrebama samog poslovanja.[119]

Umjesto toga, kontinuitet poslovanja je usmjeren na održavanje proizvoda i usluga. Prema tome, postoji značajan fokus standarda kontinuiteta poslovanja, smjernica i tekstova o upravljanju utjecajima.

3.7.1. Razvoj kontinuiteta poslovanja

U ovom dijelu rada kratko ćemo objasniti i razvoj kontinuiteta poslovanja i njegovih početaka. Razvoj kontinuiteta poslovanja prema sadašnjem stanju je rezultat promjena i razvoja i utječe na razvoj organizacije, regulacije i zakona uz razmišljanje o analizi i odgovoru na događaje, incidente i druga pitanja.

Dakle, sustav kontinuiteta poslovanja se po nužnosti pretvorio u zbirku praksi i povezanih procesa koji trebaju imati agilnost, fleksibilnost i brzinu reakcije koje će biti u mogućnosti predvidjeti i upravljati utjecajima. Jednako važno, zadatak okrenut prema BC stručnjaku jest taj da će biti u mogućnosti osigurati da sustav kontinuiteta poslovanja i povezane poruke nisu samo komplementarne, nego i ugrađene unutar organizacijskih procesa i praksi, kao da ne postoji svijest i sposobnost prema odgovarajućem standardu, na odgovarajućoj razini.[120]

3.7.2. Poslovni procesi

Kvaliteta, cijena, predanost kupcu te brzina reakcije i prilagodbe promjenama su karakteristike uspješnih poslovnih subjekata. Svaka organizacija mora imati odredbene ciljeve u svom poslovanju. Poslovni sustavi s dobro ustrojenim poslovnim procesima ubrzavaju rad tvrtke kojoj pripadaju, povećavaju unutarnji red, smanjuju troškove te povećavaju kvalitetu proizvoda. Poslovno okruženje se neprekidno mijenja, brzina i količina promjena dramatično se povećava, konkurenti dolaze i nestaju, nestabilnost tržišta i globalizacija iz temelja mijenjaju način poslovanja.

[119] ITGI (2007.), CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models, IT Governance Institute, Rolling Meadows, SAD.

[120] International Organization for Standardization (ISO), (2005). Code of Practice for Information Security Management, ISO/IEC 17799, Switzerland

Neprekidno unaprjeđivanje poslovnih procesa jedan je od ključnih faktora uspjeha. Iako je sam pojam poslovnog procesa prilično dugo prisutan, disciplina koja se bavi upravljanjem poslovnim procesima počela se razvijati tek posljednjih dvadesetak godina. Posljedica je to razvitka računala i softvera, povećanja njihovih mogućnosti i brzine rada.

Upravljanje poslovnim procesima ima nekoliko osnovnih aktivnosti.[121] To su dizajn i modeliranje poslovnog procesa, izvođenje procesa te mjerenje njegove uspješnosti. Poslovni proces se u fazi dizajna opisuje, dokumentira te se utvrđuje važnost i značaj određenih parametara u istom. Također, u ovoj fazi se može identificirati određeni postotak neefikasnih, nepotrebnih i/ili suvišnih procesa ili njihovih dijelova. Jednom opisani poslovni proces može poslužiti npr. za obuku novih djelatnika ili kao dio dokumentacije za dobivanje nekog industrijskog certifikata. U drugoj fazi proces se počinje izvoditi na način koji je opisan modeliranjem. Tada se sudionicima u procesu omogućuje da budu produktivniji jer u određenom trenutku znaju koji koraci su potrebni, koje su ulazne vrijednosti parametara i koji su očekivani rezultati za bilo koji korak u procesu. Jedini način da se zna je li poslovni proces dobar ili nije, jest da ga se prati i mjeri. Time se dolazi do treće faze koja se naziva faza praćenja ili nadzora. Što se mjeri, ovisi o procesu, grani djelatnosti, te cilju koji se želi ostvariti. Čak i ako nije poznato koji su ključni pokazatelji uspješnosti, samo mjerenje će kroz vrijeme pokazati napredak ili nazadovanje.[122]

Neprekidno poboljšavanje poslovnog procesa na temelju mjerenja rezultata uspješnosti tog procesa daje upravljanju poslovnim procesima smisao. Podaci o rezultatima uspješnosti, podaci o opisu poslovnih procesa, dokumentaciji itd. su danas najčešće pohranjeni u digitalnom obliku te je njihova sigurnost ugrožena sve većim brojem sigurnosnih prijetnji koje haraju internetom. Pojam mrežne sigurnosti je danas neizbježan u poslovanju neke organizacije.

3.7.3. Informacijska sigurnost

Razvijene države (npr. SAD, Japan i UK) postavile su barem minimalne, a najčešće i odgovarajuće sigurnosne pravne standarde i kriterije informacijske sigurnosti. Nacionalnom politikom informacijske sigurnosti postavljaju opći okvir kojeg ostvaruju odgovarajućim zakonima kao što su:[123]

- Zakon o sigurnosnim službama
- Zakon o zaštiti tajnosti podataka
- Zakon o zaštiti osobnih podataka
- Zakon o pravu pristupa informacijama
- Kazneno zakonodavstvo

[121] Panian, Ž., (2001). Kontrola i revizija informacijskih sustava, Sinergija, Zagreb

[122] Nolan, R. and McFarlan, F.W., (2005.): Information Technology and Board of Directors, Harvard Business Review, October

[123] Spremić, M. (2005.): Procjena razine pouzdanosti internih kontrola informacijskog sustava s pomoću CobiT metodologije, Revizija, računovodstvo i financije, br. 12/2005

Pravni okvir ovog područja u poslovnim sustavima čine i statut, sigurnosna politika tvrtke, pravilnici, sigurnosne procedure itd. Uzme li se u obzir činjenica da je informacijsko - komunikacijska tehnologija infrastruktura svakog poslovanja, tada su brojne sigurnosne prijetnje (virusi, trojanski konji i dr.) prisutne na globalnoj internet mreži izvor zahtjeva za odgovarajućom informacijskom sigurnosti.

Brzi razvoj primjene informacijsko-komunikacijske tehnologije uzrokuje sve veće mogućnosti napada na informacijske sustave i zlouporabu informacija, o čemu govore brojna upozorenja iz svijeta. O ovom aspektu postoje brojni i uglavnom dostupni izvori (FBI, CSI, SANS institute i dr.). Istraživanja navedenih institucija prikazuju da je godišnji porast broja napada na informacije kroz informatičke sustave negdje oko 90% i da broj novootkrivenih oblika ranjivosti informacijskih sustava raste eksponencijalno. Rastuće su i opasnosti od zatajenja informacijskih sustava, odnosno velikih šteta koje nastaju uslijed zastoja rada informacijskih sustava.[124]

[124] Srića, V., Spremić, M., (2000.): Informacijskom tehnologijom do poslovnog uspjeha, Sinergija.

4. PREGLED SVJETLOVODNOG MEDIJA PRIJENOSA

4.1.Svjetlovodno vlakno kao prijenosni medij

Glavna karakteristika optičkih sustava prijenosa koje kao primarnu komunikaciju koristi plinski operater je mogućnost prijenosa velike količine informacija u jedinici vremena, uz korištenje manje energije u usporedbi s drugim prijenosnim sustavima. Ovakav sustav podrazumijeva prijenos informacija po optičkim svjetlovodima koji predstavljaju medij za usmjereni prijenos optičkih signala. Za optičke komunikacije većinom se koriste dielektrični valovodi cilindrične strukture za koje je usvojen naziv ***optičko vlakno*.**[125]

Najvažnije osobine optičkog vlakna su:

- Veliki informacijski kapacitet, odnosno velike brzine prijenosa
- Male dimenzije
- Malo prigušenje (ispod 0,1 db/km) neovisno o frekvenciji signala (za bakar raste s frekvencijom)
- Širok frekvencijski pojas (do par stotina ghz po kilometru),
- Neosjetljivost na elektromagnetske smetnje, nema međuutjecaja između svjetlovoda, ne utječe na ostale vodove
- Otežano ometanje i prisluškivanje
- Iznimno velik međurepetitorski razmak (do par stotina km)

Kao nedostaci mogu se navesti:

- Nemogućnost prijenosa analognih signala zbog nelinearnosti
- Osjetljivo rukovanje u odnosu na bakrene kabele zbog male mehaničke čvrstoće
- Zahtjevno spajanje svjetlovodnih vlakana i neosjetljivost na ionizirajuća zračenja
- Cijene svjetlovoda, pripadnih uređaja i postupaka
- Upotreba nije prihvatljiva za prijenose malih brzina, svjetlovodno vlakno je idealan medij za prijenos digitaliziranih informacija velikih brzina gdje praktički nema konkurencije, te za neke posebne primjene

[125] Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998, str. 12.

Svako svjetlovodno vlakno sastoji se od jezgre koja vodi svjetlovod i odraznog plašta koji sprečava bijeg svjetlosti iz jezgre. Na slici 4 prikaz je monomodnog svjetlovodnog vlakna pod (A) i multimodnog pod (B)

Slika 4. Vrste svjetlovoda s obzirom na broj modova koje mogu prenositi.

Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998, str. 9.[126]

Svi oblici moderne komunikacije, radio i televizijski signali, telefonski razgovori, kompjuterski podaci, zasnivaju se na prijenosnom signalu određene frekvencije. Elektromagnetski signali opisuju se pomoću njihove valne duljine ili frekvencije.

[126] Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998, str. 9

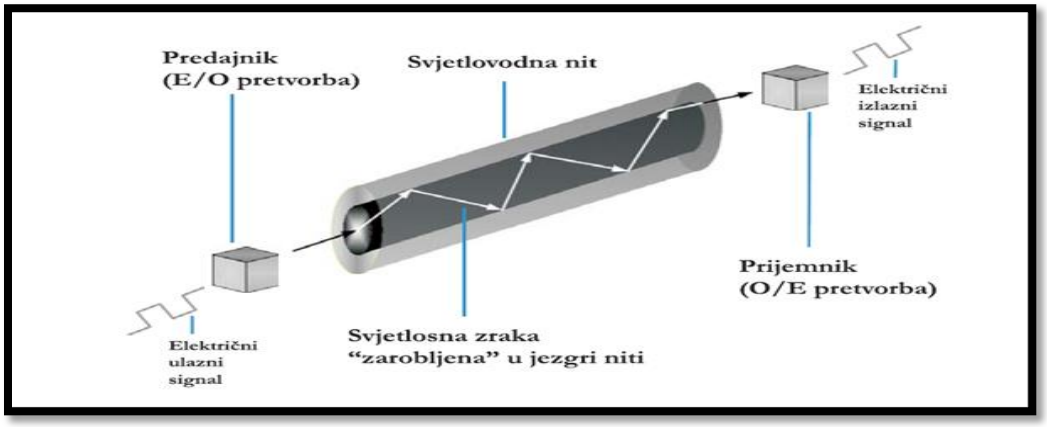
4.2.Princip svjetlovodnog prijenosa

Svjetlovodni sustavi prijenosa sastoje se od predajnika, prijenosnog medija te prijemnika (slika 5). Zadatak predajnika je pretvorba električnog signala u svjetlosni. Izvori svjetlosnog signala su svjetleće diode (*LED-Light Emitting Diode*) ili poluvodički laseri (*LASER-Light Amplification by Stimulated Emission of Radiation*), a služe za pretvorbu električnog signala u optički signal. Za komunikacije se najčešće koriste uski pojasevi valnih duljina oko 850, 1300 i 1550 nm.[127]

Prijenosni medij je svjetlovodna nit najčešće izrađena od silicijevog dioksida SiO2 (tzv. kvarcno staklo). U novije vrijeme niti se izrađuju i od plastike (*POF-Polymer Optical Fiber*) te u specijalnim izvedbama kao niti sa šupljinama (*PCF-Photonic Crystal Fiber*, u obliku *Holey fiber*).

Zadatak prijamnika je pretvorba optičkog u električni signal. Kao detektori svjetlovodnog signala koriste se lavinske fotodiode (APD –avalanche photo diode) i PIN fotodiode.

Slika 5. Princip svjetlovodnog prijenosa.



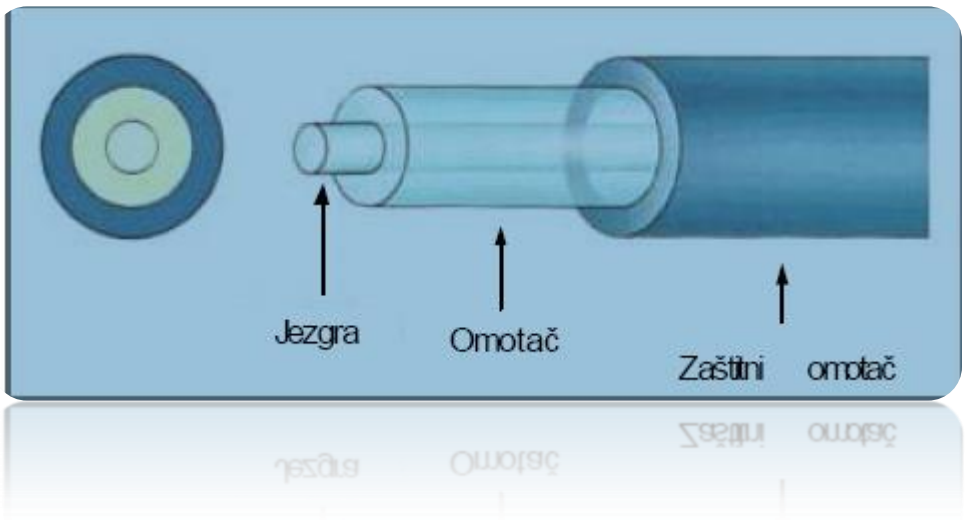
Izvor: www. Optical Laser Source.com[128]

[127] Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998, str. 9.
[128] Izvor. www. Optical Laser Source.com

4.3.Konstrukcija svjetlovodnog vlakna

Konstrukcijski dijelovi svjetlovodnog vlakna su jezgra i odrazni plašt koji sprečava bijeg svjetlosti, te primarne i sekundarne zaštite. (Slika 6).

Slika 6. Konstrukcija svjetlovodnog vlakna.



Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998. Str 8.[129]

Jezgra je dio svjetlovoda koji služi za prijenos svjetlosnog signala. Može biti od kvarcnog stakla, višekomponentnog stakla ili plastične mase. Promjer može biti od nekoliko mm do nekoliko stotina mm. Indeks loma jezgre veći je od indeksa loma odraznog plašta za 0,5-2 %.

Odrazni plašt služi za odbijanje svjetlosnog signala natrag u jezgru. Također može biti od kvarcnog stakla, višekomponentnog stakla ili plastične mase. Indeks loma odraznog plašta manji je od indeksa loma jezgre za 0,5-2 %.

Primarna zaštita služi za mehaničku zaštitu jezgre i odraznog plašta. Sastoji se od tankog sloja meke plastične mase koja se nanosi na jezgru i odrazni plašt ekstruzijom neposredno nakon izvlačenja.

Sekundarna zaštita služi za dodatnu zaštitu od vlage i raznih kemikalija. Sastoji se od debelog sloja plastične mase, koji se nanosi na vlakno s primarnom zaštitom tijesno (TIGHT) ili labavo (LOOS), s punjenjem posebnom masom ili bez punjenja. Zaštitni plašt obično se izrađuje od visoko preformirane plastike PVC, višeslojnih polimera, i tvrdih neporoznih elastomera. Prilikom spajanja na konektore taj dio se uklanja. Promjer vanjskog zaštitnog plašta je 250 μm i 900 μm. Zaštitni plašt se naziva još i primarni i nanosi se ekstruzijom nakon izvlačenja svjetlovoda.

[129] Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998. Str 8

4.4.Vrste svjetlovodnih vlakana

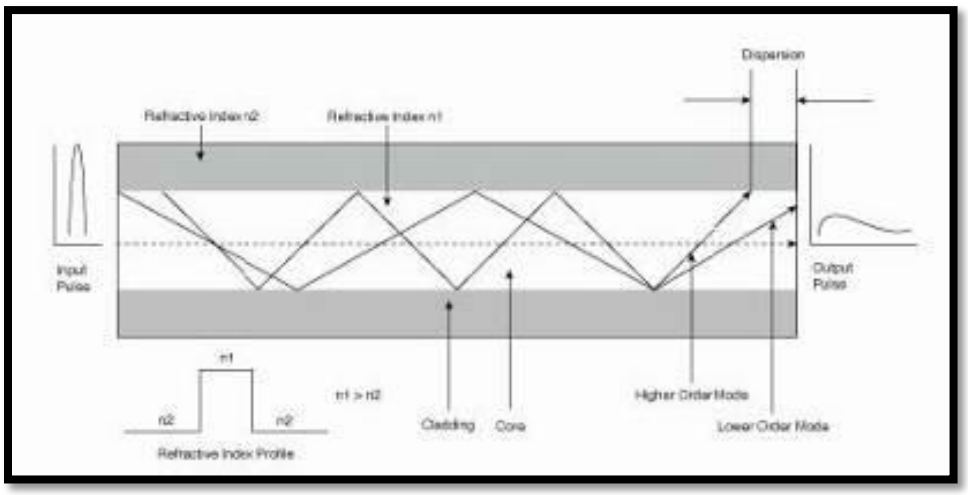
Podjelu svjetlovoda definira se s obzirom na različite aspekte.

Svjetlovodi se međusobno razlikuju prema: [130]

- Vrsti materijala od kojih je izgrađena jezgra i plašt
- Prema promjeni indeksa loma
- Broju modova koji koriste

Višemodni **MMF** (multi mode fiber) svjetlovodi sa stupnjevitom promjenom indeksa loma za prijenose koriste više modova. Na slici 7. prikazana su dva moda širenja svjetlosti. Također se vidi razlika u obliku izlaznog i ulaznog signala. Izlazni signal različit je u odnosu na ulazni. Izlazni signal je prigušen te je proširen odnosno dogodilo se raspršenje. Razlog prigušenju je polje na granici gdje se događa refleksija eksponencijalno opadajuće zrake. Tako da zrake imaju tendenciju prolaska u plašt prilikom refleksije.

Slika 7. Višemodni svjetlovod sa stupnjevitim indeksom loma.



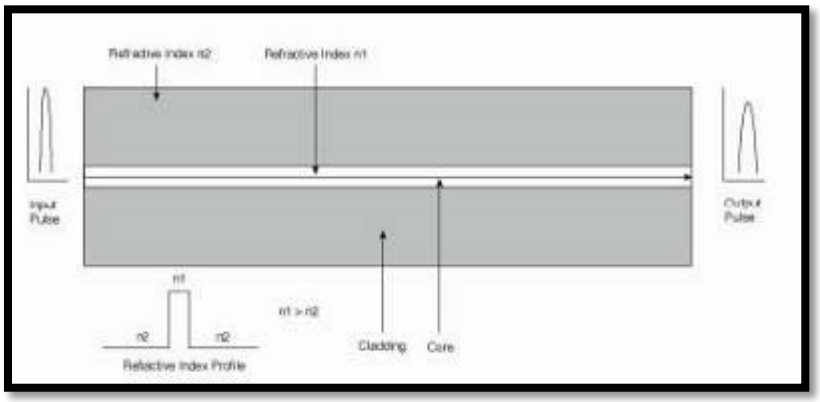
Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998. Str 25.[131]

Jednomodni **SMF** (single mode fiber) imaju jezgru promjera puno manjeg nego što je plašt te je valna duljina zrake usporediva s promjerom jezgre. Zbog tako malog promjera jezgre, ulaskom zrake u svjetlovod ne dolazi do razdvajanja zraka. Kritična valna duljina je najmanja valna duljina koja se generira u osnovnom modu. Na toj kritičnoj valnoj duljini javlja se drugi mod rada koji se propagira kroz plašt i uzrokuje gubitke. Kako se valna duljina rada svjetlovoda povećava u odnosu na kritičnu počinju se javljati gubitci osnovnog moda i sve se više energije prenosi kroz plašt. Posljedica toga je malo prigušenje izlaznog impulsa i vremensko rasipanje. Zbog malog rasipanja impulsa u vremenskoj domeni, u frekvencijskoj domeni imamo veću širinu pojasa. SMF svjetlovodi slika 8. Imaju jezgru promjera od 8 do 10µm i promjer plašta125µm. Jezgra svjetlovoda je dimenzija 50/125µm ili 62,5/125µm pri čemu jezgra promjera 50µm može propagirati samo 300 modova dok jezgra promjera 62,5µm propagira i do 1100 modova. Svjetlovod od 50µm s optičkim prozorom, tj. valnom duljinom

[130] www. Optical Laser Source.com.
[131] Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998. Str 25

zrake od 850nm podržava brzinu prijenosa do 1Gbps na udaljenosti do 0.5 km, a 62,5µm samo 275m. Nadalje SMF 50µm podržava 10Gbps do 82m nasuprot 62,5 µm koji podržava istu brzinu samo na 33m. Pri izradi se koristi OVD tehnologija (OVD – outside vapor deposition). SMF su skupi te se koriste za povezivanje globalnih mreža gdje je potrebna velika brzina i kapacitet prijenosa podataka. Također SMF svjetlovod može biti i s gradijentnim indeksom loma ili dvostrukim indeksom loma, tj. ima još jedan plašt oko primarnog plašta. Bez obzira na indeks loma SMF svjetlovodi imaju brzinu prijenosa podataka i do 50 puta veću od MMF svjetlovoda , te su kvalitetniji.

Slika 8. Jednomodni SMF svjetlovod sa stupnjevitim indeksom loma.



Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998. Str 27.[132]

4.4.1. Prijenosna svojstva svjetlovodnih vlakana

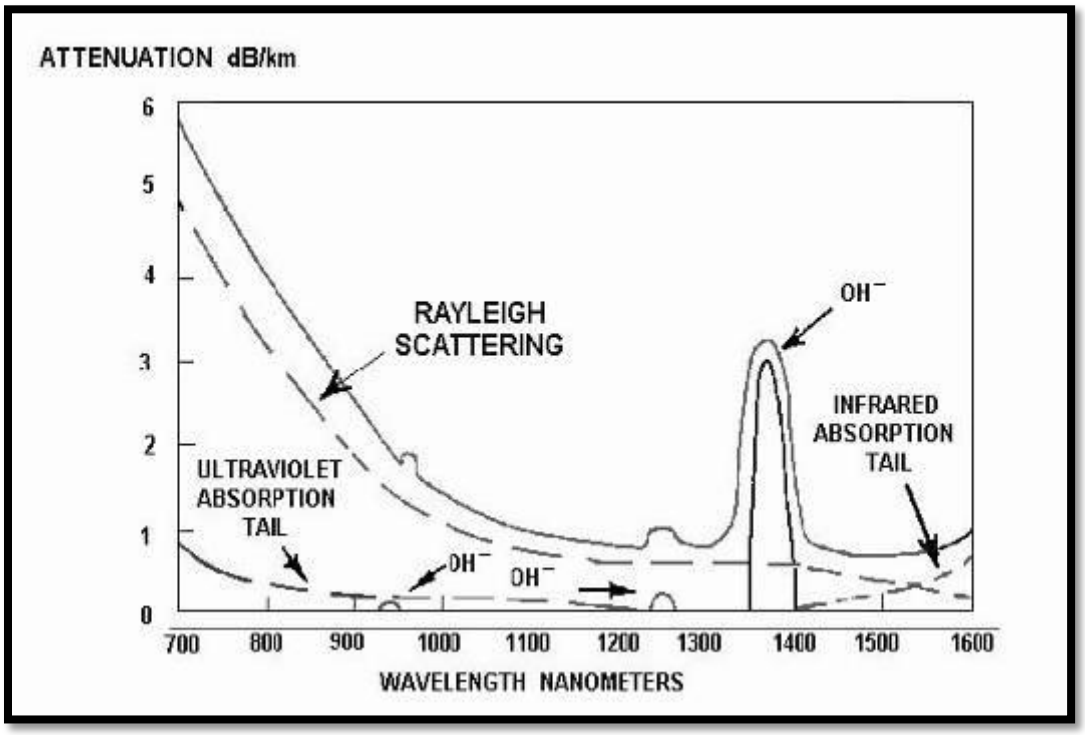
Prigušenje

Optička snaga svjetlovoda se transmisijom niti prigušuje eksponencijalno prema izrazu: $P(x)=P0\exp(-\alpha x)$, gdje je α koeficijent prigušenja i izražava se u dB/km i pokazuje gubitke u dB po jednom kilometru. Prigušenje u svjetlovodima nastaje zbog gubitaka, koji opet nastaju zbog raznih uzroka, a možemo ih podijeliti na vanjske i unutrašnje.

Unutrašnji uzrok je postojanje inherentnih nečistoća koje onda uzrokuju apsorpciju svjetlosti u materijalu zbog interakcije fotona s molekularnim nečistoćama u staklu, premještanja elektrona, te prijelaza elektrona između energetskih razina. Kada foton udari o nečistoću on će se raspršiti ili apsorbirati. Vanjski utjecaji su posljedica savijanja svjetlovoda pa se mijenja put koji zrake prolaze, što je naročito izraženo kod višemodnog svjetlovoda.

[132] Izvor: Svjetlovodi i njihovo održavanje Dr.sc.Ivan Mikula 1998. Str 27

Slika 9. Prigušenje u svjetlovodnom vlaknu.



Izvor: www. Optical Laser Source.com[133]

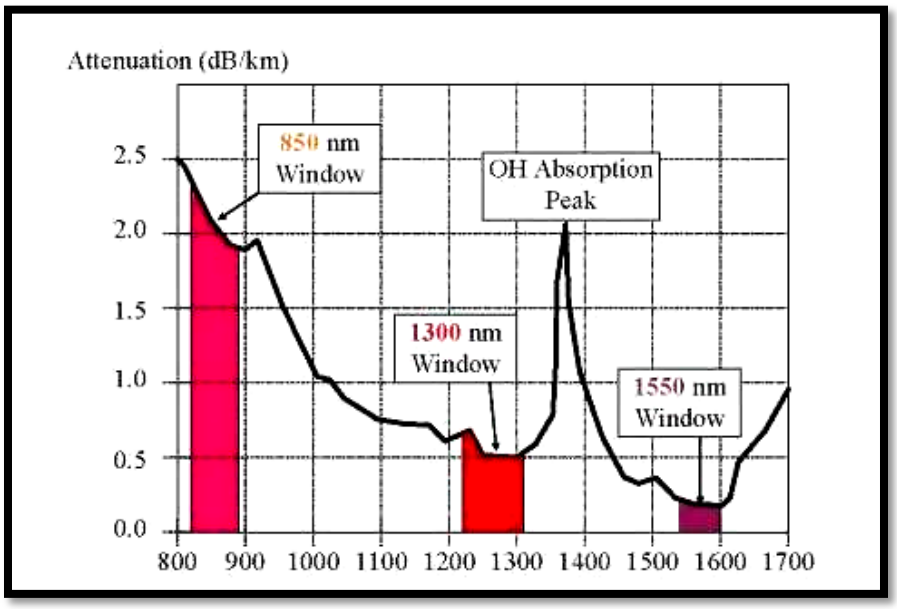
Na slici 9. su prikazani svi faktori koji se zbrajaju i određuju ukupni faktor prigušenja. Prigušenje kojem je uzrok raspršenje svjetlosti na nehomogenostima i nečistoćama u materijalu (scattering) koje postoje otprije ili nastaju za vrijeme proizvodnje svjetlovoda, kao pojava naziva se Rayleighevo raspršenje, a emitirana svjetlost Tyndallova svjetlost.

Faktoru prigušenja najviše doprinosi koeficijent prigušenja zbog Rayleighovog raspršenja čak 96%. Ono je posebno izraženo od 700 nm do 1000 nm s tim da prema većim valnim duljinama opada. Međutim na većim valnim duljinama smo ograničeni s infracrvenom svjetlošću, tj. imamo infracrvenu apsorpciju. Sve ispod 800 nm postaje neupotrebljivo.

[133] Izvor: www. Optical Laser Source.com

Na slici 10. Vidljiva su područja s lokalnim minimumima prigušenja koja se nazivaju prozori i koriste se za prijenos. Postoje tri prozora 850nm, 1300nm, 1550nm.

Slika 10. Optički prozori.



Izvor: www. Optical Laser Source.com[134]

Minimum prigušenja za prvi prozor iznosi oko 2 dB/km, za drugi 0,5 dB/km, te za treći 0,2 dB/km. Danas su već proizvedena vlakna s prigušenjem koje se bliži teoretskom, pa se danas pojavljuju nova optička vlakna koja mogu imati i više od 3 prozora jer je smanjeno prigušenje. U praksi je u početku najviše korišten I. prozor, iako to nije optimalno rješenje, ali je bilo uvjetovano početnim teškoćama u realizaciji izvora svjetlosti, a danas se koristi prvenstveno zbog jeftine realizacije izvora svjetlosti iako je na I prozoru najveće gušenje. Danas se koriste uglavnom II i III optički prozori.

Prigušenje svjetlovoda ovisi u prvom redu o vrsti materijala. Najmanje prigušenje ima kvarcno staklo (0,5-2 dB/km), nešto lošije je silikatno staklo (5-10 dB/km), dok su plastične mase znatno lošije. Daljnje prigušenje svjetlovoda ovisi o vrsti tih vlakana. Monomodna vlakna imaju najmanje prigušenje (0,2-1 dB/km), nešto su lošija multimodna vlakna s gradijentnom promjenom indeksa loma (1-5 dB/km), a najlošija su multimodna vlakna sa skokovitom promjenom indeksa loma (5-10 dB/km). Na kraju, prigušenje ovisi i o valnoj duljini svjetlosti koja se koristi za prijenos.

Disperzija

Disperzija je pojava, da se impulsi svjetlosti pri prijenosu po svjetlovodu proširuju, i tako ograničuju širinu propusnog opsega. Postoje dvije vrste disperzija a to su disperzija u materijalu i modalna disperzija.

- Disperzija u materijalu nastaje zbog različitih duljina valova, pri čemu dolazi do proširenja impulsa svjetlosti. Veličina disperzije ovisi o vrsti vlakana

[134] Izvor: www. Optical Laser Source.com

- Za svjetlovode sa skokovitom promjenom indeksa loma (multimodne i monomodne) 2-5 ns/km
- Za svjetlovode s kontinuiranom promjenom indeksa loma (multimodni - gradijentni) 0,1-2 ns/km

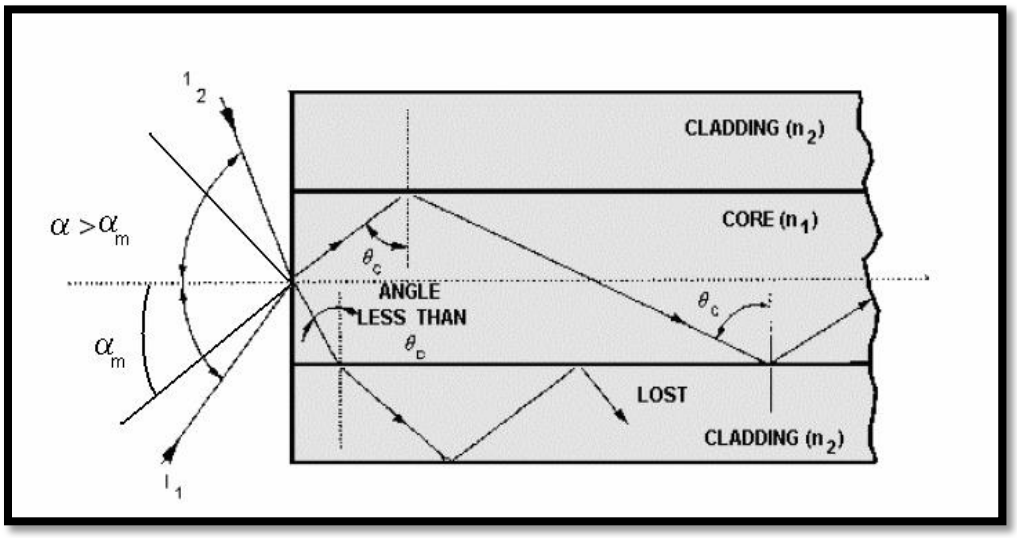
Multimodna disperzija (nekromatska) nastaje zato što različiti modovi imaju različite grupne brzine i zato dolaze na kraj linije s različitim vremenskim zakašnjenjem, posljedica čega je proširenje impulsa. Veličina te disperzije za pojedine vrste svjetlovoda je sljedeća:

- Za multimodne svjetlovode sa skokovitom promjenom indeksa loma < 20 ns/km
- Za multimodne svjetlovode s kontinuiranom promjenom indeksa loma (gradijentne) < 50 ns/km
- Za monomodne svjetlovode sa skokovitom promjenom indeksa loma Ş 0

Numerički otvor

Numercial aperture definiran je kao sinus maksimalnog kuta prihvata a ovisi o indeksu loma materijala. Njime je opisano svojstvo svjetlovodnog vlakna za prihvat svjetlosti. Numerički otvor ovisi o indeksu loma materijala jezgre i odraznog plašta. Vrijednost numeričkog otvora kreće se od 0 do 1 i izravno utječe na broj modova, koji se mogu koristiti u svjetlovodu. Slika 11.

Slika 11. Numerički otvor.



Izvor: https://hr.wikipedia.org/wiki/svjetlovodno_vlakno[135]

Širina propusnog opsega

Širina propusnog opsega ovisi o disperziji u materijalu svjetlovoda i širini opsega predajnika. Izražava se kao produkt širine propusnog pojasa i dužine dometa, koji za pojedine vrste svjetlovoda iznosi:

[135]Izvor: https://hr.wikipedia.org/wiki/svjetlovodno_vlakno

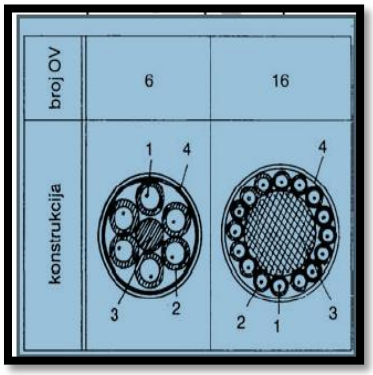
- Za monomodne, sa stupnjevitom promjenom indeksa loma 104-105 Mhz * km
- Za multimodne, s kontinuiranom promjenom indeksa loma 200-2000 Mhz*km
- Za multimodne, sa stupnjevitom promjenom indeksa loma 10-100 Mhz*km

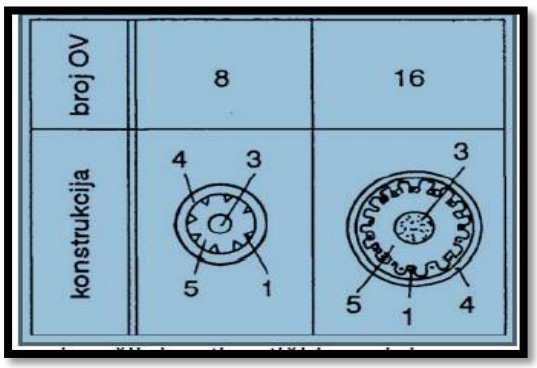
U matematičkom[12] smislu definirali smo to ovako: širina propusnog opsega (MHzKM) = širina propusnog pojasa (MHz) • duljina voda (Km)

4.5. Svjetlovodni optički kabel

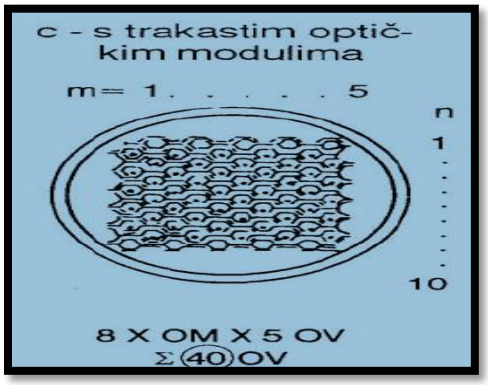
Optički kabel je skup optičkih vlakana, koja su na određeni način složena zajedno. Danas se najviše koriste tri osnovna tipa kabela slika 12.

Slika 12. Svjetlovodni optički kabeli.





Klasični optički kabel Žljebasti optički kabel.



Trakasti optički kabel

U klasičnim optičkim kabelima vlakna su složena u skupinu koncentričnim použenjem slično kao kod simetričnih kabela. Žljebasti optički kabel u kojemu su vlakna složena u utore na periferiji cilindričnog složenog elementa od plastične mase. Oblik može biti pravokutan, trokutast ili polukružan. Trakasti optički kabeli slažu se u redove tako da se dva krajnja ostavljaju prazna radi zaštite. Trakasti u kojemu su pojedinačna zaštićena i nezaštićena vlakna uložena u posebne vrpce od poliestera ili plastificiranog aluminija.

4.5.1. Konstrukcija svjetlovodnih optičkih kabela s obzirom na način polaganja

Konstrukcija svjetlovodnih optičkih kabela se razlikuje s obzirom na način polaganja. Bitni elementi konstrukcije kabela koji se projektiraju s obzirom na način polaganja su:

- Elementi za pojačanje
- Razne vrste zaštite

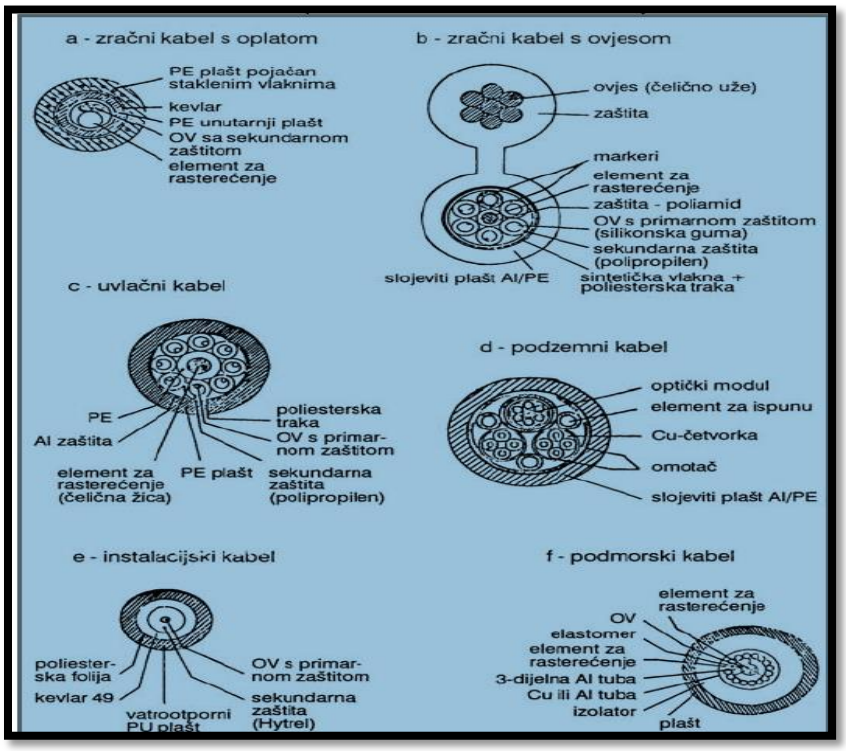
Elementi za pojačanje štite optička vlakna od prekida i/ili rastegnuća. Pojačanja se izrađuju od kovinskih žica, poliesterskih vlakana ili vlakana od plastičnih masa. Elementi za pojačanje mogu biti raspoređeni u jezgri:

- U središtu jezgre gdje je najveća fleksibilnost
- Više pojedinačnih vlakana na periferiji jezgre
- Oplet preko jezgre

Vrsta zaštite jezgre optičkog kabela ovisi o njegovoj namjeni, odnosno o predviđenom načinu polaganja, koja mogu biti, slika 13.

- Unutar zgrada (instalacijski)
- Iznad zemlje (zračni)
- Kroz kabelsku kanalizaciju (uvlačni)
- Ispod zemlje (podzemni)
- Ispod vode (podvodni)

Slika 13. Konstrukcije optičkih kabela s obzirom na način polaganja



Izvor: https://www.pfst.unist.hr/~ivujovic/stare_stranice/ppt/nastupno.ppt[136]

[136] Izvor: https://www.pfst.unist.hr/~ivujovic/stare_stranice/ppt/nastupno.ppt

4.6. Opis mjerne opreme

Zbog velike važnosti mjerenja svjetlovoda, razvijen je niz mjernih postupaka i izbor mjernih instrumenata. Mjerni postupci pomoću kojih se mogu utvrditi pojedini parametri svjetlovoda propisani su prema preporukama ITU-T. Pri tome su za mjerenje pojedinih parametara osim referentnih test metoda, utvrđene i alternativne metode, pomoću kojih se također mogu obaviti mjerenja pojedinih parametara svjetlovoda.

Na svjetlovodnim prijenosnim sustavima redovito se obavljaju mjerenja sljedećim njihovim komponentama:

- Mjerenje snage zračenja svjetlećih i laserskih dioda s pomoću poluvodičkih prijamnika
- Mjerenja na svjetlovodnoj niti
- Ispitivanje kvalitete sprežnika na svjetlovodnoj niti

Nakon što je svjetlovodni kabel spojen i završen, potrebno ga je provjeriti. Na svjetlovodnim prijenosnim sustavima prvo je potrebno ispitati njegovu neprekinutost, od kraja do kraja, a tek nakon toga treba ispitivati pogreške i probleme na njima. Ako se radi o dugačkom svjetlovodnom sustavu s puno međuspojeva svjetlovodne niti, treba provjeriti svaki spoj. Za provjeru svjetlovodnih spojeva najjednostavniji i najpouzdaniji način je mjerenje svjetlovodnim reflektometrom OTDR (Optical time domain reflectometer).

Na svjetlovodnim se nitima obavljaju mjerenja sljedećih njihovih značajki: prigušenja, disperzije, numeričke aperture, mjesta prekida ili mjesta njihove povrede.

Glavna ispitivanja (MJERENJA)

Jednomodne niti:

- Prigušenje
- Kromatska disperzija
- Kritična valna duljina

Višemodne niti:

- Prigušenje
- Višemodna disperzija
- Kromatska disperzija
- Numerička apertura

Jednomodna nit: Ako je mjerna valna duljina veća od kritične valne duljine jedne niti širit će se samo jedan mod. Uz ovaj uvjet mjerenja prigušenja jednomodne niti su manje komplicirane od onih na višemodnoj niti. Da bi se održala stalna pobuda niti, mjerenja treba obaviti u dva koraka:

- Prvo treba izmjeriti izlaznu snagu na daljem kraju
- Zatim se prereže nit na ulaznom kraju i ponovo se izmjeri snaga
- Razlika u razinama snaga u dB je prigušenje, to je metoda skraćivanja niti (cutback).

Druga metoda je analiza OTDR-om, koja zahtjeva pristup sa samo jedne strane što je jako praktično. Širina pojasa jednomodne niti ovisi o kromatskoj disperziji, koja je kod višemodnih niti zanemariva. Osnovna ideja mjerenja kromatske disperzije je slanje uskih impulsa kratkih valnih duljina (boja) kroz nit i mjerenje njihovih različitih vremena dolaska. Kritična valna duljina jednomodne niti definira najmanju valnu duljinu koja bi se trebala koristiti ako je važan širok propusni pojas. Ispod te duljine širi se više modova. Kritična valna duljina se mjeri tako da se pošalje široki spektar (na primjer iz volframove lampe) u kratku nit, te se mjeri prigušenja svake spektralne komponente. Kritična valna duljina je vidljiva kao diskontinuitet krivulje prigušenja.

Višemodna nit: najvažniji parametar niti je prigušenje svjetlosti. Ispitivanje prigušenja višemodnih niti je otežano zbog širenja mnogo modova, od kojih svaki ima svoje karakteristike širenja.

Osnova za mjerenje prigušenja su izvori svjetlosti i mjerač snage, pri čemu se izdvajaju dva načina mjerenja:

- Metoda skraćivanja niti
- Metoda povratnog raspršenja.

Višemodna disperzija predstavlja proširenje impulsa uslijed različitih brzina širenja kod različitih modova. Osnovni koncept mjerenja je da se nit pobudi kratkim impulsom, u kojem su modovi ravnotežno raspoređeni, te se izmjeri širina impulsa na kraju niti.

Numerički otvor (NA) i promjer jezgre određuju kolika se snaga može unijeti u višemodnu nit. NA definira maksimalni kut pod kojim zrake mogu ući u nit, uvijek se mjeri na izlazu iz niti (na udaljenom kraju) jer je maksimalni kut promatran na izlazu približno jednak istom na ulazu. Za mjerenja na svjetlovodnim kabelima potrebno je imati sljedeće:

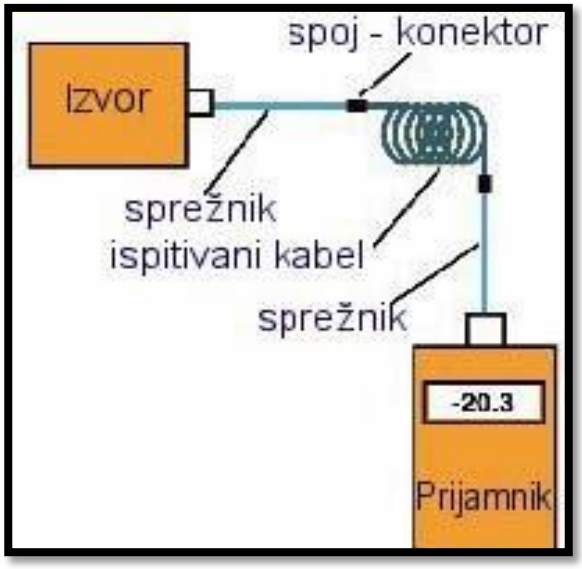
- Svjetlosni izvor i prijamnik za mjerenje izračene snage, mjerač gubitaka na svjetlosnoj niti s pripadajućom opremom
- Dovoljan broj kvalitetnih sprežnika s pripadajućim spojnicama konektorima, prilagođenih prema ispitivanoj niti
- OTDR s pripadajućom opremom za terenski rad
- Materijal i pribor za čišćenje svjetlovodnih niti i spojeva

4.6.1. Opis postupka mjerenja na svjetlovodnom kabelu

Prigušenje je omjer svjetlosne snage na ulazu i izlazu svjetlovoda. Kod mjerenja prigušenja na svjetlovodnom kabelu potrebno je izmjeriti izračenu snagu svjetlosnog izvora i svjetlosnu snagu na kraju svjetlovodnog vlakna. Za sva mjerenja na svjetlovodnom kabelu potrebno je osigurati svjetlosni izvor koji će izračiti energiju u obliku elektromagnetskog vala. Izračena snaga iz svjetlosnog predajnika je zapravo ulazna snaga u svjetlovodni prijenosni sustav. Apsolutna razina snage za mjerenja u svjetlovodnim sustavima iznosi 1 mW, a valne duljine elektromagnetskih valova su 850, 1310 i 1550 nm. Iz praktičnih razloga u mjernoj tehnici se rabi relativna izračena snaga izražena u dBm. To znači da u svjetlovodnoj tehnici apsolutna snaga 1 mW predstavlja relativnu snagu od 0 dBm, ili preko jedinice decibel: db=(10▪log P_1)/P_0, gdje je P1 apsolutna snaga u mW, a P0 referentna apsolutna razina snage od 1mW. Prigušenje (gubici) svjetlosne snage u svjetlovodnim kabelima ovisno je o valnoj duljini λ

zračenja koje prolazi kroz svjetlovod. Mjerenje prigušenja svjetlovodne niti obavlja se pomoću izvora referentne svjetlosti i prijamnika. Slika 14.

Slika 14. Mjerenje prigušenja na svjetlovodnom kabelu



Izvor: NBG Fiber Optic GMBH, Modular Cable System[137]

Prilikom mjerenja na svjetlovodu, iako svjetlosni izvori u svjetlovodne sustave izručuju relativno malu snagu, potrebno je voditi računa o zaštitnim mjerama (zaštita organa vida). Prilikom mjerenja ne smije se gledati u svjetlovodnu nit kada je uključen izvor svjetlosti. Nadalje, potrebno je sva rastavljiva spojna mjesta označiti zaštitnom oznakom za lasersko zračenje.

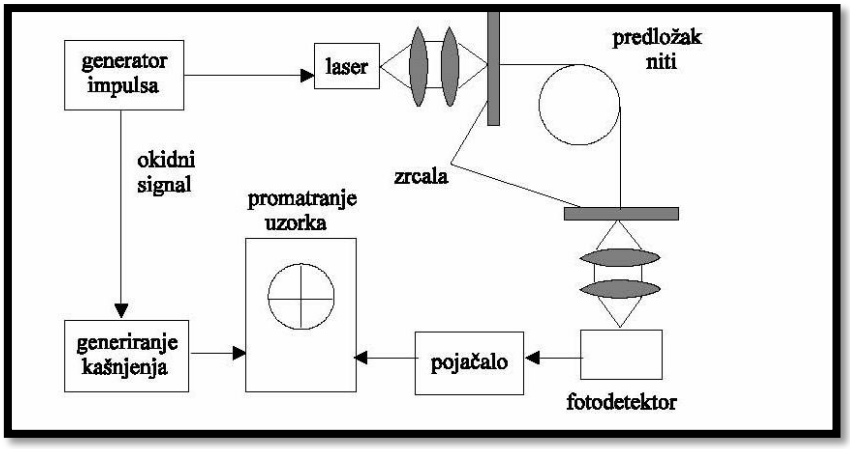
Mjerenje disperzije svjetlovoda u vremenskom području

Mjerenje disperzije na svjetlovodu u vremenskom području odnosi se na mjerenje širine (trajanja) impulsa na početku i kraju svjetlovoda i spada u najjednostavniji način mjerenja disperzije. Mjerenje se obavlja tako što se na jedan kraj svjetlovoda uvede optički impuls, a na drugom kraju svjetlovoda detektiraju i mjere prošireni impulsi. Kao izvor svjetlosti koristi se impulsni laser valne duljine $\lambda = 0{,}9\ \mu m$. Karakteristika ove metode je u tome da se na početku i na kraju svjetlovoda nalaze djelomično prozračna zrcala. Svjetlosni impulsi prolaze preko ulaznog zrcala u svjetlovod i cirkuliraju između njegovih krajeva.[138]

Disperzija se određuje na osnovu uspoređivanja na ekranu osciloskopa širine impulsa koji se vraćaju nakon uzastopnih cirkulacija u svjetlovodu sa širinom ulaznog impulsa. Usklađivanje impulsa usklađuje se pomoću linije kašnjenja. Ova mjerna metoda omogućava da se pomoću relativno kratkog odsječka emitiraju uvjeti prelaska signala po liniji veće duljine. Slika 15.

[137] Izvor: NBG Fiber Optic GMBH, Modular Cable System
[138] NBG Fiber Optic GMBH, Modular Cable System

Slika 15. Mjerenje disperzije svjetlovoda u vremenskom području.



Izvor : Sustavi strukturnog kabliranja, II dio: Svjetlovodni (pod) sustavi, EDZ Zagreb[139]

Mjerenje disperzije na svjetlovodu u frekvencijskom području daje, uspoređivanjem signala na ulazu i izlazu svjetlovoda, informaciju o amplitudno-frekvencijskoj i fazno-frekvencijskoj karakteristici svjetlovoda, koji su vrlo značajni podaci naročito kod projektiranja svjetlovodnih prijenosnih sustava.

Procedura za mjerenje amplitudnog odziva je vrlo jednostavna, sastoji se u mjerenju i usporedbi amplituda signala na ulazu i izlazu svjetlovoda, a za što se može koristiti spektralni analizator.

Kod mjerenja ukupne disperzije u frekvencijskom području, u svjetlovod se unosi svjetlosni signal promjenjive frekvencije, a stalne amplitude i faze. Aparatura za mjerenje fazno - frekvencijske karakteristike je vrlo precizna i skupa, pa se obično mjeri samo amplitudni odziv, iz kojeg se izračunava fazni odziv. Kao izvor svjetlosti mogu se koristiti LED ili laserske diode, čije se svjetlost direktno modulira strujnim signalima. Kao foto detektori se primjenjuju PIN ili lavinske fotodiode. Predajnik i prijamnik moraju imati približno isti frekvencijski opseg kao i svjetlovod, jer inače može doći do pogreške pri mjerenju.[140]

Određivanje mjesta prekida ili oštećenja na svjetlovodnoj niti. Karakteristično za oštećenje svjetlovoda je narušavanje cjelovitosti svjetlovoda i zaštitnog plašta. Metoda određivanja mjesta i vrsta oštećenja plašta analogne su metodama koje se koriste kod električnih vodova Međutim, oštećenja svjetlovoda su specifična. Pod oštećenjem svjetlovoda podrazumijeva se svaka nehomogenost koja dovodi do pogoršanja prijenosnih osobina svjetlovoda. Jedno od najčešćih oštećenja svjetlovoda je njegov prekid.

U osnovi postoje tri metode određivanja mjesta prekida svjetlovoda:

- Mjerenje svjetlosne energije izračene u okoliš
- Mjerenje jakosti povratnog Rayleighovog raspršenja

[139] Izvor : Sustavi strukturnog kabliranja, II dio: Svjetlovodni (pod)sustavi, EDZ Zagreb

[140] Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004

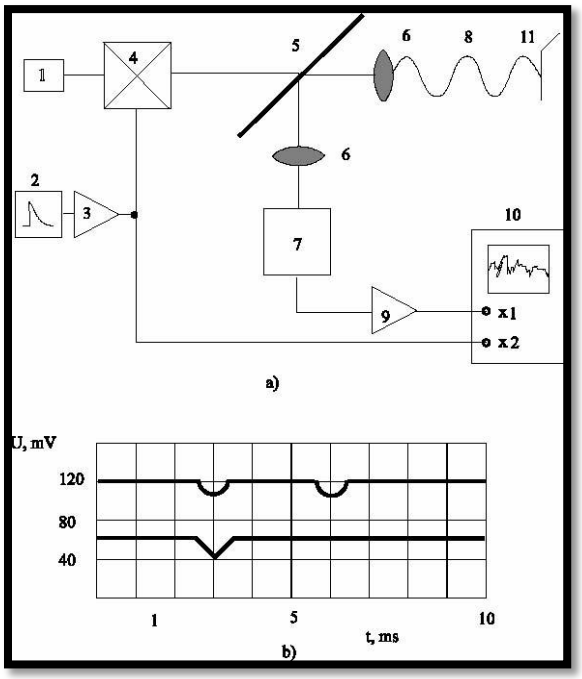
- Impulsno-lokacijska metoda

Prva metoda nije doživjela razvoj jer zahtjeva prijamni uređaj širokog dinamičkog raspona (110-140 dB). **Nedostatak druge** metode je niska razina tijeka povratnog raspršivanja, koja ne omogućava uporabu za mjesta prekida svjetlovoda jako velikih valnih duljina. **Impulsna metoda** ima visoku razlučivost i omogućuje identifikaciju kako mjesta nehomogenosti svjetlovoda tako i mjesta njegovog potpunog prekida.

Impulsno-lokacijska metoda mjerenja prekida slika 16. na svjetlovodnoj niti sastoji se od:

- Laser
- Generator impulsa
- Širokopojasno pojačalo
- Vanjski modulator
- Poluprozračna pločica
- Leća za fokusiranje
- Fotodioda
- Svjetlovodna nit
- Širokopojasno pojačalo
- Osciloskop
- Zrcalo

Slika 16. Impulsno lokacijska metoda mjerenja prekida svjetlovodne niti: a) blok shema mjernog uređaja; b) oscilogram impulsnog mjerenja



Izvor : NBG Fiber Optic GMBH, Modular Cable System[141]

Shema uređaja za impulsno-lokacijska mjerenja prikazana je na slici 16. (A). U nit se šalje skup sondirajućih impulsa i na osnovi vremena potrebnog za povratak reflektiranih impulsa

[141] Izvor : NBG Fiber Optic GMBH, Modular Cable System

od mjesta prekida, određuje mjesto prekida. Kada prođe kroz element za fokusiranje, svjetlosni snop lasera pada na poluprozirnu pločicu.
Poluprozirna pločica razdijeli svjetlosni snop na dva dijela: jedan, koji putem elemenata za fokusiranje dolazi u svjetlovod, a nakon toga u uređaj koji prigušuje sporedne modove i drugi koji se reflektira od zrcala i poluprozirne pločice te, pada na prijamnik koji se sastoji od uređaja za fokusiranje, fotodiode, pojačala i osciloskopa. Svjetlost reflektirana od mjesta povrede vraća se po niti i preko poluprozirne pločice, također dolazi u prijamnik. Na osnovi razlike vremena dolaska obaju impulsa određuje se udaljenost mjesta povrede niti. [142]

Na slici 16. (B). prikazan je oscilogram mjerenja u kojem prvi impuls, doveden na ulaz **x1** osciloskopa, odgovara impulsu reflektiranom od ulaznog poprečnog presjeka niti spram površine fokusirajuće leće. Drugi impuls odgovara impulsu reflektiranom od zrcala na kraj niti. Ova metoda omogućuje određivanje mjesta povrede niti (kabela) s točnošću od nekoliko metara. Za razliku od mjerenja izračene snage pomoću izvora i prijamnika, koji mjere prigušenje na svjetlovodnoj niti direktno, optički reflektometar radi indirektno. Izvor i prijamnik kopiraju stvarni predajnik i prijamnik na svjetlosnom prijenosnom sustavu, te se tako može vidjeti korelacija između stvarnog i mjernog sustava.

Kod OTDR-a slika 17. uporabom povratnog impulsa svjetlosti možemo otkriti prigušenja u svjetlovodnoj niti. Kao i klasični reflektometri, na ulazu u svjetlovodnu nit se pošalje uski impuls svjetlosti i promatra povratni impuls koji nastaje zbog nesavršenstva svjetlovodne linije ili refleksije zbog spojeva odnosno kraja linije. U svakoj točki vremena, svjetlo poslano iz OTDR-a prolazi kroz cijelu mjerenu duljinu svjetlovodne niti. Samo mali dio izračene svjetlosti vraća se natrag, ali uporabom osjetljivih prijamnika i normiranjem signala, moguća su mjerenja i na relativno dugim dionicama svjetlovodnih niti.

Slika 17. Primjeri proizvoda OTDR-a.

Izvor: Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004.[143]

[142] Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004

[143] Izvor: Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004.

Uz poznatu brzinu širenja impulsa svjetlosti duž svjetlovodne niti, reflektometrom se može izmjeriti vrijeme, a time je moguće izračunati vremensku poziciju impulsa u svjetlovodnoj niti, koja odgovara stvarnom položaju u njoj.

Kako se svjetlosni impuls prigušuje tijekom prolaza kroz svjetlovodnu nit i dodatno prigušuje na spojevima, ukupna snaga poslanog impulsa će se smanjivati u ovisnosti o prolazu kroz cijelu nit. Tako je pomoću odgovarajućeg programa moguće prikazati prigušenje svjetlovodne niti u odnosu na njenu duljinu. Karakteristična slika na ekranu optičkog reflektometra prikazana je slikom 18.

Slika 18. Prikaz niti na ekranu OTDR-a.

Izvor: Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004.

5. PRIMJER HAVARIJE KOD PLINSKOG OPERATERA TE NAČINI OČUVANJA KONTINUITETA POSLOVNOG PROCESA

5.1. Opći i specifični primjeri prekida poslovanja kod plinskog operatera

U završnome poglavlju rada prikazat će se primjeri prekida poslovanja kod plinskog operatera. Pažnja će biti usmjerena na uzroke prekida, utjecaj na poslovanje, načine detektiranja kvarova, postupke nakon detekcije kvarova, sekundarne načine komunikacije te naposljetku vračanje kontinuiteta poslovanja i primarne komunikacije u njegov normalan tok.

Kao primjere prekida poslovanja prikazat će se dva opća primjera prekida poslovnog procesa i dva specifična primjera prekida poslovanja kao i postupci vračanja poslovnog procesa u kontinuitet rada. Svi primjeri su primjeri stvarnih događaja na izdvojenim dionicama plinskog operatera. Primjeri prekida rasporedit će se po regijama Republike Hrvatske, regija Istok, Jug.

Prva dva primjera navesti će se kao opći primjer prekida poslovanja, odnosno kontinuiteta poslovanja kod plinskog operatera. To su primjeri grešaka koje su se ponavljale kroz poslovanje u periodu od 10 godina.

Druga dva primjera su specifična i zabilježena su svega tri ispada poslovanja i kontinuiteta poslovnog procesa u zadnjih 10 godina poslovanja plinskog operatera. Postupci detekcije kvarova kao i njihovo uklanjanje detaljno će se opisati i prikazati u zadnjem primjeru prekida poslovanja.

Prvi opći primjer prekida poslovanja spada u regiju Zapad. Ispad sustava primarne komunikacije dogodio se u mjesecu studenom kada je pravovremena isporuka energenta izuzetno bitna zbog niskih temperatura karakterističnih za to doba godine. Ispad sustava poslovanja dogodio se na izdvojenoj blokadnoj stanici (BS) glavnog pravca u opskrbi energentom. Razlog prekida rada primarnog sustava komuniciranja bilo je otuđenje opreme s BS stanice. U sustavu je prekid komunikacije detektiran gotovo momentalno jer osobe koje su otuđile opremu iz komunikacijskog ormara nisu znale da su na ulaznim vratima postavljeni detektori neovlaštenog ulaza. Otuđena oprema iz komunikacijskog ormara spada u vrlo skupocjenu opremu, prvenstveno to je oprema koja spada u aktivnu i pasivnu komunikacijsku opremu kao što su: UPS baterije neprekidnog napajanja, Cisco switch aktivne opreme koji je spojen s optičkim Cisco panelom pasivne optičke opreme i ostala oprema koja se nalazila u komunikacijskom ormaru a vezana je više za električne instalacije. U ovom slučaju incident koji se dogodio i izazvao prekid poslovanja u primarnom načinu komuniciranja između stanica nažalost nije izolirani incident i ponavljao se više puta kroz vremenski period od 10 godina. Komuniciranje i poslovanje nastavljeno je putem sekundarne komunikacije jer unutarnja jedinica sekundarne komunikacijske opreme nije bila otuđena. Način na koji se ovaj incident riješio je jednostavan i procedura je nalagala da oprema koja je otuđena iz komunikacijskog ormara postavi ponovo. S obzirom na to da ovo nije izoliran incident stanje na zalihama komunikacijske opreme je bilo dostatno da se ubrzo isti dan uspostavi primarna komunikacija. Gubitci poslovanja koji su ovim putem uzrokovani su bili neznatni s obzirom na to da su mogli biti puno veći.

Drugi opći primjer prekida primarnog komuniciranja i poslovanja a koji se ponavljao kroz period od 10 godina dogodio se u regiji Jug. Razlog je bila loša izvedba optičkih spojnica i spojeva u njoj a koje se nalaze na trasi između stanica plinovoda. Kod izvedba optičkih spojnica jako je bitno slijediti proceduru njihove izvedbe. Kod njihove izvedbe ključno je pravilno i kvalitetno izvesti spoj na svakoj optičkoj niti. U ovome slučaju ispada sustava problem je bio u prevelikom zagušenju optičkog signala koji se nije prikazivao kod mjerenja optičkim instrumentima nakon izvedbe optičke spojnice ali se zbog loše izvedbe spajanja optičke niti pojavio nakon nekog vremena. Detektiran je prekid signala na niti koja je bila aktivna u slanju podataka drugoj stanici trase plinovoda. Prekid poslovanja primarne komunikacije iziskivao je visoke troškove iskopa i pronalaska spojnice koja je bila postavljena na trasi plinovoda a zbog zahtjevne konstrukcije terena nije se slijedila procedura koja nalaže postavljanje velikog betonskog zdenca D4 radi zaštite optičke spojnice pa je spojnica postavljena u zemlju bez odgovarajuće zaštite. Činjenica da je spojnica postavljena protivno pravilnika struke nije bila ključna za ovaj incident već loše izveden spoj na niti kod spajanja i izrade spojnice. U ovome incidentu sekundarni način komunikacije također je preuzeo ulogu primarne i nije uzrokovao kompletan ispad sustava, velike troškove te neisporuku energenta do krajnjih korisnika.

Treći primjer prekida primarne komunikacija poslovanja nije se ponavljao tijekom 10 godina i zabilježen je samo jednom. Štetan događaj dogodio se u regiji Istok. Incident se dogodio zbog lošeg planiranja trase plinovoda. Trasa plinovoda u cilju smanjenja njene duljine i troškova postavljena je na terenu koji je otprije bio poznat kao "problematičan". Kod istraživanja tla i snimanja terena prije iskopa trase plinovoda, geolozi su ustvrdili da postoji mogućnost klizišta i podzemnih voda. Nažalost ispad sustava dogodio se upravo zbog nepoštivanja pravila struke i upozorenja stručnjaka. Trasa plinovoda na tome djelu je imala veliku visinsku razliku između dviju stanica i upravo na tome djelu pokrenulo se klizište. Klizište se pokrenulo uslijed velikih oborina i za sobom je povuklo i u potpunosti uništilo zdenac D4, sve optičke spojeve i dio plinovoda koji se nalazio na tom djelu trase plinovoda. Taj događaj iziskivao je enormne troškove izmještanja trase plinovoda s problematičnog terena, također je uzrokovao i neisporuku energenta krajnjem korisniku. U ovome slučaju sekundarna komunikacija između stanica također je preuzela način komuniciranja. Bilo je to od izuzetne važnosti jer je dio slobodnih, neaktivnih optičkih niti zakupio telekomunikacijski operater za svoje interne potrebe slanja podataka. Niti u jednom trenutku nije dovedena u pitanje njihova sigurnost i protok. Bez obzira na tu činjenicu nanesena je velika šteta plinskom operateru a sve zbog nepoštivanja pravila struke i nekompetentnosti nadređenih za izvedbu trase plinovoda na problematičnom terenu.

U svim navedenim i opisanim primjerima sekundarna komunikacija koja će biti opisana u sljedećem poglavlju je bila krucijalna za poslovanje plinskog operatera.

5.2. Primjer prekida na dionici A-B

Nakon opisa općih i jednog specifičnog primjera prekida primarne komunikacije poslovnog procesa kod plinskog operatera najbolji primjer za prikaz neprekinutog kontinuiteta poslovnog procesa i zadovoljavajuće razine sigurnosti je prekid na stvarnoj dionici A-B plinovoda. Primjer prekida na izdvojenoj dionici plinovoda, plinskog operatera koristit će se zamjenski nazivi A i B. Problem koji se dogodio na izoliranom incidentu u regiji Istok je specifičan i također je zabilježen jednom u 10 godina poslovanja plinskog operatera.

A predstavlja početnu točku s koje odlaze poslovni podaci kao dio poslovnog procesa. B predstavlja točku koja zaprima podatke, obrađuje ih i prosljeđuje dalje prema drugim stanicama koje zaprimaju podatke. Podatci koji dolaze na stanicu prikazuju se na PLC sustavu nadzora. Prikazuje se količina dolaza plina, njegova gustoća u cijevima, pritisak u cijevima prilikom prolaza plina te interni podaci tvrtke vezane za transakcije plina s opskrbljivačima. Prekid na dionici najčešće je plod ljudske nepažnje što uvelike utječe na sigurnost procesa i informacija koje su neophodne za neprekinuti kontinuitet samog poslovnog procesa. Primjer prekida vidljiv je na slikama 19.

Slika 19. Prikaz stvarnog prekida komunikacije na dionici A-B.

Havarija je nastala uslijed kopanja mehaničkim strojem radi detekcije mjesta ispuštanja plina iz plinske cijevi te je zbog ljudske nepažnje prekinuta komunikacija između dvije stanice A-B.

Slika 20. Prekinuta veza između dvije stanice A-B, zaštitna cijev FD FI 50 koja služi kao zaštita za svjetlovodni kabel potpuno je uništena

5.2.1. Postupci uslijed havarije

Zbog ljudske neopreznosti dogodila se havarija, sustav evidentira prekid na dionici A-B. Prekid je vidljiv gotovo momentalno na glavnom računalu u bazi plinskog operatera koje nadzire sve dionice plinovoda. Alarmi i lokatori koji su postavljeni na svim dionicama prikazuju dionice koje su u prekidu. Nakon što se dogodila havarija i prekinut je poslovni proces vrijeme odziva zaposlenika plinskog operatera je maksimalno 1 (jedan) sat od početka havarije. Dežurna ekipa izlazi na teren i vizualno pokušava detektirati kvar koji je zabilježen u bazi. Usporedno s odzivom zaposlenika poziv je usmjeren i prema vanjskim izvođačima kao back up potpora zaposlenicima plinskog operatera. Nakon 1 sata poziv je upućen prema izvođačima radova koji su dužni izaći na teren unutar 2 sata od primanja poziva.

Izlazak na teren mjesta prekida zahtijeva po ugovoru između izvođača radova i plinskog operatera 1 (jedan) inženjer kao nadzornika radova i 5 (pet) montera koji obavljaju tehnički dio zahvata na dionici. Zahtijeva svu pripadajuću opremu za detekciju kvarova, otklanjanje kvarova i vračanje primarne komunikacije u prvobitno stanje. Vrijeme odziva ponekada ovisi i o važnosti pojedine dionice, ako je dionica "manje" bitna tada se vrijeme odziva prolongira na drugi radni dan ali najčešće je unutar zadanih parametara 1 (jedan) sat, odnosno 2 (dva) za izvođače radova. Najčešće su to BS (blokadne stanice) koje se koriste isključivo za preusmjeravanje prometa prilikom rekonstrukcija glavnih stanica na plinovodu.

Slika 21. Vizualna detekcija kvara na stvarnoj dionici A-B.

Da bi se dionica A-B vratila u kontinuirani poslovni proces angažirana je pravna služba, sudski vještak te osiguravajuće kuće uz već opisane ekipe zaposlenika za detekcije kvarova. Pravna služba utvrđuje s angažiranim sudskim vještakom razloge prekida, tako štiti tvrtku i njen poslovni proces da bi se takve nezgode što više svele na minimum. Sudski vještak utvrđuje razloge prekida na terenu i visinu tražbine a pravna služba prosljeđuje izvješće do okrivljenika. Osiguravajuća kuća utvrđuje sa geodetskim uredom i geodetskim elaboratom zone zahvata jer nerijetko se instalacije nalaze u privatnim posjedima pa se utvrđuje i visina naknade za drugu oštećenu osobu na čijoj se katastarskoj čestici nalaze instalacije. Cijeli proces traje maksimalno tri dana.

5.2.2. Načini sekundarne komunikacije

Paralelno sa svjetlovodnim sustavom komunikacija, plinski operater je osigurao da se u slučaju štetnog događaja komunikacija ne prekine i dalje nastavi putem radiolinkova odnosno radiokomunikacijskih sustava prijenosa podataka. Dakle kod ispada jednog sustava komunikacije, drugi se aktivira momentalno. Kod štetnog događaja radio linkovima se privremeno preuzima komunikacija između stanice A-B. Način na koji se podatci sa stanice i dalje prosljeđuju je putem baznih postaja.

Slika 22. Primjer bazne postaje.

Izvor: Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004.[144]

Radio modemi se u UHF i VHF frekvencijskom području koriste za širok spektar aplikacija za komunikaciju u kritičnim situacijama, SCADA komunikaciju te nadzor i telemetriju. Ovi sustavi koriste niže frekvencijsko područje koje uvjetuje uske radijske kanale širine 12.5 ili 25 kHz što za posljedicu ima niže kapacitete, ali i iznimno robusnu komunikaciju dometa većeg od 100 km. Iako je komunikaciju korištenjem difrakcije moguće ostvariti i u uvjetima kada nema optičke vidljivosti, ovi sustavi mogu koristiti jedan ili više repetitora za povećavanje dometa i pokrivanja nekog područja. Sustav je industrijske građe, vrlo je robustan i pouzdan a veze tipično nude visoku raspoloživost. Zbog uskih RF kanala trošak korištenja RF spektra je nizak.

Da bi se osigurao kvalitetan signal koriste se radio platforme marke ECLIPSE koji pretvaraju signal pogodan za odašiljanje i po radio linku i po svjetlovoda. Uređaji su instalirani na stanicama A-B u komunikacijskom ormaru te na komunikacijskim stupovima ispred stanica.

Eclipse je mikrovalna radio platforma nove generacije koja podržava kapacitete prijenosa od 4xE1 (4x2.048 Mbit/s) do 2xSTM-1 (2x155 Mbit/s; 311 Mbit/s) i do 462 Mbit/s Native Ethernet prometa korištenjem jedne vanjske radio jedinice i jednog radio kanala širine 56 MHz. Eclipse je dostupan u širokoj paleti radnih frekvencija od 5 do 42 GHz unutar istog kućišta uz programski odabir modulacijskog postupka između QPSK, 16QAM, 32QAM, 64QAM, 128QAM i 256QAM.

[144] Izvor: Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004.

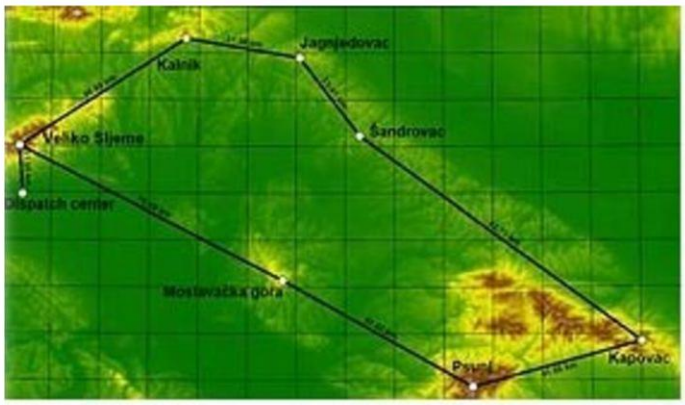
Eclipse packet node platforma koja se koristi na stanicama na jedinstven način kombinira visoku brzinu i transparentni prijenos Ethernet i TDM prometa, pružajući rješenje koje podržava jednostavan prijelaz s postojeće TDM mrežne infrastrukture na potpuno paketsku infrastrukturu. Eclipse radio sustav je zasnovan na učinkovitoj tzv. split-mount arhitekturi, odnosno sastoji se od unutarnje jedinice (INU), vanjske jedinice (ODU) te antenskog sustava. Unutarnja jedinica Eclipse slika 23. mikrovalnog radio komunikacijskog sustava modularnog je tipa tj. koncipirana je na metodologiji utičnih modula čime je omogućena redundancija, brza i jednostavna nadogradnja i održavanje uređaja za vrijeme eksploatacije. Dostupna je u dvije varijante: standardna INU s 4 utična modula visine 1RU i proširena INUe s 10 utičnih modula visine 2RU. Na stanicama se koristi druga navedena s 10 utičnih modula.

Slika 23. Unutarnja jedinica Eclipse.

Eclipse platforma

Izvor: http://www.microlink.hr/eclipse-platforma.aspx[145]

Također na stanice A-B ugrađuju se i ECLIPSE vanjske antene koji pretvoreni signal šalju na bazne postaje koje signal prosljeđuju dalje u bazu tvrtke.



Izvor: http://www.microlink.hr/eclipse-platforma.aspx[146]

[145] http://www.microlink.hr/eclipse-platforma.aspx

Modem koji omogućuje da se podatci prosljeđuju dalje od stanica su marke Apriza SR +, slika 24.

Slika 25. Modem Apriza SR +

Izvor: http://www.microlink.hr/eclipse-platforma.aspx[147]

Funkcioniranje je bazirano na sljedeći način:

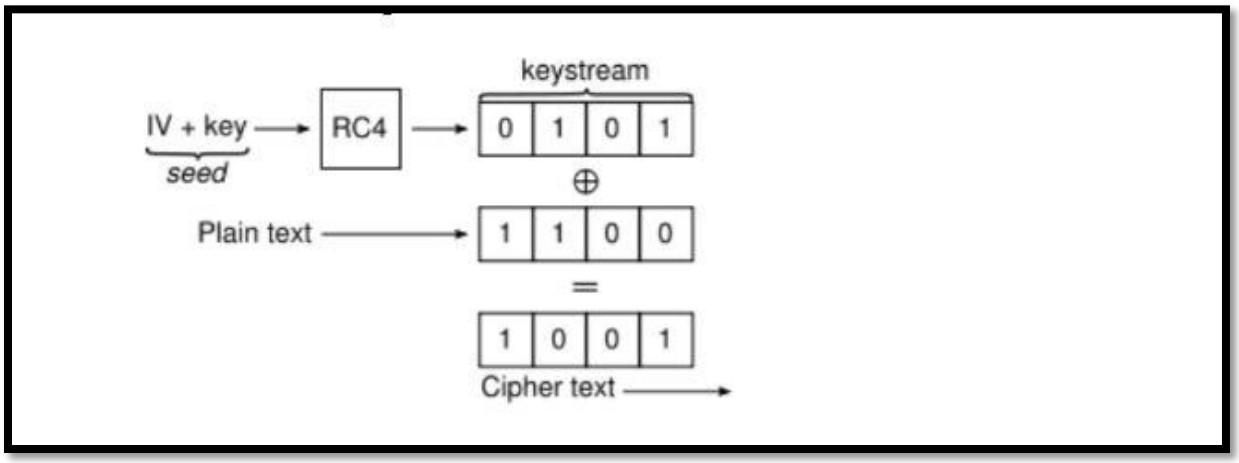
Apriza SR radio modem omogućava izgradnju komunikacijskih sustava u konfiguraciji točka prema više točaka namijenjenih za nadzor, mjerenje i upravljanje industrijskim postrojenjima putem SCADA sustava. SR radio modem podržava rad u VHF i UHF frekvencijskim pojasevima. Podržava spajanje putem serijskog ili Ethernet sučelja te podržava opciju spajanja dviju antena. Podržava rad na jednoj ili dvije frekvencije u half-dupleks načinu rada. Nominalno napajanje uređaja je 13,8 VDC. Snaga odašiljanja je podesiva od 0.1 do 5 W što omogućava prijenos informacija na velike udaljenosti, dok je osjetljivost prijamnika 117 dBm za širinu kanala od 12.5 kHz, odnosno 114 dBm za širinu kanala od 25 kHz. Uređaj koristi 4-CPFSK modulacijski postupak koji omogućava postizanje brzina prijenosa od 9,6 kbit/s za širinu kanala od 12,5 kHz odnosno 19,2 kbit/s za širinu kanala od 25 kHz. Na opisani se način dakle prosljeđuju podatci sa stanica uslijed havarije. Opisanoj opremi potrebno je godišnji pregled u jesen i prolijeće. Jesen da bi se uvidjeli nedostaci i pripremilo se za zimu a prolijeće da se uvidi na moguće posljedice zimskih uvjeta rada i da se otklone.

[146] Izvor: http://www.microlink.hr/eclipse-platforma.aspx
[147] Izvor: http://www.microlink.hr/eclipse-platforma.aspx

5.1.2.1. Sigurnost podataka uslijed sekundarne komunikacije

Uslijed sekundarne komunikacije bitan čimbenik za nastavak poslovnog procesa je i sigurnost podataka. Način na koji se štite podatci između stanica A-B je enkripcijom zaštićene prstenaste konfiguracije. Enkripcija slika 26. podrazumijeva da radio signali pretvaraju u nule i jedinice. Radio šalju signale na frekvencijama 2.4 GHz (802.11b i 802.11g standardi) i 5 GHz (802.11a), gdje se koriste mnogo naprednije tehnike kodiranja kao što su OFDM (orthogonal frequency-division multiplexing) i CCK (Complementary Code Keying) pomoću kojih se ostvaruju mnogo veće brzine prijenosa podataka samo uz pomoć radio valova.

Slika 26. Primjer kriptiranog signala



WEP je najraširenija enkripcija jer pruža osnovnu sigurnosnu zaštitu protiv većine korisnika koji slučajnu upadnu na nečiju mrežu. Implementirani sustav za zaštitu podataka je produženi 128-bit WEP protokol koristeći 104-bit key (ključ) veličinu (WEP-104). 128-bit WEP key (ključ) je gotovo uvijek unošen kao string od 26 Hexadecimalnih (Hex) znakova (0-9 i A-F). Svaki znak predstavlja 4 bita od key (ključ). 4 × 26 = 104 bita, dodajući 24-bita IV donosi nam, što zovemo "128-bit WEP key (ključ)". Sa gore navedenim sustavom, 24 bita od toga je za I.V., ostavljajući 232 stvarnih bitova za zaštitu. Ovo se tipično unosi sa 58 Heksadecimalnih znakova. (58 × 4 = 232 bits) + 24 I.V. bits = 256 bita od WEP zaštite.

Key (ključ) veličina nije jedino sigurnosno ograničenje u WEP-u. Krekiranje dužeg key-a (ključ) zahtjeva presretanje više paketa, ali postoje aktivni napadi koji stimuliraju neželjen promet. Postoje i druge slabosti u WEP-u, uključujući mogućnost od IV kolizije i promijenjenih paketa kojima ne pomaže nimalo dulji key (ključ).

Autentifikacija: dvije metode autentifikacije se mogu koristiti kod WEP-a:

- Open System authentication
- Shared Key (ključ) authentication.

Kada govorimo o WEP autentifikaciji, govorimo o infrastrukturnom modu (između WLAN klijenta i Access Pointa), ali debata se može primijeniti i na Ad-Hoc mode. Kod autentifikacije otvorenog sustava, WLAN klijent ne smije pružiti svoje isprave Access Pointu

prilikom autentifikacije. Bilo koji klijent bez obzira na njegov WEP key (ključ), može autentificirati sam sebe s Access Point-om i onda pokušati pridružiti.
Poslije autentifikacije i pridruživanja, WEP se može koristiti za enkripciju podatkovnih okvira. U ovom trenutku, klijent mora imati pravi ključ. Kod Shared Key (ključa) autentifikacije, WEP se koristi za autentifikaciju. Koristi se četverosmjerni challenge-response handshake.I) Klijentska postaja šalje autentifikacijski zahtjev prema Access Point.II) Access Point šalje natrag clear-text challenge.III). Klijent mora enkriptirati challenge text koristeći konfigurirani WEP key (ključ) i poslati ga natrag u drugom autentifikacijskom zahtjevu.IV) Access Point dekriptira materijal i uspoređuje ga s clear-text kojeg je poslao. Ovisno o uspješnosti ove usporedbe, Access Point šalje natrag pozitivan ili negativan odgovor.

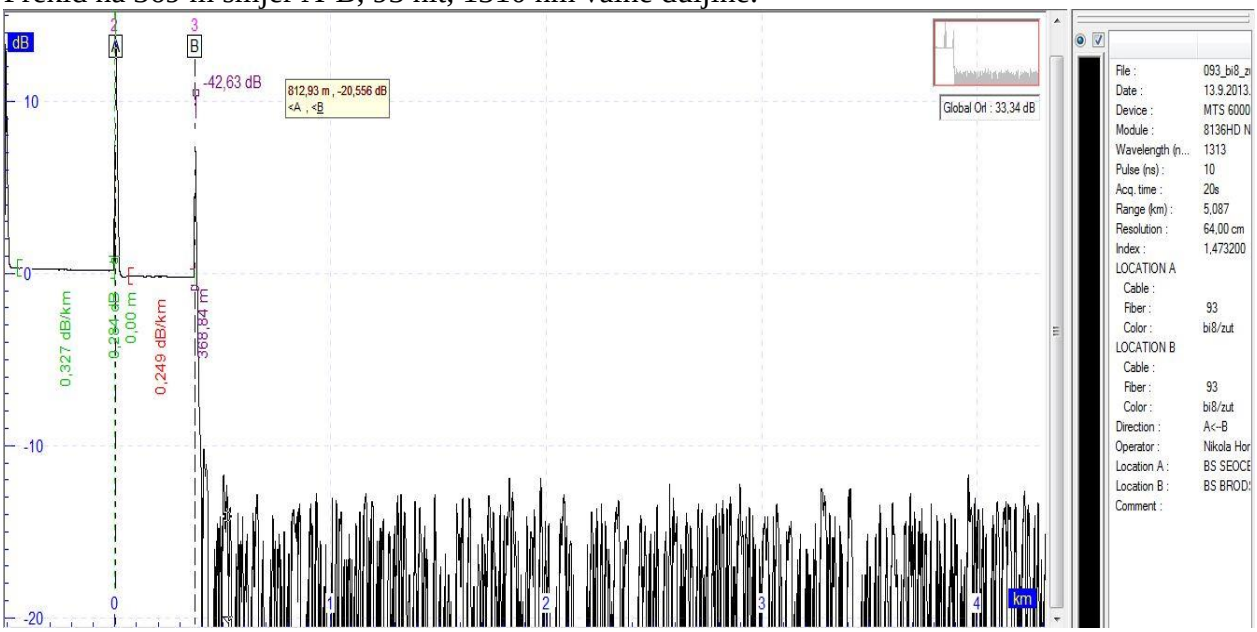
Poslije autentifikacije i pridruživanja, WEP se može koristiti za enkripciju podatkovnih okvira. Na prvi pogled se čini da Shared Key (ključ) autentifikacija je više sigurna nego Open System autentifikacija. No ipak je obrnuto. Moguće je stvoriti static WEP key (ključ) stavljanjem četiri handshake okvira u Shared Key (ključ) autentifikaciji. Preporučljivo je koristiti Open System autentifikaciju za WEP autentifikaciju.

5.2.3. Rezultati mjerenja nakon ponovne uspostave primarne komunikacija

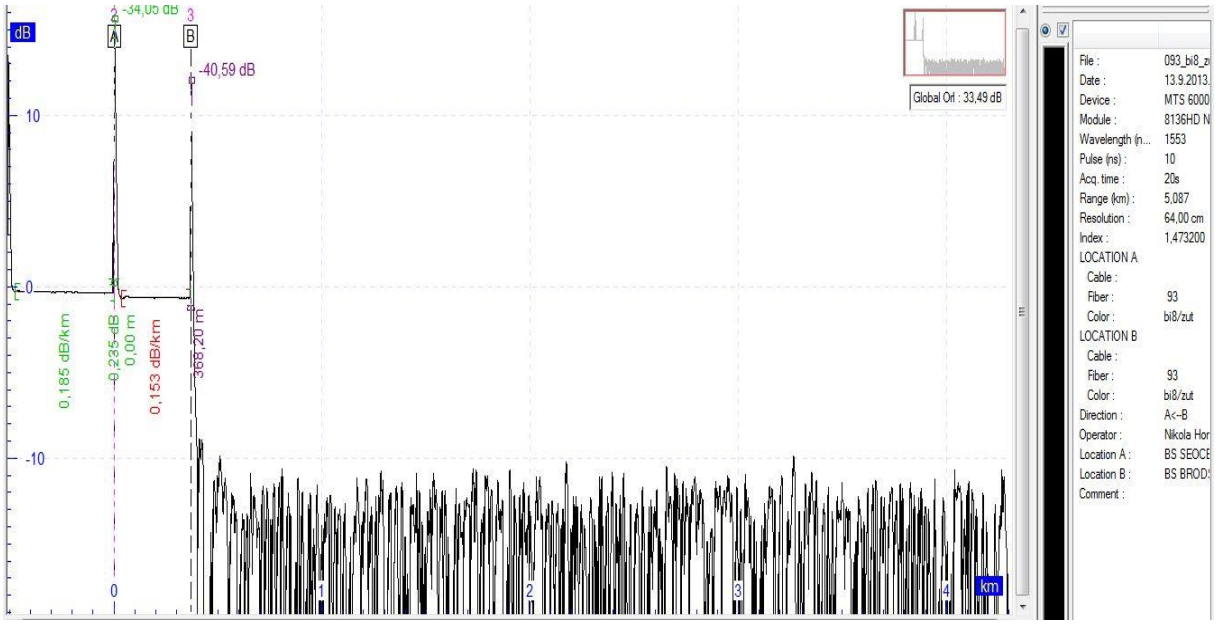
Nakon otkrivanja mjesta prekida na dionici A-B potrebna je njezina sanacija. Najbolji prikaz je u tablicama koji prikazuje mjerenja neposredno nakon štetnog događaja. Duljina dionice A-B iznosi 15,514 km. Prekid će biti jasno vidljiv na prvoj tablici. Prekid se dogodio na 368 m od početka dionice A-B. Mjerenje je izvršeno na valnim duljinama 1310 i 1550 nm. Mjerenje je izvršeno na zadnjih 6 niti na obje valne duljine 96 nitnog kabela. Primjer koji će se koristiti jest 93 nit, 96 nitnog kabela. Mjerenje nije izvršeno i na suprotnoj strani B-A jer prekid je bio jasno vidljiv vizualno pa nije bilo potrebe, potrebna je bila potvrda da nije dionica još negdje oštećena u blizini štetnog događaja.

Slika 27. Program fibre trace koji se koristi za očitavanje rezultata mjerenja s OTDR-a.

Prekid na 369 m smjer A-B, 93 nit, 1310 nm valne duljine.



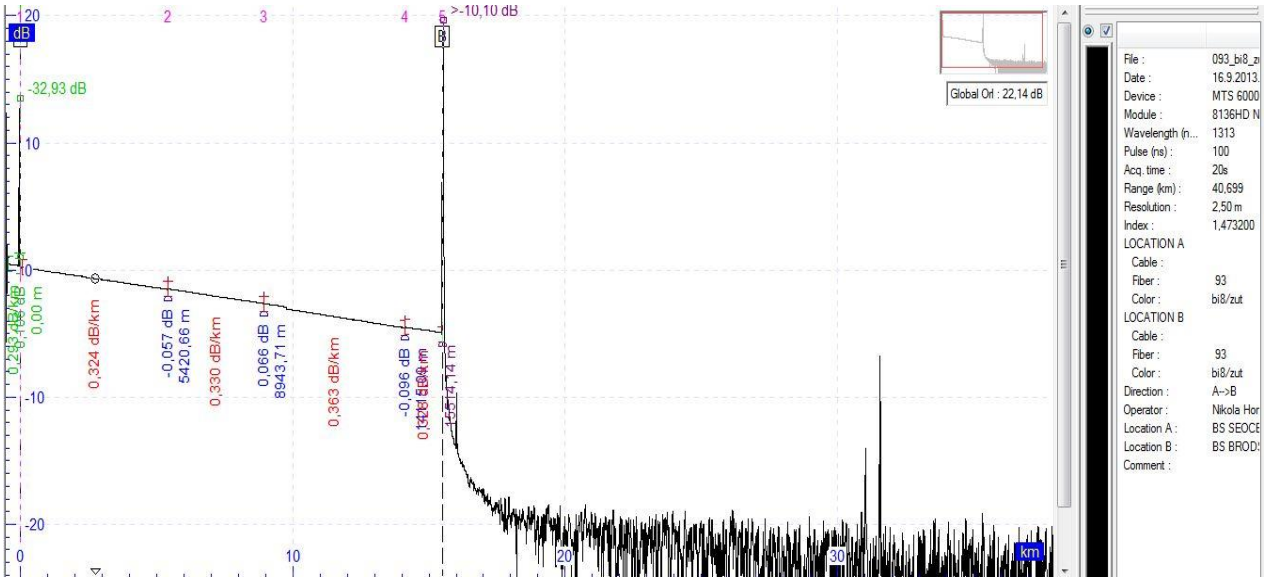
Slika 28. Program fibre trace koji se koristi za očitavanje rezultata mjerenja s OTDR-a. Prekid na 369 m smjer A-B, 93 nit, 1550 nm valne duljine.



Nakon potvrde prekida pristupljeno je sanaciji mjesta štetnog događaja i uspostave primarne komunikacije u cilju uspostave poslovnog procesa. Duljina dionice A-B iznosi 15,514 km. Primjer mjerenja s obje strane A-B i B-A na 1310nm valne duljine je prikazan u slikama 29 i 30.

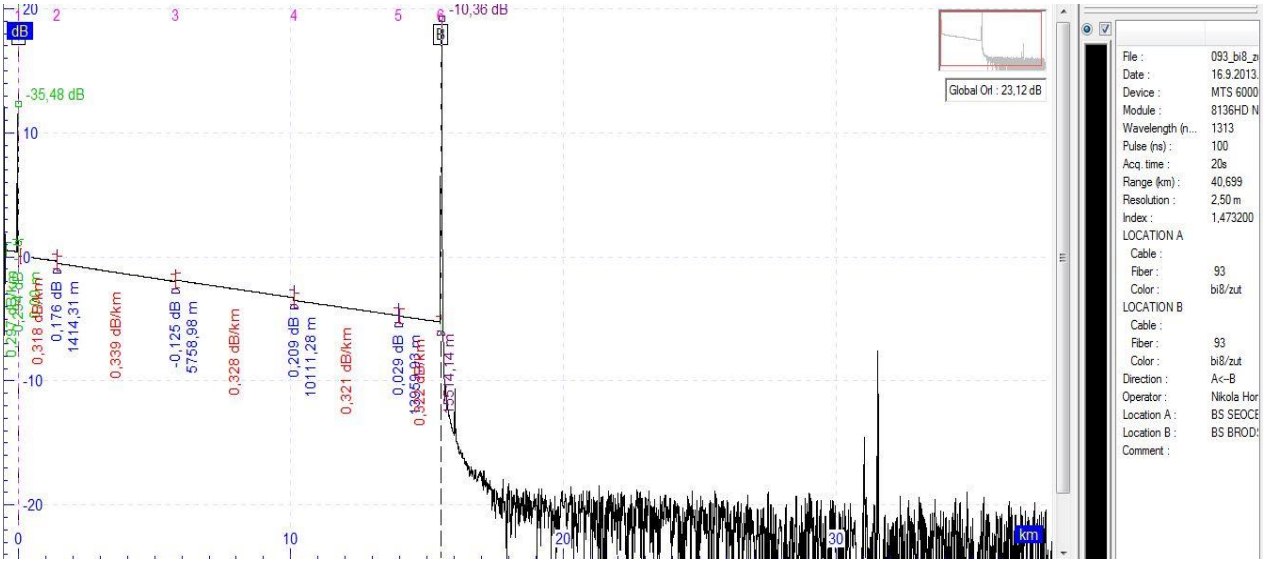
Slika 29 Program fibre trace koji se koristi za očitavanje rezultata mjerenja s OTDR-a.

Potvrda uspostave primarne komunikacije dionice A-B 15,514, 93 nit ,1310 nm valne duljine.



Slika 30. Program fibre trace koji se koristi za očitavanje rezultata mjerenja s OTDR-a.

Potvrda uspostave primarne komunikacije dionice smjer B-A 15,514, 93 nit ,1310 nm valne duljine.



5.2.4. Validacija svjetlovodnih linkova, analize i liste mjerenja

Nakon uspostavljene komunikacije potrebno je prema plinskom operateru ispostaviti kompletnu tehničko-opisnu dokumentaciju. Dokumentacija podrazumijeva:

- Iznos troškova sanacije
- Iznos radnih sati
- Mjerenje OTDR-om
- Mjerenje optical power metrom
- Tablice mjerenja kao validacija i dokaz za ponovnu uspostavu komunikacije
- Slike s mjesta štetnog događaja

Tablica 6, tablica mjerenja zadnjih 6 niti, 1310 nm valne duljine, crvenom bojom podcrtana 93 nit i njenog ukupno gušenje po dionici koje je u razinama prihvatljivosti kao primjer uspostave komunikacije.

Tablica 6. Završno mjerenje dionice A-B, dokaz uspostave primarne komunikacije valna duljina 1310 nm.

Dionica:		Lokacija A:	A		Razdjelnik :	-OR1	
		Lokacija B:	B		Razdjelnik :	-OR1	
Datum:		rujan, 2013.		Tip mjernog instrumenta:	1. JDSU MTS-6000 OTDR PLATFORM 2. JDSU 8136HD OTDR MODULE 3. MJERNO PREDVLAKNO DUŽINE 500m		
Mjerio:							
Duljina dionice:		15.514 m @1310nm					
Broj spojeva:		6		Mjerna metoda:	BACKSCATTERING		
Br.konekt.(par):		2		Tip kabela:	A-DQ(ZN)2Y 1X12 NZDSF + 7X12 SMF		
Redni broj niti		Valna duljina (nm)					
		Izmjereno gušenje (dB)					
Lok. A	Lok. B	1310 nm		1550 nm		1625 nm	
		A → B	B → A	A → B	B → A	A → B	B → A
91	91	3,27	2,98				
91	92	3,14	2,99				
93	93	3,32	3,14				
94	94	3,27	3,26				
95	95	3,25	3,23				
96	96	3,28	3,07				

Tablica 7. Završno mjerenje dionice A-B, dokaz uspostave primarne komunikacije valna duljina 1510 nm.

Dionica:		**Lokacija A:**	**A**		**Razdjelnik :**	**-OR1**	
		Lokacija B:	**B**		**Razdjelnik :**	**-OR1**	
Datum:		**rujan, 2013.**		**Tip mjernog instrumenta:**	1. JDSU MTS-6000 OTDR PLATFORM 2. JDSU 8136HD OTDR MODULE 3. MJERNO PREDVLAKNO DUŽINE 500m		
Mjerio:							
Duljina dionice:		**15.514 m @1550nm**					
Broj spojeva:		**6**		**Mjerna metoda:**	**BACKSCATTERING**		
Br.konekt.(par):		**2**		**Tip kabela:**	**A-DQ(ZN)2Y 1X12 NZDSF + 7X12 SMF**		
Redni broj niti		**Valna duljina (nm)**					
		Izmjereno gušenje (dB)					
Lok. A	**Lok. B**	**1310 nm**		**1550 nm**		**1625 nm**	
		A → B	**B → A**	**A → B**	**B → A**	**A → B**	**B → A**
91	91			2,99	2,97		
91	92			3,14	3,25		
93	93			3,04	3,27		
94	94			3,07	2,97		
95	95			3,06	3,05		
96	96			3,19	3,07		

Svi podaci mogu se koristiti kao dokaz protiv okrivljenika ili kao smjernica za neki mogući budući štetni događaj. Plinski operater nakon pregleda svih dokumenata i pohranjivanja u bazu podataka daje završni potpis kao dokaz za dobro obavljen posao i ponovnu uspostavu poslovnog procesa između stanica A-B.

5.3. Kontinuitet poslovnih procesa

Osnovna ideja kontinuiteta poslovanja zapravo je zaštititi informacije u slučaju neke veće i neočekivane nezgode (dakle, osigurati dostupnost informacija). Nažalost, nezgode koje mogu biti kobne za poslovanje su sve više prisutne. Tu se ne misli samo na terorističke napade, nego i na potrese, požare, poplave, kvarove sklopovlja te programske podrške i sl. Upravljanje kontinuitetom poslovanja predviđa pisanje planova koji određuju na koji način je potrebno postupiti u izvanrednim situacijama (priprema rezervne lokacije, određivanje vremena oporavka, priprema komunikacije u slučaju krize i sl.). Krajem 2006. godine, objavljene su norme BS 25999-1 i BS 25999-2 koje detaljnije opisuju upravljanje kontinuitetom poslovanja.

Prema tim normama, plan kontinuiteta poslovanja mora se sastojati od: [148]

1. Plana odaziva na incident

Plan odaziva na incident obično je jedinstven plan koji se odnosi na cijelu organizaciju i opisuje radnje koje se moraju poduzeti odmah nakon pojave havarije, smanjenje posljedica incidenta, komunikacija sa službama za hitne slučajeve, evakuacija zgrade, okupljanje na zbornim mjestima, organizacija transporta na rezervnu lokaciju i sl.

2. Plana oporavka

Plan oporavka se obično piše zasebno za svaku kritičnu aktivnost i mora obuhvaćati sljedeće korake:

- Vrijeme i način na koji se komunicira s raznim zainteresiranim stranama (zaposlenicima i njihovim obiteljima, dioničarima, klijentima, partnerima, državnim službama, javnim medijima i dr.)
- Princip sastavljanja tima
- Provođenje oporavka infrastrukture
- Provjera funkcionalnosti aplikacija i kontrole pristupa
- Provjerava podataka koji nedostaju i utvrđivanje svega što je oštećeno u havariji
- Oporavak podataka i uspostava normalnih aktivnosti

[148] Spremić, M. (2005.): Managing IT risks by implementing information system audit function, Proceedings of the 3rd International Workshop in Wireless Security Technologies, Westminster University, London, 04-05.04.2005

5.3.1. Veza između kontinuiteta poslovnih procesa i informacijske sigurnosti

Na prvi pogled reklo bi se da kontinuitet poslovanja i informacijska sigurnost nemaju puno veze. No, iz dubljeg promatranja njihove povezanosti proizlazi zaključak da postoje poveznice, i to velike. Naime, informacijska sigurnost se brine o povjerljivosti, integritetu i dostupnosti (raspoloživosti) informacija u nekoj organizaciji, dok se kontinuitet poslovanja u prvom redu brine da su informacije dostupne onima koji ih trebaju. Suština kontinuiteta poslovanja jest da osigurava kontinuitet ključnih poslovnih procesa u nekoj organizaciji. Kako se svaki poslovni proces bazira na protoku informacija, tako je fokus kontinuiteta poslovanja na dostupnosti, odnosno očuvanju i oporavku vitalnih poslovnih informacija. Sličnosti postoje i u nekim provedbenim dokumentima. Na primjer, svaka metodologija za kontinuitet poslovanja propisuje potrebu procjene rizika, koja se provodi na isti način kao i procjena rizika za informacijsku sigurnost. Dakle, dio dokumentacije će biti zajednički i za kontinuitet poslovanja i informacijsku sigurnost. S organizacijske strane isto tako postoje poveznice. Naime, vrlo često se funkcijska jedinica zadužena za brigu o kontinuitetu poslovanja nalazi baš unutar organizacijske jedinice koja je nadležna za informacijsku sigurnost.[149]

5.3.2. Strategija i planiranje kontinuiteta poslovnih procesa

Strategija kontinuiteta poslovanja donosi niz stavki, koje u slučaju nezgode služe za uspostavu funkcionalnosti poslovanja. Bitne stavke strategije kontinuiteta poslovanja su.:

- Ciljano vrijeme oporavka za pojedine poslovno kritične funkcije (eng. RTO - Recovery Time Objective)
- Minimalne obveze koje se moraju izvoditi tijekom nezgode u kritičnim situacijama vjerojatno neće biti moguće izvoditi pun opseg redovnih aktivnosti, pa treba odlučiti koje su nužne, a bez kojih se može (i koliku štetu one predstavljaju)
- Pronaći rezervnu lokaciju na kojoj će se ponovo uspostaviti svi poslovno kritični procesi, uključujući i informacijsku infrastrukturu, obradu podataka i sl
- Odrediti resurse koji će biti potrebni na rezervnoj lokaciji ne samo računalne resurse, već i ljudske resurse, računalne servise te dokumente u papirnatom obliku i ostalu opremu
- Članovi kriznog menadžmenta te zaduženja u situacijama nezgode
- Ciljana točka oporavka za podatka, odnosno koliko unatrag će biti moguće rekonstruirati podatke ako podaci budu uništeni u nezgodi

Ovaj zahtjev izravno određuje strategiju učestalosti izrade pričuvne pohrane podataka. [150]

- Jedinstvene i kritične točke koje mogu prouzročiti prekid u radu. U preventivnim aktivnostima se treba fokusirati na to da se osigura bolja zaštita upravo tih resursa
- Izvor i način nabave sve potrebne opreme u slučaju nezgode (ICT oprema, namještaj, vozila, strojevi, itd.)

[149] Symons, C., (2005.): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.

[150] Symons, C., (2005.): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.

5.3.3. Planiranje kontinuiteta poslovnih procesa

Planiranje kontinuiteta poslovanja je interdisciplinarna aktivnost, a obuhvaća metodologiju koja se koristi kako bi se stvorio praktičan plan oporavka. Plan koji opisuje način na koji će se organizacija oporaviti i vratiti u prijašnje stanje nakon djelomičnog ili potpunog prekida kritičnih poslovnih funkcija. Poseban naglasak nalazi se na realizaciji plana unutar unaprijed određenog vremena nakon nastupa prekida ili katastrofe. Plan koji je rezultat te aktivnosti naziva se planom kontinuiteta poslovanja. Plan kontinuiteta poslovanja opisuje način na koji se organizacija priprema za buduće incidente koji bi mogli ugroziti osnovnu poslovnu djelatnost i dugoročnu stabilnost poduzeća. Takvi incidenti uključuju:

- Lokalne incidente (npr. požar, poplava)
- Regionalne incidente (npr. zemljotres)
- Nacionalne incidente (npr. pandemija)

U prosincu 2006. godine Britanski institut za standardizaciju izdao je novi standard - BS 25999, koji se naslanja na standarde BS 7799 odnosno ISO/IEC 27001. Taj novi standard proteže se na organizacije svih veličina, vrsta i svrha postojanja, bez obzira na to da li su vladine ili privatne, profitne ili neprofitne, velike ili male, te neovisno o vrsti industrijskog sektora. Dovršeni plan kontinuiteta poslovanja podrazumijeva izdavanje formalnog pisanog priručnika koji mora biti raspoloživ za korištenje prije, tijekom i nakon što je došlo do prekida poslovanja ili katastrofe. Njegova je osnovna svrha umanjiti negativne posljedice po zainteresirane strane, kako po pitanju vrste katastrofe, tako i po pitanju duljine trajanja. Pri tome treba imati na umu da se nazivom "katastrofa" obuhvaćaju svi oblici ekonomskih, građanskih, prirodnih, tehničkih, sekundarnih i posljedičnih incidenata koji imaju negativan utjecaj na poslovanje. Osnovni dio izrade plana kontinuiteta poslovanja je određivanje ciljnog vremena oporavka (eng. RTO - Recovery Time Objective). [151]

RTO u biti predstavlja vrijeme unutar kojeg se poslovni procesi moraju ponovno uspostaviti kako bi se izbjegle nepoželjne posljedice povezane s kontinuitetom prekida. RTO se određuje u fazi analize utjecaja (od strane vlasnika procesa), u suradnji s osobom koja izrađuje plan kontinuiteta poslovanja. Potrebno je napomenuti da je RTO cilj a ne točno određena vrijednost. Stoga će u praksi vrlo često biti odabrana strategija koja neće uspjeti dostići RTO, no on svejedno ostaje cilj sljedeće revizije strategije. Stvarna vrijednost u ovom kontekstu naziva se RTA (eng. RTA -Recovery Time Actual), dok se razlika do RTO naziva "gap". Do stvarne RTA vrijednosti se dolazi simulacijama ili vježbama, odnosno empirijski, u slučaju nastupa stvarnog prekida poslovanja. Metodologija planiranja kontinuiteta poslovanja mora biti prilagođena svim organizacijama neovisno o veličini i složenosti. Iako ona ima korijene u industrijskom sektoru, svaka organizacija može stvoriti svoj plan kontinuiteta poslovanja. Statistike istraživanja provedenih na Business Continuity Institutu u Velikoj Britaniji (BCI) govore da poduzeća ne ulažu dovoljno vremena i resursa u pripremu plana kontinuiteta poslovanja, pa tako recimo požari rezultiraju zatvaranjem 44% poduzeća u kojima se dogode.

[151] Weill, P., Ross, J.W., (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvards Business School Press.

5.3.4. Izrada plana kontinuiteta poslovnih procesa

Plan kontinuiteta poslovanja mora biti izrađen tako da bude realističan i da se tijekom krize može koristiti na jednostavan način. Krizno rukovodstvo raspolaže planom kontinuiteta poslovnih procesa te njime upotpunjuje plan oporavka od katastrofe osnovne faze izrade plana kontinuiteta poslovanja su sljedeće:

- Analiza
- Dizajn rješenja
- Implementacija
- Ispitivanje i prihvaćanje od strane organizacije
- Održavanje prihvaćenog plana

Institut za kontinuitet poslovanja iz Velike Britanije prikazuje u dijagramu životne cikluse Plana kontinuiteta poslovanja (eng. Life Cycle Business Continuity Planing BCP.) Dijagram prikazuje bitne dijelove vremenskom toku izrade plana. Potrebno je prije svega [152]

- Ustanoviti moguće rizike te utjecaj pojedinih rizika (eng. Identify, Risk Assessment);
- Provesti detaljnu analizu utjecaja na posao (eng. Business Impact Analysis)
- Dizajnirati rješenje te odabrati strategiju plana oporavka (eng. Design, Strategy selection)
- Implementirati dizajn i odabranu strategiju (eng. Execute, Plan Develop / Execution);
- Provesti mjerenja i ispitivanja provedenog plana te održavanje plana u budućnosti (eng. Measure, Plan Test and Maintenance)

5.3.5. Matrica razine rizika

Razina rizika utvrđuje se množenjem ocjene koja je dodijeljena vjerojatnosti da izvor prijetnje iskoristi ranjivost s ocjenom učinka neželjenog događaja, pri čemu se uzima u obzir prikladnost planiranih ili postojećih kontrola. Matrica razine rizika daje jednostavan primjer kako se mogu odrediti rizici na temelju podataka o vjerojatnosti da izvor prijetnje iskoristi ranjivost i o učinku. Ovisno o izvor prijetnje mogu imati ranjivost (veliku, srednju ili malu) i učinka (velikog, srednjeg i malog), koja prikazuje kako se računa ukupna razina rizika. Na primjer:

- Ocjena vjerojatnosti da izvor prijetnje iskoristi ranjivost koja se pripisuje svakoj razini vjerojatnosti prijetnje jest 1,0 za veliku, 0,5 za srednju i 0,1 za malu
- Ocjena učinka koja se dodjeljuje svakoj razini jačine učinka jest 100 za veliku, 50 za srednju i 10 za malu. Ovisno o potrebama i detaljnosti procjene rizika može se koristiti matrica proizvoljnih dimenzija

[152] Weill, P., Ross, J.W., (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvards Business School Press.

5.3.6. Analiza kontinuiteta poslovanja

Faza analize kontinuiteta poslovanja sastoji se od analize utjecaja na poslovanje, analize prijetnji i izrade scenarija utjecaja. Kao rezultat ove faze dobiva se jasna podjela između kritičnih i nekritičnih funkcija u organizaciji. Poslovna funkcija se smatra kritičnom, ako utjecaj realizacije nekog izvanrednog događaja ima neprihvatljive posljedice po nju i po interese organizacije. Percepcija prihvatljivosti posljedica nastupa izvanrednih događaja može se promijeniti ako se prezentira trošak uspostavljanja i održavanja odgovarajućih poslovnih ili tehničkih rješenja oporavka. S druge strane, određena funkcija može se smatrati kritičnom (ako je takvom definira lokalna zakonska legislativa). Analiza utjecaja na poslovanje (eng. Business Impact Analysis) je jedan od ključnih koraka u upravljanju kontinuitetom poslovanja. Naime, nije dovoljno samo odrediti rezervnu sigurnu lokaciju i napisati planove oporavka za poslovno kritične funkcije, nego je potrebno odrediti i ciljano vrijeme oporavka. Ciljano vrijeme oporavka je ništa drugo nego maksimalno vrijeme koje si organizacija može priuštiti da joj pojedini ključni poslovni procesi (npr. naplata usluge, interakcija s korisnicima itd.) ne funkcioniraju. [153]

Pored toga, potrebno je odrediti međuovisnosti između različitih poslovnih procesa (npr. većina poslovnih procesa ovisi o informatičkoj potpori, što znači da će se taj poslovni proces odnosno funkcija morati prvo oporaviti). Te informacije su bitne zato što se u sljedećem koraku upravljanja kontinuitetom poslovanja puno jednostavnije može odrediti strategija za nivo opremljenosti rezervne lokacije. Ako je poslovni proces potrebno oporaviti u iznimno kratkom roku (npr. 4 sata od incidenta), onda će investicija u rezervnu lokaciju biti bitno veća jer će se tada morati unaprijed instalirati sklopovlje, programska oprema, komunikacijski kanali i baze podataka. Ako je poslovni proces takav da je dozvoljeno vrijeme oporavka nešto duže (npr. 4 dana), onda će investicija u rezervnu lokaciju biti puno manja. Razlog tome jest što se tijekom tih 4 dana može nabaviti većina opreme (što znači da se unaprijed ne mora investirati previše novca), uspostaviti komunikacijski kanali i restaurirati programi i baze iz sigurnosnih kopija.

Dakle, pažljivo napravljena i odmjerena analiza utjecaja na poslovanje može donijeti velike uštede organizaciji, a da se pri tome ne naruši sigurnost poslovanja. Tijekom analize utjecaja na poslovanje obično se procjenjuju sljedeći elementi vezani za pojedinu poslovno kritičnu funkciju:[154]

- Koliko tržišnog udjela organizacija može izgubiti?
- Kako će klijenti karakterizirati takav prekid poslovanja?
- Kako će to utjecati na ugled organizacije?
- Koliko podataka organizacija može izgubiti?
- Kakve su izravne financijske posljedice (zakonske ili ugovorne kazne)?
- Sve te elemente potrebno je promatrati u različitim vremenskim razmacima, i na neki način ih valorizirati. Odrediti prioritet svakog elementa zasebno s obzirom na poslovanje organizacije

[153] Weill, P., Ross, J.W., (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvards Business School Press.

[154] Spremić, M. (2005.): Procjena razine pouzdanosti internih kontrola informacijskog sustava s pomoću CobiT metodologije, Revizija, računovodstvo i financije, br. 12/2005

5.3.7. Analiza prijetnji

Analiza prijetnji slijedi analizu utjecaja. U ovoj fazi potrebno je identificirati sve potencijalne prijetnje kako bi se detaljno opisali specifični koraci oporavka u slučaju katastrofe. Neke uobičajene prijetnje koje se obrađuju u ovoj fazi su:[155]

- Zarazne bolesti
- Zemljotres
- Požar
- Poplava
- Napad preko kompjutorske mreže
- Nestanak struje i vode
- Terorizam

Sve navedene prijetnje, osim bolesti, dijele zajednički utjecaj na organizaciju, a to je njihov potencijal za oštećivanjem infrastrukture. Utjecaj bolesti usmjeren je primarno na ljudsku komponentu organizacije i može se umanjiti tehničkim i poslovnim rješenjima. Međutim, ako bolesti pogode osobe u organizaciji koje stoje iza provođenja plana oporavka poslovne aktivnosti, primarna zadaća neće biti ispunjena zato što je sudjelovanje rukovodećih osoba u provođenju plana oporavka od neizmjerne važnosti. Rješenje takve ekstremne situacije kao što je bolest rukovodećih osoba u provedbi plana oporavka je samo jako dobro pripravljen plan, spreman podnijeti i najekstremnije situacije.[156]

5.3.8. Dizajn rješenja i implementacija

Cilj faze dizajna je identifikacija troškovno najpovoljnijeg rješenja oporavka od katastrofe koji u sebi pomiruje dva osnovna zahtjeva iz faze analize utjecaja, a to su detaljna analiza prijetnji i analiza mogućih scenarija utjecaja. U fazi dizajna, definirani zahtjevi oporavka i ciljevi oporavka prevode se operativno u konkretne mjere. Najvažniji proizvod ove faze uspostavljanje je organizacije oporavka (eng. Business Recovery Organization). Konkretan rezultat uspješnog provođenja ove faze stvaranje je procedura za eskalaciju, obavještavanje i aktivaciju samog plana oporavka s fokusom na kritične poslovne funkcije organizacije. Tipično, zahtjevi organizacije mogu se izraziti na sljedeći način:[157]

- Minimalni zahtjevi za aplikacijama i podacima
- Vremenski rok u kojemu minimalni zahtjevi za aplikacijama i podacima mogu postati opet raspoloživi.

[155] Srića, V., Spremić, M., (2000.): Informacijskom tehnologijom do poslovnog uspjeha, Sinergija.

[156] Srića, V., Spremić, M., (2000.): Informacijskom tehnologijom do poslovnog uspjeha, Sinergija.

[157] Srića, V., Spremić, M., (2000.): Informacijskom tehnologijom do poslovnog uspjeha, Sinergija.

Rezultat faze dizajna rješenja detaljan je opis sljedećih funkcija i aktivnosti:

- Zapovjedna struktura kriznog rukovodstva
- Lokacija sekundarnog radnog mjesta (zgrade)
- Telekomunikacijska struktura između primarnog i sekundarnog radnog mjesta
- Način replikacije podataka
- Aplikacije i programska podrška koji trebaju biti operativni na sekundarnom radnom mjestu
- Fizički zahtjevi sekundarne radne lokacije

5.3.9. Faza implementacije

Implementacija je faza u kojoj se elementi dizajna identificirani u fazi dizajniranja provode u djelo. Nju se može promatrati i odvojeno od faze dizajna rješenja no nastavlja se neposredno na nju, i zbog svog operativnog karaktera, predstavlja značajan dio plana kontinuiteta poslovanja kako troškovno, tako i vremenski. Korak izvođenja i implementacije plana kontinuiteta poslovanja u pravilu ne može biti uspješan ako nije uspostavljen centar ili odbor za izvođenje hitnih akcija, te ako u prethodnim fazama nisu adekvatno definirane procedure za nastavak rada, oporavka i obnavljanja svih nužnih poslovnih resursa. Za većinu organizacija je značajan i sustav održavanja te stalna procjena ugovora s vanjskim dobavljačima, te održavanje kontingentnih rezervi svih kritičnih resursa. Naposljetku, u fazi implementacije započinje se s internim kampanjama o važnosti praćenja procedura vezanih uz stvaranje plana kontinuiteta i oporavka, te treningom, kako svih izravno uključenih u akcije oporavka, tako i svih korisnika usluga poslovnog sustava.[158]

[158] Weill, P., Ross, J.W., (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvards Business School Press.

6. ZAKLJUČAK

Glavni ciljevi rada bili su **(1)** objasniti pojam kontinuiteta poslovanja i prihvatljive razine rizika te prikazati i analizirati model kontinuiteta poslovanja te **(2)** analizirati odabrani model očuvanja kontinuiteta poslovanja.

(1) Prikazano je da svako uspješno poduzeće svoje uspjehe može ponajprije zahvaliti praksi upravljanja poslovnim procesima. Primjenama informacijskih tehnologija i znanja upravljanja poslovnim procesima zaposlenika koji su zaduženi za njeno funkcioniranje i razvoj osiguran je dugoročan i uspješan razvoj poduzeća. Upravljanje poslovnim procesima priprema poduzeće i podiže stupanj kompetitivnosti i spremnosti poduzeća na brze promjene ili u ovome slučaju prekid poslovnog procesa uslijed havarije.

Bitan čimbenik za poslovanje poduzeća i neprekinutost poslovnog procesa je informacijska sigurnost i procjena rizika od upada u sustav i priprema za potencijalne prekide u poslovanju. Ako se na kvalitetan način izvrši provođenje procesa procjene rizika, to će rukovodnim strukturama omogućiti sagledavanje stvarnog stanja sigurnosti te im tako olakšati donošenje odluka o načinu upravljanja sigurnošću informacijskih sustava. Uz neminovno iskustvo, vrlo važan čimbenik kod procjene rizika predstavlja i dostupna dokumentacija o sustavu za koji se radi procjena rizika, odnosno podaci koji govore o nastalim incidentima unutar samog sustava.

Među ključnim ciljevima svake tvrtke odnosno poslovne organizacije predstavlja osiguranje neprekinutosti poslovanja, koje u značajnoj mjeri ovisi o zaštiti informacijskih resursa. Uslijed toga, uvođenje sustava upravljanja sigurnošću informacijskog sustava predstavlja provedbu potrebnih mjera za postizanje zadovoljavajuće razine informacijske sigurnosti unutar jedne poslovne organizacije. Tako se pruža nesmetanost vršenja djelatnosti tvrtke, ali i tvrtka postaje prepoznata kao pouzdan poslovni partner, koja se u svakom trenutku može suočiti s najnovijim sigurnosnim prijetnjama i na vrijeme reagirati na moguće sigurnosne incidente odnosno eventualne neovlaštene upade u sustav.

Da bi se sustav osigurao čak kada se dogodi i pad primarne komunikacije putem optičkog vlakna koje se pokazalo kao izvrstan potez poduzeća koje su ga uvele paralelno se uvelo i sekundarna komunikacijska veza putem radio linkova. Optičko vlakno uvode sve napredne tvrtke u želji za poboljšanjem i unapređenjem poslovnog procesa. Napuštaju se zastarjele tehnologije i uvode se nove koje mogu obraditi neusporedivo mnogo više podataka od prijašnjih tehnologija.

(2) Na temelju analize odabranog modela očuvanja kontinuiteta poslovanja pokazano je za da neprekinutost opskrbe plinom plinski operater poduzeo sve upravljačko-sigurnosne korake da bi se čak i uslijed havarije poslovni proces bez gubitaka podataka neometano nastavio. Iskustvo terena i ljudi koje rade na poslovima osiguranja i sigurnosti poslovnog procesa govore da je najbitnija pomna priprema i slijed protokola kada se havarija i dogodi. Protokoli su jasno propisani i ljudi koji su na njemu angažirani bogati su iskustvom nošenja sa situacijama kada se prekid poslovnog procesa doista i dogodi. Primjer prikazan u ovome radu najbolji je primjer kako se ti protokoli slijede, na koji se način vodi cijeli proces uspostave ponovne komunikacije te kako se štiti sigurnost podataka uslijed havarije kod sekundarne komunikacije.

Što se tiče specifičnih ciljeva rada:

a) Prikazana je važnosti kontinuiteta poslovnog procesa i informacijske sigurnosti te posljedica koje mogu nastati prekidom poslovnih procesa kod plinskog operatera i istražiti mogućnosti sprječavanja tih scenarija. Većina poslovnih procesa ovisi o informacijsko -komunikacijskoj tehnološkoj infrastrukturi te o kvantiteti, kvaliteti i dostupnosti informacija koje takva infrastruktura osigurava i podržava.

b) Opisani su načini zaštite sustava i postupci uslijed havarije te prijedlog rješenja uslijed štetnog događaja na temelju čega je jasno vidljiva kompleksnost ovih procesa.

c) Prikazan je opis procesa upravljanja u situacijama havarije odnosno prekida neometanog protoka informacija u svrhu zaštite podatka i nastavka procesa protoka istih na temelju čega se uočava važnost uspostave protokola i strogog pridržavanja istog.

d) Jasno je ukazano na nužnost upravljanja informacijskom sigurnošću tog zatvorenog sustava sa samodostatnom optičkom mrežom te je analizira modela očuvanja njegova kontinuiteta upotrebom sekundarnog načina komuniciranja pokazala da je takva opcija nužna;

e) Opisane su značajke svjetlovodnih vlakana i svjetlovodnih kabela te je na temelju primjera greške na izdvojenoj dionici trase plinovoda pod nazivom A-B te kompletnog procesa opisa tehničkog dijela otklanjanja grešaka kao i prethodno zaštite sustava poslovnog procesa dokazana i istaknuta važnost pojedinih postupaka za očuvanje kontinuiteta poslovanja.

f) Prikazani su načini uštede vremena i resursa na temelju čega je vidljivo koliko je važno da opskrba energentom teče neprekidno da bi se poslovni proces odvijao unutar zadanih rokova isporuke.

Svrha opisane svjetlovodne dionice A-B je prijenos podataka protoka plina, zapremnine plina, njegove gustoće i kvalitete te upravljanje podacima putem SCADA sustava upravljanja. Prikaz konkretne havarije na dionici A-B je primjer dobrog upravljanja poslovnim procesom uslijed štetnog događaja. Rezultati koji su prikazani putem fiber trace programa za čitanje rezultata mjerenja su stvarni podaci sa štetnog događaja koji nam pokazuju i vode nas kroz cijeli proces uspostave primarne komunikacije.

Radom je prikazan način na koji se kvalitetno upravlja ljudima, znanjem, tehnologijama, sigurnošću i svakako bi mogao biti primjer upotrebljiv na drugim kompanijama koje imaju potrebe i teže suvremenim poslovnim procesima. Posebno je važno da poslovni proces nema potpuni prekid komunikacije jer on u konačnici rezultira financijskim gubitcima, neisporukom energenta i nezadovoljstvom korisnika, a to je nešto što svaka kompanija želi (i mora) izbjeći.

7. POPIS SLIKA

8. POPIS TABLICA

9. LITERATURA

1. Alter, S. (1996). "Information Systems-A Management Perspective", The Benjamins/ Cummings Publishing Company Inc, 1996.
2. Battles, B. E., Mark, D., Ryan, C. (1996). "An Open Letter to CEOs: How Otherwise Good Managers Spend Too Much on Information Technology", The McKinsey Quarterly, 1996, No. 3.
3. British Standards Institution (2006). Business continuity management-Part 1: Code of practice : London
4. British Standards Institution (2012). Societal security – Business continuity management Systems – Requirements: London
5. Brumec, J. (1996). Projektiranje i metodika razvoja informacijskog sustava, Euro Data, Zagreb, 1996.
6. Brumec, J. (1996). Projektiranje i metodika razvoja informacijskog sustava, Euro Data, Zagreb, 1996.m str. 37-45.
7. BSi (2012) ISO 22301:2012 Societal Security – Business Continuity Management Systems – Requirements, London: Bs
8. Bubić V., Šmidl, I. (2008). Risk Management of Working Capital Requirements, CECIIS 2008 Proceedings, Faculty of Organization and Informatics, Varaždin, 2008.,
9. Business Continuity Institute (2013) Good Practice Guidelines Global Edition, Caversham: BCI
10. Bysinger, B., Knight, K. (1996). "Investing in Information Technology", Van Nostrand Reinhold, 1996.,
11. Certifikati iz područja informacijske sigurnosti (2011.), LSS-PUBDOC-2011-01-BBB, Zagreb
12. Centar informacijske sigurnosti: "Upravljanje kontinuitetom poslovnih procesa", dostupno na: http://www.cis.hr/dokumenti/upravljanje-kontinuitetom-poslovnih-procesa.html; pristup: 18.10.2016
13. CARNet (2010.): "Upravljanje kontinuitetom poslovnih procesa", Nacionalni CERT+, LSS, Zagreb
14. Cabinet Office. (2004). overview of the Act. In: Civil Contingencies Secretariat Civil Contingencies Act 2004: a short. London: Civil Contingencies Secretariat
15. Campbell. K. et al. (2003). "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," J. Computer Security, vol. 11, no. 3, 2003
16. Clark, T. D., Zmud, R. W., McCray, G. E. (1995). "The Outsourcing of Information Services: Transforming the Nature of Business in the Information Industry", Journal of Information Technology,1995., 10.
17. Dempsey, J. S. (2008). Introduction to private security. Belmont, CA: Thomson Wadsworth.
18. Dutta S., Bilbao-Osorio B. (2012). *The Global Information Technology Report 2012: Living in a Hyperconnected World*, Geneva, World Economic Forum., str. 66.
19. Dvorak, R. E., Hollen, E., Mark, D., Meehan, W. F. (1996). "Six Principles of High-Performance IT", The McKinsey Quarterly, 1997, No. 3.
20. Dvorak, R. E., Hollen, E., Mark, D., Meehan, W. F. (1996). "Six Principles of High-Performance IT", The McKinsey Quarterly, 1997, No. 3.
21. Devane, T. (2004.): „Integrating Lean Six Sigma and High-Performance Organizations: Leading the charge toward dramatic, rapid, and sustainable improvement", John Wiley & Sons, San Francisco

22. Dutta S., Bilbao-Osorio B. (2012.): „The Global Information Technology Report 2012: Living in a Hyperconnected World“, Geneva, World Economic Forum
23. Đuričin, D., Janošević, S. (2006.): „Menadžment i strategija“, Ekonomski fakultet, Beograd
24. Gugić, A. (2014): „Poslovne sigurnosne politike i procedure“, predavanje, Veleučilište Marko Marulić, Knin
25. Girard, A. (2005.): „FTTx PON Technology and Testing“
26. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5.
27. Elliott D, Swartz E and Herbane B (2010) Business Continuity Management: A Crisis
28. Elliott D, Swartz E and Herbane B (2010) Business Continuity Management: A Crisis Management Approach, New York: Routledge.
29. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5.
30. Gugić A. (2014). Poslovne sigurnosne politike i procedure; predavanje Veleučilište Marko Marulić, Knin., str. 34
31. http://www.veleri.hr/files/datoteke/nastavni_materijali/k_sigurnost_s2/sigurnost_informacijskih_ sustava.pdf (pristupljeno: 30.03.2016.)
32. http://www.snt.hr/boxcontent/news/Propisi_sigurnost.pdf (pristupljeno: 29.03.2016.)
33. Hallenbeck, W. H. (1986). *Quantitative risk assessment for environmental and occupational health.* Chelsea, Mich.: Lewis Publishers
34. Humphreys, E., (2011). "Information security management system standards". *Datenschutz und Datensicherheit - DuD*. **35** (1)
35. Hayes, J: „Fiber Optics – Technician's Manual“, 2th edition
36. International Organization for Standardization (ISO), (2005). Code of Practice for Information Security Management, ISO/IEC 17799, Switzerland
37. Information technology – Security techniques – Information security management systems – Requirements ”, ISO/IEC 27001:2005
38. Implementacija sustava upravljanja sigurnošću informacija (ISMS), Computer Systems. Dostupno na: http://www.cs.hr/konzultanti-iso-bs.asp (pristupljeno: 28.4.2015.)
39. ITGI (2007.), CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models, IT Governance Institute, Rolling Meadows, SAD.
40. Jo, H., Kim, S., Won, D., (2011). "Advanced information security management evaluation system". *KSII Transactions on Internet and Information Systems*. **5**(6)
41. Jurison, J. (1995). “The Role of Risk and Return in Information Technology Outsourcing Decisions, Journal of Information Technology”, 1995, 10. str. 34-42.
42. JDSU, Reference Guide to Fibre Optic Testing,Volumen 1,2007.
43. Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X., Ratick, S. (1988). "The social amplification of risk: A conceptual framework". *Risk Analysis*. **8** (2)
44. Kempis, R. D., Ringbeck, J. (1998). “Manufacturing use and abuse of IT”, The McKinsey Quarterly, 1998, No.1.
45. Kotler, P., Lee, N. (2009). „Društveno odgovorno ponašanje“, MEP CONSULT, Zagreb, 2009.
46. Ma, Q., Schmidt, M. B., Pearson, M., (2009). An integrated framework for information security management". *Review of Business*. **30** (1)
47. Mikula, I. (1998.): „Svjetlovodi i njihovo održavanje“
48. Nolan, R. and McFarlan, F.W., (2005.): Information Technology and Board of Directors, Harvard Business Review, October

49. O'Brien, M., (2002), *Making better environmental decisions: an alternative to risk assessment,* Cambridge, Massachusetts: MIT Press
50. Panian, Ž., (2001). Kontrola i revizija informacijskih sustava, Sinergija, Zagreb
51. Pintar, D. (2009). Model uslužno orjentirane arhitekture za stvarnovremensko skladištenje podataka zasnovano na metapodacima – doktorska disertacija. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva.
52. Rimljak, J. (2015). Informacijska sigurnost u suvremenom poslovanju. Veleučilište „Marko Marulić" u Kninu.
53. Spremić, M. (2005.): Procjena razine pouzdanosti internih kontrola informacijskog sustava s pomoću CobiT metodologije, Revizija, računovodstvo i financije, br. 12/2005
54. Spring, J., Kern, S., Summers, A. (2015). "Global adversarial capability modeling". *2015 APWG Symposium on Electronic Crime Research (eCrime)*: 1–21.
55. Srića, V., Spremić, M., (2000.): Informacijskom tehnologijom do poslovnog uspjeha, Sinergija.
56. Strukturno kabliranje – planiranje, projektiranje, izvođenje i održavanje, FER ZESOI/LS&S Zagreb, siječanj 2004.
57. Symons, C., (2005.): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.
58. Tuđman, M. (2008). „Informacijsko ratište i informacijska znanost", Zagreb, 2008
59. Weill, P., Ross, J.W., (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvards Business School Press.
60. Wright, C.S. (2005). Implementing an information security management system (ISMS): Training Process. SANS Institute.

10. ŽIVOTOPIS

- **Radno iskustvo**

- (Kronološki od starijeg k novijem datumu):

- 2003-2010 Voditelj ugostiteljskog objekta "Merlin" Ivanić-Grad.

- 2011-2012 Tehničar Telekomunikacija, administrator sustava, Luxor D.O.O.

- 2012-2015 Tehničar-inženjer Telekomunikacija, odjel Informatike, Optike i TS stanica, Elektro Centar Petek, Ivanić-Grad.

- 2015 do danas - Tehnički voditelj, izrada tehničkih rješenja za optičke i bakrene veze, Luxor D.O.O.

11. KOMPETENCIJE MENTORA

Popis do 5 objavljenih relevantnih radova u zadnjih 5 godina:

- **Spremić, M**. (2013): Holistic approach for governing information system security, *Lecture Notes in Engineering and Computer Science* 2 LNECS pp. 1242 – 1247, IAENG (International Association of Engineering), Hong Kong, China
- **Spremić, M.,** Bajgorić, N., Turulja, L. (2013): Implementation of IT governance standards and business continuity management in transition economies: The case of banking sector in Croatia and Bosnia-Herzegovina, *Ekonomska istraživanja – Economic research, Volume* 26, Issue 1, pp. 183 – 202.
- **Spremić, M**. (2012): Corporate IT Risk Management Model: a Holistic view at Managing Information System Security Risks,*Proceedings of the 34rd International Conference on Information Technology Interfaces (ITI),* Cavtat, June 25-38, 2012, pp. 299-304
- **Spremić, M.,** Galetić, F., Jaković, B. (2012): Group buying portals in Croatia, *Proceedings of the 6th International Conference 'An Enterprise Odyssey'*, Šibenik, June 13-15, 2012, pp.
- **Spremić, M.** (2012): Measuring IT Governance Performance: A Research Study on Cobit- Based Regulation Framework Usage, *International Journal of Mathematics and Computers in Simulation*, Volume 1, Issue 6, pp. 17-25, ISSN: 1998-0159.